Elements of Mathematical Logic
Version of September 28, 2023

Alessandro Andretta

alessandro.andretta@unito.it

Contents

Introduction

A new book in logic? Do we need another logic textbook? Considering the enormous amount of time and energy invested, the author of a math textbook in any subject X may not give the most unbiased answer to the question "do we need a new textbook in X?". Yet I feel that there are sound reasons to justify the existence of a book like this one, so let me elaborate a bit.

This book is aimed at advanced undergraduates or beginning graduate students in mathematics that want to learn the basics of the subject. It is different from most other logic textbooks in that it is geared towards the general mathematical public, rather than towards would-be logicians. In the first chapters we strive to present applications to various problems in mathematics, rather than proving results in logic, while this approach is reversed in the last chapters.

For the reader

These notes grew out of several logic courses that I have taught at my University for the last decade. Keep in mind that this is work-in-progress so some parts are reasonably polished, while other are still in a rough form. Those sections that can (should) be skipped on first read are marked with an asterisk.

Clearly these notes owe a great debt to many classic logic textbooks, like the ones by Shoenfield, Mendelson, Hinman, ...

Feedback

I greatly appreciate any feed-back, criticism, suggestions, etc. If you want to point-out a typo, or a more substantial mathematical shortcoming, you should send me back an annotated .pfd file, rather than a message saying that "on page n, line k, the symbol such-and-such..." as the incriminated part might have moved somewhere else, or might have been removed completely.

Change history

Every now and then I will post a new version of this book. Here I list all the *main* changes for each release—obviously some typos are removed (and some other are, unfortunately, added) but there is no point in referring to each of them.

July 16, 2019: initial release.

: the old Chapter III is split into two chapters. The content of the current Chapters I–IV has been revised the most.

Preliminaries

We collect here some of the basic notions that the reader is supposed to know.

Sets and functions

By $x \in A$ we mean that the object x **belongs to the set** A, or is an **element of** A. The collection of all x that enjoy property P is denoted by $\{x \mid P(x)\}$. If every element of A belongs to B then A **is contained in** B, and we write $A \subseteq B$; this does not forbid that A and B be the same set—if instead we want that A and B be distinct we write $A \subset B$. The **empty set** is denoted by $\emptyset$. The **set of all subsets of** A is $\mathscr{P}(A) \overset{\text{def}}{=} \{X \mid X \subseteq A\}$ and it is calle the **powerset** of A.

The **union** of two sets A and B is the set $A \cup B$ of the objects that are in A or in B, the **intersection** is the set $A \cap B$ of the objects that are in both A and B, the **difference** is the set $A \setminus B$ of the objects that are in A but not in B, the **symmetric difference** is the set $A \mathbin{\triangle} B$ of the objects that are in $A \cup B$ but not in $A \cap B$. The **intersection of the family of sets** $\{A_i \mid i \in I\}$, written as $\bigcap_{i \in I} A_i$ or also $\bigcap \{A_i \mid i \in I\}$ is the collection of all objects that belong to *every* A_i; analogously, the **union of the family** $\{A_i \mid i \in I\}$ is the set of all items that belong to *some* A_i, and it is denoted by $\bigcup_{i \in I} A_i$ or by $\bigcup \{A_i \mid i \in I\}$. The **cartesian product** of two sets A and B is the set $A \times B$ of all ordered pairs (a, b) with $a \in A$ and $b \in B$. The **disjoint union** $A \uplus B$ of two sets A, B is $(\{0\} \times A) \cup (\{1\} \times B)$. The disjoint union $\uplus_{i \in I} A_i$ of the sets A_i is $\bigcup_{i \in I}(\{i\} \times A_i)$.

A **(binary) relation** is a collection of ordered pairs; if $f \subseteq A \times B$ is a relation such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$, we shall say that f is a **function** from A to B, and we shall write $f \colon A \to B$.

Suppose $f\colon A \to B$. If $a \in A$, the unique $b \in B$ such that $(a, b) \in f$ is denoted by $f(a)$, and $\operatorname{ran}(f)$ is the set of all $b \in B$ such that $b = f(a)$ for some $a \in A$. If $A_0 \subseteq A$ we write $f \restriction A_0$ for the restriction of f to the set A_0, and $f[A_0] \stackrel{\text{def}}{=} \{f(x) \mid x \in A_0\}$. If $B_0 \subseteq B$, then $f^{-1}[B_0] \stackrel{\text{def}}{=} \{x \in A \mid f(x) \in B_0\}$.

A **partial function** from A to B is an $f\colon A' \to B$ with $A' \subseteq A$. When we want to stress that a (partial) function f from A to B is a subset of the cartesian product $A \times B$, we will consider its **graph** $\operatorname{Gr}(f) = \{(a, b) \in A \times B \mid (a, b) \in f\}$; in any case, *there is no difference between a function and its graph.*

The set of all functions from A to B is denoted by ${}^{A}B$ or by B^A. (The two notations are equivalent: the former is useful in set theory, but the latter is more common in other areas of mathematics.) We say that $f \in B^A$ is injective if $f(a_1) \neq f(a_2)$ for all choices of distinct $a_1, a_2 \in A$; f is surjective if for all $b \in B$ there is an $a \in A$ such that $f(a) = b$; f is bijective if it is injective and surjective. Sometimes the notation $f\colon A \rightarrowtail B$ will be used to say that f is injective, while $f\colon A \twoheadrightarrow B$ means that it is surjective. The **identity function** on a set A is the map $\operatorname{id}_A\colon A \to A$ defined by $\operatorname{id}_A(a) = a$ for all $a \in A$. If $B \subseteq A$, the **characteristic function of** B **in** A is $\boldsymbol{\chi}^A_B\colon A \to \{0, 1\}$ defined by $\boldsymbol{\chi}^A_B(x) = 1$ if and only if $x \in B$.

The elements of $A_0 \times A_1$ can be identified with the functions with domain $\{0, 1\}$ and such that $f(i) \in A_i$. This suggests to define the **cartesian product** of a family of sets A_i, with $i \in I$, as

$$\times_{i\in I} A_i = \{f \mid f \text{ is a function, } \operatorname{dom}(f) = I, \text{ and } \forall i \in I\, (f(i) \in A_i)\}.$$

If E is an **equivalence relation** on a set A, then $[a]_E \stackrel{\text{def}}{=} \{b \in A \mid (a, b) \in E\}$ is the equivalence class of the element $a \in A$; when E is clear from the context, we simply write $[a]$. The **quotient set** A/E is the set of all $[a]_E$ with $a \in A$.

The notation for the number systems is standard: $\mathbb{N}$ is the set of all natural numbers (including 0), $\mathbb{Z}$ is the set of all integers (positive, negative, or null), $\mathbb{Q}$ is the set of all rational numbers, $\mathbb{R}$ is the set of all real numbers, $\mathbb{C}$ is the set of all complex numbers. The symbol $\mathbb{R}_+$ is for the set of all positive reals, that is strictly bigger than 0; similarly $\mathbb{R}_-$ is for the set of all negative reals, strictly smaller than 0. More generally, let $\mathbb{R}_{<a} = \{x \in \mathbb{R} \mid x < a\}$ and $\mathbb{R}_{>a} = \{x \in \mathbb{R} \mid x > a\}$, and similarly when $<$ is replaced by $\leq$. A similar notational convention applies when $\mathbb{R}$ is replaced by $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$. If a, b, c are integers, we shall say that a and b are congruent modulo c, in symbols $a \equiv b \mod c$, if $a - b$ is divisible by c. The ring of the integers modulo c is denoted by $\mathbb{Z}/c\mathbb{Z}$ or by $\mathbb{Z}(c)$.

A **set is finite** if it is in bijection with the set $\{0, \dots, n-1\}$ for some $n \in \mathbb{N}$; when $n = 0$ then the set is $\emptyset$, the empty set. A set which is not finite is said to be **infinite**. A set is **countable** if it is finite, or in bijection with $\mathbb{N}$, otherwise it is **uncountable**.

Algebra

A **semigroup** is a set $S \neq \emptyset$ with an associative binary operation $*$. If a semigroup S has an element e such that $a * e = e * a = a$ for all $a \in S$ we have a **monoid**; the element e is unique, and it is called the **neutral element** and it is denoted by 1. A **group** is a monoid where every element has an inverse, that is for any $x \in S$ there is $y \in S$ such that $x * y = y * x = 1$. The inverse of x is unique and it denoted by x^{-1}. A group is **commutative** or **abelian** if $*$ is commutative; in this case we often adopt the additive notation $+$ for the binary operation, $-x$ is for the inverse (the opposite) and 0 is the neutral element.

A **rng** is a set $R \neq \emptyset$ with two binary operations $+$ and $\cdot$ such that: $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup, and multiplication is distributive with respect to addition. If $(R, \cdot)$ is a monoid we say that R is a **ring**.[1] A rng is **commutative** if the operation $\cdot$ is commutative. An **integral domain** is a commutative rng without zero-divisors, that is if $x \cdot y = 0$ then $x = 0$ or $y = 0$. A **skew-field** or **division ring** is a ring R such that $0 \neq 1$ and such that every non-zero element has an inverse. A commutative skew-field is a **field**. The **characteristic** of a ring is the smallest $n > 0$ such that $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$, if such an n exists, otherwise we say that the characteristic is 0. In the case of integral domains (and in particular in the case of fields), if the characteristic is $n > 0$ then n is prime. If R is a rng, then $R[X]$ is the rng of polynomials with coefficients in R. A field $\Bbbk$ is **algebraically closed** if every non-zero polynomial of $\Bbbk[X]$ has a root in $\Bbbk$. A complex number is **algebraic** if it is the root of a polynomial of $\mathbb{Q}[X]$—equivalently, it is root of a polynomial of $\mathbb{Z}[X]$. A complex number that it is not algebraic is **transcendental**. The set of algebraic numbers is an algebraically closed field $\overline{\mathbb{Q}}$, and it is the smallest algebraically closed field of characteristic zero.

A **vector space** on a field $\Bbbk$ is an abelian group $\langle V, +, \mathbf{0} \rangle$ together with a map $\Bbbk \times V \to V$, $(r, \mathbf{v}) \mapsto r\mathbf{v}$ called scalar multiplication, satisfying the following identities, for all $r, s \in \Bbbk$ and all $\mathbf{u}, \mathbf{v} \in V$:

$$\begin{aligned} r(\mathbf{u} + \mathbf{v}) &= r\mathbf{u} + r\mathbf{v} & \qquad (r + s)\mathbf{u} &= r\mathbf{u} + s\mathbf{u} \\ (r \cdot s)\mathbf{u} &= r(s\mathbf{u}) & 1_{\Bbbk}\mathbf{u} &= \mathbf{u}. \end{aligned}$$

Elements of V are called **vectors**, elements of $\Bbbk$ are called **scalars**. A set $X \subseteq V$ is linearly dependent if there are $\mathbf{v}_1, \ldots, \mathbf{v}_n \in X$ and scalars $r_1, \ldots, r_n \in \Bbbk$ such that $(r_1, \ldots, r_n) \neq (0_{\Bbbk}, \ldots, 0_{\Bbbk})$ and $\sum_{i=1}^{n} r_i \mathbf{v}_i = \mathbf{0}$. Otherwise X is

[1] Many books use *ring* and *unitary ring* instead of *rng* and *ring*.

linearly independent. We say that $X \subseteq V$ is a set of generators for V, if every $\mathbf{v} \in V$ can be written as linear combination $\mathbf{v} = \sum_{i=1}^{n} r_i \mathbf{v}_i$, for some $\mathbf{v}_1, \dots, \mathbf{v}_n \in X$ and $r_1, \dots, r_n \in \Bbbk$. A vector space is **finitely generated** if it has a finite set of generators. A **basis** of a vector space V is a linearly independent set of generators of V.

Topology

A **topological space** is a set X endowed with a family $\mathcal{T} \subseteq \mathscr{P}(X)$ containing $\emptyset$ and X, and closed under finite intersections and arbitrary unions. The family $\mathcal{T}$ is called a **topology** and its elements are called **open sets**. If $x \in V \subseteq X$ and if there is $U \in \mathcal{T}$ such that $x \in U \subseteq V$ then V is a **neighborhood** of x. A topological space is **first-countable** if every $x \in X$ has a neighborhood system $\{V_n \mid n \in \mathbb{N}\}$ such that every neighborhood of x contains a V_n. We say that $x \in X$ is an **isolated point** if $\{x\}$ is open. The complement of an open set is **closed**. The spaces X where the only sets that are simultaneously open and closed are $\emptyset$ and X are said to be **connected**; otherwise they are disconnected.

For $Y \subseteq X$ the **interior** of Y and the **closure** of Y are, respectively, the largest open set contained in Y and the smallest closed set containing Y, that is $\mathrm{Int}(Y) = \bigcup\{U \subseteq Y \mid U \in \mathcal{T}\}$ and $\mathrm{Cl}(Y) = \bigcap\{C \supseteq Y \mid X \setminus C \in \mathcal{T}\}$. The **frontier** of Y is $\mathrm{Fr}(Y) = \mathrm{Cl}(Y) \setminus \mathrm{Int}(Y)$. We say that $Y \subseteq X$ is **dense** in X if $\mathrm{Cl}(Y) = X$. A space admitting a countable dense subset is **separable**.

The **topology induced by** X **on** $Y \subseteq X$ is $\{Y \cap U \mid U \in \mathcal{T}\}$ and Y endowed with this topology is a subspace of X. A map between topological spaces is **continuous** if the preimage of an open set is open—the inclusion map between a subspace and a space is continuous.

We say that $\mathcal{B} \subseteq \mathscr{P}(X)$ is a **base** or a **basis for a topology** $\mathcal{T}$ on X if every $U \in \mathcal{T}$ is of the form $\bigcup \mathcal{A}$ for some $\mathcal{A} \subseteq \mathcal{B}$. For all $\mathcal{S} \subseteq \mathscr{P}(X)$ the family $\mathcal{S}^{\cap} = \{A_1 \cap \dots \cap A_n \mid A_1, \dots, A_n \in \mathcal{S}\} \cup \{X\}$ is a base for the topology $\hat{\mathcal{S}} = \{\bigcup_{i \in I} B_i \mid \{B_i \mid i \in I\} \subseteq \mathcal{S}^{\cap}\}$ on X, and we say that $\mathcal{S}$ is a **subbase** for this topology. If a topological space has a countable base then it is **second countable**.

A topological space $(X, \mathcal{T})$ is T_0 if distinct points have distinct neighborhood families, that is if $x \neq y$ then either there is an $U \in \mathcal{T}$ such that $x \in U$ and $y \notin U$ or else there is $V \in \mathcal{T}$ such that $y \in V$ and $x \notin V$. A topological space is T_1 if distinct points can be separated by open sets, that is if $x \neq y$ there are $U, V \in \mathcal{T}$ such that $x \in U$, $y \notin U$, $y \in V$, and $x \notin V$; equivalently: $\{x\}$ is closed, for all $x \in X$. A topological space is T_2 or **Hausdorff** if distinct points can be separated by *disjoint* open sets, that is if $x \neq y$ then there are $U, V \in \mathcal{T}$ such that $x \in U$ and $y \in V$ and $U \cap V = \emptyset$. A topological space is **regular** if a point x and a closed set C can be separated by disjoint open sets, that is if $x \notin C$ then there are $U, V \in \mathcal{T}$ such that $x \in U$ and $C \subseteq V$ and $U \cap V = \emptyset$; equivalently: for all $x \in U$ with U open, there is an open set V such that $x \in V \subseteq \mathrm{Cl}(V) \subseteq U$. A topological space is T_3 if it is regular and T_2 or, equivalently, regular and T_0.

Let X be a topological space. A **open covering** of $Y \subseteq X$ is a family $\{A_i \mid i \in I\}$ of open sets such that $Y \subseteq \bigcup_{i \in I} A_i$. A topological space X is **compact** if every open covering $\{A_i \mid i \in I\}$ of X admits a **finite subcovering**, that is there is a finite $I_0 \subseteq I$ such that $X = \bigcup_{i \in I_0} A_i$; equivalently, X is compact if every family $\mathcal{C} = \{C_i \mid i \in I\}$ of closed subsets of X has the **finite intersection property**, that is if $C_{i_1} \cap \dots \cap C_{i_n} \neq \emptyset$ for all $i_1, \dots, i_n \in I$, then $\bigcap_{i \in I} C_i \neq \emptyset$. If $\mathcal{B}$ is a base for the topology of X, then X is compact if and only if every covering consisting of sets in $\mathcal{B}$ has a finite subcovering.

A **metric space** is a set X endowed with a **distance** or **metric**, that is a function $d\colon X \times X \to [0; +\infty)$ satisfying: $d(x, y) = 0 \Leftrightarrow x = y$, $d(x, y) = d(y, x)$ and $d(x, y) \leq d(x, z) + d(z, y)$, for all $x, y, z \in X$. If the first bi-implication is weakened to $d(x, x) = 0$, the resulting function is a **pseudo-distance** or **pseudo-metric**, and the resulting object is a **pseudo-metric space**. If (X, d) is a pseudo-metric space, then $(\tilde{X}, \tilde{d})$ is a metric space, where $\tilde{X} = X/{\sim}$ and $\sim$ is the equivalence relation $x \sim y \Leftrightarrow d(x, y) = 0$, and $\tilde{d}([x], [y]) = d(x, y)$. Given a (pseudo-)metric space, the **open ball** with center $x \in X$ and radius $r > 0$ is the set $\mathrm{B}(x; r) = \{y \in X \mid d(x, y) < r\}$, while the closed ball $\mathrm{B}(x; r)^{\mathrm{cl}}$ has the same definition, with $\leq$ in place of $<$.

A pseudo-metric space is a topological space, taking as a subbase the family of open balls. The topology thus obtained is T_0 if and only if d is a metric, and in this case the space is Hausdorff, T_3, and first countable. A separable metric space is second countable: if D is a countable dense subset, take $\{\mathrm{B}(x; q) \mid x \in D \wedge q \in \mathbb{Q}_+\}$ as a base.

A sequence $(x_n)_n$ in a metric space (X, d) converges to $x \in X$ if for every $\varepsilon > 0$ there is N such that for all $n > N$ we have that $d(x_n, x) < \varepsilon$. We say that $(x_n)_n$ is a **Cauchy sequence** if for every $\varepsilon > 0$ there is N such that for all $n, m > N$ we have that $d(x_n, x_m) < \varepsilon$. A metric space is **complete** if every Cauchy sequence converges in X, and in this case the metric is **complete**.

Chapter I

Introduction to mathematical logic

The purpose of this chapter is to familiarize the reader with the basic aspects of mathematical logic, using examples from various parts of mathematics. The focus is not so much on proving theorems, but rather on how logic can be used to *formalize* various problems, and how this formalization process helps us to better understand the mathematical problem at hand. In some sense, the present chapter provides the basic training that will handsomely reward the student in the later chapters—the reader who feels already at ease with the arguments presented here, can safely jump to the later chapters.

1. Axiomatic systems

Mathematics differs from other scientific disciplines in the method employed to establish new results. It is neither sufficient nor, in most cases, necessary to conduct measurements, experiments, or simulations. No experiment can decide whether $\sqrt{2}$ is a rational number, since both $\mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ are dense in the real line.[1] To assert that $\sqrt{2}$ is not a rational number, it is mandatory to show that there are no non-zero integers n and m such that $n^2 = 2m^2$. Sometimes examples provide *hints* about the truth or falsehood of a conjecture. For example, it has been verified that in the decimal expansion of π up to 3×10^7 decimals, the digits, the pairs of digits, the triplets of digits, etc. are uniformly distributed [**Bai88**], and these computations corroborate the conjecture that π is a normal number, that is every string of digits of length k appears with frequency 10^{-k}, in the limit. But these calculations

[1] See the observations in [**Sha03**, pp. 6–7].

cannot guarantee the validity of the (still open) conjecture that π is normal. In some cases, numerical evidence can be misleading.

- Fermat conjectured that all numbers of the form $2^{2^n}+1$ were prime, after having checked this for $n \leq 4$, but Euler refuted this conjecture by showing that $2^{2^5}+1 = 4292967297 = 641 \times 6700417$.
- The property $P(n)$ defined by "$n^2 - 79n + 1601$ is prime" is true for $1 \leq n < 80$ but false for $n = 80$ since $80^2 - 79 \times 80 + 1601 = 1681 = 41^2$.
- Pell's equation is $x^2 - ky^2 = 1$, with $k > 1$ a natural number. By a theorem of Lagrange's this equation has infinitely many integer solutions if k is not a square. In particular there are infinitely many $n > 0$ such that $991n^2+1$ is a square, yet the first such integer is $12055735790331359447442538767 \approx 10^{29}$. Thus numerical evidence would have suggested the false conjecture "$991n^2+1$ is never a square, for all $n > 0$".
- Littlewood proved that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely often, where $\pi(x)$ is the number of primes $\leq x$ and $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}$. But numerical evidence suggests that $\pi(x) < \mathrm{Li}(x)$ for all x; in fact the least x such that $\pi(x) > \mathrm{Li}(x)$ is huge—it is conjectured that the size of such x is 10^{316}.

The preceding examples, drawn from number theory, show that numerical evidence can be of little use in pure mathematics. The next two examples, drawn from combinatorics, further corroborate this point.[2]

Example 1.1. The **pure base b representation of n**, where $b, n > 1$ are natural numbers, is defined as follows. First write n as sum of powers of b, then repeat this procedure for the exponents, and the exponents of the exponents, ... until all digits in the representation are less or equal than b. For example the pure base b representation of $n = 1931$ when $b = 2$ is

$$1931 = 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2+1} + 2 + 1$$

Let $F_b(n)$ be the number so defined: represent n in pure base b, replace every b in such representation with $b+1$, compute the resulting number and subtract 1. For each n define the sequence $G_k(n)$ as follows: $G_0(n) = n$ and $G_{k+1} = F_{k+2}(G_k(n))$. Thus $G_k(n) = F_{k+1}(F_k(\dots F_2(n)\dots))$. The numbers $G_k(n)$ grow extremely quickly as k increases, even when n is very small, so one would expect that the sequence $(G_k(n))_k$ diverges to infinity for all sufficiently large n. Yet Goodstein proved that for any n there is a k such that $G_k(n) = 0$. The function $g \colon \mathbb{N} \to \mathbb{N}$ assigning to each n the least k such that $G_k(n) = 0$ grows at an incredible speed, dwarfing any function encountered in ordinary mathematics.

Example 1.2. Consider the following game, in which Hercules battles against the hydra, a multiple-headed serpentine monster with an amazing regenerating

[2] Examples 1.1 and 1.2 will be studied in Section 13.J.

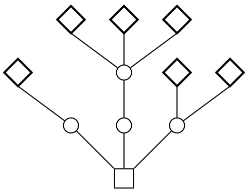
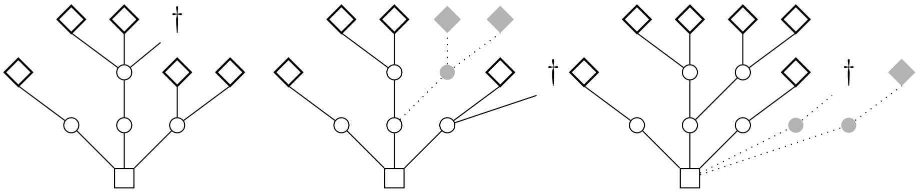


Figure 1. A hydra

property: each time a head is chopped off, several new heads spring from the wounded neck. Mathematically a hydra is a finite tree (Section 3.D.4), i.e. a collection of segments each joining two nodes, such that each node is connected by a unique path to a specific node called the root; the nodes other than the root that are connected to a single node are called heads. (See Figure 1, where the root is depicted by □, a node by ○, a head by ◇.) The rules of the game are as follows. At stage $n \geq 1$ Hercules chops off a head of the hydra. If the head was immediately above the root, then the hydra suffers in silence. If instead the head is immediately above a node x that is not the root, then from the node immediately below x the hydra sprouts n brand new copies of the part of the hydra above it. Here are the first three rounds of a run of the game starting with the hydra of Figure 1—the head that Hercules cuts at a given round is denoted by † and the new nodes and heads that the hydra generates after the amputation are drawn in light grey colour and dotted lines.



The remarkable fact is that no matter how big the original hydra is, Hercules will end up killing it, regardless of the strategy he follows.

The main activity of a mathematician is to prove theorems. A **proof** is an argument that allows us to reach a desired conclusion, starting from certain initial assumptions. The initial assumptions are called **axioms** or **postulates**, and are different, depending on the area of mathematics considered. The results obtained by means of proofs are called **theorems** and they must be deduced in a rigorous fashion from the axioms, without any appeal to extraneous principles. For example, we cannot establish a new result in Euclidean geometry by using arguments based on our geometric intuition, or on results from other parts of mathematics. Proofs are strings of statements, each one being an axiom, or being obtained from preceding statements using the **logical axioms and rules**. These axioms and rules, as it will be explained in Section 6.A and more extensively in Chapter VII, are *the same* for all mathematical theories.

Let us see some examples of axiomatization in mathematics.

Geometry. Euclid in the III century B.C. developed geometry starting from some undefined notions (point, line, plane, etc.) and by five axioms, known as Euclid's postulates. This axiomatic system, known as Euclidean geometry, was presented by Euclid in his monumental opus, the *Elements.* For many centuries this book was the epitome of mathematical rigor, and it was only in the nineteenth century that its logical underpinnings were placed under scrutiny by Hilbert.

Arithmetic and Analysis. In the second half of the nineteenth century, the foundations of analysis were recast in rigorous form. This endeavor, known as arithmetization of analysis, culminated with the work of Weierstraß. The elementary properties of natural numbers can be derived from axioms introduced by Dedekind and Peano at the end of the nineteenth century. This axiomatic system is known as **Peano arithmetic** (Section 12.D).

Sets. Also set theory, invented by Dedekind and Cantor at the end of the nineteenth century, can (in fact: must) be developed from axioms. The most common among the axiomatizations of set theory is due to Zermelo and Frænkel.

Algebra and Topology. The axiomatic method is a staple feature of algebra and topology—groups, rings, fields, and topological spaces are defined from axioms and their properties are proved from general principles, rather than by looking at specific examples.

The examples above are quite different, but can be partitioned into two big camps:

- *classical* axiomatizations (Euclidean geometry, Peano's arithmetic, and axiomatic set theory) aiming to describe certain specific mathematical entities (the plane and the three dimensional space, the natural numbers, the universe of sets);
- *modern* axiomatizations (algebraic and topological structures, . . .) aiming to characterize families of objects up to isomorphism.

This distinction is only apparent, since every first-order theory[3] belongs to the second group, that is to say: none of the axiomatic theories described above can capture up to isomorphism a single mathematical structure.

[3] First-order theories will be officially defined on page 57.

2. Symbols

If you browse through a calculus book you will see different kind of symbols.

- The letters x, y, z, ... usually denote arbitrary real numbers.
- Other letters denote specific real numbers—for example $\pi = 3.14159\dots$ and $\mathrm{e} = 2.71828\dots$.
- The symbols $+$, $\cdot$ denote the operations of sum and product, and these are specific functions from pairs of reals to reals.
- The symbol $<$ denotes the order relation, that is a specific subset of $\mathbb{R}^2$.

The meaning of symbols may vary from one subject to another—e.g. in an algebra book the symbol $+$ is typically used to denote the operation in an abelian group, and the symbol 1 is used for the identity in a group, written in a multiplicative notation. The only symbol whose meaning everybody agrees upon is the equality symbol $=$ stating that the object written on the lefthand side coincides with the one written on the righthand side.

There are certain expressions that occur in every mathematical text:

"not" "or" "and" "if ... then ..." "... if and only if ..."

and

"for every x ..." "there is an x such that ...".

In order to state in a succinct manner the above expressions, we introduce the **logical connectives**

$$\neg \qquad \vee \qquad \wedge \qquad \Rightarrow \qquad \Leftrightarrow$$

and the **quantifiers**

$$\forall \qquad \exists.$$

Connectives and quantifiers are called **logical constants**, and have the following meaning.

- $\neg$ is the **negation** and it is used to assert the contrary of the statement it is applied to.
- $\vee$ is the **disjunction** and corresponds to the *inclusive* or: this *or* that *or* maybe both.
- $\wedge$ is the **conjunction**, and it is used to assert that two facts holds simultaneously. Also the particles "but" and "whereas" are conjunctions, to which we attach an adversative connotation. Yet, in mathematics the meaning of "A but B" or of "A whereas B" is the same as "A and B" and hence they are rendered as "A $\wedge$ B".
- $\Rightarrow$ is the **implication** corresponding to the expression "if... then ...". When in mathematics we state that "if A then B", we are stating that the

only problematic case is when the premise A holds while the consequence B does not hold. In particular, if the premise is false, then the implication is arguably true. For example, if in a calculus book we see $(x > 0) \Rightarrow (x = y^2$ for some $y > 0)$, we agree that this implication holds, since either x is positive and hence it has a positive square root, or else it is negative or null and the result holds vacuously. An implication does not entail any causality between the premise and the consequence—the only meaning of $\mathrm{A} \Rightarrow \mathrm{B}$ is that it cannot be the case that A holds but B does not. The expressions "whenever A then B" or "in order to have A it is necessary that B" mean that "if A then B" and hence will be written as $\mathrm{A} \Rightarrow \mathrm{B}$, while "in order to have A it is sufficient to have B" means that A holds when B holds, that is $\mathrm{B} \Rightarrow \mathrm{A}$. Let us stress that an implication $\mathrm{A} \Rightarrow \mathrm{B}$ and its converse $\mathrm{B} \Rightarrow \mathrm{A}$ have completely different meanings, although math freshmen tend to confuse the two notions.

- $\Leftrightarrow$ is the **bi-implication** and corresponds to the expression "if and only if". When asserting that "A if and only if B" we mean that "if A then B, and if B then A". Often in mathematics "A if and only if B" is rendered, in a more ornate fashion, by "a necessary and sufficient condition for A, is B".
- $\exists$ is the **existential quantifier**. The expression $\exists x\mathrm{A}$ reads: "there is an x such that A", or "A holds, for some x" and states that there is *at least one* item that enjoys property A.
- $\forall$ is the **universal quantifier**. The expression $\forall x\mathrm{A}$ reads: "for every x property A holds", or "A holds, for all x" and states that *every* item enjoys property A.

Remark 2.1. Our notation is fairly standard, but far from being universally accepted. While the disjunction is almost always denoted by $\vee$, it is not uncommon to see & and $\sim$ for conjunction and negation. The symbols $\rightarrow$ and $\leftrightarrow$ are common choices for the implication and bi-implication—the rationale for us to adopt $\Rightarrow$ (and hence $\Leftrightarrow$) is that $\rightarrow$ is already used for the functional notation. Quantifiers are almost always denoted by $\forall$ and $\exists$, but ⩕ and ⩖ are sometimes used. Older books employ $\supset$ and $\equiv$ for the implication and bi-implication, and (x) and $\mathsf{E}x$ instead of $\forall x$ and $\exists x$, but it is safe to say that these notations are quite obsolete.

2.A. The meaning of logical constants. It is useful to introduce a specific notation to discuss logical rules. The expression

$$\frac{\mathrm{A}_1 \qquad \mathrm{A}_2 \qquad \dots \qquad \mathrm{A}_n}{\mathrm{B}}$$

says that "B follows from $\mathrm{A}_1, \dots, \mathrm{A}_n$".

2.A.1. *Connectives.* In order to show that A ∧ B it is enough to prove both A and B, in symbols

$$\frac{\mathrm{A} \qquad \mathrm{B}}{\mathrm{A} \wedge \mathrm{B}} \,.$$

Conversely, from A ∧ B we can infer both A and B, that is

$$\frac{\mathrm{A} \wedge \mathrm{B}}{\mathrm{A}} \quad \text{and} \quad \frac{\mathrm{A} \wedge \mathrm{B}}{\mathrm{B}} \,. \tag{2.1}$$

The connective ∧ is commutative, in the sense that asserting A∧B is equivalent to asserting B ∧ A: if we assume A ∧ B first we infer B and then A, whence B ∧ A; similarly B ∧ A entails A ∧ B. It is associative, as the meaning of (A ∧ B) ∧ C is the same as A ∧ (B ∧ C).

Given A, we can weaken our result by asserting A ∨ B, with B arbitrary. Similarly, from B one gets A ∨ B, for any A. Therefore

$$\frac{\mathrm{A}}{\mathrm{A} \vee \mathrm{B}} \quad \text{and} \quad \frac{\mathrm{B}}{\mathrm{A} \vee \mathrm{B}} \,.$$

From A ∨ B one cannot conclude that A or that B (Example 2.2). On the other hand, knowing A ∨ B and the negation of either A or B, allows us to deduce the other statement, that is

$$\frac{\mathrm{A} \vee \mathrm{B} \qquad \neg\mathrm{A}}{\mathrm{B}} \quad \text{and} \quad \frac{\mathrm{A} \vee \mathrm{B} \qquad \neg\mathrm{B}}{\mathrm{A}} \,. \tag{2.2}$$

The connective ∨ is commutative and associative, meaning that A ∨ B is like saying B ∨ A, and that (A ∨ B) ∨ C is like saying A ∨ (B ∨ C).

Suppose A holds: we cannot infer ¬A, otherwise a contradiction would arise, so we conclude that ¬¬A holds. Conversely assume ¬¬A: if A does not hold, then ¬A would follow, whence a contradiction. Summarizing: the rule of double negation states that from A we deduce ¬¬A, and conversely:

$$\frac{\mathrm{A}}{\neg\neg\mathrm{A}} \quad \text{and} \quad \frac{\neg\neg\mathrm{A}}{\mathrm{A}} \,. \tag{2.3}$$

The argument above is an example of a proof by contradiction: in order to derive A from given assumptions, it is enough to add ¬A to these assumptions and obtain a contradiction, i.e. a statement of the form B ∧ ¬B. Similarly, in order to prove ¬A from some given assumptions, it is enough to prove that A together with said assumptions yields a contradiction, and use rule (2.3).

We can now prove De Morgan's laws, that is

$$\frac{\mathrm{A} \wedge \mathrm{B}}{\neg(\neg\mathrm{A} \vee \neg\mathrm{B})} \quad \text{and} \quad \frac{\mathrm{A} \vee \mathrm{B}}{\neg(\neg\mathrm{A} \wedge \neg\mathrm{B})} \,.$$

Proof. Suppose A ∧ B and, towards a contradiction, assume ¬A ∨ ¬B. By rule (2.1) we obtain A from A ∧ B and applying the double negation rule (2.3) ¬¬A is derived. Thus, applying rule (2.2) to ¬A ∨ ¬B, ¬B is derived. Since B follows from A ∧ B by rule (2.1), a contradiction is reached, and we can conclude that ¬ (¬A ∨ ¬B) as required.

The other logical law, that is $\neg(\neg \mathrm{A} \wedge \neg \mathrm{B})$ follows from $\mathrm{A} \vee \mathrm{B}$, is proved in a similar fashion. □

By De Morgan's laws $\wedge$ and $\vee$ are definable one from the other using $\neg$, so we could use just one of these two connectives, if we wished so.

Example 2.2. Consider the statements:

$$\mathrm{A}: \quad \pi + \mathrm{e} \notin \overline{\mathbb{Q}}, \qquad\qquad \mathrm{B}: \quad \pi \cdot \mathrm{e} \notin \overline{\mathbb{Q}},$$

where $\overline{\mathbb{Q}}$ is the field of algebraic numbers. In other words A asserts "$\pi + \mathrm{e}$ is transcendental" and B asserts "$\pi \cdot \mathrm{e}$ is transcendental". Since e, π are the only solutions of the equation $x^2 - (\pi + \mathrm{e}) \cdot x + \pi \cdot \mathrm{e} = 0$ and both are transcendental numbers, then $\pi + \mathrm{e} \in \overline{\mathbb{Q}}$ and $\pi \cdot \mathrm{e} \in \overline{\mathbb{Q}}$ cannot both be true, that is $\neg\,(\neg \mathrm{A} \wedge \neg \mathrm{B})$, and by De Morgan's law we can assert that $\mathrm{A} \vee \mathrm{B}$. To this day, the transcendence of $\mathrm{e} + \pi$ and $\mathrm{e} \cdot \pi$ are open problems, i.e. there is no proof of either A or B.[4]

Example 2.3. Let P be the set of all primes, and let

$$W = \left\{p \in P \mid p^2 \mid (2^{p-1} - 1)\right\}.$$

Consider the following statements:

$$\mathrm{A}: \quad W \text{ is infinite}, \qquad\qquad \mathrm{B}: \quad P \setminus W \text{ is infinite}.$$

Since P is infinite, at least one amongst W and $P \setminus W$ is infinite, that is $\mathrm{A} \vee \mathrm{B}$ is true. The only known primes in W are 1093 and 3511, and it is not known whether there are infinitely many primes not in W. In other words: both A and B are open.

Remarks 2.4. (a) Several experts in number theory believe that both W and $P \setminus W$ are infinite.

(b) If $p < 1093$ is prime, then $2^{p-1} - 1$ is not divisible by p^2, so numerical evidence would have led us to believe that $W = \emptyset$, that is $p^2 \nmid 2^{p-1} - 1$ for all primes. This could be added to the list of examples on page 2.

From what we said about implication, asserting $\neg(\mathrm{A} \Rightarrow \mathrm{B})$ means that A holds while B does not hold. Thus it is equivalent to saying that $\mathrm{A} \wedge \neg \mathrm{B}$ which, by De Morgan's laws, is equivalent to $\neg(\neg \mathrm{A} \vee \mathrm{B})$. We have thus verified that $\neg(\mathrm{A} \Rightarrow \mathrm{B})$ is equivalent to $\neg(\neg \mathrm{A} \vee \mathrm{B})$, that is $\mathrm{A} \Rightarrow \mathrm{B}$ is equivalent to $\neg \mathrm{A} \vee \mathrm{B}$, in symbols

$$\frac{\mathrm{A} \Rightarrow \mathrm{B}}{\neg \mathrm{A} \vee \mathrm{B}} \quad \text{and} \quad \frac{\neg \mathrm{A} \vee \mathrm{B}}{\mathrm{A} \Rightarrow \mathrm{B}}.$$

[4] The received opinion among number theorists is that both problems have affirmative answer, that is both A and B are true, hence $\mathrm{A} \wedge \mathrm{B}$ holds.

The rule (2.2) can be recast for implication as: from $\mathrm{A} \Rightarrow \mathrm{B}$ and A we can infer B. This rule is called ***Modus Ponens***:

$$\text{(MP)} \qquad \frac{\mathrm{A} \Rightarrow \mathrm{B} \qquad \mathrm{A}}{\mathrm{B}}\,.$$

Using the double negation rule (2.3) it is easy to check that

$$\frac{\mathrm{A} \Rightarrow \mathrm{B}}{\neg\mathrm{B} \Rightarrow \neg\mathrm{A}}\,.$$

$\neg\mathrm{B} \Rightarrow \neg\mathrm{A}$ is called the **contrapositive** of $\mathrm{A} \Rightarrow \mathrm{B}$. The connective $\Rightarrow$ is neither commutative, nor associative, as the meaning of $\mathrm{A} \Rightarrow \mathrm{B}$ and $\mathrm{B} \Rightarrow \mathrm{A}$ is completely different, and so is the meaning of $(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{C}$ and $\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})$. Observe that $\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})$ means that assuming A and B, we can infer C, and hence it is equivalent to $(\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{C}$.

The bi-conditional $\Leftrightarrow$ is the conjunction of two implications, in symbols

$$\frac{\mathrm{A} \Leftrightarrow \mathrm{B}}{\mathrm{A} \Rightarrow \mathrm{B}} \qquad \text{and} \qquad \frac{\mathrm{A} \Leftrightarrow \mathrm{B}}{\mathrm{B} \Rightarrow \mathrm{A}}$$

and

$$\frac{\mathrm{A} \Rightarrow \mathrm{B} \qquad \mathrm{B} \Rightarrow \mathrm{A}}{\mathrm{A} \Leftrightarrow \mathrm{B}}\,.$$

The bi-conditional is easily seen to be commutative, that is $\mathrm{A} \Leftrightarrow \mathrm{B}$ and $\mathrm{B} \Leftrightarrow \mathrm{A}$ have the same meaning. It can be shown that $\Leftrightarrow$ is associative, but the verification of this is postponed to Exercise 3.40. The statement "A if and only if B if and only if C" is rendered by $(\mathrm{A} \Leftrightarrow \mathrm{B}) \wedge (\mathrm{B} \Leftrightarrow \mathrm{C})$. In many books (including this one) there are multi-lined formulæ in which the connectives $\Rightarrow$ and $\Leftrightarrow$ are treated like the symbols $\leq$ and $=$, so that from

$$\begin{aligned} \mathrm{A}_1 &\Rightarrow \mathrm{A}_2 \\ &\Leftrightarrow \mathrm{A}_3 \end{aligned} \tag{2.4}$$

we infer that $\mathrm{A}_1 \Rightarrow \mathrm{A}_3$. The argument described in the diagram (2.4) is formalized as $(\mathrm{A}_1 \Rightarrow \mathrm{A}_2) \wedge (\mathrm{A}_2 \Leftrightarrow \mathrm{A}_3)$, which indeed yields $\mathrm{A}_1 \Rightarrow \mathrm{A}_3$.

There are a few more connectives that occasionally appear in a mathematical text.

- The **exclusive disjunction** (corresponding to the latin *aut*, and usually dubbed in computer science as *xor*) is $\mathrm{A} \dot\vee \mathrm{B}$ meaning "either A or B, but not both", or equivalently: "exactly one between A and B holds". Observe that $\mathrm{A} \dot\vee \mathrm{B}$ is equivalent to $(\mathrm{A} \vee \mathrm{B}) \wedge \neg(\mathrm{A} \wedge \mathrm{B})$, and also to $\neg(\mathrm{A} \Leftrightarrow \mathrm{B})$. The connective $\dot\vee$ is commutative and associative.
- **Sheffer' stroke** defined by $\mathrm{A} \mid \mathrm{B}$ if and only if "it is not the case that both A and B hold", and **Peirce's arrow** defined by $\mathrm{A} \uparrow \mathrm{B}$ if and only if "neither A nor B". Thus $\mathrm{A} \mid \mathrm{B}$ has the same meaning as $\neg\,(\mathrm{A} \wedge \mathrm{B})$, while $\mathrm{A} \uparrow \mathrm{B}$ has the same meaning as $\neg\,(\mathrm{A} \vee \mathrm{B})$, and for this reason in computer science $\mid$ and $\uparrow$ are called *nand* and *nor*.[5]

[5] The connectives $\mid$ and $\uparrow$ are named after the logicians Sheffer and Peirce.

- The **majority connective** $M(\mathrm{A},\mathrm{B},\mathrm{C})$ stating "at least two among A, B, C, hold".

All connectives seen so far, except $\neg$ and the majority connective, are binary, meaning they operate on two propositions. (The majority connective is ternary, while $\neg$ is unary). All these can be written using $\neg, \vee, \wedge$; in fact this applies to any k-ary connective—see Section 3.C.1.

2.A.2. *Quantifiers.* When we write statements like $\exists x \mathrm{A}$ or $\forall x \mathrm{A}$ we implicitly mean that A asserts some property of x. For example, if A is the equation $x^2 + x = 0$, the expression $\exists x \mathrm{A}$ says that the equation admits a solution—which is true in every field. Instead $\forall x \mathrm{A}$ says that every number is a solution of A—which is true in just one field, $\mathbb{Z}(2)$. If A does not say anything about x, the meaning of $\exists x \mathrm{A}$ and of $\forall x \mathrm{A}$ is exactly that of A—for example $\exists x \exists y \left(y^2 + y = 0\right)$ and $\forall x \exists y \left(y^2 + y = 0\right)$ are both equivalent to $\exists y \left(y^2 + y = 0\right)$. Negating $\forall x \mathrm{A}$ means that not every x enjoys property A, that is to say: there is at least one x for which we can assert $\neg \mathrm{A}$. Conversely, denying $\exists x \mathrm{A}$ means that it is not the case that there is an x such that A, that is: $\neg \mathrm{A}$ must hold for all x. In symbols

$$\frac{\neg \forall x \mathrm{A}}{\exists x \neg \mathrm{A}} \qquad \text{and} \qquad \frac{\neg \exists x \mathrm{A}}{\forall x \neg \mathrm{A}} .$$

When writing $\forall x \forall y \mathrm{A}$ we mean that no matter how x and y are chosen, A holds, and this is the same thing as saying $\forall y \forall x \mathrm{A}$. Similarly $\exists x \exists y \mathrm{A}$ has the same meaning of $\exists y \exists x \mathrm{A}$. Thus

$$\frac{\exists x \exists y \mathrm{A}}{\exists y \exists x \mathrm{A}} \qquad \text{and} \qquad \frac{\forall x \forall y \mathrm{A}}{\forall y \forall x \mathrm{A}} .$$

Suppose $\exists x \forall y \mathrm{A}$ holds: thus there is $\bar{x}$ such that for all y it is true that A. Therefore given an arbitrary y we can always find an x such that A: just pick $\bar{x}$. In other words,

$$\frac{\exists x \forall y \mathrm{A}}{\forall y \exists x \mathrm{A}} .$$

This rule cannot be reversed: from $\forall y \exists x \mathrm{A}$ we cannot conclude $\exists x \forall y \mathrm{A}$—to see this consider the statements $\forall y \exists x (y < x)$ and $\exists x \forall y (y < x)$ in $\mathbb{N}$.

The existential quantifier distributes over disjunction, in the following sense: saying "there is an x such that A or there is an x such that B" is the same as saying "there is an x such that A or B", in symbols

$$\frac{(\exists x \mathrm{A}) \vee (\exists x \mathrm{B})}{\exists x (\mathrm{A} \vee \mathrm{B})} \qquad \text{and} \qquad \frac{\exists x (\mathrm{A} \vee \mathrm{B})}{(\exists x \mathrm{A}) \vee (\exists x \mathrm{B})} .$$

For the existential quantifier and conjunction we have just one rule: if "there is an x such that A and B" then "there is an x such that A, and there is an x such that B", that is

$$\frac{\exists x (\mathrm{A} \wedge \mathrm{B})}{(\exists x \mathrm{A}) \wedge (\exists x \mathrm{B})} .$$

The converse is false: there are even numbers, and there are odd numbers, but no number can be even and odd. Similarly, the universal quantifier distributes with respect to conjunction

$$\frac{(\forall x \mathrm{A}) \wedge (\forall x \mathrm{B})}{\forall x\, (\mathrm{A} \wedge \mathrm{B})} \qquad \text{and} \qquad \frac{\forall x\, (\mathrm{A} \wedge \mathrm{B})}{(\forall x \mathrm{A}) \wedge (\forall x \mathrm{B})}\,,$$

but only partially with respect to disjunction

$$\frac{(\forall x \mathrm{A}) \vee (\forall x \mathrm{B})}{\forall x\, (\mathrm{A} \vee \mathrm{B})}\,.$$

This analogy between existential quantification and disjunction on one hand, and universal quantification and conjunction on the other, is not that surprising, since quantifiers can be seen as generalized conjunctions and disjunctions: saying that $\exists x P(x)$ holds in $\mathbb{N}$ is tantamount to $P(0) \vee P(1) \vee P(2) \vee \dots$, while asserting $\forall x P(x)$ in $\mathbb{N}$ is tantamount to $P(0) \wedge P(1) \wedge P(2) \wedge \dots$.

In order to assert $\exists x \mathrm{A}$ we do not require to exhibit a witness x that satisfies A. For example, to show $\exists x \mathrm{A}$ it is possible to argue by contradiction, that is to say: show that $\forall x \neg \mathrm{A}$ yields a contradiction. Many results in number theory are of this kind—it is shown that there must be a number that enjoys a certain property, but often it is not even possible to establish an upper bound for such integer. The following example gives an existential statement where it is not easy to determine the witness.

Example 2.5. The statement $\exists x\, (P(x) \Rightarrow \forall y P(y))$ is always true, regardless of the meaning of P.[6]

To check this we proceed by cases.

- Property P holds of every individual, that is $\forall y P(y)$. Then by properties of implication $P(x) \Rightarrow \forall y P(y)$ holds, hence any individual witnesses $\exists x\, (P(x) \Rightarrow \forall y P(y))$.
- There is an individual a that does not satisfy P: then a witnesses that $\exists x (P(x) \Rightarrow \forall y P(y))$, since it falsifies $P(x)$ and hence the implication $P(x) \Rightarrow \forall y P(y)$ is true.

Therefore $\exists x\, (P(x) \Rightarrow \forall y P(y))$ holds true in every case.

Example 2.6. The **Möbius function** $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ is defined by $\mu(0) = \mu(1) = 0$ and

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 \mid n \text{ for some prime } p, \\ 1 & \text{if } n = p_1 \cdots p_k \text{ with } p_1 < \cdots < p_k \text{ prime and } k \text{ even}, \\ -1 & \text{if } n = p_1 \cdots p_k \text{ with } p_1 < \cdots < p_k \text{ prime and } k \text{ odd}. \end{cases}$$

[6] The student might want to apply this to the case when $P(x)$ says that x successfully passes the final test in a given class.

It is known that

$$|\textstyle\sum_{k=1}^{n} \mu(k)| > \sqrt{n}, \tag{2.5}$$

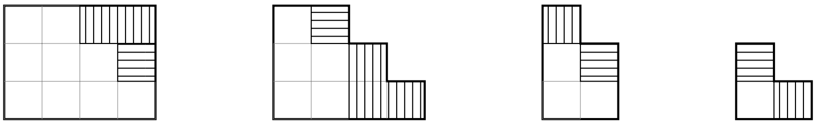
for infinitely many ns, so in particular $\exists x\,(|\sum_{k=1}^{x} \mu(k)| > \sqrt{x})$. On the other hand, no explicit example of a number satisfying (2.5) is known: the least such n lies in the interval $(10^{14}; \mathrm{e}^{1.59\cdot 10^{40}})$.[7]

There are situations where it is known that the witness of an existential quantification $\exists x\mathrm{A}$ appears in a finite list of individuals $a_1, \dots, a_k$, although we are not able to determine which one is the witness, i.e. we are not able to pin-down a number i such that a_i satisfies A.

Example 2.7. Consider the following game in which Alice and Bob take turns and eat a chocolate bar of size $n \times m$. If each square of the bar is identified with its coordinate (i, j) with $1 \leq i \leq n$ and $1 \leq j \leq m$, then the rules of the game are:

- at any round Alice plays first, and each player picks a square (i, j) still present on the bar and removes that and all the squares that lie above or to the right of it, i.e. all (i', j') with $i \leq i'$ and $j \leq j'$;
- the player that picks the last square $(1, 1)$ in the lower left corner loses.

If the chocolate bar is of size 1×1 it has just one square so Alice, the first player, loses right away. Let us see a run of the game on a bar of size 4×3. Alice starts by picking $(3, 3)$ removing thus two squares, and Bob responds by chipping away the square $(4, 2)$. In the second round Alice picks $(3, 1)$ removing three squares, and Bob responds by removing $(2, 3)$. In the third round Alice and Bob choose $(1, 3)$ and $(2, 2)$, respectively, while in the fourth round Alice chooses $(2, 1)$ and Bob $(1, 2)$. Here is the picture of the first four rounds with ▥ denoting Alice's moves, and ▤ denoting Bob's moves.



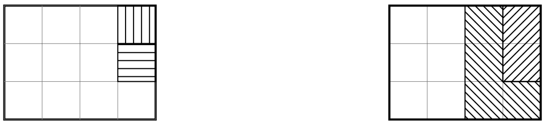
As Alice is the next to move, and must pick the last square, she loses.

A strategy for either player is a set of instructions telling how to respond to the opponent's moves. A strategy for a player is winning if any run of the game according to such strategy guarantees victory for the player.

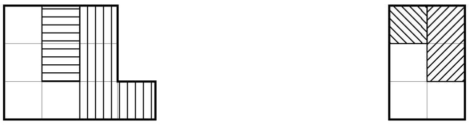
Proposition. *If $(n, m) \neq (1, 1)$ Bob does not have a winning strategy in the game of size $n \times m$.*

[7] This example further corroborates what was said on page 1: sometimes numerical evidence is misleading.

Proof. Towards a contradiction, suppose Σ is a winning strategy for Bob in the game of size $n \times m$, with $(n, m) \neq (1, 1)$. We will pit Σ against itself by constructing two runs of the game in which the roles of Alice and Bob are reversed, and show that this leads to a contradiction. As first move, say Alice picks the square (n, m) in the upper right corner. Then Σ tells Bob how to respond to Alice's first move, and the key observation is that the squares removed after the first inning could be seen as a legal move for the first player (that is: Alice) in another run of the game. Then Σ can respond to this move as well, and this move can be used by Alice on the original board. Here is a picture: the main game is the one played on the board on the left, while the side board is on the right, in which Alice's and Bob's moves are denoted by ▨ and ▧ respectively



Thus on the left board Alice plays $(4, 3)$ and Bob (using Σ) responds $(4, 2)$; on the right board Alice plays $(4, 2)$ and Bob (again using Σ) responds $(3, 1)$. In the next inning, Alice can play $(3, 1)$ on the left board, and Bob responds by playing, say $(2, 2)$; then Alice can play $(2, 2)$ on the right board, and Bob will respond according to Σ:



After finitely many moves the two games come to an end, and Bob, having played according to Σ, should be the winner in both runs of the game. But the roles and the moves of Alice and Bob are exchanged in the two games, so Bob wins the game on the left board if and only if he loses the game on the right board. A contradiction is reached, so our assumption about the existence of a winning strategy for Bob must be rejected. □

The game lasts a finite number of moves, so by a brute-force analysis[8] of all possible moves and runs of the game, one can argue that one (and only one) of the two players has a winning strategy, and therefore Alice *must* have a winning strategy in any game except the one of size 1×1. Thus we have proved that if $(n, m) \neq (1, 1)$

$$\exists \Sigma \, (\Sigma \text{ is a winning strategy for Alice in the game of size } n \times m)$$

but we have no idea as to what such strategy might be.

[8] For a more elegant, complete argument see **??**.

Example 2.8. The statement

$$\mathrm{A}: \quad \exists x \exists y\, (x \text{ and } y \text{ are irrational and } x^y \text{ is rational})$$

is true. In fact if

$$\mathrm{B}: \quad \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$$

is true, then take $x = y = \sqrt{2}$; if instead $\neg$B is true, then take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$.

Example 2.8 highlights another proof technique: the proof-by-cases method asserts that if A follows from B and from $\neg$B, then A is proved,

$$\frac{\mathrm{B} \Rightarrow \mathrm{A} \qquad \neg\mathrm{B} \Rightarrow \mathrm{A}}{\mathrm{A}} .$$

The statement B is called **conditional assumption**.

Remark 2.9. Deciding whether n satisfies the inequality (2.5) is a problem that can be solved, at least in principle, in a mechanical way. Therefore to determine the least n satisfying (2.5) it is enough to check the finite list of all possible candidates. But when numbers become too large, as in Example 2.6, the computational obstacles become insurmountable.

Example 2.8 illustrates the opposite situation: it is known that the pair witnessing A can be taken to be either $(\sqrt{2}, \sqrt{2})$ or else $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$, but since determining whether a number of the form a^b is rational or not is a non-trivial matter, the argument above does not allow us to decide whether B or $\neg$B holds.

2.B. Formalization. Using the logical constants it is possible to recast in symbolic form the mathematical statements written in the natural language—this translation procedure is called **formalization** and the symbolic expressions obtained this way are called formulæ. Formulæ will be properly introduced in Section 3.A, for the time being we will just look at some examples. The simplest are the atomic formulæ, and correspond to statements that cannot be further analyzed using the logical constants. They are either of the form $a = b$ or else of the form $P(a_1, \dots, a_n)$, where the letter P stands for an n-ary predicate, that is an elementary statement about items $a_1, \dots, a_n$. When P is a binary (i.e. 2-ary) predicate, we often write $a_1 \mathrel{P} a_2$ instead of $P(a_1, a_2)$.

A unary predicate is used to describe properties of objects: for example, working in the complex field, we might want to consider the property of “being a transcendental number”. Binary predicates are used to describe binary relations (orderings, equivalences). Predicates of arity n, for $n \geq 3$, occurring in geometry are the ternary predicate of collinearity, and the 4-ary predicate for complanarity.

An interesting example of ternary relation is given by the so-called **circular orders**. The interval $[0;1)$ can be identified with the unitary circle $\mathbb{S}^1$ via the map $f(x) = \mathrm{e}^{2\pi \mathrm{i} x}$, and the ordering on $[0;1)$ yields a *direction of rotation* (counter-clockwise) on $\mathbb{S}^1$, which is captured by the relation $B(x,y,z)$ defined by "going from x to z you pass through y". Therefore if $a \leq b \leq c$ are in $[0;1)$, then $B(f(a),f(b),f(c))$, but also $B(f(b),f(c),f(a))$ and $B(f(c),f(a),f(b))$.

Theorems in elementary mathematics can be stated without quantifiers, or by adding a stack of universal quantifiers at the beginning of the statement, for example:

- "the commutative and associative properties hold for $\cdot$" can be formalized as $(x \cdot y = y \cdot x) \wedge ((x \cdot y) \cdot z = x \cdot (y \cdot z))$, or as $\forall x \forall y \forall z \big((x \cdot y = y \cdot x) \wedge ((x \cdot y) \cdot z = x \cdot (y \cdot z)) \big)$, or also as $\forall x \forall y (x \cdot y = y \cdot x) \wedge \forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$,
- "a triangle is equilateral if and only if all angles are the same" can be formalized as $T(x) \Rightarrow (L(x) \Leftrightarrow A(x))$ or as $\forall x \, (T(x) \Rightarrow (L(x) \Leftrightarrow A(x)))$, where T is the predicate "being a triangle", L is the predicate "being a polygon with equal sides " and A is the predicate "being a polygon with equal internal angles". We added parentheses around the bi-implication to highlight that the main connective is an implication: if x is a triangle, then $\dots$,
- "the product of two numbers is zero if and only if at least one of them is zero" can be formalized as $x \cdot y = 0 \Leftrightarrow (x = 0 \vee y = 0)$, or as $\forall x \forall y (x \cdot y = 0 \Leftrightarrow (x = 0 \vee y = 0))$.

In the second example the indefinite article "a" means "any". Formalizing a statement requires to know which symbols we are entitled to use, and the *environment* to which the statement refers—e.g. some set endowed with a binary operation, the set of all polygons endowed with suitable predicates, the set of all integers with multiplication and with a distinguished element. These environments are called *structures*, and will be introduced in Section 3.C. For the time being we gloss over this issue and naively assume that the environment will be clear from the context.

If we want to express more advanced concepts, alternations of quantifiers must be used. For example $\forall x (x \neq 0 \Rightarrow \exists y (x \cdot y = 1))$ formalizes "a non-zero element has an inverse", a statement that holds true in every field. The expression $x \neq 0$ is an abbreviation of $\neg(x = 0)$—more generally $a \neq b$ stands for $\neg(a = b)$.

In the preceding example, expressions of the form

$$\text{every } x \text{ such that } P(x) \ (\dots)$$

mean: "given an x, if $P(x)$ then $(\dots)$" whence the use of $\Rightarrow$ in the formalization. Using $\wedge$ instead of $\Rightarrow$ would yield a formula saying that "every x enjoys property P and $(\dots)$", a completely different sentence! For example $\forall x(x \neq 0 \wedge \exists y(x \cdot y = 1))$ says that "every x is non-zero and has an inverse", a statement false in every field, since it fails when x is 0.

Expressions like

$$\text{there is an } x \text{ such that } P(x) \text{ for which } (\dots)$$

are formalized as

$$\exists x\,(P(x) \wedge (\dots))\,.$$

In particular the expression $\exists x > 0(\dots)$ is an abbreviation of $\exists x(x > 0 \wedge (\dots))$, and not of $\exists x(x > 0 \Rightarrow (\dots))$. Denying a statement of the form

$$\text{every } x \text{ such that } P(x)\ (\dots)$$

amounts to saying:

$$\text{there is an } x \text{ such that } P(x) \text{ and not } (\dots).$$

In fact, by properties of quantifiers $\neg\forall x\,(P(x) \Rightarrow (\dots))$ is equivalent to $\exists x\,\neg\,(P(x) \Rightarrow (\dots))$ and since $P(x) \Rightarrow (\dots)$ means that $\neg P(x) \vee (\dots)$, by De Morgan's laws we get $\exists x\,(\neg\neg P(x) \wedge \neg(\dots))$ and hence $\exists x\,(P(x) \wedge \neg(\dots))$. Similarly, denying a statement of the form

$$\text{there is an } x \text{ such that } P(x) \text{ and } (\dots)$$

means that

$$\text{for all } x \text{ such that } P(x) \text{ it is not true that } (\dots),$$

in other words: $\neg\exists x\,(P(x) \wedge (\dots))$ is equivalent to $\forall x\,(P(x) \Rightarrow \neg(\dots))$.

A statement of the form

$$\text{there is a unique } x \text{ such that } P(x) \tag{2.6}$$

means that "there is an x such that $P(x)$ and every other y that has property P is the same as x", that is

$$\exists x\,(P(x) \wedge \forall y\,(P(y) \Rightarrow y = x))\,,$$

or, equivalently,

$$\exists x\,(P(x) \wedge \forall y\,(y \neq x \Rightarrow \neg P(y)))\,.$$

Another equivalent way of writing the statement above is "$P(x)$ for some x, and any two objects satisfying P must coincide", that is

$$\exists x P(x) \wedge \forall x \forall y\,(P(x) \wedge P(y) \Rightarrow x = y)\,.$$

(Asserting only $\forall x \forall y\,(P(x) \wedge P(y) \Rightarrow x = y)$ is not enough, since property P could be always false, thus, vacuously, two elements satisfying P coincide!) A further way to formalize (2.6) is

$$\exists x \forall y\,(P(y) \Leftrightarrow x = y)$$

that is "there is an x such that $P(y)$ if and only if $y = x$, for every y". We write

$$\exists! x P(x)$$

for anyone of the formulæ above. Thus $\exists!$ is not a new quantifier, it is just an abbreviation.

Statements like "$P(x)$, for all sufficiently large x" are formalized as

$$\exists y \forall x\,(y < x \Rightarrow P(x))\,.$$

When talking of natural numbers, the statement above is often formulated as "for all but finitely many x, $P(x)$ holds", while the statement "for infinitely many x, $P(x)$ holds" is rendered as

$$\forall y \exists x\,(y < x \wedge P(x))\,.$$

2.C. Examples of formalizations.

2.C.1. Given function symbols f and g, the statement "$f \circ g$ has a fixed point" is formalized as $\exists x\,(f(g(x)) = x)$, or as $\exists x \exists y\,(f(x) = y \wedge g(y) = x)$.

2.C.2. Given a unary predicate symbol P, the statement "there are at least three elements such that P" is formalized as

$$\exists x_1 \exists x_2 \exists x_3\,(P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)\,,$$

while "there are at most three elements such that P" is equivalent to the negation of "there are at least four elements such that P" and hence it is formalized as

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \bigl(P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge P(x_4) \Rightarrow \\ x_1 = x_2 \vee x_1 = x_3 \vee x_1 = x_4 \vee x_2 = x_3 \vee x_2 = x_4 \vee x_3 = x_4\bigr).$$

For the sake of brevity we shall write the conjunctions $\varphi_1 \wedge \cdots \wedge \varphi_n$ and the disjunctions $\varphi_1 \vee \cdots \vee \varphi_n$ as

$$\bigwedge_{1 \leq i \leq n} \varphi_i \quad \text{and} \quad \bigvee_{1 \leq i \leq n} \varphi_i,$$

while the blocks of quantifiers (of the same kind) $\forall x_1 \dots \forall x_n$ and $\exists x_1 \dots \exists x_n$ are written as $\forall x_1, \dots, x_n$ and $\exists x_1, \dots, x_n$. Therefore the formula above is written as $\forall x_1, \dots, x_4 \Big(\bigwedge_{1 \le i \le 4} P(x_i) \Rightarrow \bigvee_{1 \le i < j \le 4} x_i = x_j \Big)$. For $n \ge 1$ the formulæ

$$\exists x_1, \dots, x_n \Big(\bigwedge_{1 \le i \le n} P(x_i) \wedge \bigwedge_{1 \le i < j \le n} x_i \neq x_j \Big)$$
$$\forall x_1, \dots, x_{n+1} \Big(\bigwedge_{1 \le i \le n+1} P(x_i) \Rightarrow \bigvee_{1 \le i < j \le n+1} x_i = x_j \Big)$$

formalize, respectively, the sentences "there are *at least* n elements such that P holds" and "there are *at most* n elements such that P holds"; for ease of notation they are abbreviated as

$$\exists^{\ge n} x P(x) \quad \text{and} \quad \exists^{\le n} x P(x),$$

while $\exists^{=n} x P(x)$ stands for $\exists^{\ge n} x P(x) \wedge \exists^{\le n} x P(x)$. It is useful to introduce a notation for certain formulæ:

$$(\boldsymbol{\varepsilon}_{\ge n}) \qquad \exists x_1, \dots, x_n \left(\bigwedge_{1 \le i < j \le n} x_i \neq x_j \right)$$

formalizes the statement "there are at least n elements",

$$(\boldsymbol{\varepsilon}_{\le n}) \qquad \forall x_1, \dots, x_{n+1} \left(\bigvee_{1 \le i < j \le n+1} x_i = x_j \right)$$

formalizes the statement "there are at most n elements" and

$$(\boldsymbol{\varepsilon}_{n}) \qquad \boldsymbol{\varepsilon}_{\le n} \wedge \boldsymbol{\varepsilon}_{\ge n}.$$

formalizes the statement "there are exactly n elements". These definition are meant for $n \ge 2$. When $n = 1$ let

$$(\boldsymbol{\varepsilon}_{\ge 1}) \qquad \exists x_1 \, (x_1 = x_1) \, ,$$
$$(\boldsymbol{\varepsilon}_{\le 1}) \qquad \forall x_1, x_2 \, (x_1 = x_2) \, ,$$
$$(\boldsymbol{\varepsilon}_{1}) \qquad \boldsymbol{\varepsilon}_{\le 1} \wedge \boldsymbol{\varepsilon}_{\ge 1}.$$

Since $\exists x_1 \, (x_1 = x_1)$ is trivially true, $\boldsymbol{\varepsilon}_{\le 1}$ and $\boldsymbol{\varepsilon}_1$ are equivalent.

2.C.3. Consider a phrase like: "between two rationals there is an irrational, and conversely" or more generally, a phrase like "between two elements that have property P there is an element with property Q, and conversely". Here "conversely" means that "between two elements that have property Q there is an element with property P". In order to formalize it, we need two unary predicates P and Q and the symbol $<$ for the ordering:

$$\begin{aligned} &\forall x \forall y \, ((x < y \wedge P(x) \wedge P(y)) \Rightarrow \exists z \, (x < z \wedge z < y \wedge Q(z))) \\ &\qquad \wedge \forall x \forall y \, ((x < y \wedge Q(x) \wedge Q(y)) \Rightarrow \exists z \, (x < z \wedge z < y \wedge P(z))) \, . \end{aligned}$$

2.C.4. A celebrated theorem of Euclid's says that there are infinitely many prime numbers, that is

$$\forall x \exists y \, (x < y \wedge \mathrm{Pr}(y))$$

where Pr is the unary predicate "being a prime number". If we want to formalize this statement using only the divisibility relation, $\mid$ (besides the ordering relation), we translate $\mathrm{Pr}(y)$ into

$$1 < y \wedge \forall z \, (z \mid y \Rightarrow z = 1 \vee z = y)$$

and hence Euclid's theorem becomes

$$\forall x \exists y \, (x < y \wedge 1 < y \wedge \forall z \, (z \mid y \Rightarrow z = 1 \vee z = y)) \, .$$

We have eliminated the predicate Pr, but we have introduced the constant 1. To get rid of it, observe that 1 is the only natural number that divides every natural number, that is $\exists! u \forall w (u \mid w)$, thus Euclid's theorem can be formalized as

$$\exists u \forall w \Big(u \mid w \wedge \forall x \exists y \big(x < y \wedge u < y \wedge \forall z \, (z \mid y \Rightarrow z = u \vee z = y) \big) \Big) .$$

Since $z \mid y$ if and only if $\exists v \, (v \cdot z = y)$, it is possible to formalize everything using the ordering and multiplication (Exercise 2.10).

2.C.5. Distinct natural numbers x and y can have the same prime factors, but if we consider also $x+1, x+2, \ldots, x+k$ and $y+1, y+2, \ldots, y+k$ with k sufficiently large, it is possible to find a prime p that divides exactly one among the $x+i$ and $y+i$, for $i \leq k$. The **Erdős-Woods conjecture** says that there is a universal k. In other words:

> There is an integer $k > 0$ such that every integer x is completely determined by the primes that divide $x, x+1, \ldots, x+k$

The formalization of this conjecture is

$$\exists k \, \forall x, y \, \big[x \neq y \Rightarrow \exists i, p \, (i \leq k \wedge \mathrm{Pr}(p) \wedge (p \mid (x+i) \Leftrightarrow p \nmid (y+i))) \big] .$$

The symbol Pr can be eliminated as in the preceding example, while the inequality $i \leq k$ can be reformulated as $\exists z \, (i + z = k)$.

Exercises

Exercise 2.10. Formalize Euclid's theorem on prime numbers using only multiplication $\cdot$ and the order relation $<$.

Exercise 2.11. Formalize the following sentences on natural numbers, using the given symbols:

(i) **Bertrand's postulate**: for every $n > 1$ there is at least a prime between n and $2n$, using the ordering $<$, the sum $+$, the constant 1, and the divisibility relation $|$. Do the same using $+$ and $|$.

(ii) **Legendre's conjecture**: for all $n > 1$ there is a prime between n^2 and $(n+1)^2$, using $<$, 1, and multiplication $\cdot$. Do the same using $<$ and $\cdot$.

(iii) The **twin primes conjecture**: there are infinitely many primes of the form p, $p+2$, using $<$ and the divisibility relation $|$.

(iv) **Goldbach's conjecture**: every even number larger than two is the sum of two primes, using $<$, the constant 2, addition $+$, and $|$. Do the same using $+$ and $|$.

(v) **Vinogradov's theorem**: every sufficiently large odd number is sum of three (not necessarily distinct) primes, using $<$, $+$, and $|$. Do the same using $+$ and $|$.

(vi) "Every sufficiently large natural number is sum of at most four cubes", using $<$, $+$, and $\cdot$. Do the same using $+$ and $\cdot$.

(vii) **Fermat's last theorem**: no cube is the sum of two cubes, no fourth power is sum of two fourth powers, and so on, using $<$, 2, $+$ and the exponential function x^y. Do the same using $+$ and x^y.

(viii) **Dirichlet's theorem**: if a and b are relatively prime, the there are infinitely many primes congruent to a modulo b, using $<$, $+$ and $\cdot$. Do the same using $+$ and $\cdot$.

(ix) The **Green-Tao theorem**: the set of primes contains arbitrarily long arithmetic progressions, using $<$, $+$, and $\cdot$. Do the same using $+$ and $\cdot$.

(x) **Beal's conjecture**: if a, b, c, x, y, z are natural numbers such that $a^x + b^y = c^z$, with $a, b, c > 1$ and $x, y, z > 2$, then a, b and c have a common prime factor, using $<$, 1, $+$, $\cdot$ and x^y. Do the same using $+$, $\cdot$ and x^y.

Exercise 2.12. (i) Formalize the following sentences, using the symbol f:

- f is injective,
- f is surjective,
- f is bijective,
- $f \circ f$ is the identity,
- the fibers of f have size at most three.

(ii) If $f, g\colon A \times A \to A$, let $\langle f, g\rangle\colon A \times A \to A \times A$ be the function defined by $(a_1, a_2) \mapsto (f(a_1, a_2), g(a_1, a_2))$. Repeat part (i) with $\langle f, g\rangle$ instead of f, using the symbols f and g.

Exercise 2.13. Formalize the following statement:

> among six persons, there are at least three that either are acquainted with each other, or else that mutually unfamiliar

using the predicates $A(x, y)$ to express the fact that x and y know each other, and $U(x, y)$ to express the fact that x and y do not know each other. (Clearly it is possible to use just one of the two predicates A, U and define the other by negation.)

Exercise 2.14. Let f be a real variable function of one real variable. Using the symbols f, $+$, $\cdot$, $|\cdot|$, and $<$, formalize the statements: "f is continuous" and "f is differentiable". Repeat the exercise using only f, $+$, and $\cdot$.

Exercise 2.15. Let $f\colon \mathbb{R}^2 \to \mathbb{R}$. Using the symbols f, $+$, $\cdot$, x_0 and y_0 formalize the implicit function theorem:

> If f is continuously differentiable in (x_0, y_0) and $\partial f/\partial y$ does not vanish in (x_0, y_0), then there is an open neighborhood U of x_0 and an open neighborhood V of y_0 such that for every $x \in U$ there is exactly one $y \in V$ such that $f(x, y) = 0$.

Exercise 2.16. Formalize the following statements:

(i) there is a line passing through two points;

(ii) there is exactly one line passing through two distinct points;

(iii) there is exactly one plane passing through three non-collinear points;

using the unary predicates $P(x)$, $Q(x)$, $R(x)$ for "x is a point", "x is a line", "x is a plane" and the binary predicate $L(x, y)$ for "x lies on y".

Notes and remarks

The fact that Euler's constant e is transcendental was proved in 1873 by Hermite, and that π is transcendental was proved in 1882 by von Lindeman—see Example 2.2. The prime numbers p that satisfy $p^2 \mid (2^{p-1} - 1)$ (Example 2.3) are called **Wieferich's primes**, from the mathematician that first defined and studied them in 1909.

Example 2.6 illustrates how theorems can contradict opinions based upon experiments and numerical simulations. Stieltjes conjectured nel 1885 in a letter to Hermite and Mertens that $\forall n\, (\left|\sum_{k=1}^{n} \mu(k)\right| < \sqrt{n})$, and this became known as **Mertens' conjecture**. This conjecture was refuted in [**OtR85**]. The function μ is named after Möbius.

Example 2.8 is a showcase for the power and simplicity of non-constructive arguments, and for the method of proof-by-cases, that is the proof of a statement B from an additional assumption A, and from its negation ¬A, on whose validity we know little. Truth be told, the existence of irrational numbers whose exponential is rational follows immediately from the following result proved in 1934 by Gelfond and independently by Schneider: if $a \neq 0, 1$ is algebraic and b is irrational, then a^b is transcendental. (The statement of this theorem was the seventh on Hilbert's celebrated 1900 list of open problems in mathematics.) Therefore statement A in Example 2.8 is false. The proof-by-cases method has been employed many times in number theory using as a conditional assumption one of the most important open problems in mathematics, the generalized Riemann hypothesis [**IR90**, pp. 358–361].

The Erdős-Woods conjecture was formulated by Erdős and studied by Woods [**Woo81**] in connection with interesting problems in logic (see page 288). Not much is known on this conjecture, except that follows from the *abc* conjecture (Example 3.4) and that $k \neq 1$, since the pairs $(2, 3)$ and $(8, 9)$ have the same prime factors; it is not known if $k \neq 2$. For further information see [**Guy04**, B29].

The statements in Exercise 2.11 are either open problems or important theorems in number theory. Bertrand's postulate was conjectured in 1845 by Bertrand and proved in 1850 by Chebyshev. Vinogradov proved in 1937 the theorem named after him. (Note that Goldbach's conjecture implies this result.) The theorems in (viii) and (ix) were proved by Dirichlet in 1837, and by Green and Tao in 2004.

The conjectures of Legendre, Goldbach, the twin prime conjecture, Beal's conjecture, and part (vi) of Exercise 2.11 are open. The first two conjectures are named after the mathematicians that formulated them, Goldbach and Legendre, while Beal's conjecture was introduced in1993 by Beal[9] and, independently, by Granville. Part (vi) of Exercise 2.11 becomes a theorem if seven cubes, rather than four cubes are considered—see Notes and Remarks on page 69.

Fermat around 1637 wrote in the margins of Diophantus' *Arithmetica* book:

> I found a truly marvelous proof that it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. This margin is too narrow to contain this proof.[10]

Fermat never gave a proof of this statement (although he gave a proof in the case of exponent 4) which became known as *Fermat's last theorem*—Exercise 2.11 part (vii). In the following years this became one of the best known open problems in mathematics, and it was finally solved in 1995 by Wiles and Taylor, finally reaching the status of theorem.

[9] Andrew Beal is tycoon from Texas with a knack for number theory, and has offered \$100.000 for a proof or disproof of his conjecture. On the other hand, Italian tycoons (from Brianza, or elsewhere) seem to have different kind of hobbies.

[10] Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

The statement in Exercise 2.13 is a particular case of a result in graph theory known as Ramsey's Theorem (see page 258), which can be stated as follows: for every n there is an $m > n$ such that given m persons, there are at least n of them that know each other, or that they don't know each other.

Exercises 2.15 and 2.16 are from [**PD11**].

3. Languages

3.A. Symbols, terms, and formulæ.

Symbols. A first-order language $\mathcal{L}$ is made up of the following items:

- the parentheses (and) ,
- the symbols $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, $\forall$, and $\doteq$,
- an infinite list of symbols $v_0, v_1, v_2, \ldots$ called **variables**. The letters $x, y, z, \ldots$, possibly decorated with indices, stand for a generic variable v_n,
- constant symbols, usually denoted by $c, d, e, \ldots$,
- function symbols, usually denoted by $f, g, h, \ldots$,
- predicate symbols, usually denoted by $P, Q, R, \ldots$.

Every function or predicate symbol has a positive integer attached to it, called its **arity**—symbols of arity 1, 2 and 3 are called, respectively, unary, binary, and ternary symbols. Constant, function, and predicate symbols are dubbed non-logical symbols, and characterize the language in question. For the time being we shall assume that there are finitely many such symbols; for a different examples see Section 9.B.3.

Terms. The set of **terms** of $\mathcal{L}$ is inductively defined as follows:

- a variable is a term,
- a constant symbol is a term,
- an expression of the form $f(t_1, \ldots, t_n)$ is a term, where f is an n-ary function symbol and $t_1, \ldots, t_n$ are terms called the sub-terms of $f(t_1, \ldots, t_n)$.

Remark 3.1. The careful reader might have noticed that $f(t_1, \ldots, t_n)$ contains the comma (which is not present in the official list of symbols) to parse the terms t_i. This is purely for typographical reasons, to visually delimit the objects, and the correct way would be to write $f(t_1 \ldots t_n)$ rather than $f(t_1, \ldots, t_n)$. This move implicitly assumes that the ensuing expressions can be unambiguously read: if an $\mathcal{L}$-term can be read as $f(t_1 \ldots t_n)$ and as $g(u_1 \ldots u_m)$ then $n = m$, $f = g$ and $t_i = u_i$ for $i = 1, \ldots, n$. In Section 23 a result asserting the unique readability of expressions will be proved, so, in principle, we could dispense with commas, and even parentheses. But at the beginning of an exposition of mathematical logic, a slightly redundant notation is preferable to an exceedingly terse one.

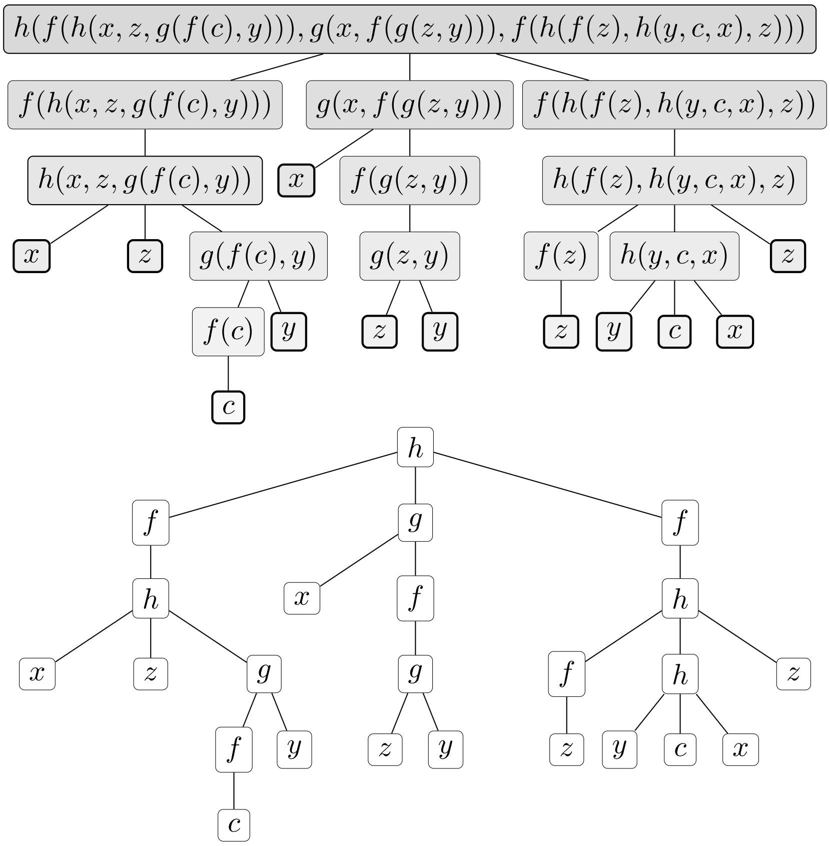


Figure 2. The syntactic tree of the term described in (3.1) and its simplified form.

A term t is a finite sequence of symbols (obtained following a well-established protocol), but can be better visualized by means of its **syntactic tree**[11] where the root is labelled by t and the other nodes are labelled by the terms that t is made of. For example the syntactic tree of the term

$$h(f(h(x,z,g(f(c),y))),g(x,f(g(z,y))),f(h(f(z),h(y,c,x),z))), \tag{3.1}$$

where c is a constant symbol and f, g and h are function symbols of arity 1, 2, and 3, is the object described in the upper part of Figure 2. The terminal nodes, i.e. those that have no nodes below them, are labelled with variables or constant symbols, and are highlighted with a thicker frame. We could simplify the notation by putting in every non-terminal node the function symbol used to build such term. This way the syntactic tree can be drawn as in the lower part of Figure 2. The nodes of the syntactic tree of t are

[11] The botany of logic (and of computer science) is a tad peculiar, since trees grow downwards. Maybe *roots* would be a more appropriate name, but then we would need a different name to denote the top-most node.

the sub-terms t. Observe that parentheses are not needed for describing a syntactic tree, corroborating Remark 3.1.

Notation. When f is a binary function symbol, the infix notation $t_1 \, f \, t_2$ rather than the prefix notation $f(t_1, t_2)$ is preferred. In particular we shall write $t_1 + t_2$ and $t_1 \cdot t_2$ instead of $+(t_1, t_2)$ and $\cdot(t_1, t_2)$.

When f is a binary function symbol, the expression $t_1 \; f \; \ldots \; f \; t_n$ is ambiguous, since its meaning depend on where the parentheses are placed. For example, the possible meaning of $t_1 \; f \; t_2 \; f \; t_3$ are two: $t_1 \; f \; (t_2 \; f \; t_3)$ and $(t_1 \; f \; t_2) \; f \; t_3$. For this reason we make the following:

Convention. When writing $t_1 \, f \ldots f \, t_n$ it is understood that we associate on the right, that is $t_1 \, f \, (t_2 \, f \, (\ldots (t_{n-1} \, f \, t_n) \ldots))$. In particular $t_1 + \cdots + t_n$ stands for $t_1 + (\cdots + (t_{n-1} + t_n) \cdots)$ and $t_1 \cdot \cdots \cdot t_n$ stands for $t_1 \cdot (\cdots \cdot (t_{n-1} \cdot t_n) \cdots)$. We will use the following shorthand

$$nt \text{ instead of } \underbrace{t + \cdots + t}_{n} \quad \text{and} \quad t^n \text{ instead of } \underbrace{t \cdot \cdots \cdot t}_{n}.$$

Finally, when f is a unary function symbol and t is a term,

$$f^{(n)}(t) \text{ denotes the term } \underbrace{f(\ldots f}_{n \text{ times}}(t) \ldots).$$

A measure of complexity for terms is a function from the set of all terms taking values in the natural numbers, such that the number assigned to a term t is larger than the numbers assigned to the terms that t is made of. There are two natural complexity measures for a term t:

- $\mathrm{lh}(t)$, the **length** (including parentheses) of the string t, and
- $\mathrm{ht}(t)$, the **height** of t, that is the length of the longest path in the syntactic tree of t starting from the root and arriving to a terminal node, counting from zero.

It is customary to count from zero when computing the height, therefore if t is the term described in (3.1) on page 24, then $\mathrm{lh}(t) = 48$ and $\mathrm{ht}(t) = 5$.

Complexity measures are useful for proving results by induction on the set of terms. In order to show that every term enjoys property $\mathcal{P}$, it is enough to check that $\mathcal{P}$ holds for all terms with minimal complexity (base case) and that if $\mathcal{P}$ holds for all terms of complexity less than that of t, then also t has property $\mathcal{P}$.

The expression $t(x_1, \ldots, x_n)$ means that the variables occurring in t are among $x_1, \ldots, x_n$. (We do not require that *every* x_i occurs in t.) In algebra, when $f(X_1, \ldots, X_n)$ denotes a polynomial in the variables $X_1, \ldots, X_n$, and if $g_1, \ldots, g_n$ are polynomials, then $f(g_1, \ldots, g_n)$ is the polynomial f where $X_1, \ldots, X_n$ have been replaced by $g_1, \ldots, g_n$. Similarly, given terms

$t(x_1, \dots, x_n)$ and $s_1, \dots, s_n$, then $t[s_1/x_1, \dots, s_n/x_n]$ is the term obtained by replacing s_i in place of x_i . When the variables are clear from the context, we may write $t(s_1, \dots, s_n)$. Before we move on, we need to check that $t[s_1/x_1, \dots, s_n/x_n]$ is indeed a term.

Lemma 3.2. *If $s_1, \dots, s_n, t(x_1, \dots, x_n)$ are terms, then $t[s_1/x_1, \dots, s_n/x_n]$ is a term.*

Proof. We proceed by induction on $\mathrm{ht}(t)$. If $\mathrm{ht}(t) = 0$ then t is either a constant c, and therefore $t[s_1/x_1, \dots, s_n/x_n]$ is c, or else it is x_i, and therefore $t[s_1/x_1, \dots, s_n/x_n]$ is s_i. If $\mathrm{ht}(t) > 0$, then t is $f(u_1, \dots, u_k)$ where $u_1, \dots, u_k$ are terms of height $< \mathrm{ht}(t)$, and any variable occurring in one of them is among $x_1, \dots, x_n$. By inductive assumption, every $u_j[s_1/x_1, \dots, s_n/x_n]$ is a term, and so is

$$f(u_1[s_1/x_1, \dots, s_n/x_n], \dots, u_k[s_1/x_1, \dots, s_n/x_n])$$

which is $t[s_1/x_1, \dots, s_n/x_n]$. □

The syntactic tree of $t[s_1/x_1, \dots, s_n/x_n]$ is obtained from the syntactic tree of t by attaching to the terminal nodes labelled with $x_1, \dots, x_n$ the syntactic trees of $s_1, \dots, s_n$.

It is important that the swapping of $x_1, \dots, x_n$ with $s_1, \dots, s_n$ happens simultaneously: if t is $f(x_1, x_2)$ and s_1, s_2 are x_2, x_1 respectively, then $t[s_1/x_1, s_2/x_2]$ is $f(x_2, x_1)$, while $(t[s_1/x_1])[s_2/x_2]$ is $f(x_1, x_1)$. A term is **closed** if it contains no variables, i.e. it is built from constant and function symbols. (If the language has no constant symbols, there are no closed terms.)

Formulæ. An **atomic formula** is an expression of the form

$$P(t_1, \dots, t_n) \qquad \text{or} \qquad t_1 \eqcirc t_2$$

where $t_1, t_2, \dots, t_n$ are terms and P is an n-ary predicate symbol.

Remark 3.3. On the meaning of the symbol $\eqcirc$. The atomic formula $t_1 \eqcirc t_2$ says t_1 and t_2 denote the same as the object, while $t_1 = t_2$ means that the term (i.e. the string of symbols) t_1 is the same as the term t_2. For example, in the language with two binary function symbols $+$ and $\cdot$ we write the atomic formula $(x + y) \cdot (x + y) \eqcirc (x \cdot x) + ((x \cdot y) + ((y \cdot x) + (y \cdot y)))$, although the two term $(x + y) \cdot (x + y)$ and $(x \cdot x) + ((x \cdot y) + ((y \cdot x) + (y \cdot y)))$ are distinct. These kind of distinctions are crucial in computer science: these two terms are *different programs* that compute the *same function.* Although the distinction between $\eqcirc$ and $=$ avoids ambiguities, in order to keep the notation simple we will often write "t is s" rather than "$t = s$". For the time being, the reader can safely consider $\eqcirc$ to be tantamount to $=$, but telling apart the two notions will be important in Section 9.E. Notice though that in the formalizations of Section 2 we should have used $\eqcirc$ instead of $=$.

The set of **formulæ** is defined inductively by the following clauses:

- an atomic formula is a formula,
- if φ is a formula, then $(\neg\varphi)$ is a formula,
- if φ and ψ are formulæ, then $(\varphi \land \psi)$, $(\varphi \lor \psi)$, $(\varphi \Rightarrow \psi)$, and $(\varphi \Leftrightarrow \psi)$ are formulæ,
- if φ is a formula and x is a variable, then $\exists x\varphi$ and $\forall x\varphi$ are formulæ.

The Greek lower case letters φ, ψ, and χ, will range on formulæ.[12] A formula of the form $(\neg\varphi)$ is called a negation; similarly, a formula of the form $(\varphi \land \psi)$, $(\varphi \lor \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$, $\exists x\varphi$ and $\forall x\varphi$ is called conjunction, disjunction, implication, bi-implication, **existential formula**, and **universal formula**, respectively.

Conventions. (i) For the sake of readability, parentheses will be suppressed whenever this move does not cause ambiguity. For example, we shall write $\varphi \land \psi$, $\varphi \lor \psi$, $\varphi \Rightarrow \psi$ and $\varphi \Leftrightarrow \psi$ instead of $(\varphi \land \psi)$, $(\varphi \lor \psi)$, $\dots$; but if we need to take negation of any of these formulæ parentheses shall be reinstated. We shall follow the convention that $\land$ and $\lor$ bind more tightly than $\Rightarrow$ and $\Leftrightarrow$, and that $\neg$ binds more tightly than any other connective. Therefore $\varphi \land \psi \Rightarrow \chi$ and $\neg\varphi \lor \psi$ are shorthand for $((\varphi \land \psi) \Rightarrow \chi)$ and $((\neg\varphi) \lor \psi)$, respectively. In analogy with the case of terms, if $\odot$ is a binary connective (that is: it is not $\neg$) we shall write $\varphi_1 \odot \cdots \odot \varphi_n$ rather than $\varphi_1 \odot (\varphi_2 \odot (\cdots \odot \varphi_n) \dots)$.

(ii) If P is a binary relation symbol, the infix notation $t_1\ P\ t_2$ will generally be preferred to the prefix notation $P(t_1, t_2)$. In particular, we shall write $s < t$ instead of $<(s, t)$.

(iii) The formula $\neg(t_1 = t_2)$ is written as $t_1 \neq t_2$.

The **sub-formulæ** of φ are φ and the formulæ used in the construction of φ. A sub-formula of φ different from φ is a **proper sub-formula**. In other words:

- if φ is atomic, then it has no proper sub-formulæ,
- if φ is $\neg\psi$, then its proper sub-formulæ are ψ and all of the proper sub-formulæ of ψ,
- if φ is $\psi \odot \chi$ with $\odot$ a binary connective, then its proper sub-formulæ are: ψ, χ, the proper sub-formulæ of ψ and the proper sub-formulæ of χ,
- if φ is $\exists x\psi$ or $\forall x\psi$, then the proper sub-formulæ of φ are ψ and all proper sub-formulæ of ψ.

[12] Sometimes upper case Roman letters like A, B, C, ... will be used to denote formulæ, a practice that was already implicitly followed in Section 2.A.

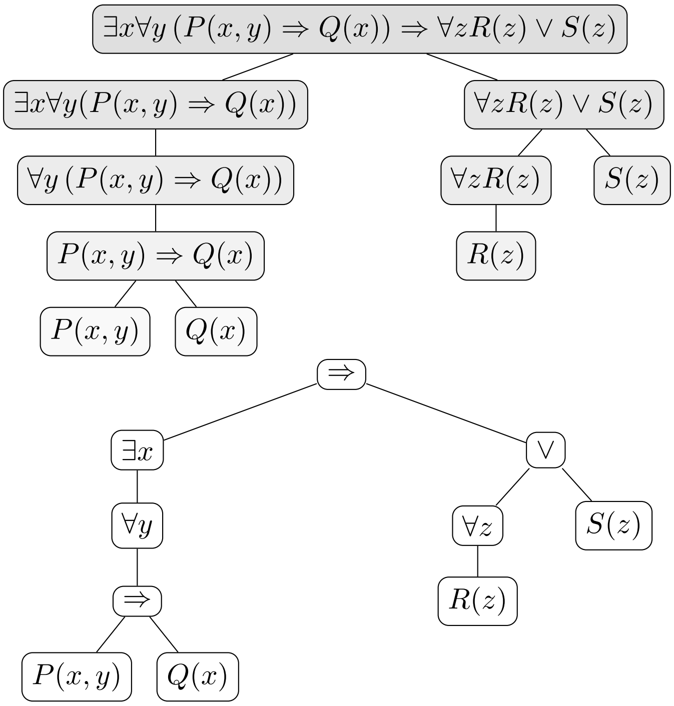

$\exists x \forall y\,(P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \lor S(z)$
$\exists x \forall y (P(x,y) \Rightarrow Q(x))$
$\forall z R(z) \lor S(z)$
$\forall y\,(P(x,y) \Rightarrow Q(x))$
$\forall z R(z)$
$S(z)$
$P(x,y) \Rightarrow Q(x)$
$R(z)$
$P(x,y)$
$Q(x)$
$\Rightarrow$
$\exists x$
$\lor$
$\forall y$
$\forall z$
$S(z)$
$\Rightarrow$
$R(z)$
$P(x,y)$
$Q(x)$

Figure 3. The syntactic tree of the formula $\exists x \forall y\,(P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \lor S(z)$ and its simplified version.

For example, the proper sub-formulæ of

$$\exists x \forall y\,(P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \lor S(z) \tag{3.2}$$

are $\exists x \forall y\,(P(x,y) \Rightarrow Q(x))$, $\forall z R(z) \lor S(z)$ and all of their proper sub-formulæ. Therefore the complete list of all sub-formulæ of (3.2) is:

$$\begin{array}{ccc}
\exists x \forall y (P(x,y) \Rightarrow Q(x)) & & \forall z R(z) \lor S(z) \\
\forall y (P(x,y) \Rightarrow Q(x)) & & \forall z R(z) \\
P(x,y) \Rightarrow Q(x) & & R(z) \\
P(x,y) & & S(z) \\
Q(x) & &
\end{array}$$

Just like the terms, also formulæ can be described by means of trees: the syntactic tree of the formula (3.2) and its simplified version are shown in Figure 3. The nodes of the syntactic tree of φ are the sub-formulæ of φ. Also in this case we have two competing notions of complexity: the length and the height, defined in the same way it was done for terms on page 25.

3.B. More on formalization. In the preceding pages we have seen some examples of statements formalizable in a given language $\mathcal{L}$, but we will often encounter statements that are *not* formalizable in $\mathcal{L}$, although they might be formalizable in a stronger language. In mathematics one often uses expressions involving quantifiers that turn out not to be formulæ according to our official definition, thus we must learn how to distinguish official formulæ from impostors, which will be called **pseudo-formulæ**. These are simply abbreviations, symbolic shorthand of mathematical statements written in natural language. For example $x \cdot y$ cannot be rendered as

$$\underbrace{x + \cdots + x}_{y}$$

when x, y are natural numbers: the expression above is not a term, since its length is not some fixed integer, but varies with y. (Naturally, an expression of the kind $x \cdot 3$ can be written as $x + (x + x)$, which is a term.) Similarly, in Exercise 2.11(vii) the exponentiation cannot be rendered by

$$x^y = \underbrace{x \cdots x}_{y}$$

since the right-hand side is not a term. As we shall see in Section 11.B, exponentiation can be written using only addition and multiplication, but this result is far from trivial. In general, expressions containing ellipsis mean trouble for formalization. For example,

Waring's problem. *For all $k > 1$ there is an n such that every natural number is the sum of n-many numbers that are powers of exponent k.*

is usually formalized as

$$\forall k > 1 \exists n \forall x \exists y_1, \ldots, y_n \left(x = y_1^k + \cdots + y_n^k \right). \tag{3.3}$$

The expression above, although perfectly acceptable in everyday usage, is a pseudo-formula, since the number of quantifiers in the block $\exists y_1, \ldots, y_n$ is not fixed once and for all. This does not mean that there is something wrong or questionable in (3.3)—it simply means that it is not a formula according to our official definition. It doesn't mean either that Waring's problem is not formalizable as a first-order formula in the language with addition and multiplication—see Exercise 11.52.

In some cases it might not be obvious how to formalize a statement in a given language.

Example 3.4. The ***abc* conjecture** says that for every $\varepsilon > 0$ there is a constant κ_ε such that if a, b, c are coprime and $c = a + b$, then $c \leq \kappa_\varepsilon d^{(1+\varepsilon)}$, where d is the product of the distinct prime factors of a, b and c.

At first sight the formalization of this statement in the language of arithmetic seems unlikely because of the real numbers ε and $d^{(1+\varepsilon)}$. On the other hand ε can be taken to be arbitrarily small, say of the form $1/n$, while

κ_ε must be sufficiently large so that the inequality $c \leq \kappa_\varepsilon d^{(1+\varepsilon)}$ becomes $c^n \leq md^{n+1}$. Thus the *abc* conjecture is formalizable as:

$$\begin{aligned}
&\forall n\,\exists m\,\forall a,b,c,d\,\bigl(n>0\ \wedge\\
&\qquad\quad \boxed{d\text{ is the product of the distinct prime factors of }a,\ b\text{ and }c}\\
&\qquad\qquad\qquad\qquad \wedge\ \boxed{a,\ b,\ c\text{ are coprime}} \wedge c = a+b \Rightarrow c^n \leq md^{n+1}\bigr),
\end{aligned}$$

where $\boxed{d\text{ is the product of the distinct prime factors of }a,\ b\text{ and }c}$ can be rendered as

$$\forall p\,\bigl(\mathrm{Pr}(p) \Rightarrow p^2 \nmid d \wedge (p \mid d \Leftrightarrow p \mid a \vee p \mid b \vee p \mid c)\bigr)$$

and $\boxed{a,\ b,\ c\text{ are coprime}}$ can be rendered as

$$\neg\exists p\,[\mathrm{Pr}(p) \wedge ((p \mid a \wedge p \mid b) \vee (p \mid a \wedge p \mid c) \vee (p \mid b \wedge p \mid c))]\,.$$

We can get dispense with the symbols 0, $<$, $\mid$ and Pr by using their definitions in terms of addition and multiplication, and by what we said above, exponentiation can be scraped as well.

3.C. Structures and validity. First-order formulæ are used, implicitly or explicitly, throughout mathematics as they are handy tools for studying algebraic or ordered structures. In order to talk of the properties of a structure, we need a suitable language—for example, in order to define the notion of semigroup we start from a non-empty set S endowed with a binary associative operation $*$ such that

$$\forall x,y,z \in S\,((x*y)*z = x*(y*z)) \tag{3.4}$$

Examples of semigroups are: the natural numbers $\mathbb{N}$ with the addition operation $+$, the set $M_{n,n}(R)$ of all $n \times n$ matrices on a rng R with the operation of matrix-product, and the set F of all functions from a set X to itself with the composition operation $\circ$. The expression (3.4) is a pseudo-formula, since we have followed the usual habit of binding quantified elements to some set, diverting from our official definition of formula. In mathematical logic we start from a language (in this case containing only the binary operation symbol $*$) and say that the formula

$$\forall x,y,z\,((x*y)*z = x*(y*z)) \tag{3.5}$$

is true in the structures $(\mathbb{N},+)$, $(M_{n,n}(R),\cdot)$, $(F,\circ)$, $\ldots$. In other words: the binary symbol $*$ is understood from time to time to denote a different operation, depending on the chosen structure.

Our goal is to

Find a procedure to check whether a formula is true in a structure.

First of all notice that some formulæ are true in every structure, regardless of the meaning we give to the symbols of the language—such formulæ are said to be **valid**. At the other end of the spectrum we have the **unsatisfiable** formulæ which are false in every structure. In other words: a formula is unsatisfiable if and only if its negation is valid. For example, if P and f are n-ary predicate and function symbols, then the formulæ

$$\begin{gathered} x = x \\ x = y \Rightarrow y = x \\ x = y \land y = z \Rightarrow x = z \\ x_1 = y_1 \land \cdots \land x_n = y_n \Rightarrow (P(x_1, \ldots, x_n) \Leftrightarrow P(y_1, \ldots, y_n)) \\ x_1 = y_1 \land \cdots \land x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \end{gathered} \tag{3.6}$$

are valid, since we have agreed that $=$ stands for equality relation. On the other hand the formula

$$\forall x, y\, (x \cdot y = y \cdot x)$$

is **satisfiable** (that is to say: not unsatisfiable) but not valid, since it is either true or false depending whether $\cdot$ denotes an operation that is commutative or not. Similarly $\forall x, y\, (x < y \Rightarrow \exists z\, (x < z \land z < y))$ is a statement true in the rationals or in the reals, but false in the integers, thus it is a satisfiable formula, but not a valid one. In order to establish a procedure to check whether a formula is true in a structure, we must begin to examine the atomic formulæ. But even this case is problematic. For example, to check whether $x < y$ is true in an ordered set $(M, \lhd)$ we must give a value to the variables x and y. By contrast, there are formulæ with free variables whose truth or falsity is not an issue.

Example 3.5. The formula $\neg(x < y) \lor (x < y)$ is true in any structure $(M, \lhd)$, regardless of the value assigned to the variables.

In fact if the variables x, y are given values $a, b \in M$, then the formula holds in $(M, \lhd)$ if either $a \ntriangleleft b$ or else $a \lhd b$, and this is obviously true independently of what a, b and $\lhd$ are.

Arguing as above, any formula of the form $\varphi \Rightarrow \varphi$ or $\neg\varphi \lor \varphi$ is valid, regardless of what φ says.

3.C.1. *Tautologies.* From the examples above we can see as certain formulæ are true by virtue of the meaning of the connectives. In order to study these validities, we must analyze how a formula is built from the atomic, the existential, and the universal ones. As the meaning of $\forall x \varphi$ is the same as $\neg\exists x \neg\varphi$, we may replace the universal quantifiers with its existential quantifiers and negations so that the formula we are considering does not contain the symbol $\forall$. A formula φ is **Boolean combination**[13] of formulæ

[13] The reason for the attribute *Boolean* will become clear in the next sections.

$\mathrm{A}_1, \dots, \mathrm{A}_n$ if φ is obtained from these without using quantifiers. If the A_i's are atomic or existential (that is: they are not Boolean combination of sub-formulæ), then $\mathrm{A}_1, \dots, \mathrm{A}_n$ are the **primitive components** of φ. In other words, they occur as those nodes in the syntactic tree of φ above which no formula is quantified. For example the formula φ in (3.2) on page 28 is first re-written as $\exists x \neg \exists y \neg (P(x, y) \Rightarrow Q(x)) \Rightarrow \neg \exists z \neg R(z) \vee S(z)$, so that its primitive sub-formulæ are

$$\underset{\mathrm{A}}{\boxed{\exists x \neg \exists y \neg (P(x, y) \Rightarrow Q(x))}} \qquad \underset{\mathrm{B}}{\boxed{\exists z \neg R(z)}} \qquad \underset{\mathrm{C}}{\boxed{S(z)}}$$

and hence φ can be written as $\mathrm{A} \Rightarrow \neg \mathrm{B} \vee \mathrm{C}$.

If arbitrarily truth vales are assigned to the primitive sub-formulæ, the truth value of the formula is computed by means of the properties of connectives: if S is the set of all atomic or existential formulæ then any $v \colon S \to \{\text{true}, \text{false}\}$ can be extended to the collection of *all* formulæ by requiring that $v(\neg\varphi) = \text{true}$ just in case $v(\varphi) = \text{false}$, $v(\varphi \wedge \psi) = \text{true}$ just in case $v(\varphi) = v(\psi) = \text{true}$, etc. This construction can be stated in a general form.

Definition 3.6. Let S be a non-empty set of **propositional letters**. Let $\mathrm{Prop}_0(S) = \{(\mathrm{A}) \mid \mathrm{A} \in S\}$, and let

$$\begin{aligned} \mathrm{Prop}_{n+1}(S) = \mathrm{Prop}_n(S) \cup \{(\neg \mathrm{P}) \mid \mathrm{P} \in \mathrm{Prop}_n(S)\} \cup \\ \{(\mathrm{P} \odot \mathrm{Q}) \mid \mathrm{P}, \mathrm{Q} \in \mathrm{Prop}_n(S), \odot \text{ a binary connective}\} \end{aligned}$$

so that $\mathrm{Prop}_0(S) \subset \mathrm{Prop}_1(S) \subset \mathrm{Prop}_2(S) \subset \dots$. The set of all **propositions** over S is

$$\mathrm{Prop}(S) = \textstyle\bigcup_n \mathrm{Prop}_n(S).$$

The set $\mathrm{Prop}(S)$ can be seen as the collection of all closed terms of a language such that every $\mathrm{A} \in S$ is a constant symbol and with the connectives construed as function symbols, and with the convention that each term must start and end with a parenthesis. Thus $\mathrm{ht}(\mathrm{P})$, the height of P, is the least n such that $\mathrm{P} \in \mathrm{Prop}_n(S)$; equivalently it is the height of the syntactic tree of P construed as a term. It is not hard to see (Exercise 3.39) that if $\mathrm{ht}(\mathrm{P}) = n+1$, then either $\mathrm{P} = (\neg \mathrm{Q})$ for some unique Q of height n, or else $\mathrm{P} = (\mathrm{Q} \odot \mathrm{R})$ for a unique choice of $\odot, \mathrm{Q}, \mathrm{R}$, and such that $\max(\mathrm{ht}(\mathrm{Q}), \mathrm{ht}(\mathrm{R})) = n$; we call $\neg$ and $\odot$ the main connective of P.

Remarks 3.7. (a) In order to simplify the notation, we follow the convention adopted for formulæ and drop parentheses whenever possible. In particular we write $\mathrm{A} \in \mathrm{Prop}_0(S)$, rather than $(\mathrm{A}) \in \mathrm{Prop}_0(S)$. Thus with a minor blurring of vision we may assume that $S \subseteq \mathrm{Prop}(S)$.

(b) If $\mathcal{L}$ is a first-order language and S is the set of $\mathcal{L}$-formulæ that are atomic or existential, then $\mathrm{Prop}(S)$ can be construed as the set of *all* $\mathcal{L}$-formulæ.

(c) A proposition over S is a finite string of symbols, so if $\mathrm{P} \in \mathrm{Prop}(S)$ then $\mathrm{P} \in \mathrm{Prop}(S')$ for some finite $S' \subseteq S$. If $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \ldots, \mathrm{A}_n\})$ then any letter of S present in P is among $\mathrm{A}_1, \ldots, \mathrm{A}_n$, but this does not imply that each these propositional letters appears in P.

A **valuation** is a function $v \colon S \to \{0, 1\}$ where 0 represents falsehood and 1 represents truth. Every valuation v can be extended to a map from $\mathrm{Prop}(S)$ to $\{0, 1\}$ by abiding by the meaning of the logical constants—Section 2.A.

Lemma 3.8. *Every* $v \colon S \to \{0, 1\}$ *can be extended to a unique* $\bar{v} \colon \mathrm{Prop}(S) \to \{0, 1\}$ *such that*

$$\begin{aligned}
\bar{v}(\neg\mathrm{P}) &= 1 - \bar{v}(\mathrm{P}) \\
\bar{v}(\mathrm{P} \wedge \mathrm{Q}) &= \min\{\bar{v}(\mathrm{P}), \bar{v}(\mathrm{Q})\} = \bar{v}(\mathrm{P}) \cdot \bar{v}(\mathrm{Q}) \\
\bar{v}(\mathrm{P} \vee \mathrm{Q}) &= \max\{\bar{v}(\mathrm{P}), \bar{v}(\mathrm{Q})\} \\
\bar{v}(\mathrm{P} \Rightarrow \mathrm{Q}) &= 1 - (\bar{v}(\mathrm{P}) \cdot (1 - \bar{v}(\mathrm{Q}))) \\
\bar{v}(\mathrm{P} \Leftrightarrow \mathrm{Q}) &= \bar{v}(\mathrm{P}) + \bar{v}(\mathrm{Q}) + 1 \pmod 2 \\
\bar{v}(\mathrm{P} \veebar \mathrm{Q}) &= \bar{v}(\mathrm{P}) + \bar{v}(\mathrm{Q}) \pmod 2.
\end{aligned}$$

Proof. It is enough to construct $\bar{v}_n \colon \mathrm{Prop}_n(S) \to \{0, 1\}$ satisfying the conditions above and such that $\bar{v}_0 = v$ and $\bar{v}_{n+1}$ extends $\bar{v}_n$. Suppose $\mathrm{P} \in \mathrm{Prop}_{n+1}(S)$. If $\mathrm{P} \in \mathrm{Prop}_n(S)$ then $\bar{v}_{n+1}(\mathrm{P}) = \bar{v}_n(\mathrm{P})$, so we may assume that $\mathrm{P} \in \mathrm{Prop}_{n+1}(S) \setminus \mathrm{Prop}_n(S)$. Then P is either $\neg\mathrm{Q}$ for some unique $\mathrm{Q} \in \mathrm{Prop}_n(S)$ or else it is of the form $\mathrm{Q} \odot \mathrm{R}$ with $\odot$ and $\mathrm{Q}, \mathrm{R} \in \mathrm{Prop}_n(S)$ uniquely determined. Then the conditions above force the definition of $\bar{v}_{n+1}(\mathrm{P})$. □

For notational ease, we use the same letter v to denote both the function $S \to \{0, 1\}$ and its extension $\mathrm{Prop}(S) \to \{0, 1\}$.

Definition 3.9. A proposition P is a **tautology** if $v(\mathrm{P}) = 1$ for all v; it is a **propositional contradiction** if $v(\mathrm{P}) = 0$ for all v. We say that

- P is **tautologically equivalent** to Q if $v(\mathrm{P}) = v(\mathrm{Q})$ for all valuations v,
- P is a **tautological consequence** of Γ, a collection of propositions if for all valuations v such that $v(\mathrm{Q}) = 1$ with $\mathrm{Q} \in \Gamma$, we have that $v(\mathrm{P}) = 1$.

Table 1 lists some of the most common tautologies—two are named after the logicians who discovered them, other carry their a latin name from the Middle Ages. Two propositions P and Q are tautologically equivalent just in case $\mathrm{P} \Leftrightarrow \mathrm{Q}$ is a tautology. If Γ is a finite collection of propositions $\mathrm{Q}_1, \ldots, \mathrm{Q}_n$,

$(\mathrm{A} \Rightarrow \mathrm{B}) \vee (\mathrm{B} \Rightarrow \mathrm{A})$	Dummet's law
$((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{A}) \Rightarrow \mathrm{A}$	Peirce's law
$\neg\mathrm{A} \Rightarrow \mathrm{A} \Rightarrow \mathrm{B}$	*ex falso quodlibet*
$\mathrm{A} \Rightarrow \mathrm{B} \Rightarrow \mathrm{A}$	
$(\neg\mathrm{A} \Rightarrow \mathrm{A}) \Rightarrow \mathrm{A}$	
$\mathrm{A} \wedge (\mathrm{A} \vee \mathrm{B}) \Leftrightarrow \mathrm{A}$	
$\mathrm{A} \vee (\mathrm{A} \wedge \mathrm{B}) \Leftrightarrow \mathrm{A}$	
$((\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{C} \Rightarrow \mathrm{D})) \Rightarrow (\mathrm{A} \wedge \mathrm{C} \Rightarrow \mathrm{B} \wedge \mathrm{D})$	
$((\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{C} \Rightarrow \mathrm{D})) \Rightarrow (\mathrm{A} \vee \mathrm{C} \Rightarrow \mathrm{B} \vee \mathrm{D})$	
$(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \wedge \mathrm{C}) \Rightarrow \mathrm{B}$	
$(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{A} \Rightarrow \mathrm{B} \vee \mathrm{C}$	
$(\neg\mathrm{B} \Rightarrow \neg\mathrm{A}) \Rightarrow (\neg\mathrm{B} \Rightarrow \mathrm{A}) \Rightarrow \mathrm{B}$	*reductio ad absurdum*
$(\mathrm{C} \Rightarrow \mathrm{A}) \Rightarrow (\mathrm{C} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{C} \Rightarrow (\mathrm{A} \wedge \mathrm{B})$	
$(\mathrm{A} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{A} \vee \mathrm{B}) \Rightarrow \mathrm{C}.$	

Table 1. Some tautologies

then P is tautological consequence of Γ just in case $(\mathrm{Q}_1 \wedge \cdots \wedge \mathrm{Q}_n) \Rightarrow \mathrm{P}$ is a tautology. Equivalently: if $v\,(\mathrm{Q}_1 \wedge \cdots \wedge \mathrm{Q}_n) \leq v(\mathrm{P})$ for any v.

Rather than working with valuations, it is often more handy to look at the **truth tables**. The truth table of $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \dots, \mathrm{A}_n\})$ has $n+1$-many columns labelled with A_1, $\mathrm{A}_2, \dots, \mathrm{A}_n, \mathrm{P}$, and 2^n-many rows—one for each valuation of $\mathrm{A}_1, \dots, \mathrm{A}_n$—and the corresponding truth value of P.

A_1	A_2	$\dots$	A_n	P
0	0	$\dots$	0	i_1
0	0	$\dots$	1	i_2
$\vdots$	$\vdots$		$\vdots$	$\vdots$
1	1	$\dots$	1	i_{2^n}

Connectives are described by truth tables: the one for negation is

A	$\neg$A
0	1
1	0

while those of the binary connectives are

A	B	$\mathrm{A} \vee \mathrm{B}$	$\mathrm{A} \wedge \mathrm{B}$	$\mathrm{A} \Rightarrow \mathrm{B}$	$\mathrm{A} \Leftrightarrow \mathrm{B}$	$\mathrm{A} \veebar \mathrm{B}$
0	0	0	0	1	1	0
1	0	1	0	0	0	1
0	1	1	0	1	0	1
1	1	1	1	1	1	0

The truth table of P encodes $v(\mathrm{P})$ for any valuation v of $\mathrm{A}_1, \ldots, \mathrm{A}_n$. Equivalently it can be seen as a function $f_{\mathrm{P}} \colon \{0,1\}^n \to \{0,1\}$ that maps $(i_1, \ldots, i_n)$ to the value $v(\mathrm{P})$ when $v(\mathrm{A}_k) = i_k$, $k = 1, \ldots, n$.

Observe that P is a tautology if and only if the column corresponding to P does not contain 0, that is f_{P} is identically equal to 1.

If $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \ldots, \mathrm{A}_n\})$ and $\mathrm{Q}_1, \ldots, \mathrm{Q}_n \in \mathrm{Prop}(\{\mathrm{B}_1, \ldots, \mathrm{B}_m\})$, then

$$\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]$$

is the element of $\mathrm{Prop}(\{\mathrm{B}_1, \ldots, \mathrm{B}_m\})$ obtained from P by replacing each occurrence of A_i with Q_i, where $i = 1, \ldots, n$. (That $\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]$ is indeed a proposition is a consequence of Lemma 3.2.)

Proposition 3.10. *With the notation above,* $f_{\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]}$ *is the composition of* f_{P} *and* $f_{\mathrm{Q}_1}, \ldots, f_{\mathrm{Q}_n}$*, that is for all* $\vec{x} \in \{0,1\}^m$

$$f_{\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]}(\vec{x}) = f_{\mathrm{P}}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x})).$$

Proof. By induction on k, the height of P. If $k = 0$ then P is A_i for some $1 \leq i \leq n$, so $\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]$ is Q_i, and the result follows at once. So suppose $k = l + 1$ and that the result holds for l. If P is $\neg \mathrm{P}_0$ then P_0 is of height l, so

$$\begin{aligned} f_{\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]}(\vec{x}) &= 1 - f_{\mathrm{P}_0[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]}(\vec{x}) \\ &= 1 - f_{\mathrm{P}_0}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x})) \\ &= f_{\mathrm{P}}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x})). \end{aligned}$$

So we may assume that P is $\mathrm{P}_0 \odot \mathrm{P}_1$ with $\odot$ a binary connective, and that at least one among $\mathrm{P}_0, \mathrm{P}_1$ is of height l. For the sake of definiteness, suppose $\odot$ is $\wedge$ and let R_i be $\mathrm{P}_i[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]$. Then

$$\begin{aligned} f_{\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]}(\vec{x}) &= \min(f_{\mathrm{R}_0}(\vec{x}), f_{\mathrm{R}_0}(\vec{x})) \\ &= \min(f_{\mathrm{P}_0}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x})), f_{\mathrm{P}_1}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x}))) \\ &= f_{\mathrm{P}}(f_{\mathrm{Q}_1}(\vec{x}), \ldots, f_{\mathrm{Q}_n}(\vec{x})). \end{aligned}$$

The argument for the other connectives is similar. □

Corollary 3.11. *If* $\mathrm{Q}_1, \ldots, \mathrm{Q}_n \in \mathrm{Prop}(S)$ *and* $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \ldots, \mathrm{A}_n\})$ *is a tautology, then so is* $\mathrm{P}[\mathrm{Q}_1/\mathrm{A}_1, \ldots, \mathrm{Q}_n/\mathrm{A}_n]$.

Remarks 3.12. (a) While the notion of *equivalence of formulæ* was introduced in an informal way—two formulæ are equivalent if they assert the same thing—the notion of *tautological equivalence* is a genuine mathematical notion.[14] The definition of *logical equivalence* (formalizing the intuitive idea of equivalence between formulæ) will be introduced in Chapter VII.

(b) If every connective can be expressed using connectives from some fixed list, such list will be said to be an **adequate set of connectives**. In other words: in order to define the set of propositions we could have restrained ourselves to connectives from the given list. Since $\mathrm{A} \vee \mathrm{B}$ and $\mathrm{A} \wedge \mathrm{B}$ are tautologically equivalent to $\neg(\neg\mathrm{A} \wedge \neg\mathrm{B})$ and to $\neg(\neg\mathrm{A} \vee \neg\mathrm{B})$, respectively, it follows that $\{\neg, \wedge\}$ and $\{\neg, \vee\}$ are adequate sets of connectives.

Suppose that $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \dots, \mathrm{A}_n\})$. Since $\mathrm{B} \Rightarrow \mathrm{C}$ is tautologically equivalent to $\neg\mathrm{B} \vee \mathrm{C}$ and since $\mathrm{B} \Leftrightarrow \mathrm{C}$ is tautologically equivalent to $(\neg\mathrm{B} \vee \mathrm{C}) \wedge (\neg\mathrm{C} \vee \mathrm{B})$ then P can be transformed into a tautologically equivalent proposition containing the same letters $\mathrm{A}_1, \dots, \mathrm{A}_n$ and only the connectives $\neg$, $\vee$ and $\wedge$. By repeated applications of De Morgan's laws, and by the double negation rule, this formula can be further transformed so that the negation symbol $\neg$ appears only in front of the propositional letters $\mathrm{A}_1, \dots, \mathrm{A}_n$. Finally, by repeated application of the distributivity laws between conjunction and disjunction, P can be turned into a disjunction

$$\mathrm{D}_1 \vee \cdots \vee \mathrm{D}_m$$

where each D_i is a conjunction

$$\mathrm{C}_{i,1} \wedge \cdots \wedge \mathrm{C}_{i,k_i}$$

where each $\mathrm{C}_{i,j}$ is either an A_i, or the negation of an A_i. Such a proposition is said to be in **disjunctive normal form**. If P is a propositional contradiction, then it is tautologically equivalent to $(\neg\mathrm{A}_1 \wedge \mathrm{A}_1) \vee \cdots \vee (\neg\mathrm{A}_n \wedge \mathrm{A}_n)$. Exercise 3.46 shows how to use truth tables to compute the disjunctive normal form of a proposition.

Let's go back to first-order logic. An $\mathcal{L}$-formula φ is a **tautology** if it is of the form $\mathrm{P}[\psi_1/\mathrm{A}_1, \dots, \psi_n/\mathrm{A}_n]$ where $\psi_1, \dots, \psi_n$ are sub-formulæ of φ and $\mathrm{P} \in \mathrm{Prop}(\{\mathrm{A}_1, \dots, \mathrm{A}_n\})$ is a tautology in the sense of Definition 3.9. Arguing as in Example 3.5 any formula which is a tautology is valid, but the converse is not true. For example $x = x$, or more generally the formulæ in (3.6) on page 31, is valid, but $v(x = x)$ could be 0 for suitable v.

[14] The algebraic aspect of the notion of tautological equivalence is analyzed in Section 7.F.

3.C.2. *Free and bound variables.* Every formula contains a finite number of variables and every time a variable shows up in a formula we have an **occurrence of the variable in the formula**. For example the variable z occurs three times in $\exists x \forall y\, (P(x,y) \Rightarrow Q(x)) \Rightarrow \forall z R(z) \vee S(z)$: in the first two occurrences z is mute, since $\forall z R(z)$ has the same meaning of $\forall u R(u)$, that is every item enjoys property R, while the third occurrence asserts that z enjoys property S. Occurrences of the first kind are called **bound**, those of the second kind are called **free**. The free occurrences of a variable v in a formula φ are those in the terminal nodes of the syntactic tree (i.e. the atomic subformulæ of φ) such that there is no node above them labelled with $\exists v$ or $\forall v$. Using boldface letters to highlight bound occurrences, we have $\exists \boldsymbol{x} \forall \boldsymbol{y}\, (P(\boldsymbol{x},\boldsymbol{y}) \Rightarrow Q(\boldsymbol{x})) \Rightarrow \forall \boldsymbol{z} R(\boldsymbol{z}) \vee S(z)$ as one can easily see from the syntactic tree of this formula on page 28.

Definition 3.13. Let φ be a formula and x a variable.

- If φ is atomic then every occurrence of x in φ is free.
- If φ is of the form $\neg\psi$, the free occurrences of x in φ are exactly those of x in ψ.
- If φ is of the form $\psi \odot \chi$, where $\odot$ is a binary connective, the free occurrences of x in φ are exactly those of x in ψ and those of x in χ.
- Suppose φ is of the form $\exists y \psi$ or $\forall y \psi$. If y is the variable x, then all occurrences of x in φ are bound. If instead y is a variable different from x, then the free occurrences of x in φ are exactly those of x in ψ.

The variable x occurs freely in φ (equivalently: x is a free variable of φ) if there is at least a free occurrence of x in φ. In analogy with what was done for terms on page 25, the notation

$$\varphi(x_1, \dots, x_n)$$

is used to highlight that the variables that occur freely in φ are among the $x_1, \dots, x_n$. (We do not require that *every* $x_1, \dots, x_n$ occurs freely, or occurs at all, in φ; it is perfectly possible that the formula contains no free variable, or no variable at all.) A **sentence** or **closed formula** is a formula without free variables. The **universal closure of a formula** φ is the formula $\varphi^\forall$ obtained by universally quantifying all free variables of φ; if instead all free variables are existentially quantified the **existential closure** $\varphi^\exists$ is obtained.

3.C.3. *Substitutability.* A term can replace a variable in an other term (see p. 26), or in a formula. If $t_1, \dots, t_n$ are terms, the expression

$$\varphi[t_1/x_1, \dots, t_n/x_n]$$

obtained by replacing *all occurrences* of x_i in φ with t_i, need not be a formula: for example if φ is $\exists x(x < y) \wedge x = y$ and c is a constant, then $\varphi[c/x]$ is

$\exists c(c < y) \land c = y$ which is not a formula, since quantifiers can be applied only to variables. We will write

$$\varphi(\!|t_1/x_1, \dots, t_n/x_n|\!)$$

for the formula obtained by replacing all *free occurrences* of x_i in φ with t_i, $(i = 1, \dots, n)$. If one of these variables, for example x_1, does not occur free in φ, then the formula becomes $\varphi(\!|t_2/x_2, \dots, t_n/x_n|\!)$, and hence the definition is of interest when every $x_1, \dots, x_n$ occurs free in φ. In this case the formula φ asserts something about items $x_1, \dots, x_n$ and $\varphi(\!|t_1/x_1, \dots, t_n/x_n|\!)$ should say the same thing about $t_1, \dots, t_n$. In order to be sure that this will be the case, it is important that no variable of a t_i will be bound after the substitution is performed. If this does not happen, the meaning of $\varphi(\!|t_1/x_1, \dots, t_n/x_n|\!)$ could change drastically: for example, working in the realm of natural numbers, the formula

$$\exists y\,(2 \cdot y + 1 = x) \tag{3.7}$$

says that x is odd, $\exists y(2 \cdot y + 1 = z + 2)$ says that $z + 2$ is odd, but $\exists y(2 \cdot y + 1 = w + y)$ says that w is not zero! A term t is **substitutable** for x in φ if none of the variables of t is bound by a quantifier in $\varphi(\!|t/x|\!)$. In particular, if x does not occur free in φ or t is a closed term (i.e. it contains no variables), then t is substitutable for x in φ.

The formulæ

$$\exists z\,(2 \cdot z + 1 = x), \quad \exists w\,(2 \cdot w + 1 = x), \quad \exists u\,(2 \cdot u + 1 = x), \quad \dots$$

obtained by changing everywhere y with a new variable, are called **variants** of the formula (3.7), and they all state that x is odd. The only exception is when y is replaced by x, since $\exists x\,(2 \cdot x + 1 = x)$ *does not say* that x is odd. This is similar to what happens in calculus: when f is integrable the expressions $\int_0^1 f(x, y)\,\mathrm{d}y$ and $\int_0^1 f(x, z)\,\mathrm{d}z$ are completely equivalent, and denote a real function of x, while $\int_0^1 f(x, x)\,\mathrm{d}x$ is a real number. In general, a variant of $\varphi(x_1, \dots, x_n)$ is a formula $\varphi'(x_1, \dots, x_n)$ with the same free variables, and it is obtained by swapping some bound variables with other variables so that no free occurrence of x_i in φ turns out to be bound in φ'.

This algorithm is completely general, and allows us to define the substitution operation in general: given a formula $\varphi(x_1, \dots, x_n)$ and terms $t_1, \dots, t_n$, construct a variant φ' of φ so that none of the variables that are bound in φ' is one of $x_1, \dots, x_n$ or appears in some t_i (so that the terms $t_1, \dots, t_n$ are substitutable for $x_1, \dots, x_n$ in φ'). Then the formula $\varphi'(\!|t_1/x_1, \dots, t_n/x_n|\!)$ is defined to be $\varphi'[t_1/x_1, \dots, t_n/x_n]$.

Convention. Whenever there is no danger of confusion $\varphi(t_1, \dots, t_n)$ stands for $\varphi'[t_1/x_1, \dots, t_n/x_n]$ where φ' is a variant of φ in which none of the variables with bound occurrence is one of $x_1, \dots, x_n$ or appears in some t_i.

This convention is particularly handy when φ has just one free variable, and the term is another variable. For example if $\varphi(x)$ is $x \neq 1 \land \forall y \forall z (y \cdot z = x \Rightarrow y = 1 \lor z = z)$ saying that "x is prime", then $\varphi(y)$ is $y \neq 1 \land \forall w \forall z (w \cdot z = y \Rightarrow w = 1 \lor z = z)$ and says that "y is prime".

If x does not occur free in φ, then φ is equivalent to both $\exists x \varphi$ and $\forall x \varphi$—for example $\exists x\, (y^2 - 3y + 2 = 0)$ and $\forall x\, (y^2 - 3y + 2 = 0)$ are equivalent to $y^2 - 3y + 2 = 0$. The notion of free/bound variable allows to prove the manipulations on quantifiers that were informally introduced on page 10. Recall that

$$\begin{array}{ll} \forall x\, (\varphi \land \psi) \Leftrightarrow \forall x \varphi \land \forall x \psi, & \exists x\, (\varphi \lor \psi) \Leftrightarrow \exists x \varphi \lor \exists x \psi, \\ \forall x \varphi \lor \forall x \psi \Rightarrow \forall x\, (\varphi \lor \psi)\,, & \exists x\, (\varphi \land \psi) \Rightarrow \exists x \varphi \land \exists x \psi, \end{array}$$

are valid formulæ and that the last two implications cannot be turned into bi-implications. Suppose now that x does not occur free in φ: if $\varphi \land \exists x \psi$ holds, then the x about which we are predicating ψ is mute in φ, and it follows that $\exists x\, (\varphi \land \psi)$. Similarly, from $\forall x\, (\varphi \lor \psi)$ it follows that $\varphi \lor \forall x \psi$.

Therefore *if x does not occur free in φ*, the formulæ

$$\varphi \land \exists x \psi \Leftrightarrow \exists x\, (\varphi \land \psi) \qquad \text{and} \qquad \varphi \lor \forall x \psi \Leftrightarrow \forall x\, (\varphi \lor \psi)$$

are valid, and since φ is equivalent to $\exists x \varphi$ and to $\forall x \varphi$, then

$$\forall x \varphi \lor \forall x \psi \Leftrightarrow \forall x\, (\varphi \lor \psi) \qquad \text{and} \qquad \exists x \varphi \land \exists x \psi \Leftrightarrow \exists x\, (\varphi \land \psi)$$

are valid. For example, consider the formula

$$\exists x \left(x^2 - 3x + 2 = 0\right) \land \exists x \left(x^2 + x - 12 = 0\right)$$

asserting that the two equations of second degree have a root. This formula (that is true when x varies on the reals) is equivalent to the formula

$$\exists x \left(x^2 - 3x + 2 = 0 \;\land\; \exists x \left(x^2 + x - 12 = 0\right)\right)$$

and to the formula

$$\exists x \left(\exists x \left(x^2 - 3x + 2 = 0\right) \;\land\; x^2 + x - 12 = 0\right).$$

If we wanted to modify this last formula by moving outside the innermost quantifier, we should first of all replace $\exists x \left(x^2 - 3x + 2 = 0\right)$ with its variant $\exists y \left(y^2 - 3y + 2 = 0\right)$, thus obtaining

$$\exists x \exists y \left((y^2 - 3y + 2 = 0) \;\land\; (x^2 + x - 12 = 0)\right).$$

Had we not changed this variable, we would commit an offence and obtain the formula $\exists x \exists x ((x^2 - 3x + 2 = 0) \land (x^2 + x - 12 = 0))$ which is equivalent to $\exists x \left((x^2 - 3x + 2 = 0) \land (x^2 + x - 12 = 0)\right)$ asserting that the two equations have a common root (which is false when x varies on the reals).

3.C.4. *Prenex form.* The above equivalences are very useful to transform a formula $\varphi(x_1, \ldots, x_n)$ into an equivalent one $\varphi'(x_1, \ldots, x_n)$ having the same free variables and in **prenex form**, that is of the form

$$\mathsf{Q}_1 y_1 \mathsf{Q}_2 y_2 \ldots \mathsf{Q}_m y_m \psi,$$

where the Q_is are quantifiers and ψ is **open**, that is to say: quantifier-free. The block of quantifiers $\mathsf{Q}_1 y_1 \mathsf{Q}_2 y_2 \ldots \mathsf{Q}_m y_m$ is the **prefix**, and ψ is the **matrix** of the formula.

Warning. If a formula is not open, it does not mean that it is closed, and conversely.

Let us show how to obtain a prenex formula equivalent to (3.2) on page 28

$$\exists x \forall y\, (\neg P(x, y) \vee Q(x)) \Rightarrow \forall z R(z) \vee S(z).$$

Firstly turn the implication into a disjunction $\neg(\exists x \forall y(\neg P(x, y) \vee Q(x))) \vee \forall z R(z) \vee S(z)$, then turn $\neg(\exists x \forall y(\neg P(x, y) \vee Q(x)))$ into $\forall x \exists y(P(x, y) \wedge \neg Q(x))$, and $\forall z R(z)$ into $\forall w R(w)$, so that we get

$$\forall x \exists y\, (P(x, y) \wedge \neg Q(x)) \vee \forall w R(w) \vee S(z)$$

thus $\forall w R(w) \vee S(z)$ becomes $\forall w\, (R(w) \vee S(z))$, whence

$$\forall x \exists y\, (P(x, y) \wedge \neg Q(x)) \vee \forall w\, (R(w) \vee S(z))$$

and finally, since $(P(x, y) \wedge \neg Q(x)) \vee \forall w(R(w) \vee S(z))$ is equivalent to $\forall w((P(x, y) \wedge \neg Q(x)) \vee R(w) \vee S(z))$ we obtain

$$\forall x \exists y \forall w\, ((P(x, y) \wedge \neg Q(x)) \vee R(w) \vee S(z))\,.$$

This example suggests the following algorithm to construct a prenex formula $\varphi'(x_1, \ldots, x_n)$ from $\varphi(x_1, \ldots, x_n)$:

Step 1: transform all implications $\mathrm{A} \Rightarrow \mathrm{B}$ into $\neg\mathrm{A} \vee \mathrm{B}$ and all bi-implications $\mathrm{A} \Leftrightarrow \mathrm{B}$ into $(\neg\mathrm{A} \vee \mathrm{B}) \wedge (\neg\mathrm{B} \vee \mathrm{A})$,

Step 2: by De Morgan's laws, the double negation rule, and the transformation on quantifiers of Section 2, move the negation symbols inside, down to the level of atomic sub-formulæ,

Step 3: repeatedly apply the following operation: transform all sub-formulæ of the form $(\mathsf{Q}x\mathrm{A}) \odot (\mathsf{Q}'y\mathrm{B})$ where Q, Q' are quantifiers and $\odot$ is $\vee$ or $\wedge$, into $\mathsf{Q}z\mathsf{Q}'w\, (\mathrm{A}\llparenthesis z/x \rrparenthesis \odot \mathrm{B}\llparenthesis w/y \rrparenthesis)$ where z is substitutable in A for x and does not occur free in B, and w is substitutable in B for y and does not occur free in A.

A prenex form formula equivalent to a given formula is far from being unique—for example in Step 3 we could transform $(\mathsf{Q}x\mathrm{A}) \odot (\mathsf{Q}'y\mathrm{B})$ into $\mathsf{Q}'w\mathsf{Q}z\, (\mathrm{A}\llparenthesis z/x \rrparenthesis \odot \mathrm{B}\llparenthesis w/y \rrparenthesis)$. In particular

$$\forall w \forall x \exists y\, ((P(x, y) \wedge \neg Q(x)) \vee R(w) \vee S(z))$$

is a prenex formula equivalent to (3.2).

If $\forall x \varphi \Rightarrow \psi$ or $\exists x \varphi \Rightarrow \psi$ are turned into prenex form, and x does not occur free in ψ, then $\exists x\, (\varphi \Rightarrow \psi)$ and $\forall x\, (\varphi \Rightarrow \psi)$ are obtained. In other words: if B does not mention x, a statement like

if A holds for some x, then B

is equivalent to

for all x, if A holds of x then B.

For example the statement "if y is a square, then it is bigger or equal than zero" is formalized as $\exists x\, (y = x \cdot x) \Rightarrow y \geq 0$ or equivalently as $\forall x\ (y = x \cdot x \Rightarrow y \geq 0)$. The other equivalence between

if A is true for all x, then B

and

there is an x such that: if A is true of x then B

is more surprising (naively one would have expected that $\forall x \varphi \Rightarrow \psi$ should be equivalent to $\forall x\, (\varphi \Rightarrow \psi)$) and shows that carless use of quantifiers in natural language is prone to errors. For example, consider the following statement of set theory:[15] *two sets are equal if they have the same elements.* It is formalized as $\forall x \forall y\, (\forall z\, (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$, that, in prenex form, becomes

$$\forall x \forall y \exists z\, ((z \in x \Leftrightarrow z \in y) \Rightarrow x = y)\,,$$

which reads: *given two sets x and y there is an element z such that: if z belongs to x if and only if z belongs to y, then x and y coincide.* What is this z? To find out, it is enough to take the contrapositive of what is inside the parentheses, that is

$$\forall x \forall y \exists z\, (x \neq y \Rightarrow ((z \in x \wedge z \notin y)\ \vee\ (z \in y \wedge z \notin x)))$$

which reads: *given two sets x and y there is an element z such that: if x and y are distinct, then z belongs to one of the two sets but not to the other.* Therefore, given two sets x and y it is enough to choose a z that belongs to one of the two sets but not the other, if x and y are distinct, or z arbitrary when x and y are the same.

It is possible to prove the results on formulæ in prenex form by induction on the length of the prefix: one shows that a certain property $\mathcal{P}$ holds for all quantifier free formulæ, and that if $\mathcal{P}$ holds for a certain φ, then it holds for $\exists x \varphi$ and for $\forall x \varphi$. Since every formula is equivalent to a prenex formula, this technique can be used for proving that a property $\mathcal{P}$ holds for all formulæ.

The length of the prefix is a measure of complexity for formulæ in prenex form, just like the notion of length and height seen at the end of Section 3.A.

[15] This is known as the axiom of extensionality—see Chapter V, p. 369–370.

In many situations it is more convenient to use yet another measure of complexity, based on alternation of blocks of quantifiers in the prefix:

- if the prefix is just one block of universal quantifiers, it is a $\forall$-formula; if the prefix is just one block of existential quantifiers, it is a $\exists$-formula,
- if the prefix is a block of universal quantifiers followed by a block of existential quantifiers, it is a $\forall\exists$-formula; if the prefix is block of existential quantifier followed by a block of universal quantifiers, it is a $\exists\forall$-formula,
- if the prefix is a block of universal quantifiers, followed by a block of existential quantifiers, followed by a block of universal quantifiers, it is a $\forall\exists\forall$-formula; if the prefix is block of existential quantifiers followed by a block of universal quantifiers, followed by a block of universal quantifiers, it is a $\exists\forall\exists$-formula,

and so on. The negation of a $\forall$-formula is equivalent to a $\exists$-formula, and conversely; the negation of a $\forall\exists$-formula is equivalent to a $\exists\forall$-formula, and conversely; etc.

3.D. First-order structures. A **finitary function** or **operation** on a set M is a function $f\colon M^n \to M$, with $n \in \mathbb{N}$. The integer n is the **ariety** of the operation. When $n = 0$ then $M^n = \{\emptyset\}$ so f can be identified with a specific element of M. An **algebraic structure** is a set $M \neq \emptyset$ with a bunch of operations. Groups, rngs, ... can be construed as algebraic structures. A **relational structure** is a set $M \neq \emptyset$ with a bunch of relations $R \subseteq M^n$, with $n \in \mathbb{N} \setminus \{0\}$. Also in this case the integer n is called the ariety of the relation. A function/relation with arity $1, 2, 3$ is called a unary, binary, ternary function/relation.

We pause to review some well-known facts about relational structures of the form (M, R) with $R \subseteq M \times M$. Most of these facts are standard—the only reason to present them now is to fix the notation and terminology.

3.D.1. *Binary relations.* A binary relation R on M is

reflexive: if $\forall x \in M\ ((x, x) \in R)$;

irreflexive: if $\forall x \in M\ ((x, x) \notin R)$;

symmetric: if $\forall x, y \in M\ ((x, y) \in R \Rightarrow (y, x) \in R)$;

asymmetric: if $\forall x, y \in M\ ((x, y) \in R \Rightarrow (y, x) \notin R)$;

antisymmetric: if $\forall x, y \in M\ ((x, y) \in R \wedge (y, x) \in R \Rightarrow x = y)$;

transitive: if $\forall x, y, z \in M\ ((x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R)$;

total: if $\forall x, y \in M\ ((x, y) \in R \vee x = y \vee (y, x) \in R)$,

free: if $\forall x, y \in M\ (x \neq y \Rightarrow (x, y) \notin R \wedge (y, x) \notin R)$.

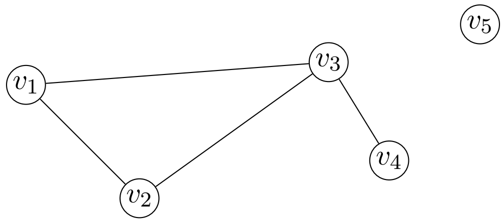


Figure 4. A finite graph.

An $X \subseteq M$ is **independent** for R if $R \cap X \times X$ is free; it is **connected** for R if $R \cap X \times X$ is total.

The **inverse** or **converse** of R is the binary relation R^{-1}

$$R^{-1} = \left\{(b, a) \in M^2 \mid (a, b) \in R\right\}.$$

If R is reflexive (or: irreflexive, symmetric, asymmetric, antisymmetric, transitive, total, free) then so is R^{-1}. If $\mathcal{R}$ is a family of binary relations on M, and every $R \in \mathcal{R}$ is reflexive (or: irreflexive, symmetric, asymmetric, antisymmetric, transitive, total, free) then so is

$$\bigcap \mathcal{R} = \{(a, b) \in M^2 \mid \forall R \in \mathcal{R}\ ((a, b) \in R)\}.$$

If every $R \in \mathcal{R}$ is reflexive (or: irreflexive, symmetric, total, free) then so is

$$\bigcup \mathcal{R} = \{(a, b) \in M^2 \mid \exists R \in \mathcal{R}\ ((a, b) \in R)\}$$

but need not be antisymmetric, asymmetric or transitive, even if each $R \in \mathcal{R}$ is so.

The **transitive closure of** $R \subseteq M^2$ is the smallest transitive binary relation containing R, that is

$$\bigcap \{S \subseteq M^2 \mid R \subseteq S \wedge S \text{ transitive}\}.$$

3.D.2. *Graphs.* A **graph** is a non-empty set V whose elements, called **vertices**, are variously connected.[16] A vertex is never connected to itself and if two vertices are connected, then the connection is unique. The connections are called **edges**. Formally a graph is a pair (V, E) where $V \neq \emptyset$ is the set of vertices and E is a subset of

$$\{\{v, w\} \mid v, w \in V \wedge v \neq w\}.$$

Two vertices of a graph v and w are connected if $\{v, w\}$ is an edge, and conversely $\{v, w\} \in E$ means that v and w are connected by an edge. The set E of unordered pairs of vertices can be identified with the symmetric subset

[16] This concepts should not be confused with the notion of *graph of a function* $\mathrm{Gr}(f)$.

of $V \times V \setminus \{(v, v) \mid v \in V\}$ given by $R = \{(v, w) \mid \{v, w\} \in E\}$, so a graph is simply a structure (V, R) with R an irreflexive, symmetric relation.

Finite graphs (that is: graphs whose set of vertices is finite) can be drawn as points on the plane joined by (possibly curved) lines: the points represent vertices, the lines represent the edges. The **degree** of a vertex v is the number of vertices connected to v by an edge. Figure 4 shows a graph whose vertices v_1, v_2, v_3 are mutually connected, v_4 is connected only to v_3, and v_5 is not connected to any other vertex, that is it is an isolated vertex. In other words, it is the graph (V, E) with $V = \{v_1, v_2, v_3, v_4, v_5\}$ and $E = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_3, v_4\}\}$. The vertices v_1 and v_2 have degree 2, the vertex v_3 has degree 3, the vertex v_4 has degree 1, and the vertex v_5 has degree 0.

An n-**cycle** ($n \geq 3$) in a graph is a finite sequence of distinct vertices $v_1, \ldots, v_n$ such that v_i is connected to v_{i+1} and v_n is connected to v_1. A cycle is an n-cycle for some n, and a graph is **acyclic** if it does not contain cycles. A k-**path** from v to w is a finite sequence of vertices

$$v = z_0, z_1, \ldots, z_k = w$$

such that every z_i is connected to z_{i+1} and $k \geq 1$. A path is a k-path for some k. A graph is **connected** if every pair of vertices is connected by a path; otherwise it is disconnected—the graph in Figure 4 is disconnected, since v_5 is isolated.

3.D.3. *Directed graphs.* If in the definition of graph we assume that links between vertices posses a direction, and that a vertex may be linked with itself, we obtain the notion of **directed graph** or **digraph**. Formally a directed graph is a non-empty set of vertices V together with $R \subseteq V \times V$ a family of oriented edges, and every binary relation R on a non-empty set V can be seen as a directed graph. Thus a directed graphs is just any relational structure (V, R) with $R \subseteq V^2$. For example, if $V = \{v_1, v_2, v_3, v_4, v_5\}$ and

$$R = \{(v_1, v_1), (v_1, v_2), (v_1, v_3), (v_2, v_1), (v_2, v_3), (v_3, v_2), (v_3, v_3), (v_4, v_3)\},$$

then the directed graph (V, R) is shown in Figure 5. Note that the vertices v_1, v_2 are linked in both directions, and so are the vertices v_2, v_3.

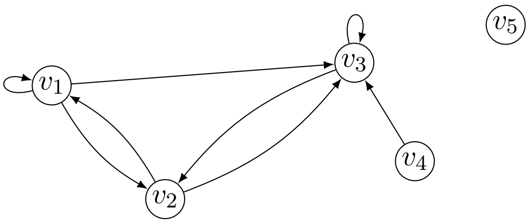


Figure 5. A finite directed graph.

3.D.4. *Ordered sets.* A reflexive and transitive relation $R \subseteq M^2$ is a **preorder** or **quasi-order**, and the resulting structure (M, R) is called a **preordered set** or **quasi-ordered set**. A symmetric preorder is an **equivalence relation**, an antisymmetric preorder is an **order** or **ordering**. An **ordered set** is a structure (M, R) with $R \subseteq M^2$ an order. We will often blur the distinction between the relation and the structure and say that (M, R) is a (pre)order, rather than a (pre)ordered set. The **strict part** of a relation R is $R \setminus R^{-1}$, the strict part of a preorder is a **strict preorder** and the strict part of an order is a **strict order**. This terminology is a bit unfortunate, since a strict (pre)order is not a (pre)order, but this wording has become standard. It is customary (but not compulsory) to use the symbols $\leq$, $\preceq$, $\trianglelefteq$, ... for (pre)orders, $<$, $\prec$, $\triangleleft$, ... for strict (pre)orders, and $\sim$, $\approx$, $\equiv$, ... for equivalence relations. If R is a preorder on M, then $R \cap R^{-1}$ is an equivalence relation, and the relation $\leq$ on the quotient $M/R \cap R^{-1}$ defined by

$$[a] \leq [b] \Leftrightarrow a\, R\, b$$

is an order, called the **order induced by the preorder** R.

If $(M, \leq)$ and $(N, \preceq)$ are preordered sets, a function $f \colon M \to N$ such that $a \leq b \Rightarrow f(a) \preceq f(b)$ for all $a, b \in M$ is said to be **monotone** or **isotone** or **order preserving**; if instead $a \leq b \Rightarrow f(b) \preceq f(a)$ then f is **antitone** or **order reversing**. If $<$ and $\prec$ are strict orders on M and N, then f is **increasing** if and only if $a < b \Rightarrow f(a) \prec f(b)$ for all $a, b \in M$; by abuse of language, a function between ordered sets is said to be increasing, if it is such when considering the strict orders associated. If $(M, \leq)$ is an ordered set, a function $f \colon M \to M$ is **progressive** or **inflationary** if and only if $a \leq f(a)$ for all $a \in M$; it is **idempotent** if and only if $f(f(a)) = f(a)$ for all $a \in M$.

Let $(M, \leq)$ be an ordered set and let $a, b, c \in M$. Then

- c is an **upper bound** of a, b if $a \leq c$ and $b \leq c$. Dually, c is an **lower bound** of a, b if $c \leq a$ and $c \leq b$.
- c is the **least upper bound** of a, b, in symbols $\sup(a, b)$, if it is an upper bound of a, b, and $c \leq c'$ for any upper bound c' of a, b. Dually c is the **greatest lower bound** of a, b in symbols $\inf(a, b)$ or $a \curlywedge b$, if it is a lower bound of a, b, and $c' \leq c$ for any lower bound c' of a, b.

An ordered set $(M, \leq)$ is

- **upward directed** if any two elements have an upper bound, and **downward directed** if any two elements have a lower bound;
- an **upper semi-lattice** if $\sup(a, b)$ exists for any two $a, b \in M$, and a **lower semi-lattice** if $\inf(a, b)$ exists for any two $a, b \in M$;
- a **lattice** if it is simultaneously an upper and lower semi-lattice;

- **linear** or **total** if $\leq$ is total on M, that is to say: $a \leq b$ or $b \leq a$ for all $a, b \in M$.

A linear order is a lattice, and an upper/lower semi-lattice is upward/downward directed, but none of the implications can be reversed. For example looking at the orders of Figure 6, we see that the first is a lattice, while the second is upward and downward directed but not a lattice, and the third is a tree and a lower semi-lattice, but not a lattice. Observe that if in the second order the maximum element is removed, the resulting order is not upward directed; similarly if the minimum is removed the resulting order will not be downward directed.

If $(M, \leq)$ is an ordered set then a is a **predecessor** of b, or, equivalently, that b is a **successor** of a if $a < b$, where $<$ is the strict part of $\leq$; if moreover there is no $c \in M$ such that $a \leq c \leq b$ then a is an **immediate predecessor** of b, and b is an **immediate successor** of a. (If $\leq$ is linear, the immediate predecessor and immediate successor of an element are unique, if they exist.) The **covering relation** induced by $\leq$ is the relation $\blacktriangleleft$ on M defined by

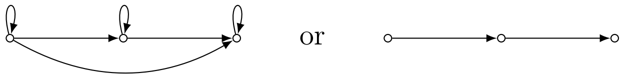
$$a \blacktriangleleft b \Leftrightarrow a \text{ is an immediate predecessor of } b.$$

Observe that $a \blacktriangleleft b \Rightarrow a < b$, and that if M is finite, then $<$ is the transitive closure of $\blacktriangleleft$.

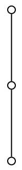
A subset of an ordered set $(M, \leq)$ is a **chain** if it is linearly ordered by $\leq$. For $a < b$ the **intervals of endpoints** a **and** b are

$$(a; b) = \{c \in M \mid a < c < b\} \qquad [a; b] = \{c \in M \mid a \leq c \leq b\}$$
$$(a; b] = \{c \in M \mid a < c \leq b\} \qquad [a; b) = \{c \in M \mid a \leq c < b\}.$$

A finite order can be visually described by its directed graph, or by the directed graph of its covering relation. For example, a linear order with three elements is represented by



Moreover we can use undirected graphs if we agree to draw smaller elements below the larger ones, so the preceding linear order becomes



Such drawings are called **Hasse diagrams**.

A **finite tree** is a finite order with a least element called the **root** and such that for every element there is a unique path from the root to it. Finite

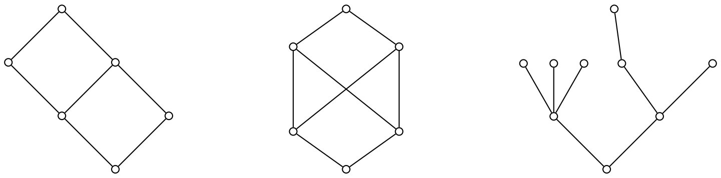


Figure 6. Examples of finite orders

linear orders and the hydras of Example 1.2 are finite trees, while any order containing a diamond-shaped order ◇ as suborder is not a tree.

Remarks 3.14. (a) Syntactic trees are related to, but different from, finite trees: a syntactic tree is a finite tree (drawn upside down) but with an ordering of the leaves sprouting from a node. The syntactic tree of the term $f(x, y)$ must keep track of the fact that f is the root and that the inputs are x and y in that specific order.

(b) A connected, acyclic graph is called a **combinatorial tree**. The Hasse diagram of a finite tree is a finite combinatorial tree. Conversely, any finite combinatorial tree with a distinguished vertex (acting as root) yields a finite tree.

3.D.5. *Calculus of relations**. The collection $\mathscr{P}(M \times M)$ of all binary relations on some fixed non-empty set M can be seen as a structure. It is ordered under inclusion, and being a power-set we have the usual Boolean operations: given R, S we can construct new binary relations by means of the usual set-theoretic operations $R \cup S$, $R \cap S$, $R^{\complement} = M^2 \setminus R$, ... As we are looking at *relations* rather than just *sets* we can define new operations such as R^{-1} and the **composition** of R and S

$$R \mid S \overset{\text{def}}{=} \{(x, y) \in M^2 \mid \exists z \in M\, ((x, z) \in R \wedge (z, y) \in S)\}.$$

Observe that if R and S are functions from M to itself, then the composition of R and S as relations is their composition as functions in the reverse order, that is $R \mid S = S \circ R$. The notion of $R \dagger S$, the **sum** of R and S, is obtained by dualizing the definition of composition, swapping $\exists$ with $\forall$ and $\wedge$ with $\vee$

$$R \dagger S \overset{\text{def}}{=} \{(x, y) \in M^2 \mid \forall z \in M\, ((x, z) \in R \vee (z, y) \in S)\}.$$

As in the case of functions, for all $R \subseteq M^2$

$$R \mid \mathrm{id} = \mathrm{id} \mid R = R$$

where $\mathrm{id} = \mathrm{id}_M = \{(x, x) \mid x \in M\}$ is the identity relation. For the sum we have an analogous identity, namely

$$R \dagger \mathrm{id}^{\complement} = \mathrm{id}^{\complement} \dagger R = R.$$

$R \mid S = (R^{\complement} \dagger S^{\complement})^{\complement}$	$R \dagger S = (R^{\complement} \mid S^{\complement})^{\complement}$
$(R \mid S) \mid T = R \mid (S \mid T)$	$(R \dagger S) \dagger T = R \dagger (S \dagger T)$
$(R \cup S) \mid T = (R \mid T) \cup (S \mid T)$	$R \mid (S \cup T) = (R \mid S) \cup (R \mid T)$
$(R \cap S) \dagger T = (R \dagger T) \cap (S \dagger T)$	$R \dagger (S \cap T) = (R \dagger S) \cap (R \dagger T)$
$R \mid \mathrm{id} = R = \mathrm{id} \mid R$	$R \dagger \mathrm{id}^{\complement} = R = \mathrm{id}^{\complement} \dagger R$
$(R^{-1})^{-1} = R$	$(R \mid S)^{-1} = S^{-1} \mid R^{-1}$
$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$	$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

Table 2. Some laws of calculus of relations

The **language of calculus of relations** $\mathcal{L}$ is meant for studying the structure

$$(\mathscr{P}(M \times M), \cup, \cap, \mid, \dagger, {}^{\complement}, {}^{-1}, \mathrm{id}).$$

It has four binary function symbols $\cup, \cap, \mid, \dagger$, two unary function symbols ${}^{\complement}, {}^{-1}$, and a constant symbol id. In order to keep the number of parentheses to a minimum we convene that the unary operations have the priority over the binary ones, and that $\mid$ and $\dagger$ bind more than $\cup, \cap$. In other words $R \cup S \mid T^{\complement}$ is shorthand for $R \cup (S \mid (T^{\complement}))$. The operations $R \setminus S$ and $R \triangle S$ can be recast as $R \cap S^{\complement}$ and $(R \cap S^{\complement}) \cup (S \cap R^{\complement})$, respectively.

Observe that $R \subseteq S$ if and only if one of the following holds:

$$R \cup S = S, \qquad R \cap S = R, \qquad R^{\complement} \cup S = M \times M, \qquad R \cap S^{\complement} = \emptyset$$

where $\emptyset$ and $M \times M$ are shorthand of $\mathrm{id} \cap \mathrm{id}^{\complement}$ and $\mathrm{id} \cup \mathrm{id}^{\complement}$. Therefore any formula $t(x_1, \dots, x_n) \subseteq s(x_1, \dots, x_n)$ with t, s terms of $\mathcal{L}$ can be reformulated as an identity $t'(x_1, \dots, x_n) \doteq s'(x_1, \dots, x_n)$ for suitable terms t', s'.

Besides the De Morgan identities for $\cup, \cap, {}^{\complement}$ there are laws governing the operations $\mid, \dagger, {}^{-1}$ and their interactions with the set-theoretic operations. Some of these laws are collected in Table 2—the first one illustrates a duality between the operations $\mid$ and $\dagger$, showing that one can be defined from the other, so $\mathcal{L}$ is redundant.

The next law of the calculus of relations can be used to prove many other laws—see Section 7.M.

Proposition 3.15. $R^{-1} \mid (R \mid S)^{\complement} \subseteq S^{\complement}$.

Proof. Suppose $(x, y) \in R^{-1} \mid (R \mid S)^{\complement}$. Then there is z such that $(x, z) \in R^{-1}$ and $(z, y) \notin R \mid S$, so that $(z, x) \in R$ and $(z, w) \in R^{\complement}$ or $(w, y) \in S^{\complement}$, for any w. The last clause when $w = x$ yields $(z, x) \in R^{\complement}$ or $(x, y) \in S^{\complement}$: the first is impossible, so the second must hold. This proves that $(x, y) \in R^{-1} \mid (R \mid S)^{\complement} \Rightarrow (x, y) \in S^{\complement}$. □

Observe that a binary relation R on M is

reflexive: if and only if $\mathrm{id} \subseteq R$,

irreflexive: if and only if $R \subseteq \mathrm{id}^{\complement}$,

symmetric: if and only if $R^{-1} \subseteq R$,

asymmetric: if and only if $R^{-1} \cap R = \emptyset$,

antisymmetric: if and only if $R \cap R^{-1} \subseteq \mathrm{id}$,

transitive: if and only if $R \mid R \subseteq R$,

total: if and only if $R \cup R^{-1} \cup \mathrm{id} = M \times M$

free: if and only if $R \cup R^{-1} \subseteq \mathrm{id}$.

As $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$ and $(R^{-1})^{-1} = R$, symmetry for R can be written as $R^{-1} = R$.

It is possible to characterize properties of relations in terms of identities (or inequalities using $\subseteq$) in the language $\mathcal{L}$. For example R is a preorder on M if and only if R is reflexive and transitive, which is the same thing as saying $\mathrm{id} \subseteq R$ and $R \mid R \subseteq R$. These two inclusions can be rewritten as $\mathrm{id} \cup R = R$ and $(R \mid R) \cup R = R$, so

$$R \text{ is a preorder if and only if } (\mathrm{id} \cup R) \cap ((R \mid R) \cup R) = R.$$

The trick here is that R is contained in $A \overset{\text{def}}{=} \mathrm{id} \cup R$ and $B \overset{\text{def}}{=} (R \mid R) \cup R$, so $\mathrm{id} \cup R = R$ and $(R \mid R) \cup R = R$ hold simultaneously if and only if $A \cap B = R$. There are other ways to turn a conjunction of two identities into a single identity. For example, one transforms these identities as

- $t_1 \eqcirc \emptyset$ and $t_2 \eqcirc \emptyset$ and then merge them into $t_1 \cup t_2 = \emptyset$, or else
- $t_1 \eqcirc M^2$ and $t_2 \eqcirc M^2$ and then merge them into $t_1 \cap t_2 = M^2$.

Using these tricks, properties of a relation R (like: being an order, equivalence relation, a graph, ...) can be stated as an identity of terms of $\mathcal{L}$ involving only the variable R—see Exercise 3.49.

3.E. Finite sequences. If A is a set then

$$A^{<\mathbb{N}} = \{s \mid \exists n \in \mathbb{N}\, (s \colon \{0, \dots, n-1\} \to A)\}$$

is the set of all **finite sequences** or **strings** from A. The values $s(i)$ are often denoted with s_i and we write

$$\langle s_0, \dots, s_{n-1} \rangle$$

to denote an element s of A, where $n = \mathrm{lh}(s)$ is the **length of** s. When $n = 0$ we obtain the empty sequence $\langle\rangle$. (Computer scientists often write A^* instead of $A^{<\mathbb{N}}$ and ε instead of $\langle\rangle$.) The **concatenation of** $s, t \in A^{<\mathbb{N}}$ is the string $s^\frown t$ obtained by listing the elements of s first, and then those of t. In other words if $s = \langle s_0, \dots, s_{n-1} \rangle$ and $t = \langle t_0, \dots, t_{m-1} \rangle$ then

$$s^\frown t = \langle s_0, \dots, s_{n-1}, t_0, \dots, t_{m-1} \rangle$$

is a sequence of length $n + m$. The operation of concatenation is associative, and since $\langle\rangle^\frown s = s^\frown\langle\rangle$ it follows that $A^{<\mathbb{N}}$ is a monoid.

For any $a \in A$ we write

$$a^{(n)} = \langle \underbrace{a, \dots, a}_{n \text{ times}} \rangle. \tag{3.8}$$

Thus $a^{(0)} = \langle\rangle$ is the empty string, and with a minor blurring of vision we can identify an element $a \in A$ with $\langle a \rangle$, a sequence of length 1. In fact if there is no danger of confusion we forgo the angular brackets so that for $a, b \in A$ the finite sequence $\langle a, b, a, a, a, b, a, b, b \rangle$ is written as $abaaababb$ or $aba^{(3)}bab^{(2)}$. Similarly we often write st instead of $s^\frown t$.

If $A = \{a\}$ is a singleton, then $A^{<\mathbb{N}} = \{a^{(n)} \mid n \in \mathbb{N}\}$ with the operation of concatenation is isomorphic to $(\mathbb{N}, +)$. If A has at least two elements a, b then $(A^{<\mathbb{N}}, {}^\frown)$ is not abelian, since $ab \neq ba$.

Definition 3.16. If $t, s \in A^{<\mathbb{N}}$ and $t = u^\frown s^\frown v$ for some u, v, then s **occurs** in t, in symbols $s \sqsubseteq t$. If in the definition above $u = \langle\rangle$ then s is an **initial segment** or **prefix** of t, in symbols $s \sqsubseteq_{\mathrm{i}} t$, and if $v = \langle\rangle$ then s is a **final segment** of t, in symbols $s \sqsubseteq_{\mathrm{f}} t$.

It is immediate to check that the relations in Definition 3.16 are orderings on $A^{<\mathbb{N}}$. As the elements of $A^{<\mathbb{N}}$ are functions from a finite initial segment of $\mathbb{N}$ into A, then $s \sqsubseteq_{\mathrm{i}} t$ if and only if $s \subseteq t$.

3.E.1. *Another look at terms and formulæ.* Terms and formulæ are defined by an inductive construction that can be cast in terms of finite sequences.

Definition 3.17. Let S be a non-empty set of symbols, and let $a \colon S \to \mathbb{N}$ be any function. The set of **terms** on (S, a) is $\mathrm{Term}(S, a) = \bigcup_{n \in \mathbb{N}} \mathrm{Term}_n(S, a)$ where $\mathrm{Term}_n = \mathrm{Term}_n(S, a)$ is defined inductively by

$$\begin{aligned} \mathrm{Term}_0 &= \{\langle s \rangle \mid s \in S \wedge a(s) = 0\} \\ \mathrm{Term}_{n+1} &= \{\langle s, t_1, \dots, t_k \rangle \mid s \in S \,\wedge\, a(s) = k \,\wedge\, t_1, \dots, t_k \in \mathrm{Term}_n\}. \end{aligned}$$

The least n such that t belongs to Term_n is called the **height** of the term t.

Given a first order language $\mathcal{L}$, let S be the set of all variables, and all constant and function symbols of $\mathcal{L}$, and let $s \colon S \to \mathbb{N}$ be the arity function, that is $a(f) = k$ if f is a k-ary function symbol, and $c(x) = a(c) = 0$ for all variables x and all constant symbols c. Thus the $\mathcal{L}$-term $f(x, g(c))$ can be identified with $\langle f, x, \langle g, \langle c \rangle \rangle \rangle$ where $a(f) = 2$, $a(g) = 1$, and $a(x) = a(c) = 0$.

If every $s \in S$ such that $a(s) = 0$ is a finite sequence, then the elements of $\mathrm{Term}_0(S, a)$ would be of the form $\langle\langle x_1, \dots, x_n\rangle\rangle$ for suitable $x_1, \dots, x_n$, making the definition of term of height 0 unreasonably baroque. For this reason we stipulate the following

Convention 3.18. If $a\colon S \to \mathbb{N}$ and every $s \in S$ with $a(s) = 0$ is a finite sequence, then $\mathrm{Term}_0(S, a)$ is $\{s \mid s \in S \wedge a(s) = 0\}$.

An atomic $\mathcal{L}$-formula can be seen as a finite sequence, either of the form $\langle =, s, t\rangle$ with s, t $\mathcal{L}$-terms, or else of the form $\langle R, t_1, \dots, t_n\rangle$ with R an n-ary relation symbol and $\mathcal{L}$-terms $t_1, \dots, t_n$. The collection of $\mathcal{L}$-formulæ can be seen as $\mathrm{Term}(S, a)$ where S is the set of all atomic formulæ, connectives, and symbols $\exists x$, $\forall x$, for any variable x, and $a\colon S \to \mathbb{N}$ is defined by

- $a(\varphi) = 0$ if φ is an atomic formula,
- $a(\neg) = 1$ and $a(\odot) = 2$ for any binary connective $\odot$,
- $a(\exists x) = a(\forall x) = 1$, for any x.

Thus the formula in (3.2) can be written (following Convention 3.18) as

$$\langle \Rightarrow, \langle \exists x, \langle \forall y, \langle \Rightarrow, \langle P, x, y\rangle, \langle Q, x\rangle\rangle\rangle\rangle, \langle \vee, \langle \forall z, \langle R, z\rangle\rangle, \langle S, z\rangle\rangle\rangle.$$

The advantage of writing $\mathcal{L}$-terms and $\mathcal{L}$-formulæ this way is that we can avoid (,) completely, and the syntactic tree can be obtained in a straightforward way.

3.F. Satisfaction of sentences. The notion of **first-order structure** is obtained by merging the two notions of algebraic/relational structure, as in the case of ordered groups (Section 9.A.2). Suppose $\mathcal{L}$ has predicate symbols $P, Q, \dots$, function symbols $f, g, \dots$, and constant symbols $c, d, \dots$. An **$\mathcal{L}$-structure**

$$\mathcal{M} = (M, P^{\mathcal{M}}, Q^{\mathcal{M}}, \dots, f^{\mathcal{M}}, g^{\mathcal{M}}, \dots, c^{\mathcal{M}}, d^{\mathcal{M}}, \dots)$$

consists of:

- a non-empty set M, called the **universe** or **domain** of $\mathcal{M}$,
- subsets $P^{\mathcal{M}} \subseteq M^n$, $Q^{\mathcal{M}} \subseteq M^k$, ... where n is the arity of the symbol P, k is the arity of the symbol Q, ...
- operations $f^{\mathcal{M}}, g^{\mathcal{M}}, \dots$ on M of the same arity as the symbols $f, g, \dots$,
- some specified elements $c^{\mathcal{M}}, d^{\mathcal{M}}, \dots$ of M, one for each constant symbol of the language $\mathcal{L}$.

Remark 3.19. This maxim "a mathematician should never be enslaved by her/his own notational conventions" applies also to us. In particular:

- It is customary to use the same letter with different fonts (calligraphic vs. roman) to distinguish the structure from its underlying universe, but there will be times when this convention is ignored.
- Structures are often identified with their universe, as happens in other parts of mathematics—in algebra one says "given a group G" rather than "given a group $\mathcal{G} = (G, *)$".
- For the seek of readability, we might use the letter M (or its calligraphic counterpart $\mathcal{M}$) as subscript rather than superscript and write c_M, $*_M$, $+_M$, P_M ... for the specified elements, operations, and relations of the structure.

If $\mathcal{M}$ is an $\mathcal{L}$-structure and $x_1, \ldots, x_n$ are the variables occurring in a term t, the **function induced by** t is the n-ary function

$$t^{\mathcal{M}} \colon M^n \to M$$

mapping $(a_1, \ldots, a_n) \in M^n$ to the element $t^{\mathcal{M}}(a_1, \ldots, a_n)$ obtained by replacing the function and constant symbols with the corresponding functions and constants of $\mathcal{M}$. For example the term[17] $t(x, y, z)$ given by $x \cdot (y \cdot y) + ((x \cdot y) + 1)$ in the language of rings defines a polynomial function $R^3 \to R$ in every ring R, mapping $(a, b, c) \in R^3$ to $ab^2 + ab + 1_R \in R$.

Definition 3.20. Given an $\mathcal{L}$-sentence σ, consider the pseudo-formula $\sigma^{\mathcal{M}}$ obtained by replacing the symbols $P, Q, \ldots, f, g, \ldots, c, d, \ldots$ with the relations $P^{\mathcal{M}}, Q^{\mathcal{M}}, \ldots$, functions $f^{\mathcal{M}}, g^{\mathcal{M}}, \ldots$, and elements $c^{\mathcal{M}}, d^{\mathcal{M}}, \cdots \in M$, and by bounding all quantifiers to M. We will say that $\mathcal{M}$ **satisfies** σ, in symbols

$$\mathcal{M} \vDash \sigma$$

if $\sigma^{\mathcal{M}}$ is true in $\mathcal{M}$. If this is not the case, we write $\mathcal{M} \nvDash \sigma$.

Observe that

the expression...	amounts to saying that...
$\mathcal{M} \vDash \neg\sigma$	$\mathcal{M} \nvDash \sigma$,
$\mathcal{M} \vDash \sigma \wedge \tau$	$\mathcal{M} \vDash \sigma$ and $\mathcal{M} \vDash \tau$,
$\mathcal{M} \vDash \sigma \vee \tau$	$\mathcal{M} \vDash \sigma$ or $\mathcal{M} \vDash \tau$,
$\mathcal{M} \vDash \sigma \Rightarrow \tau$	if $\mathcal{M} \vDash \sigma$ then $\mathcal{M} \vDash \tau$,
$\mathcal{M} \vDash \sigma \Leftrightarrow \tau$	$\mathcal{M} \vDash \sigma$ if and only if $\mathcal{M} \vDash \tau$.

Example 3.21. Let $\mathcal{L}$ be the language with only one binary predicate symbol R, and let $\mathcal{M} = (M, R^{\mathcal{M}})$ be an $\mathcal{L}$-structure. Then $\mathcal{M}$ is a preordered set if

[17] Recall the convention on page 25 according to which the variables in $t(x, y, z)$ are *among* the x, y, z.

and only if $\mathcal{M}$ satisfies the sentences

$$\forall x\ (x\ R\ x) \tag{3.9a}$$

$$\forall x, y, z\ (x\ R\ y \land y\ R\ z \Rightarrow x\ R\ z) \tag{3.9b}$$

which is to say that $\forall x \in M\ \big((x, x) \in R^{\mathcal{M}}\big)$ and $\forall x, y, z \in M\ \big((x, y) \in R^{\mathcal{M}} \land (y, z) \in R^{\mathcal{M}} \Rightarrow (x, z) \in R^{\mathcal{M}}\big)$. If moreover $\mathcal{M}$ satisfies

$$\forall x, y\ (x\ R\ y \land y\ R\ x \Rightarrow x = y) \tag{3.9c}$$

that is $\forall x, y \in M\ \big((x, y) \in R^{\mathcal{M}} \land (y, x) \in R^{\mathcal{M}} \Rightarrow x = y\big)$, then $\mathcal{M}$ is an ordered set. If $\mathcal{M}$ satisfies (3.9a), (3.9b) and

$$\forall x, y\ (x\ R\ y \Rightarrow y\ R\ x) \tag{3.9d}$$

which is to say that $\forall x, y \in M\ \big((x, y) \in R^{\mathcal{M}} \Rightarrow (y, x) \in R^{\mathcal{M}}\big)$, then $\mathcal{M}$ is a non-empty set endowed with an equivalence relation.

Although this language $\mathcal{L}$ is suitable for axiomatizing orders, equivalence relations, graphs, digraphs, ..., when dealing with (pre)orders it is customary to use the symbol $\leq$ rather than R, and denote the language by $\mathcal{L}_{\text{Ordr}}$.

Example 3.22. The language $\mathcal{L}_{\text{Grps}}$ for groups has a symbol $\cdot$ for the binary operation, a symbol f for a unary operation, and a constant symbol 1. In order to conform with standard mathematical notation, we shall write x^{-1} instead of $f(x)$. Atomic formulæ are of the form $t_1 = t_2$, with t_1 and t_2 terms. A structure for this language consists of a set M together with a specified element 1^M, a binary operation $(x, y) \mapsto x \cdot^M y$, and a unary operation $x \mapsto x^{-1_M}$. We say that M is a group if it satisfies the axioms

$$\forall x, y, z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z) \tag{3.10a}$$

$$\forall x\,(x \cdot 1 = x\ \land\ 1 \cdot x = x) \tag{3.10b}$$

$$\forall x\,\big(x \cdot x^{-1} = 1\ \land\ x^{-1} \cdot x = 1\big)\,. \tag{3.10c}$$

Example 3.23. The language $\mathcal{L}_{\text{ORings}}$ for ordered fields, has one binary relation symbol $<$, two binary function symbols $+$ and $\cdot$, one symbol for a unary functiom $-$, and two constant symbols 0 and 1. A structure for this language is a non-empty set M and two (not necessarily distinct) elements 0^M and 1^M, two (not necessarily distinct) binary operations $+^M$ and $\cdot^M$, a unary operation $-^M$, and a binary relation $<^M$. In general M will not be an ordered field—to enforce this we require that M satisfies the axioms for abelian groups

$$\forall x, y, z\ ((x + y) + z = x + (y + z)) \tag{3.11a}$$

$$\forall x, y\ (x + y = y + x) \tag{3.11b}$$

$$\forall x\,(x + 0 = x) \tag{3.11c}$$

$$\forall x\,(x + (-x) = 0)\,, \tag{3.11d}$$

those for rings

$$\forall x, y, z\ ((x \cdot y) \cdot z = x \cdot (y \cdot z)) \tag{3.12a}$$

$$\forall x\,(x \cdot 1 = x\ \wedge\ 1 \cdot x = x) \tag{3.12b}$$

$$\forall x, y, z\ ((x + y) \cdot z = (x \cdot z) + (y \cdot z))\,, \tag{3.12c}$$

the axiom for commutativity of the product

$$\forall x, y\ (x \cdot y = y \cdot x)\,, \tag{3.13}$$

the axioms for fields

$$0 \neq 1 \tag{3.14a}$$

$$\forall x\,(x \neq 0 \Rightarrow \exists y\,(x \cdot y = 1))\,, \tag{3.14b}$$

and the axioms for total orders

$$\neg\exists x\,(x < x) \tag{3.15a}$$

$$\forall x, y, z\,(x < y \wedge y < z \Rightarrow x < z) \tag{3.15b}$$

$$\forall x, y\ (x < y \vee x = y \vee y < x)\,. \tag{3.15c}$$

Finally we must have axioms guaranteeing compatibility of the ordering with the algebraic operations:

$$\forall x, y, z\ (x < y \Rightarrow x + z < y + z) \tag{3.16a}$$

$$\forall x, y\ (0 < x \wedge 0 < y \Rightarrow 0 < x \cdot y)\,. \tag{3.16b}$$

Example 3.24. Let $\mathcal{L}_{\text{CONC}}$ be the language with a binary function symbol $*$ and three constant symbols $\mathbf{0}, \mathbf{1}, \varepsilon$. Let A be a set with at least two elements a, b. The set of all finite strings from A can be construed as an $\mathcal{L}$-structure $\mathcal{M} = (A^{<\mathbb{N}}, *^{\mathcal{M}}, \mathbf{0}^{\mathcal{M}}, \mathbf{1}^{\mathcal{M}}, \varepsilon^{\mathcal{M}})$ with $s *^{\mathcal{M}} t = s^\frown t$, $\mathbf{0}^{\mathcal{M}} = \langle a \rangle$, $\mathbf{1}^{\mathcal{M}} = \langle b \rangle$, and $\varepsilon^{\mathcal{M}} = \langle\rangle$, satisfying the set of sentences T_{CONC} consisting of: the axioms for monoids ($\forall x, y, z\,(x * (y * z) = (x * y) * z)$ and $\forall x\,(x * \varepsilon = x \wedge \varepsilon * x = x)$) together with

$$\neg\exists x, y\,(x \neq \varepsilon \wedge y \neq \varepsilon \wedge (\mathbf{0} = x * y \vee \mathbf{1} = x * y))$$
$$\mathbf{0} \neq \mathbf{1}$$

stating that $\mathbf{0}$ and $\mathbf{1}$ are distinct sequences that cannot be factored into smaller items, and

$$\begin{aligned}&\forall x, y, z, w\,(x * y = z * w \Rightarrow \\ &\qquad\qquad \exists u\ ((x * u = z \wedge y = u * w) \vee (z * u = x \wedge w = u * y)))\end{aligned}$$

asserting that if a sequence is factored in two different ways $x * y$ and $z * w$, then either x is an initial segment of z and w is a final segment of y, or z is an initial segment of x and y is a final segment of w (see Definition 3.16).

If $\mathcal{M}$ satisfies every σ in some set of sentences Σ, we say that $\mathcal{M}$ is a **model** of Σ, in symbols

$$\mathcal{M} \vDash \Sigma.$$

Since a structure satisfies a conjunction if and only if it satisfies all formulæ that compose such conjunction, saying that $\mathcal{M}$ is a model of a finite set of sentences $\{\sigma_1, \dots, \sigma_n\}$ amounts to saying that $\mathcal{M} \vDash \bigwedge_{1 \leq i \leq n} \sigma_i$.

To recap, we have seen a few first-order languages tailored to study certain classes of mathematical structures:

- $\mathcal{L}_{\mathrm{O{\scriptsize RDR}}}$ has a binary predicate symbol $\leq$. A structure for this language is a preorderd set if it satisfies $T_{\mathrm{pO{\scriptsize RDR}}}$, that is the axioms (3.9a) and (3.9b). An ordered set is an $\mathcal{L}_{\mathrm{O{\scriptsize RDR}}}$-structure satisfying $T_{\mathrm{O{\scriptsize RDR}}}$, obtained by adding axiom (3.9c) to $T_{\mathrm{pO{\scriptsize RDR}}}$.
- $\mathcal{L}_{\mathrm{G{\scriptsize RPS}}}$ has a binary function symbol $\cdot$, a unary operation symbol $^{-1}$, and a constant symbol 1. A structure for such language is a group if and only if it satisfies $T_{\mathrm{G{\scriptsize RPS}}}$, the set of all sentences (3.10). Replacing $\cdot, {}^{-1}, 1$ with $+, -, 0$ the language $\mathcal{L}_{\mathrm{A{\scriptsize B}G{\scriptsize R}}}$ is obtained. A structure for this language is an abelian group if and only if it satisfies the set $T_{\mathrm{A{\scriptsize B}G{\scriptsize R}}}$ consisting of the sentences (3.11).
- The language $\mathcal{L}_{\mathrm{R{\scriptsize NGS}}}$ is obtained adding the binary function symbol $\cdot$ to $\mathcal{L}_{\mathrm{A{\scriptsize B}G{\scriptsize R}}}$. An $\mathcal{L}_{\mathrm{R{\scriptsize NGS}}}$-structure is a rng if it satisfies the set $T_{\mathrm{R{\scriptsize NGS}}}$ obtained by adding the sentences (3.12a) and (3.12c) to $T_{\mathrm{A{\scriptsize B}G{\scriptsize R}}}$, it is a commutative rng if it satisfies $T_{\mathrm{CR{\scriptsize INGS}}}$, obtained by adding the sentence (3.13) to $T_{\mathrm{R{\scriptsize NGS}}}$. The language $\mathcal{L}_{\mathrm{R{\scriptsize INGS}}}$ is obtained by adding a new constant symbol 1; a structure for this language is a ring if it satisfies the set $T_{\mathrm{R{\scriptsize INGS}}}$ given by $T_{\mathrm{R{\scriptsize NGS}}}$ together with (3.12b). If we also add (3.13) we obtain the set of sentences $T_{\mathrm{CR{\scriptsize INGS}}}$, whose models are exactly the commutative rings, and if the sentences (3.14) are added, we obtain the set $T_{\mathrm{F{\scriptsize LDS}}}$, whose models are the fields. Adding a binary relation symbol $<$, the language $\mathcal{L}_{\mathrm{OR{\scriptsize INGS}}}$ is obtained. An ordered field is an $\mathcal{L}_{\mathrm{OR{\scriptsize INGS}}}$-structure satisfying the set of axioms $T_{\mathrm{OF{\scriptsize LDS}}}$, obtained by adding the sentences (3.15) and (3.16) to $T_{\mathrm{F{\scriptsize LDS}}}$.

Remarks 3.25. (a) If $\mathcal{M} \vDash \Sigma$ and Σ is an infinite set of sentences, for example $\Sigma = \{\sigma_n \mid n \in \mathbb{N}\}$, we are tempted to say that M satisfies the infinite conjunction $\bigwedge_{n \in \mathbb{N}} \sigma_n$. We should however virtuously resist this temptation, since $\bigwedge_{n \in \mathbb{N}} \sigma_n$ is *not* a formula of a first-order language. There are formal systems, the so-called **infinitary logics**, where we are allowed to take infinite conjunction and disjunction of formulæ, but these are more advanced topics that will not be covered in this book.

(b) Whenever we are assessing whether a sentence σ is true in a structure $\mathcal{M}$, quantifications take place on the *elements* of M, not on *subsets*

> of M. This restriction is the quintessence of first-order logic. To be able to quantify also on subsets of a structure, a new list of variables for subsets and a symbol $\in$ to tell when an element belongs to a set must be introduced, and the satisfaction relation must be modified to take into accounts the two levels of quantification (on elements, and on subsets). The resulting system is known as **second-order logic**. More ambitiously, it is possible to define third-order logic, with three levels for quantification (elements, subsets, families of subsets) or more generally n^{th}-order logic, with the expected definition. Higher-order logics, i.e. n^{th}-order logic for $n > 1$, have an expressive power which is much stronger than first-order logic. However, as often happens in mathematics, the quest for extreme generality runs against the depth of the results, and in this book, like in most textbooks, we will focus on first-order logic.

We say that a sentence τ is a **logical consequence** of a set of sentences Σ (of the same language), or that τ **follows logically from** Σ, in symbols

$$\Sigma \models \tau$$

if and only if $\mathcal{M} \vDash \Sigma$ implies that $\mathcal{M} \vDash \tau$, for every $\mathcal{L}$-structure $\mathcal{M}$. When $\Sigma = \{\sigma\}$ is a singleton, it will be identified with its unique element, and we write $\sigma \models \tau$. Equivalently: τ is logical consequence of σ just in case $\sigma \Rightarrow \tau$ is a valid sentence. Two sentences σ and τ are **logically equivalent** if one is logical consequences of the other, that is:

$$\sigma \models \tau \quad \text{and} \quad \tau \models \sigma.$$

Equivalently: $\sigma \Leftrightarrow \tau$ is a valid sentence.

Warning. The satisfaction relation should not be confused with the notion of logical consequence! These are distinct concepts, albeit the symbols are similar. Satisfaction ($\vDash$) is a relation between an $\mathcal{L}$-structure and a sentence (or a set of sentences), while logical consequence ($\models$) is a relation between a set of sentences and a single sentence. In most textbooks these two notions are denoted with the same symbol, but in order to help the reader in telling these two notions apart, we adopt two slightly different glyphs.

Let us see how the notion of logical consequence is related to that of tautological consequence (Definition 3.9).

Example 3.26. Recall from Section 3.C.1 that given a non-empty set S of propositional letters, $\mathrm{Prop}(S)$ is the set of all propositions over S. The language $\mathcal{L}_S$ has a 1-ary relation symbol U and a constant symbol $\mathring{\mathrm{A}}$ for each $\mathrm{A} \in S$. To each proposition $\mathrm{P} \in \mathrm{Prop}(S)$ we assign a sentence σ_{P} of $\mathcal{L}_S$ as follows: to each propositional letter $\mathrm{A} \in S$ associate the sentence σ_{A} given by $U(\mathring{\mathrm{A}})$, and then extend this map by $\mathrm{P} \vee \mathrm{Q} \mapsto \sigma_{\mathrm{P}} \vee \sigma_{\mathrm{Q}}$, $\neg\mathrm{P} \mapsto \neg\sigma_{\mathrm{P}}$, etc.

A valuation $v\colon S \to \{0,1\}$ can be seen as an $\mathcal{L}_S$-structure $\mathcal{M}_v$. The universe of $\mathcal{M} = \mathcal{M}_v$ is S, and $U^{\mathcal{M}} = \{\mathrm{A} \in S \mid v(\mathrm{A}) = 1\}$, and $\mathring{\mathrm{A}}^{\mathcal{M}} = \mathrm{A}$, that is

$$\mathcal{M}_v = (S, \{\mathrm{A} \in S \mid v(\mathrm{A}) = 1\}, \mathrm{A})_{\mathrm{A} \in S}.$$

Conversely, each $\mathcal{L}_S$-structure $\mathcal{M} = (M, U^{\mathcal{M}}, \mathring{\mathrm{A}}^{\mathcal{M}})_{\mathrm{A} \in S}$ yields the valuation

$$v_{\mathcal{M}}(\mathrm{A}) = 1 \Leftrightarrow \mathring{\mathrm{A}}^{\mathcal{M}} \in U^{\mathcal{M}}.$$

A simple induction on the height of formulæ shows that

$$v(\mathrm{P}) = 1 \Leftrightarrow \mathcal{M}_v \vDash \sigma_{\mathrm{P}} \quad \text{and} \quad \mathcal{M} \vDash \sigma_{\mathrm{P}} \Leftrightarrow v_{\mathcal{M}}(\mathrm{P}) = 1.$$

Thus valuations of S correspond to $\mathcal{L}_S$-structures, and for this reason they are often called models for propositional calculus. Therefore we say that:

(i) $v\colon S \to \{0,1\}$ satisfies $\Gamma \subseteq \mathrm{Prop}(S)$ or is a model of Γ, in symbols $v \vDash \Gamma$, if $\forall \mathrm{P} \in \Gamma\, (v(\mathrm{P}) = 1)$;

(ii) if $\Gamma \subseteq \mathrm{Prop}(S)$, then P is tautological consequence of Γ, in symbols $\Gamma \models \mathrm{P}$, if and only if every model of Γ is a model of P;

(iii) if $\mathrm{P} \models \mathrm{Q}$ and $\mathrm{Q} \models \mathrm{P}$, then P and Q are tautologically equivalent, that is $v(\mathrm{P}) = v(\mathrm{Q})$, for every v.

Definition 3.27. (i) An **$\mathcal{L}$-theory** is a set T of $\mathcal{L}$-sentences, and $\mathcal{L}$ is the language of T. A **first-order theory** is an $\mathcal{L}$-theory, for some first-order language $\mathcal{L}$.

(ii) A **set of axioms** for an $\mathcal{L}$-theory T is an $\mathcal{L}$-theory T' such that for all $\mathcal{L}$-sentences σ

$$T' \models \sigma \quad \text{if and only if} \quad T \models \sigma.$$

The expressions "theory" and "set of sentences" are completely equivalent, but the former is particularly handy when speaking of first-order axiomatizations of mathematical objects. Thus we shall speak of *first-order theory of abelian groups*, *first-order theory of rings*, *first-order theory of fields*, … to denote the theories that have as a system of axioms $T_{\textsc{AbGr}}$, $T_{\textsc{Rngs}}$, $T_{\textsc{Flds}}$ …. On the other hand, expressions like *abelian group theory*, *ring theory*, *field theory*, …, are used to denote certain areas of mathematics.

Remark 3.28. Part (ii) of Definition 3.27 looks a bit silly, since any theory is a set of axioms for itself. On the other hand, a set of axioms for T need not be a subset of T. For example, the sentences: associativity of products (3.10a), $\forall x \forall y \exists z\, (x \cdot z \eqcirc y)$, and $\forall x \forall y \exists z\, (z \cdot x \eqcirc y)$ form a set of axioms for $T_{\textsc{Grps}}$.

Definition 3.29. Let T be an $\mathcal{L}$-theory. We say that T is **satisfiable** if it has a model, that is to say: there is an $\mathcal{L}$-structure $\mathcal{M}$ such that $\mathcal{M} \vDash T$. Otherwise T is **unsatisfiable**.

Let us pause for an example. Recall from page 18 the sentences ε_n asserting that the universe has exactly n elements. The non-abelian groups are exactly the models of $\Sigma = T_{\mathrm{Grps}} \cup \{\exists x \exists y (x \cdot y \neq y \cdot x)\}$, so $\Sigma \cup \{\varepsilon_5\}$ is unsatisfiable, as every group of order 5 is abelian, and $\Sigma \cup \{\varepsilon_6\}$ is satisfiable as there is a non-abelian group of order 6.

Proposition 3.30. *If $\Sigma \cup \{\tau\}$ is a set of $\mathcal{L}$-sentences, then*

$$\Sigma \models \tau \quad \textit{if and only if} \quad \Sigma \cup \{\neg\tau\} \textit{ is unsatisfiable.}$$

Proof. Suppose $\Sigma \cup \{\neg\tau\}$ is not satisfiable, and let $\mathcal{M}$ be a model of Σ. Then $\mathcal{M} \not\vDash \neg\tau$, since otherwise $\mathcal{M}$ would witness satisfiability of $\Sigma \cup \{\neg\tau\}$, so $\mathcal{M} \vDash \tau$. As $\mathcal{M}$ is arbitrary, it follows that $\Sigma \models \tau$. The other implication is immediate. □

Definition 3.31. Fix a language $\mathcal{L}$.

(i) An $\mathcal{L}$-theory T is **complete** if it is satisfiable and either $T \models \sigma$ or else $T \models \neg\sigma$, for every $\mathcal{L}$-sentence σ.

(ii) Two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{M}'$ are **elementarily equivalent** if they satisfy the same $\mathcal{L}$-sentences.

(iii) The **theory of an $\mathcal{L}$-structure** $\mathcal{M}$ is the set of all sentences σ such that $\mathcal{M} \vDash \sigma$.

Proposition 3.32. *If T is a satisfiable theory, then the following are equivalent:*

(a) *T is complete,*

(b) *T is an axiom system for the theory of some $\mathcal{L}$-structure,*

(c) *two models of T are elementarily equivalent.*

Proof. (a)⇒(b) Let $\mathcal{M}$ be a model of T and let σ be an $\mathcal{L}$-sentence: by definition of complete theory it follows that $T \models \sigma$ if and only if $\mathcal{M} \vDash \sigma$. Therefore the sentences true in $\mathcal{M}$ are exactly those that are logical consequences of T, that is to say: T is a set of axioms for the theory of $\mathcal{M}$.

(b)⇒(c) Suppose T is an axiom system for the theory of $\mathcal{M}$, that is to say: $T \models \sigma$ if and only if $\mathcal{M} \vDash \sigma$, for all $\mathcal{L}$-sentences σ. Suppose $\mathcal{N} \vDash T$: if $\mathcal{M} \vDash \sigma$ then $T \models \sigma$ and hence $\mathcal{N} \vDash \sigma$; if $\mathcal{M} \not\vDash \sigma$ then $\mathcal{M} \vDash \neg\sigma$ and therefore $T \models \neg\sigma$ whence $\mathcal{N} \vDash \neg\sigma$ and thus $\mathcal{N} \not\vDash \sigma$. Thus a model $\mathcal{N}$ of T satisfies the same sentences of the model $\mathcal{M}$, and hence two models of T satisfy the same sentences.

(c)⇒(a) We prove the contrapositive: if T is satisfiable but $T \not\models \sigma$ and $T \not\models \neg\sigma$ then there are $\mathcal{M}$ and $\mathcal{M}'$ models of T such that $\mathcal{M} \vDash \sigma$ and $\mathcal{M}' \vDash \neg\sigma$. In particular $\mathcal{M}$ and $\mathcal{M}'$ do not satisfy the same sentences. □

3.G. Truth sets. We have seen what it means for a sentence to be true in a structure, but what about formulæ that are not sentences? Some of these formulæ (e.g. a tautology or a formula as in (3.6) on page 31) have been shown to be true in all structures, and hence their negations are always false. But, in general, a formula $\varphi(x_1, \dots, x_n)$ defines a set of n-tuples of elements of the structure that, when set in place of the variables $x_1, \dots, x_n$, make φ true in the structure. More to the point: given an $\mathcal{L}$-structure $\mathcal{M}$ and a formula $\varphi(x_1, \dots, x_n)$ of $\mathcal{L}$, the **truth set** of φ in $\mathcal{M}$ is the set

$$\mathbf{T}_\varphi = \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}$$

of the n-tuples of elements of $\mathcal{M}$ that satisfy the formula $\varphi(x_1, \dots, x_n)$. For notational ease, we write

$$\mathcal{M} \vDash \varphi[a_1, \dots, a_n]$$

instead of $(a_1, \dots, a_n) \in \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}$. If $\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = M^n$ then we shall say that φ is **true** in $\mathcal{M}$. When φ is a sentence, this terminology agrees with our previous definition, since

$$\begin{aligned} \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = M^n &\quad \text{if and only if} \quad \mathcal{M} \vDash \varphi \\ \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = \emptyset &\quad \text{if and only if} \quad \mathcal{M} \vDash \neg\varphi. \end{aligned}$$

For notational ease when σ is a sentence set

$$\begin{aligned} \mathbf{T}^{\mathcal{M}}_{\sigma} = 1 &\quad \text{if and only if} \quad \mathcal{M} \vDash \sigma \\ \mathbf{T}^{\mathcal{M}}_{\sigma} = 0 &\quad \text{if and only if} \quad \mathcal{M} \vDash \neg\sigma. \end{aligned}$$

Therefore $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent if and only if $\mathbf{T}^{\mathcal{M}}_{\sigma} = \mathbf{T}^{\mathcal{N}}_{\sigma}$ for all sentences σ.

Examples 3.33. (A) If $\varphi(x_1, \dots, x_n)$ is valid then $\mathbf{T}_\varphi = M^n$, if it is unsatisfiable then $\mathbf{T}_\varphi = \emptyset$,

(B) the truth set in $\mathbb{N}$ of $\exists y\,(y + y = x)$ is the set of even numbers,

(C) the truth set in $\mathbb{N}$ of $1 < x \wedge \forall y\,(\exists z(z \cdot y = x) \Rightarrow y = 1 \vee y = x)$ is the set of prime numbers,

(D) the truth set of $x^2 < 1$ in $\mathbb{N}$ is the singleton $\{0\}$, while in $\mathbb{R}$ it is the open interval $(-1; 1)$,

(E) the truth set in $\mathbb{R}$ of $y = x^2 - 3x + 2$ is a parabola, that is a subset of $\mathbb{R}^2$,

(F) the truth set of $x^2 + y^2 = 0$ in $\mathbb{R}$ is the singleton $\{(0, 0)\} \subseteq \mathbb{R}^2$, while in $\mathbb{C}$ it is the union of the two lines in $\mathbb{C}^2$ of equation $x = \mathrm{i}y$ and $x = -\mathrm{i}y$,

(G) if $\varphi(x_1, x_2)$ is $x_1 = x_2$, then $\mathbf{T}_{\varphi(x_1,x_2)}$ is the diagonal of M^2,

(H) if $\varphi(x_1, \dots, x_n)$ is $P(x_1, \dots, x_n)$ where P is an n-ary predicate symbol of $\mathcal{L}$, then $\mathbf{T}_{\varphi(x_1,\dots,x_n)} = P^{\mathcal{M}}$.

The dimension n of $\mathbf{T}_\varphi$ depends on the formula φ and on the list $x_1, \dots, x_n$ of variables—for example if φ is the formula of Example (E), then the truth set of $\varphi(x, y, z)$ in $\mathbb{R}$ is the cylinder $\{(x, y, z) \in \mathbb{R}^3 \mid y = x^2 - 3x + 2\}$. It is immediate that given $\varphi(x_1, \dots, x_n)$ and $\psi(x_1, \dots, x_n)$

(3.17a) $$\mathbf{T}_{\neg\varphi} = M^n \setminus \mathbf{T}_\varphi$$

(3.17b) $$\mathbf{T}_{\varphi\wedge\psi} = \mathbf{T}_\varphi \cap \mathbf{T}_\psi$$

(3.17c) $$\mathbf{T}_{\varphi\vee\psi} = \mathbf{T}_\varphi \cup \mathbf{T}_\psi$$

(3.17d) $$\mathbf{T}_{\varphi\Rightarrow\psi} = (M^n \setminus \mathbf{T}_\varphi) \cup \mathbf{T}_\psi$$

(3.17e) $$\mathbf{T}_{\varphi\Leftrightarrow\psi} = M^n \setminus (\mathbf{T}_\varphi \mathbin{\triangle} \mathbf{T}_\psi).$$

Next let us describe $\mathbf{T}_{\varphi(x_1,\dots,x_n)}$ when φ is $\exists y\psi$.

Case 1: If y is not among the $x_1, \dots, x_n$, then

(3.18a) $$\mathbf{T}_{\varphi(x_1,\dots,x_n)} = p[\mathbf{T}_{\psi(y,x_1,\dots,x_n)}]$$

where $p\colon M^{n+1} \to M^n$ is the projection along the first coordinate, that is

$$p(b, a_1, \dots, a_n) = (a_1, \dots, a_n).$$

Case 2: If y is, say, x_1, then

(3.18b) $$\mathbf{T}_{\varphi(x_1,\dots,x_n)} = M \times \mathbf{T}_{\varphi(x_2,\dots,x_n)}$$

where $\mathbf{T}_{\varphi(x_2,\dots,x_n)}$ is as in Case 1.

Thus given a formula $\varphi(x_1, \dots, x_n)$ one has

(3.18c) $$\mathcal{M} \vDash \exists x_1 \dots x_n \varphi \quad \text{if and only if} \quad \mathbf{T}_{\varphi(x_1,\dots,x_n)} \neq \emptyset,$$

(3.18d) $$\mathcal{M} \vDash \forall x_1 \dots x_n \varphi \quad \text{if and only if} \quad \mathbf{T}_{\varphi(x_1,\dots,x_n)} = M^n.$$

Using these equivalences it is easy to check whether a structure M satisfies a sentence σ.

Examples 3.34. (A) $\mathcal{M} \vDash \forall x\, (\varphi(x) \Rightarrow \psi(x))$ if and only if the truth set of $\varphi(x) \Rightarrow \psi(x)$ is M, that is to say $\mathbf{T}_\varphi \subseteq \mathbf{T}_\psi$.

(B) $\forall x\, (\varphi(x) \Rightarrow \psi(x)) \Rightarrow (\forall x\varphi(x) \Rightarrow \forall x\psi(x))$ is a valid sentence. To prove this we must check that for any structure $\mathcal{M}$:

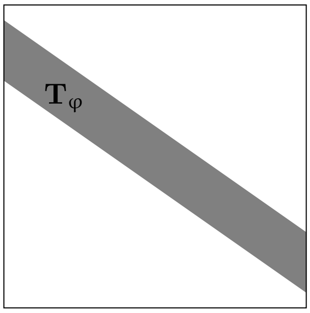
$$\text{if } \mathcal{M} \vDash \forall x\, (\varphi(x) \Rightarrow \psi(x)) \text{ then } \mathcal{M} \vDash \forall x\varphi(x) \Rightarrow \forall x\psi(x).$$

Thus suppose that $\mathcal{M}$ is a structure satisfying $\forall x\, (\varphi(x) \Rightarrow \psi(x))$ and $\forall x\varphi(x)$, that is to say $\mathbf{T}_\varphi \subseteq \mathbf{T}_\psi$ and $\mathbf{T}_\varphi = M$. Then $\mathbf{T}_\psi = M$ and hence $\mathcal{M} \vDash \forall x\psi(x)$ as required.

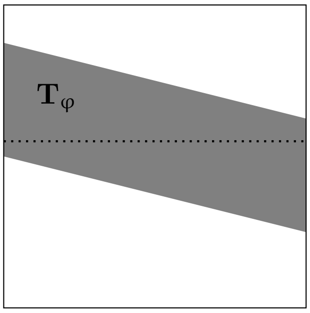
The same argument shows that

(3.19) $$\forall x_1, \dots, x_n\, (\varphi(\vec{x}) \Rightarrow \psi(\vec{x})) \models \forall x_1, \dots, x_n\, \varphi(\vec{x}) \Rightarrow \forall x_1, \dots, x_n\, \psi(\vec{x}).$$

(C) The sentence $\forall x \exists y \varphi(x, y)$ holds in $\mathcal{M}$ if and only if the set $\mathbf{T}_\varphi \subseteq M^2$ has non-empty vertical sections, while saying that $\mathcal{M} \vDash \exists y \forall x \varphi(x, y)$ means that there is an horizontal section of $\mathbf{T}_\varphi$ which is M.



$\forall x \exists y \varphi(x, y)$



$\exists y \forall x \varphi(x, y)$

(D) Consider the formula

$$\forall x(P(x) \vee Q(x)) \Rightarrow \forall x\, P(x) \vee \forall x\, Q(x). \tag{3.20}$$

Fix a structure $\mathcal{M}$. By (3.18d), asserting that $\mathcal{M} \vDash \forall x(P(x) \vee Q(x))$ amounts to saying that $\mathbf{T}_{P(x)\vee Q(x)} = \mathbf{T}_{P(x)} \cup \mathbf{T}_{Q(x)} = M$, that is $P^{\mathcal{M}} \cup Q^{\mathcal{M}} = M$; while asserting that $\mathcal{M} \vDash \forall x\, P(x) \vee \forall x\, Q(x)$ means that $P^{\mathcal{M}} = M$ or $Q^{\mathcal{M}} = M$. Therefore a structure $\mathcal{M}$ satisfies (3.20) if and only if: whenever $P^{\mathcal{M}} \cup Q^{\mathcal{M}} = M$ then $P^{\mathcal{M}} = M$ or $Q^{\mathcal{M}} = M$. For example, the structure $\mathcal{M}$ whose domain is $\mathbb{N}$ and where $P^{\mathcal{M}} = Q^{\mathcal{M}} = \emptyset$ satisfies the sentence, while the structure $\mathcal{N}$ with domain $\mathbb{N}$ with $P^{\mathcal{N}}$ and $Q^{\mathcal{N}}$ are the set of even and odd numbers, respectively, does not satisfy the sentence. It follows that the sentence (3.20) is satisfiable, but not valid.

(E) Suppose that the formula $\varphi(x_1, \dots, x_n)$ is tautological consequence of $\psi_1(x_1, \dots, x_n)$, ..., $\psi_k(x_1, \dots, x_n)$; in other words: $\psi_1 \wedge \dots \wedge \psi_k \Rightarrow \varphi$ is a tautology (see page 33). Then $\psi_1 \wedge \dots \wedge \psi_k \Rightarrow \varphi$ is valid, and hence $\mathbf{T}^{\mathcal{M}}_{\psi_1(x_1,\dots,x_n)} \cap \dots \cap \mathbf{T}^{\mathcal{M}}_{\psi_k(x_1,\dots,x_n)} \subseteq \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}$, for all structures $\mathcal{M}$. In particular, if $\varphi(x_1, \dots, x_n)$ and $\psi(x_1, \dots, x_n)$ are tautologically equivalent, then $\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^{\mathcal{M}}_{\psi(x_1,\dots,x_n)}$.

Example 3.35. Consider a language containing unary function symbols f, g and unary predicate symbols P, Q. If $\mathcal{M}$ is a structure for this language, the functions and predicates of $\mathcal{M}$ will be denoted with the same letters f, g, P, Q. The sets $f[P]$ and $g^{-1}[Q]$ are the truth sets of the formulæ $\exists y(P(y) \wedge f(y) = x)$ and $Q(g(x))$, so $g^{-1}[f[P]]$ and $f[P] \times g^{-1}[Q]$ are the truth sets of $\exists y(P(y) \wedge f(y) = g(x))$ and $\exists y(P(y) \wedge f(y) = x) \wedge Q(g(x))$, respectively. One can translate the properties of the structure $\mathcal{M}$ into statements of our language: for example $f[P] \cap g[Q] = \emptyset$ if and only if $\mathcal{M} \vDash \forall x(\exists y(P(y) \wedge f(y) = x) \Rightarrow \neg Q(g(x)))$.

The notion of logical consequence of sentences, formulated in Section 3.F, can be extended to arbitrary formulæ as follows. We say that φ **is logical consequence of a set of formulæ** Γ, in symbols $\Gamma \models \varphi$, if $\Gamma^\forall \models \varphi^\forall$, where $\Gamma^\forall$ is the set of the universal closures $\psi^\forall$ with ψ in Γ. Equivalently, $\Gamma \models \varphi$ if and only if

$$\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = M^n, \text{ for every structure } \mathcal{M} \text{ such that } \mathcal{M} \vDash \psi^\forall, \text{ for all } \psi \text{ in } \Gamma,$$

that is if φ holds true in every model of $\Gamma^\forall$. Two formulæ φ and ψ are **logically equivalent modulo** Γ or **over** Γ if and only if $\varphi \Leftrightarrow \psi$ is logical consequence of Γ.

Remarks 3.36. (a) The concept of logical equivalence of formulæ (with free variables) modulo a given set of axioms is a rather common notion in mathematics, and by Example 3.34(A) if two formulæ are logically equivalent modulo modulo some set of formulæ Γ, then so are their universal closures. For example the three formulæ $x \cdot y \doteq y \cdot x$, $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$ and $(x \cdot y)^2 \doteq x^2 \cdot y^2$ are logically equivalent modulo T_{GRPS}, that is to say: given a group G and $a, b \in G$, then $ab = ba$ if and only if $(ab)^{-1} = a^{-1}b^{-1}$ if and only if $(ab)^2 = a^2b^2$. As their universal closures are equivalent modulo the axioms for groups, it follows that which a group is abelian if and only if it satisfies $\forall x, y\, ((x \cdot y)^{-1} = x^{-1} \cdot y^{-1})$, if and only if it satisfies $\forall x, y\, [(xy)^2 \doteq x^2y^2]$. Saying that two formulæ are logically equivalent modulo Γ is stronger than saying that their universal closures are logically equivalent modulo Γ (see Remark 7.31).

(b) The satisfaction relation and truth sets yield a suitable framework for the formalizations in Sections 2.B and 2.C—for example the formalization of "there are infinitely many primes" is a way to write a sentence in the language $<, \mathrm{Pr}$ or $<, |$ asserting a certain fact in $(\mathbb{N}, <, \mathrm{Pr})$ or in $(\mathbb{N}, <, |)$.

3.H. A closer look at the satisfaction relation*. We now give a brief summary of a different, albeit completely equivalent, way to define the satisfaction relation—this approach will be expounded in detail in Section 31.A of Chapter VII. Given $\varphi(x_1, \dots, x_n)$ an $\mathcal{L}$-formula, $\mathcal{M}$ an $\mathcal{L}$-structure, and $a_1, \dots, a_n$ elements of M, the universe of $\mathcal{M}$, we define by induction of the height of the formula what it means that $\mathcal{M}$ satisfies φ when the variables $x_1, \dots, x_n$ take values $a_1, \dots, a_n$, respectively,

$$\mathcal{M} \vDash \varphi[a_1, \dots, a_n].$$

The idea is that if the free occurrences of $x_1, \dots, x_n$ in φ are replaced by $a_1, \dots, a_n$, the resulting sentence is true in $\mathcal{M}$. In particular, if φ is a sentence, then the truth of $\mathcal{M} \vDash \varphi[a_1, \dots, a_n]$ does not depend on $a_1, \dots, a_n$.

Remark 3.37. Before we jump to the technical details, recall that by our convention on page 37 the variables occurring free in φ are among the $x_1, \ldots, x_n$. Since some of the x_is might not be free in φ, then the satisfaction relation does not depend on those a_i. In other words: $\mathcal{M} \vDash \varphi[a_1, \ldots, a_n]$ holds just in case $\mathcal{M} \vDash \varphi[a_{i_1}, \ldots, a_{i_k}]$ holds, where $x_{i_1}, \ldots, x_{i_k}$ are those among $x_1, \ldots, x_n$ that occur free in φ. So why we do not require from the outset that *all* $x_1, \ldots, x_n$ occur free in φ? The reason is that a variable occurring free in a disjunction need not be free in *both* disjuncts, so following this path would only cause notational nuisance. Similarly, if $t(x_1, \ldots, x_n)$ is an $\mathcal{L}$-term and $a_1, \ldots, a_n \in M$, then $t^{\mathcal{M}}(a_1, \ldots, a_n)$ is the element of M defined on page 52, and this element depends only on those $x_{i_1}, \ldots, x_{i_k}$ that actually occur in t; in other words: $t^{\mathcal{M}}(a_1, \ldots, a_n) = t^{\mathcal{M}}(a_{i_1}, \ldots, a_{i_k})$.

The definition of $\mathcal{M} \vDash \varphi[a_1, \ldots, a_n]$ is by induction on the complexity of φ—as usual we will write $\mathcal{M} \nvDash \varphi[a_1, \ldots, a_n]$ to deny that $\mathcal{M} \vDash \varphi[a_1, \ldots, a_n]$ holds.

- If φ is atomic we consider two cases:
  - If $\varphi(x_1, \ldots, x_n)$ is $t(x_1, \ldots, x_n) \doteq s(x_1, \ldots, x_n)$, then
  $$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } t^{\mathcal{M}}(a_1, \ldots, a_n) = s^{\mathcal{M}}(a_1, \ldots, a_n).$$
  - If $\varphi(x_1, \ldots, x_n)$ is $R(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n))$ where R is an k-ary predicate symbol, then
  $$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } (t_1^{\mathcal{M}}[a_1, \ldots, a_n], \ldots, t_k^{\mathcal{M}}[a_1, \ldots, a_n]) \in R^{\mathcal{M}}.$$
- If φ is $\neg\psi$ then
$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \nvDash \psi[a_1, \ldots, a_n].$$
- If φ is $\psi_1 \vee \psi_2$ then
$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \vDash \psi_1[a_1, \ldots, a_n] \text{ or } \mathcal{M} \vDash \psi_2[a_1, \ldots, a_n].$$
- If φ is $\psi_1 \wedge \psi_2$ then
$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \vDash \psi_1[a_1, \ldots, a_n] \text{ and } \mathcal{M} \vDash \psi_2[a_1, \ldots, a_n].$$
- If φ is $\psi_1 \Rightarrow \psi_2$ then
$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if whenever } \mathcal{M} \vDash \psi_1[a_1, \ldots, a_n] \text{ then } \mathcal{M} \vDash \psi_2[a_1, \ldots, a_n].$$

- If φ is $\psi_1 \Leftrightarrow \psi_2$ then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \\ \mathcal{M} \vDash \psi_1[a_1, \ldots, a_n] \text{ exactly when } \mathcal{M} \vDash \psi_2[a_1, \ldots, a_n].$$

- If $\varphi(x_1, \ldots, x_n)$ is $\exists y \psi(x_1, \ldots, x_n, y)$ we consider three cases.
  - The variable y occurs free in ψ, and it is not one of the $x_1, \ldots, x_n$. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \\ \text{there is } b \in M \text{ such that } \mathcal{M} \vDash \psi[a_1, \ldots, a_n, b].$$

  - The variable y occurs free in ψ, and it is x_i. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \\ \text{there is } b \in M \text{ such that } \mathcal{M} \vDash \psi[a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n].$$

  - The variable y does not occur free in ψ. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \vDash \psi[a_1, \ldots, a_n].$$

- If $\varphi(x_1, \ldots, x_n)$ is $\forall y \psi(x_1, \ldots, x_n, y)$ we consider three cases.
  - The variable y occurs free in ψ, and it is not one of the $x_1, \ldots, x_n$. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \vDash \psi[a_1, \ldots, a_n, b], \text{ for every } b \in M.$$

  - The variable y occurs free in ψ, and it is x_i. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \\ \mathcal{M} \vDash \psi[a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n], \text{ for every } b \in M.$$

  - The variable y does not occur free in ψ. Then

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{M} \vDash \psi[a_1, \ldots, a_n].$$

The reader should check that for any $\varphi(x_1, \ldots, x_n)$ and any $a_1, \ldots, a_n \in M$

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \Leftrightarrow (a_1, \ldots, a_n) \in \mathbf{T}^{\mathcal{M}}_{\varphi(x_1, \ldots, x_n)}.$$

Exercises

Exercise 3.38. Let R be a binary relation on some set M. Show that:

- R is a strict preorder on M if and only if R is asymmetric and transitive on M;
- R is a strict order on M if and only if R is irreflexive and transitive on M.

Exercise 3.39. A proposition P as in Definition 3.6 is a finite string of symbols $s_1, s_2, \dots, s_n$. To each P we associate a string of integers $k_1, k_2, \dots, k_n$ keeping track of all parentheses, increasing of 1 each time we encounter (and decreasing of 1 each time we encounter), that is: set $k_0 = 0$, and if $s_i =$ (then $k_i = k_{i-1} + 1$, if $s_i =$) then $k_i = k_{i-1} - 1$, and if $s_i \notin \{(,)\}$, then $k_i = k_{i-1}$. Show that

(i) each P is a string beginning with (and ending with);

(ii) if $k_1, k_2, \dots, k_n$ is associated to some proposition P, then $k_n = 0$ and $k_i > 0$ for $1 \leq i < n$. Moreover if $\mathrm{P} \notin \mathrm{Prop}_0(S)$ its main connective is s_i, where $i \leq n$ is the unique value such that $k_i = k_{i-1}$;

(iii) if $\mathrm{ht}(\mathrm{P}) > 0$ then either $\mathrm{P} = (\neg\mathrm{Q})$ for a unique Q, or else $\mathrm{P} = (\mathrm{Q} \odot \mathrm{R})$ for unique $\odot \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow, \veebar\}$ and Q, R.

Exercise 3.40. Check that the following formulæ are tautologically equivalent:

- $\varphi \wedge (\psi \vee \chi)$ and $(\varphi \wedge \psi) \vee (\varphi \wedge \chi)$,
- $\varphi \vee (\psi \wedge \chi)$ and $(\varphi \vee \psi) \wedge (\varphi \vee \chi)$,
- $\varphi \veebar \psi$, $\neg(\varphi \Leftrightarrow \psi)$, $\varphi \Leftrightarrow \neg\psi$, and $\neg\varphi \Leftrightarrow \psi$,
- $\varphi_1 \Rightarrow (\varphi_2 \Rightarrow \dots (\varphi_n \Rightarrow \psi) \cdots)$ and $(\varphi_1 \wedge \cdots \wedge \varphi_n) \Rightarrow \psi$,
- $(\varphi_1 \Rightarrow \psi) \wedge \cdots \wedge (\varphi_n \Rightarrow \psi)$ and $(\varphi_1 \vee \cdots \vee \varphi_n) \Rightarrow \psi$,
- $(\varphi \Leftrightarrow \psi) \Leftrightarrow \chi$ and $\varphi \Leftrightarrow (\psi \Leftrightarrow \chi)$.

Exercise 3.41. For all sub-formulæ of the formula (3.2) on page 28, find the free and bound occurrences of the variables.

Exercise 3.42. Put in prenex form the following formulæ:

- $\exists y R(y, x) \Rightarrow \exists y\, (R(y, x) \wedge \neg\exists z\, (R(z, y) \wedge R(z, x)))$,
- $\exists x \forall y \exists z P(x, y, z) \vee (\exists x \forall y Q(x, y) \wedge \neg\forall x \exists y R(x, y))$,
- $\forall x \forall y\, (E(x, y) \Leftrightarrow \forall z\, (R(z, x) \Leftrightarrow R(z, y)))$.

For every such formula, compute the complexity of the prefix based on the alternation of quantifiers, as shown on page 42.

Exercise 3.43. Check that the statement "f is a continuous function from $\mathbb{R}$ to $\mathbb{R}$" is formalizable as a $\forall\exists\forall$-formula in the language with symbols f, $+$ and $<$.

Exercise 3.44. Show that if none of the variables that occur quantified in φ are among $x_1, \ldots, x_n$ or among the variables of the terms $t_1, \ldots, t_n$, then $\varphi\llparenthesis t_1/x_1, \ldots, t_n/x_n\rrparenthesis$ is the formula $\varphi[t_1/x_1, \ldots, t_n/x_n]$ obtained by substituting *every* occurrence of x_i with t_i.

Exercise 3.45. Suppose that φ is a Boolean combination of its primitive sub-formulæ $\psi_1, \ldots, \psi_n$, and let φ' be the formula obtained from φ by replacing $\psi_1, \ldots, \psi_n$, with $\psi'_1, \ldots, \psi'_n$. Show that if ψ_i is tautologically equivalent to ψ'_i $(i = 1, \ldots, n)$ then φ is tautologically equivalent to φ'.

Exercise 3.46. Suppose that φ is not a propositional contradiction and that it is a Boolean combination of primitive sub-formulæ $\mathrm{A}_1, \ldots, \mathrm{A}_n$. Let $i_1, \ldots, i_m$ be the rows of the truth table of φ where in the column for φ the value 1 occurs. Check that φ is tautologically equivalent to the disjunction $\mathrm{D}_{i_1} \vee \cdots \vee \mathrm{D}_{i_m}$ where every D_i is the conjunction $\mathrm{C}_{i,1} \wedge \cdots \wedge \mathrm{C}_{i,n}$, where $\mathrm{C}_{i,j}$ is A_j if in the entry of the truth table with coordinates (i, j) there is a 1, or $\neg\mathrm{A}_j$ if there is a 0.

Exercise 3.47. Show that:

(i) the majority connective (see page 10) can be expressed using the connectives $\wedge, \neg$, or the connectives $\vee, \neg$;

(ii) $\{\neg, \Rightarrow\}$, $\{\dot{\vee}, \Rightarrow\}$, and $\{\vee, \Leftrightarrow, \dot{\vee}\}$ are adequate;

(iii) $\{\vee, \wedge, \Leftrightarrow, \Rightarrow\}$, $\{\vee, \wedge, \dot{\vee}\}$, and $\{\neg, \dot{\vee}, \Leftrightarrow\}$ are not adequate;

(iv) **Sheffer's stroke** $|$ and **Peirce's arrow** $\uparrow$ defined by

$$\mathrm{P} \mid \mathrm{Q} \text{ if and only if } \neg\,(\mathrm{P} \wedge \mathrm{Q}) \qquad \mathrm{P} \uparrow \mathrm{Q} \text{ if and only if } \neg\,(\mathrm{P} \vee \mathrm{Q})\,.$$

are the only binary connectives $\odot$ such that $\{\odot\}$ is adequate.

Exercise 3.48. Let $\mathcal{M} = (M, E)$ where E be a binary relation on $M \neq \emptyset$. Show that the following are equivalent:

(1) E is an equivalence relation on M;

(2) E is symmetric and transitive on M, and $\mathcal{M} \vDash \forall x \exists y (x \mathrel{E} y)$;

(3) $\mathcal{M} \vDash \forall x_1, x_2, y_1, y_2 (x_1 \mathrel{E} y_1 \wedge x_2 \mathrel{E} y_2 \wedge x_1 \mathrel{E} x_2 \Rightarrow y_1 \mathrel{E} y_2)$ and E is reflexive on M.

Exercise 3.49. Let $R \subseteq M \times M$. Show that

(i) R is an order on M if and only $((\mathrm{id} \cup (R \mid R)) \cap R^{\complement}) \cup ((R \cap R^{-1}) \cap \mathrm{id}^{\complement}) = \emptyset$;

(ii) R is a total order on M if and only if $((\mathrm{id} \cup (R \mid R)) \cap R^{\complement}) \cup (R \cap R^{-1} \cap \mathrm{id}^{\complement}) \cup (R \cup R^{-1})^{\complement} = \emptyset$;

(iii) R is an equivalence relation on M if and only if $((\mathrm{id} \cup (R \mid R)) \cap R^{\complement}) \cup (R \cap (R^{-1})^{\complement}) = \emptyset$;

(iv) (M, R) is a graph if and only if $R \cap (\mathrm{id} \cup (R^{-1})^{\complement}) = \emptyset$.

Exercise 3.50. Prove the laws of calculus of relations in Table 2.

Exercise 3.51. Show that for all $R, S, T \subseteq M \times M$

$$\begin{aligned}(R \mid S) \cap T = \emptyset &\Leftrightarrow (R^{-1} \mid T) \cap S = \emptyset \\ &\Leftrightarrow (T \mid S^{-1}) \cap R = \emptyset.\end{aligned}$$

Exercise 3.52. Let $\mathcal{L}$ be the language containing a binary relation symbol R. Determine which of the following sentences

$$\begin{aligned}&\sigma_0 : \forall x, y, z\, (x \mathrel{R} y \wedge y \mathrel{R} z \Rightarrow x \mathrel{R} z)\,, && \sigma_3 : \exists x \forall y\, (y \neq x \Rightarrow x \mathrel{R} y)\\ &\sigma_1 : \forall x, y\, (x \mathrel{R} y \Rightarrow \exists z\, (x \mathrel{R} z \wedge z \mathrel{R} y))\,, && \sigma_4 : \exists x \forall y \neg\, (y \mathrel{R} x)\\ &\sigma_2 : \forall x \exists y\, (x \mathrel{R} y \wedge \neg \exists z\, (x \mathrel{R} z \wedge z \mathrel{R} y))\,, && \sigma_5 : \exists x \forall y \neg\, (x \mathrel{R} y)\,.\end{aligned}$$

are true in the structures: $(\mathbb{N}, <)$, $(\mathbb{N}, \leq)$, $(\mathbb{N}, |)$, $(\mathbb{N}, \perp)$, where $|, \perp$ are the divisibility and co-primality relations, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $((0; 1] \cup [2; 3], <)$, $(\mathscr{P}(\mathbb{N}) \setminus \{\emptyset, \mathbb{N}\}, \subset)$, $(\mathbb{S}^2, \perp)$ with $\perp$ the orthogonality relation and $\mathbb{S}^2 = \{\mathbf{x} \in \mathbb{R}^3 \mid \|\mathbf{x}\| = 1\}$.

Exercise 3.53. Find the truth sets of the following formulæ in $(\mathbb{N}, \cdot)$:

(i) $\psi(x)$: $\exists u \forall v\, (v = v \cdot u \wedge x \neq u \wedge \forall y \forall z\, (x = y \cdot z \Rightarrow y = u \vee z = u))$,

(ii) $\varphi(x)$: $\forall y \forall z\, (\psi(y) \wedge \psi(z) \wedge \exists u\, (y \cdot u = x) \wedge \exists u\, (z \cdot u = x) \Rightarrow y = z)$,

(iii) $\varphi_2(x)$: $\exists y\, (x = y \cdot y \wedge \psi(y))$,

(iv) $\chi(x)$: $\exists y \exists z\, (x = y \cdot z \wedge \psi(y) \wedge \psi(z))$.

Exercise 3.54. Determine whether the following sentences are satisfiable, valid, or unsatisfiable:

(i) $\forall x\, (P(x) \Rightarrow Q(x)) \wedge \exists x\, (Q(x) \Rightarrow R(x)) \Rightarrow \forall x\, (P(x) \Rightarrow R(x))$,

(ii) $\forall x\, (P(x) \Rightarrow Q(x)) \wedge \forall x\, (Q(x) \Rightarrow R(x)) \Rightarrow \forall x\, (P(x) \Rightarrow R(x))$,

(iii) $\exists x \exists y\, (P(x) \Rightarrow Q(y)) \Leftrightarrow \exists x\, (P(x) \Rightarrow Q(x))$,

(iv) $\exists x\, P(x) \Rightarrow \exists x\, Q(x) \Rightarrow \exists x\, (P(x) \Rightarrow Q(x))$,

(v) $(\exists x\, P(x) \Rightarrow \exists x\, Q(x)) \Rightarrow \exists x\, (P(x) \Rightarrow Q(x))$,

(vi) $\exists x\, (P(x) \Rightarrow Q(x)) \Rightarrow (\exists x\, P(x) \Rightarrow \exists x\, Q(x))$,

(vii) $(\exists x\, P(x) \Rightarrow \forall x\, \neg Q(x)) \wedge \exists x\, (P(x) \wedge Q(x))$.

Exercise 3.55. Show that:

(i) $\forall \vec{x}\ (\varphi(\vec{x}) \Leftrightarrow \psi(\vec{x})) \Rightarrow (\forall \vec{x}\, \varphi(\vec{x}) \Leftrightarrow \forall \vec{x}\, \psi(\vec{x}))$ is valid;

(ii) $(\forall \vec{x}\, \varphi(\vec{x}) \Leftrightarrow \forall \vec{x}\, \psi(\vec{x})) \Rightarrow \forall \vec{x}\ (\varphi(\vec{x}) \Leftrightarrow \psi(\vec{x}))$ is satisfiable, but not valid;

(iii) for any formula $\varphi(x, y_1, \ldots, y_n)$ the sentence $\forall \vec{y} \exists x \ (\varphi(x, \vec{y}) \Rightarrow \forall x \varphi(x, \vec{y}))$ is valid. (This generalizes Example 2.5.)

Exercise 3.56. Let $\mathcal{L}$ be a language containing only finitely many relational symbols, and let $x_1, x_2, \ldots$ be an enumeration of all variables. (We could have used the list $v_0, v_1, \ldots$ of Section 3.A, but here it is easier to start counting from 1.) Let $\mathrm{Fml}(x_1, \ldots, x_n)$ be the set of all formulæ with free variables among $\{x_1, \ldots, x_n\}$. Let $\Gamma_0(n)$ be the set of all quantifier-free formulæ in $\mathrm{Fml}(x_1, \ldots, x_n)$, and let $\Gamma_m(n)$ be the set of all formulæ in $\mathrm{Fml}(x_1, \ldots, x_n)$ that are in prenex normal form with prefix of length m, that is the prefix has m quantifiers.

Prove by induction on m that for every n there are finitely many formulæ in $\Gamma_m(n)$ that are not equivalent, that is to say: there are $\theta_1, \ldots, \theta_k$ in $\Gamma_m(n)$ for some k such that every φ in $\Gamma_m(n)$ is equivalent to one of the θ_is.

Exercise 3.57. (i) Fix a language $\mathcal{L}$ with a binary operation symbol $*$. The symbol $*$ occurs 4 times in the associative property—see (3.5) on page 30. Is it possible to find an $\mathcal{L}$ equivalent to associativity, in which $*$ occurs less than 4 times? If so, what is the minimum number of occurrences?

(ii) Fix a language $\mathcal{L}$ with a binary relation symbol R. Is it possible to find an $\mathcal{L}$ equivalent the transitive property $\forall x, y, z\, (x \mathrel{R} y \land y \mathrel{R} z \Rightarrow x \mathrel{R} z)$ the uses less than 3 occurrences of the symbol R? If so, what is the minimum number of occurrences?

[Hint: $\varphi(x_1, \ldots, x_n) \Leftrightarrow \forall y_1, \ldots, y_n \, (\bigwedge_{1 \leq i \leq n} y_i = x_i \Rightarrow \varphi(y_1, \ldots, y_n))$.]

Exercise 3.58. Let $\mathcal{L}$ be the language with binary predicate symbols R_q for $q \in \mathbb{Q}_+$.

(i) Find a set Σ of $\mathcal{L}$-sentences such that for any $\mathcal{L}$-structure $\mathcal{M}$,

$$\mathcal{M} \vDash \Sigma \quad \text{if and only if} \quad (M, d) \text{ is a pseudo-metric space}$$

where $d(x, y) < q \Leftrightarrow R_q^{\mathcal{M}}(x, y)$.

(ii) Repeat the preceding part using the language $\mathcal{L}_0$ obtained from $\mathcal{L}$ by adding one further predicate symbol R_0, and by requiring that $d(x, y) \leq q \Leftrightarrow R_q^{\mathcal{M}}(x, y)$.

Notes and remarks

Waring's problem (formula (3.3) on page 29) was formulated in 1770 by Waring and proved in 1909 by Hilbert. Thus one can define $g(k)$ for $k > 1$ as the least n such that every natural number x is sum of n powers of exponent k. The first few values of the function g are 1, 4 (Lagrange), 9, 19, ... [**HW79**]. In number theory, more than $g(k)$ is important to study $G(k)$, that is the least

n such that every sufficiently large natural number x is sum of n powers of exponent k. Clearly $G(k) \leq g(k)$ and it can be shown that $G(2) = g(2) = 4$. The exact value of $G(k)$ for $k \geq 3$ is not known—for example it is known that $4 \leq G(3) \leq 7$, that is every sufficiently large natural number is the sum of at most seven cubes, and that there are arbitrarily large natural numbers that are not sums of three cubes.

The *abc* conjecture (Example 3.4) was formulated in 1988 by Oesterlé and, independently, in 1985 by Masser; for this reason it is also known as the **Oesterlé–Masser conjecture** [**GT02**]. This conjecture, dubbed "the most important open problem in diophantine analysis" [**Gol96**], implies several results in number theory, among which: Fermat's last theorem (Exercise (vii)), the existence of infinitely many non-Wiefeirich primes (Example 2.3), the Erdős-Woods conjecture (Section 2.C.5) with the possible exception of finitely many counterexamples.

4. Morphisms, theories, compactness

First order structures are generalizations of algebraic structures (such as groups, rings, ...) and relational structures (such as orders, graphs, ...). In algebra, after introducing a specific kind of structure, say groups, one defines the notion of subgroup, homomorphism and quotient group, product of groups, and increasing union of groups. In a similar fashion we define what we mean with substructure, morphism and quotient structure, product of structure, increasing union of structures.

4.A. Substructures. Let M be a non-empty set, and let $A \subseteq M$. If f is an n-ary operation on M, we say that A is **closed under** f if $f(a_1, \ldots, a_n) \in A$ for all $a_1, \ldots, a_n \in A$, if $n > 0$, or $\bar{m} \in A$ if $n = 0$ and f is the element $\bar{m} \in M$. The **closure of** X **under** f is the smallest subset of M containing X and closed under f

$$\mathrm{Cl}_f(X) = \bigcap \{Y \subseteq M \mid X \subseteq Y \wedge Y \text{ is closed under } f\}.$$

If $\mathcal{F}$ is a collection of operations on a set M, the **closure of** X **under** $\mathcal{F}$ is the smallest subset of M containing X and closed under all $f \in \mathcal{F}$,

$$\begin{aligned}\mathrm{Cl}_{\mathcal{F}}(X) &= \bigcap \{Y \subseteq M \mid X \subseteq Y \wedge \forall f \in \mathcal{F}\, (Y \text{ is closed under } f)\} \\ &= \textstyle\bigcap_{f \in \mathcal{F}} \mathrm{Cl}_f(X).\end{aligned}$$

Definition 4.1. Given two $\mathcal{L}$-structures $\mathcal{M}$, $\mathcal{N}$ we say that $\mathcal{N}$ is a **substructure** of $\mathcal{M}$ or equivalently $\mathcal{M}$ is a **superstructure** of $\mathcal{N}$, in symbols $\mathcal{N} \subseteq \mathcal{M}$, if N, the universe of $\mathcal{N}$, is contained in M the universe of $\mathcal{M}$ and if

- $R^{\mathcal{N}} = R^{\mathcal{M}} \cap N^k$ for all k-ary relational symbols R,
- $f^{\mathcal{N}} = f^{\mathcal{M}} \restriction N^k$ for all k-ary function symbols f,
- $c^{\mathcal{N}} = c^{\mathcal{M}}$ for all constant symbols c.

In other words, a substructure is determined by a $\emptyset \neq N \subseteq M$ containing the elements $c^{\mathcal{M}}$ and closed under the functions $f^{\mathcal{M}}$; if $\mathcal{L}$ ha only relational symbols, any non-empty subset yields a substructure.

If $X \subseteq M$, the **substructure of $\mathcal{M}$ generated by X** is (the substructure whose universe is)

$$N = \bigcap \left\{ M' \mid X \subseteq M' \subseteq M \wedge M' \text{ is the universe of a substructure of } \mathcal{M} \right\}.$$

The set N is closed under every $f^{\mathcal{M}}$, and every $c^{\mathcal{M}}$ belongs to N, so N is the (universe of the) smallest substructure of $\mathcal{M}$ containing X. In other words: N is the closure of $X \cup \{c^{\mathcal{M}} \mid c \text{ a constant symbol of } \mathcal{L}\}$ under the operations of $\mathcal{M}$. The assumption that X is non-empty is needed to guarantee that the universe of the substructure is non-empty, and it can be removed if $\mathcal{L}$ has constant symbols. In other words an $\mathcal{L}$-structure $\mathcal{M}$ has a least substructure (i.e. a substructure contained in every other substructure of $\mathcal{M}$) if $\mathcal{L}$ has constant symbols. An $\mathcal{L}$-structure is **finitely generated** if it is the substructure generated by a finite subset.

For example, a substructure of an ordered field $(F, +, \cdot, -, <, 0, 1)$ is a subset $R \subseteq F$ containing 0 and 1 and closed under $+, \cdot$ and $-$, that is an ordered ring (although, in general, it is not a field); the substructure of F generated by $\emptyset$ is the prime subring, which is (isomorphic to) $\mathbb{Z}$ if the characteristic of F is 0, or it is $\mathbb{Z}(p)$ if the characteristic of F is a prime number p.

Convention. We will write $\vec{x} \in X$ for $x_1, \ldots, x_n \in X$, where $\vec{x}$ denotes a finite string $(x_1, \ldots, x_n)$. If $F \colon X \to Y$ then $F(\vec{x})$ means $(F(x_1), \ldots, F(x_n))$. If t is a term we write $t(\vec{x})$ to say that the variables occurring in t are among the ones listed in $\vec{x}$.

Proposition 4.2. *If $\mathcal{M}$ is an $\mathcal{L}$-structure generated by a subset $\emptyset \neq D \subseteq M$, then $M = \{t^{\mathcal{M}}(\vec{d}) \mid t \in \mathrm{Term}_{\mathcal{L}} \wedge \vec{d} \in D\}$.*

Proof. Let $N = \{t^{\mathcal{M}}(\vec{d}) \mid t \in \mathrm{Term}_{\mathcal{L}} \wedge \vec{d} \in D\}$. Taking t to be the variable x we see that $D \subseteq N$, and taking t to be a constant symbol c, we see that $c^{\mathcal{M}} \in N$. If f is an n-ary function symbol, then $f^{\mathcal{M}}(t_1^{\mathcal{M}}(\vec{d}), \ldots, t_n^{\mathcal{M}}(\vec{d})) = (f(t_1, \ldots, t_n))^{\mathcal{M}}(\vec{d}) \in N$. Therefore N is the universe of a substructure of $\mathcal{M}$ containing D, and hence $\mathcal{N} = \mathcal{M}$. □

4.B. Morphisms. A **morphism** or **homomorphism** between $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ is a map $F \colon M \to N$ between the universes of the structures that preserves all relations, functions, and constants: if R and g are n-ary relation and function symbols, and c is a constant symbol, then for all $a_1, \ldots, a_n \in M$

(A) if $(a_1, \ldots, a_n) \in R^{\mathcal{M}}$ then $(F(a_1), \ldots, F(a_n)) \in R^{\mathcal{N}}$,

(B) $F(g^{\mathcal{M}}(a_1, \ldots, a_n)) = g^{\mathcal{N}}(F(a_1), \ldots, F(a_n))$,

(C) $F(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

If (A) is strengthened to

(A′) $(a_1, \dots, a_n) \in R^{\mathcal{M}}$ if and only if $(F(a_1), \dots, F(a_n)) \in R^{\mathcal{N}}$

then F is **full**.

The notion of morphism of structures extends at the same time the definition of homomorphism (of groups, rings,...) and the definition of monotone function between ordered sets. If $F\colon \mathcal{M} \to \mathcal{N}$ is a bijective morphism and $F^{-1}\colon \mathcal{N} \to \mathcal{M}$ is also a morphism, then F and F^{-1} are **isomorphisms** and we say that the two structures are isomorphic, in symbols

$$\mathcal{M} \cong \mathcal{N}.$$

A full injective morphism is an **embedding**. We say that $\mathcal{M}$ embeds into $\mathcal{N}$ if there is an embedding $F\colon \mathcal{M} \to \mathcal{N}$.

Remarks 4.3. (a) It is important that a morphism preserves all constants. For example $F\colon \mathbb{Z} \to \mathbb{Z}$, $k \mapsto 0$, is a morphism of the structure $(\mathbb{Z}, +, \cdot, 0)$ in itself (that is: it is a morphism of rngs), but it is not a morphism of $(\mathbb{Z}, +, \cdot, 0, 1)$ in itself (that is: it is not a morphism of rings).

(b) An isomorphism is a bijective morphism, but not conversely. For example: if $<$ is the usual order on the natural numbers and $\prec$ is defined by $n \prec m \Leftrightarrow m = n + 1$, then $\mathrm{id}_{\mathbb{N}}\colon (\mathbb{N}, \prec) \to (\mathbb{N}, <)$ is a bijective morphism, but not an isomorphism. Similarly an embedding is an injective morphism, but not conversely.

(c) If $\mathcal{L}$ has no relation symbols, then any morphism is full. A bijective full morphism is an isomorphism, so in absence relation symbols this definition agrees with the one used in algebra.

(d) If $F\colon \mathcal{M} \to \mathcal{N}$ is a morphism, then $N' = \operatorname{ran} F$ is a non-empty subset of the universe of $\mathcal{N}$ that is closed under any operation $f^{\mathcal{N}}$, with f a function symbol of $\mathcal{L}$. Therefore N' is the universe of $\mathcal{N}'$ a substructure of $\mathcal{N}$ with the relations defined by

$$(b_1, \dots, b_n) \in R^{\mathcal{N}'} \Leftrightarrow (b_1, \dots, b_n) \in R^{\mathcal{N}}$$

R an n-ary relation symbol of $\mathcal{L}$. The requirement that F is full amounts to say that the relations $R^{\mathcal{N}'}$ can be defined by

$$(b_1, \dots, b_n) \in R^{\mathcal{N}'} \Leftrightarrow (a_1, \dots, a_n) \in R^{\mathcal{M}}$$

for some/any $a_1, \dots, a_n \in M$ such that $F(a_i) = b_i$.

If $F\colon \mathcal{M} \to \mathcal{N}$ is a full morphism then the equivalence relation $\sim$ on M given by $a \sim b \Leftrightarrow F(a) = F(b)$ satisfies the following property:

(4.1) If $a_1, \dots, a_n, b_1, \dots, b_n \in M$ and $a_i \sim b_i$ for $1 \leq i \leq n$, then $R^{\mathcal{M}}(a_1, \dots, a_n) \Leftrightarrow R^{\mathcal{M}}(b_1, \dots, b_n)$ and $f^{\mathcal{M}}(a_1, \dots, a_n) \sim f^{\mathcal{M}}(b_1, \dots, b_n)$.

Any equivalence relation satisfying (4.1) is called a **congruence** on the structure $\mathcal{M}$. If $\sim$ is a congruence on $\mathcal{M}$, then the set $N = M/{\sim}$ becomes an $\mathcal{L}$-structure $\mathcal{N}$ by letting

$$\begin{aligned} R^{\mathcal{N}}([a_1], \dots, [a_n]) &\Leftrightarrow R^{\mathcal{M}}(a_1, \dots, a_n), \\ f^{\mathcal{N}}([a_1], \dots, [a_n]) &= [f^{\mathcal{M}}(a_1, \dots, a_n)], \\ c^{\mathcal{N}} &= [c^{\mathcal{M}}], \end{aligned}$$

and $\pi \colon \mathcal{M} \twoheadrightarrow \mathcal{N}$, $a \mapsto [a]$ is a full morphism whose induced congruence is $\sim$. Therefore, any full morphism $F \colon \mathcal{M} \to \mathcal{N}$ can be factored into an embedding j, an isomorphism i, and a full surjective morphism π

$$\begin{tikzcd} \mathcal{M} \arrow[r, "F"] \arrow[d, two heads, "\pi"] & \mathcal{N} \\ \mathcal{M}/{\sim} \arrow[r, "i"] & \operatorname{ran}(F) \arrow[u, "j"] \end{tikzcd}$$

If $F \colon \mathcal{M} \to \mathcal{N}$ is a morphism of $\mathcal{L}$-structure and t is an $\mathcal{L}$-term with variables $x_1, \dots, x_n$, then

$$\forall a_1, \dots a_n \in M \big(F(t^{\mathcal{M}}(a_1, \dots, a_n)) = t^{\mathcal{N}}(F(a_1), \dots, F(a_n)) \big), \tag{4.2}$$

where $t^{\mathcal{M}}$ and $t^{\mathcal{N}}$ are the n-ary functions induced by t (see page 52). Therefore for every morphism $F \colon \mathcal{M} \to \mathcal{N}$:

- if $\varphi(x_1, \dots, x_n)$ is $t_1(x_1, \dots, x_n) = t_2(x_1, \dots, x_n)$ then

  $t_1^{\mathcal{M}}(a_1, \dots, a_n) = t_2^{\mathcal{M}}(a_1, \dots, a_n)$ implies that
  $$t_1^{\mathcal{N}}(F(a_1), \dots, F(a_n)) = t_2^{\mathcal{N}}(F(a_1), \dots, F(a_n)),$$
- if $\varphi(x_1, \dots, x_n)$ is $P(t_1(x_1, \dots, x_n), \dots, t_k(x_1, \dots, x_n))$ then

  $\left(t_1^{\mathcal{M}}(a_1, \dots, a_n), \dots, t_k^{\mathcal{M}}(a_1, \dots, a_n)\right) \in P^{\mathcal{M}}$ implies that
  $$\left(t_1^{\mathcal{N}}(F(a_1), \dots, F(a_n)), \dots, t_k^{\mathcal{N}}(F(a_1), \dots, F(a_n))\right) \in P^{\mathcal{N}}.$$

All this can be stated more succinctly as: *every morphism preserves atomic formulæ.*

Definition 4.4. A morphism $F \colon \mathcal{M} \to \mathcal{N}$ of $\mathcal{L}$-structures preserves a formula $\varphi(x_1, \dots, x_n)$ if and only if for all $a_1, \dots, a_n \in M$

$$\mathcal{M} \vDash \varphi[a_1, \dots, a_n] \text{ implies that } \mathcal{N} \vDash \varphi[F(a_1), \dots, F(a_n)].$$

In other words: the image via F of the truth set of φ computed in $\mathcal{M}$ is contained in the truth set of φ computed in $\mathcal{N}$,

$$\begin{aligned} F[\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}] &\overset{\text{def}}{=} \{(F(a_1), \dots, F(a_n)) \mid (a_1, \dots, a_n) \in \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}\} \\ &\subseteq \mathbf{T}^{\mathcal{N}}_{\varphi(x_1,\dots,x_n)}. \end{aligned}$$

Remarks 4.5. (a) If $F\colon \mathcal{M} \to \mathcal{N}$ is a morphism, then by (3.17a) F preserves φ and $\neg\varphi$ if and only if $F[\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}] = \mathbf{T}^{\mathcal{N}}_{\varphi(x_1,\dots,x_n)} \cap \operatorname{ran} F$, that is

$$\mathcal{M} \vDash \varphi[a_1,\dots,a_n] \text{ if and only if } \mathcal{N} \vDash \varphi[F(a_1),\dots,F(a_n)].$$

(b) Every morphism preserves the formula $x_1 = x_2$; a morphism F preserves the formula $x_1 \neq x_2$ if and only if F is injective.

Proposition 4.6. *Let $F\colon \mathcal{M} \to \mathcal{N}$ be a morphism.*

(a) *If F preserves φ and ψ, then it preserves also $\varphi \wedge \psi$ and $\varphi \vee \psi$.*

(b) *If F is an embedding then it preserves all quantifier-free formulæ.*

(c) *If F preserves φ, then it also preserves $\exists x \varphi$.*

(d) *If F is surjective and preserves φ, then it also preserves $\forall x \varphi$.*

(e) *If F is an isomorphism, then it preserves every formula.*

Proof. (a) follows from (3.17b) and (3.17c).

(b) Suppose F is an embedding. Let us check by induction on the height of a quantifier-free formula φ that

$$\mathcal{M} \vDash \varphi[a_1,\dots,a_n] \text{ if and only if } \mathcal{N} \vDash \varphi[F(a_1),\dots,F(a_n)].$$

The result holds at once of φ is atomic. The case when φ is $\neg\psi$ follows from Remark 4.5(a). Suppose φ is $\psi_1 \odot \psi_2$ with $\odot$ a binary connective. If $\odot$ is either $\vee$ or $\wedge$ then apply part (a), if $\odot$ is either $\Rightarrow$ or $\Leftrightarrow$ use (3.17d) and (3.17e).

(c) Suppose F preserves $\varphi(x,\vec{y})$ and that $\mathcal{M} \vDash \exists x \varphi[\vec{a}]$. Then $\mathcal{M} \vDash \varphi[b,\vec{a}]$ for some $b \in M$, so that $\mathcal{N} \vDash \varphi[F(b),F(\vec{a})]$ and therefore $\mathcal{N} \vDash \exists x \varphi[F(\vec{a})]$.

(d) We must show that if $\mathcal{M} \vDash \forall x \varphi[\vec{a}]$ then $\mathcal{N} \vDash \varphi[c,F(\vec{a})]$ for every $c \in N$. Fix such c and let $b \in M$ be such that $F(b) = c$. By assumption $\mathcal{M} \vDash \varphi[b,\vec{a}]$ so $\mathcal{N} \vDash \varphi[F(b),F(\vec{a})]$ as F preserves φ, and this is what we had to prove.

(e) As in part (b) we argue by induction on the height of φ that F preserves φ and $\neg\varphi$. The case when φ is atomic or Boolean combination of formulæ is as before, so we may assume that φ begins with a quantifier, e.g. $\exists x \psi$, and that F preserves ψ and $\neg\psi$. By part (c) and inductive assumption $\mathcal{M} \vDash \varphi[\vec{a}]$ implies $\mathcal{N} \vDash \varphi[F(\vec{a})]$. For the converse argue as follows. Suppose $\mathcal{M} \nvDash \varphi[\vec{a}]$, that is $\mathcal{M} \vDash \forall x \neg\psi[\vec{a}]$. By inductive assumption F preserves $\neg\psi$, so $\mathcal{N} \vDash \forall x \neg\psi[F(\vec{a})]$ by part (d), and therefore $\mathcal{N} \nvDash \varphi[F(\vec{a})]$. □

Therefore surjective morphisms preserve the **positive formulæ**, i.e. those formulæ obtained from atomic formulæ by means of quantifiers and the connectives $\wedge$ and $\vee$. In particular:

Proposition 4.7. *If $F\colon \mathcal{M} \to \mathcal{N}$ is a surjective morphism and $\mathcal{M} \vDash \sigma$, where σ is a positive sentence, then $\mathcal{N} \vDash \sigma$.*

The homomorphic image of a group, of an abelian group, of a ring, ... is a group, an abelian group, a ring, ..., but the homomorphic image of an integral domain need not be an integral domain since $\forall x, y (x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0)$ is not positive. Therefore Proposition 4.7 cannot be generalized to all formulæ.

If $\mathcal{M}$ is a substructure of $\mathcal{N}$, then inclusion $\mathcal{M} \hookrightarrow \mathcal{N}$ is a morphism and hence for every *atomic formula* φ and every $a_1, \dots, a_n \in M$

$$\mathcal{M} \vDash \varphi[a_1, \dots, a_n] \text{ if and only if } \mathcal{N} \vDash \varphi[a_1, \dots, a_n]$$

that is $\mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^{\mathcal{N}}_{\varphi(x_1,\dots,x_n)} \cap M^n$. Applying the identities (3.17) on page 60 and proceeding by induction on the complexity of φ, the equality above can be generalized to all *quantifier-free* φ. Applying the identity (3.18) we obtain:

Proposition 4.8. *Let $\mathcal{M}$ be a substructure of $\mathcal{N}$ and let $\varphi(x_1, \dots, x_n)$ be a quantifier-free formula. Then*

- *if $\mathcal{N} \vDash \forall x_1, \dots, x_n \varphi$ then $\mathcal{M} \vDash \forall x_1, \dots, x_n \varphi$, and*
- *if $\mathcal{M} \vDash \exists x_1, \dots, x_n \varphi$ then $\mathcal{N} \vDash \exists x_1, \dots, x_n \varphi$.*

Therefore, if T is axiomatized by universal sentences, then it is preserved by taking substructures, that is: if $\mathcal{M}$ is a substructure of $\mathcal{N}$ and $\mathcal{N} \vDash T$ then $\mathcal{M} \vDash T$. In particular: if $M \subseteq N$ and $R \subseteq N \times N$ is an order (or a linear order, or an equivalence relation) on N, then $R \cap M \times M$ is an order (or a linear order, or an equivalence relation) on M.

Proposition 4.8 admits a converse: if T is a theory such that if $\mathcal{M} \vDash T$ then $\mathcal{N} \vDash T$ for every $\mathcal{N}$ substructure of $\mathcal{M}$, then T admits an axiom system made of universal sentences—see Theorem 31.13.

4.C. Relational theories. Given a language $\mathcal{L}$, let $\mathcal{L}^{\text{rel}}$ be the language with only predicate symbols defined as follows:

- all predicate symbols of $\mathcal{L}$ are in $\mathcal{L}^{\text{rel}}$,
- an $n+1$-ary predicate symbol R_f for each n-ary function symbol f of $\mathcal{L}$,
- a unary predicate symbol R_c for each constant symbol c of $\mathcal{L}$.

For example, if $\mathcal{L} = \mathcal{L}_{\text{ORings}}$ is the language of ordered rings, then $\mathcal{L}^{\text{rel}}$ has the following relation symbols: $\leq, R_+, R_\times, R_0, R_1$. The theory of ordered rings can be re-written in $\mathcal{L}^{\text{rel}}$. First of all we have axioms stating that R_+ and $R_\times$ define binary operations and that R_0 and R_1 define singletons

$$\forall x_1, x_2 \exists! y R_+(x_1, x_2, y) \wedge \forall x_1, x_2 \exists! y R_\times(x_1, x_2, y) \wedge \exists! y R_0(y) \wedge \exists! y R_1(y).$$

Then each axiom of the theory of ordered rings T_{ORings} is transformed into a sentence of $\mathcal{L}^{\mathrm{rel}}$. The axioms for linear orders do not need any cosmetic changes, but the axioms involving the symbols $+$ and $\cdot$ need some makeover. For example commutativity and associativity of $+$ can be written as the universal closures of

$$R_+(x_1, x_2, y) \Rightarrow R(x_2, x_1, y)$$
$$R_+(x_1, x_2, y_1) \wedge R_+(y_1, x_3, y_2) \wedge R_+(x_2, x_3, y_3) \Rightarrow R(x_1, y_3, y_2).$$

This procedure is completely general: any $\mathcal{L}$-theory can be turned into an $\mathcal{L}^{\mathrm{rel}}$-theory, and any $\mathcal{L}$-structure $\mathcal{M}$ can be transformed into an $\mathcal{L}^{\mathrm{rel}}$-structure $\mathcal{M}^{\mathrm{rel}}$.

4.D. Products. The **product of two $\mathcal{L}$-structures** $\mathcal{M}_0$ and $\mathcal{M}_1$ is the $\mathcal{L}$-structure $\mathcal{M}_0 \times \mathcal{M}_1$ having $M_0 \times M_1$ as domain, and defined by:

- if R is an n-ary relation symbol, then $R^{\mathcal{M}_0 \times \mathcal{M}_1} \subseteq (M_0 \times M_1)^n$ is defined by
$$((a_1, b_1), \ldots, (a_n, b_n)) \in R^{\mathcal{M}_0 \times \mathcal{M}_1} \quad \text{if and only if} \quad (a_1, \ldots, a_n) \in R^{\mathcal{M}_0} \text{ and } (b_1, \ldots, b_n) \in R^{\mathcal{M}_1},$$
- if f is an n-ary function symbol, then $f^{\mathcal{M}_0 \times \mathcal{M}_1} \colon (M_0 \times M_1)^n \to M_0 \times M_1$ is defined by
$$f^{\mathcal{M}_0 \times \mathcal{M}_1}\big((a_1, b_1), \ldots, (a_n, b_n)\big) = \big(f^{\mathcal{M}_0}(a_1, \ldots, a_n), f^{\mathcal{M}_1}(b_1, \ldots, b_n)\big),$$
- $c^{\mathcal{M}_0 \times \mathcal{M}_1} = (c^{\mathcal{M}_0}, c^{\mathcal{M}_1})$.

It is easy to check that the maps

$$\pi_0 \colon \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{M}, (a, b) \mapsto a \quad \text{and} \quad \pi_1 \colon \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{M}_1, (a, b) \mapsto b$$

are full morphisms, and that for any $\mathcal{L}$-structure $\mathcal{N}$ and any choice of (full) morphisms $F_i \colon \mathcal{N} \to \mathcal{M}_i$ $(i = 0, 1)$ the map $\mathcal{N} \to \mathcal{M}_0 \times \mathcal{M}_1$, $x \mapsto (F_0(x), F_1(x))$ is a (full) morphism, and it is the unique (full) morphism $H \colon \mathcal{N} \to \mathcal{M}_0 \times \mathcal{M}_1$ such that the following diagram commutes

$$\begin{tikzcd}
 & \mathcal{M}_0 & \\
\mathcal{N} \arrow[ur, "F_0"] \arrow[rr, "H"] \arrow[dr, "F_1"'] & & \mathcal{M}_0 \times \mathcal{M}_1 \arrow[ul, "\pi_0"'] \arrow[dl, "\pi_1"] \\
 & \mathcal{M}_1 &
\end{tikzcd}$$

The construction of the cartesian product of structures can be generalized to an arbitrary family of factors: if $\mathcal{M}_j$ are $\mathcal{L}$-structures, $\prod_{j \in J} \mathcal{M}_j$ is the

$\mathcal{L}$-structure $\mathcal{M}$ with universe

$$\bigtimes_{j\in J} M_j = \{h \mid h \text{ is a function, } \operatorname{dom} h = I \text{ and } h(i) \in M_i, \text{ for all } i \in I\}$$

where for all $h_1, \dots, h_n \in \bigtimes_{j\in J} M_j$ and every n-ary relational symbol R

$$(h_1, \dots, h_n) \in R^{\mathcal{M}} \Leftrightarrow \forall j \in J\,[(h_1(j), \dots, h_n(j)) \in R^{\mathcal{M}_j}],$$

and similarly for the function and constant symbols. The only problem is to check that the set $\bigtimes_{j\in J} M_j$ is non-empty. In most cases this is easy, for example if the language has constant symbols, this immediate. On the other hand, there are cases when the problem is more tricky, since the statement that the cartesian product of non-empty sets is non-empty is equivalent to an important set theoretic principle, the axiom of choice (Section 14).

If $\mathcal{L}$ is the language with a binary relation symbol R and $\mathcal{M} = (M, R^{\mathcal{M}})$ and $\mathcal{N} = (N, R^{\mathcal{N}})$ are $\mathcal{L}$-structures, then $\mathcal{M} \times \mathcal{N} = (M \times N, R^{\mathcal{M}\times\mathcal{N}})$, where for all $(a, b), (c, d) \in M \times N$,

$$(a, b)\ R^{\mathcal{M}\times\mathcal{N}}\ (c, d) \quad \text{if and only if} \quad a\ R^{\mathcal{M}}\ c \text{ and } b\ R^{\mathcal{M}}\ d.$$

If $\mathcal{M}$, $\mathcal{N}$ are ordered sets, then so is $\mathcal{M} \times \mathcal{N}$ and $R^{\mathcal{M}\times\mathcal{N}}$ is called the **product ordering** on $M \times N$. Observe that the product ordering of two linear orders is never linear (unless one of the two orders is a singleton)—for example if $\mathcal{M}$, $\mathcal{N}$ are linear orders of size 2 and 3, then $\mathcal{M} \times \mathcal{N}$ is the first ordering in Figure 6 on page 47. For this reason when dealing with linear orders it is often useful to endow the cartesian product with a different ordering.

Definition 4.9. Suppose $(L_0, \leq_0)$ and $(L, \leq_1)$ are linear orders. The **lexicographic order $\leq_{\text{lex}}$ on** $L_0 \times L_1$ is defined by

$$(a, b) \leq_{\text{lex}} (c, d) \Leftrightarrow (a \leq_0 c \wedge a \neq c) \vee (a = c \wedge b \leq_1 d).$$

The **antilexicographic order** $\leq_{\text{a-lex}}$ is induced by the bijection $L_0 \times L_1 \to L_1 \times L_0$, $(a, b) \mapsto (b, a)$ when $L_1 \times L_0$ is endowed with the lexicographic order, that is

$$(a, b) \leq_{\text{a-lex}} (c, d) \Leftrightarrow (b \leq_0 d \wedge b \neq d) \vee (b = d \wedge a \leq_1 c).$$

The orders $\leq_{\text{lex}}$ and $\leq_{\text{a-lex}}$ are linear, and will play an important in the rest of this book.

We have argued that even if $\mathcal{M}, \mathcal{N}$ satisfy $\forall x, y(x\ R\ y \vee y\ R\ x)$, this sentence need not to hold in $\mathcal{M} \times \mathcal{N}$. Therefore positive sentences are not preserved under products. On the contrary, sentences of the form

$$\forall x_1, \dots, x_n\, (t(x_1, \dots, x_n) = s(x_1, \dots, x_n)) \tag{4.3}$$

where t and s are terms, are preserved by products. In fact if $\mathcal{M}$ and $\mathcal{N}$ satisfy a sentence of this kind, then for all $(a_1, b_1), \dots, (a_n, b_n) \in M \times N$

$$\begin{aligned} t^{\mathcal{M}\times\mathcal{N}}((a_1, b_1), \dots, (a_n, b_n)) &= \bigl(t^{\mathcal{M}}(a_1, \dots, a_n), t^{\mathcal{N}}(b_1, \dots, b_n)\bigr) \\ &= \bigl(s^{M}(a_1, \dots, a_n), s^{\mathcal{N}}(b_1, \dots, b_n)\bigr) \\ &= s^{\mathcal{M}\times\mathcal{N}}((a_1, b_1), \dots, (a_n, b_n)). \end{aligned}$$

Definition 4.10. Let $\mathcal{L}$ be a language without relational symbols. An $\mathcal{L}$-theory is **equational** if it can be axiomatized by sentences of the form (4.3). Since a formula is equivalent to its universal closure (see page 37), a theory is equational just in case it has a system of axioms made of **identities**, i.e. formulæ of the form

$$t(x_1, \dots, x_n) \doteq s(x_1, \dots, x_n)$$

where t and s are terms.

The collection of all models of an equational theory is called **equational class** or a **variety**. An equational theory (and the corresponding variety) is 1**-based** if it is axiomatized by a single identity.

Remark 4.11. The theory of groups (p. 53) and the theory of rings (p. 54) are examples of equational theories. It can be shown that the theory of groups is 1-based; in fact every sub-variety of the equational variety of groups is 1-based.

Since the formulæ (4.3) are universal, by what we said above, and by (4.2), we obtain:

Proposition 4.12. *An equational theory T is preserved by taking substructures, homomorphic images, and products, that is:*

(a) *if $\mathcal{M} \vDash T$ and $F \colon \mathcal{M} \twoheadrightarrow \mathcal{N}$ is a surjective morphism, then $\mathcal{N} \vDash T$,*

(b) *if $\mathcal{M} \vDash T$ and $\mathcal{N} \subseteq \mathcal{M}$ is a substructure, then $\mathcal{N} \vDash T$,*

(c) *if $\mathcal{M}_j \vDash T$ for all $j \in J$, then $\prod_{j\in J} \mathcal{M}_j \vDash T$.*

In other words, a variety is closed under homomorphic images, substructures, and products.

A theorem of Birkhoff's asserts the converse, that is: if $\mathcal{L}$ is a language without relation symbols and $\mathscr{C}$ is a class of $\mathcal{L}$-structures closed under homomorphic images, substructures, and products, then it is a variety, that is it is the class of all models of some system of equations [**Ber12**, Theorem 4.41].

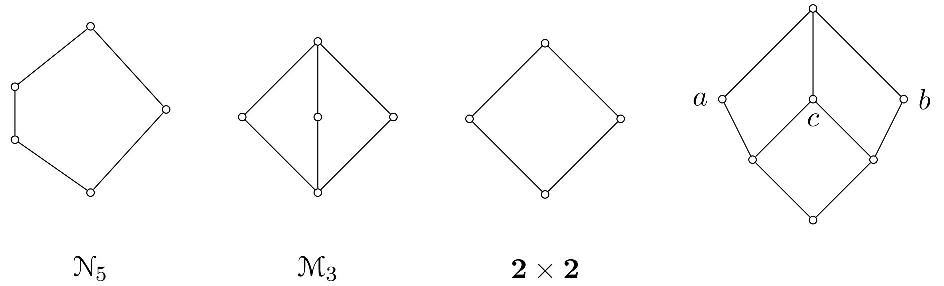


Figure 7. Some finite lattices.

4.E. A first look at lattices. Most algebraic objects can be seen as $\mathcal{L}$-structures with $\mathcal{L}$ containing only constant and function symbols, while objects stemming from combinatorics or order-theory are best described as $\mathcal{L}$-structures where $\mathcal{L}$ has only relation symbols.

Lattices were briefly introduced on page 45 and will show-up again in Section 7. They are interesting mathematical objects that can be seen either as orders with specific properties, or else as algebraic structures. For this reason lattices can be studied with different first order languages, and axioms, enabling us to use various tools and techniques.

Recall that an $\mathcal{L}_{\mathrm{ORDR}}$-structure $(M, \leq)$ is an **upper semi-lattice** if every pair of elements admits a sup, that is it satisfies

$$\forall x \, \forall y \, \exists z \; (x \leq z \wedge y \leq z \wedge \forall w \, (x \leq w \wedge y \leq w \Rightarrow z \leq w))$$

and it is a **lower semi-lattice** if every pair of elements admits an inf, that is it satisfies

$$\forall x \, \forall y \, \exists z \; (z \leq x \wedge z \leq y \wedge \forall w \, (w \leq x \wedge w \leq y \Rightarrow w \leq z)) \, .$$

A **lattice** is an ordered set which is an upper and lower semi-lattice. Therefore lattices can be seen as order satisfying certain $\mathcal{L}_{\mathrm{ORDR}}$-sentences. The element $\sup(a, b)$ is also called the **join** of a, b, while $\inf(a, b)$ is called the **meet** of a, b, and they are denoted by

$$a \curlyvee b \qquad \text{and} \qquad a \curlywedge b$$

respectively. Figure 7 shows a few finite lattices that are not linear orders.

Remark 4.13. In lattice theory, the standard notation for join and meet is $a \vee b$ and $a \wedge b$. The reason we adopted the non-standard notation $\curlyvee$ and $\curlywedge$ is that $\vee$ and $\wedge$ are already used for disjunction and conjunction.

Join and meet are binary operation on lattice satisfying the following properties: associativity

$$\forall x, y, z\,(x \curlyvee (y \curlyvee z) \eqcirc (x \curlyvee y) \curlyvee z) \tag{4.4a}$$

$$\forall x, y, z\,(x \curlywedge (y \curlywedge z) \eqcirc (x \curlywedge y) \curlywedge z), \tag{4.4b}$$

commutativity

$$\forall x, y\,(x \curlyvee y \eqcirc y \curlyvee x) \tag{4.5a}$$

$$\forall x, y\,(x \curlywedge y \eqcirc y \curlywedge x), \tag{4.5b}$$

the **absorption laws**, that is

$$\forall x, y\,((x \curlyvee y) \curlywedge y \eqcirc y) \tag{4.6a}$$

$$\forall x, y\,((x \curlywedge y) \curlyvee y \eqcirc y). \tag{4.6b}$$

Equations (4.4)–(4.6) are formulated in the **language for lattices** $\mathcal{L}_{\mathrm{LTC}}$ containing two binary operations $\curlywedge$ and $\curlyvee$.

Proposition 4.14. *Let $\mathcal{A} = (A, \curlyvee, \curlywedge)$ be an $\mathcal{L}_{LTC}$-structure satisfying* (4.4)–(4.6).

(a) *The operations $\curlywedge$ and $\curlyvee$ are idempotent, that is to say*

$$\mathcal{A} \vDash \forall x (x \eqcirc x \curlyvee x \wedge x \eqcirc x \curlywedge x)$$

(b) $\mathcal{A} \vDash \forall x, y\,(x \curlyvee y \eqcirc y \Leftrightarrow x \curlywedge y \eqcirc x)$*,*

(c) *the relation $\preceq$ defined on A by*

$$a \preceq b \Leftrightarrow a \curlyvee b = b \Leftrightarrow a \curlywedge b = a$$

is an ordering, and $(A, \preceq)$ is a lattice such that $\sup(a, b) = a \curlyvee b$ *and* $\inf(a, b) = a \curlywedge b$*.*

Proof. (a) By commutativity and absorption $a = a \curlywedge (a \curlyvee a)$ so by absorption again $a \curlyvee a = a \curlyvee (a \curlywedge (a \curlyvee a)) = a$. Similarly $a \curlywedge a = a \curlywedge (a \curlyvee (a \curlywedge a)) = a$.

(b) If $a \curlyvee b = b$ then $a \curlywedge b = a \curlywedge (a \curlyvee b) = a$ by absorption and commutativity. If $a \curlywedge b = a$ then $a \curlyvee b = (a \curlywedge b) \curlyvee b = b \curlyvee (b \curlywedge a) = a$ by commutativity and absorption.

(c) Reflexivity follows from idempotence. Suppose $a \preceq b$ and $b \preceq a$, that is $a \curlywedge b = a$ and $b \curlyvee a = a$: then $a = (b \curlyvee a) \curlywedge b = b \curlywedge (b \curlyvee a) = b$ by absorption. Hence antisymmetry holds. Suppose $a \preceq b$ and $b \preceq c$, that is $a = a \curlywedge b$ and $b = b \curlywedge c$: then

$$a \curlywedge c = (a \curlywedge b) \curlywedge c = a \curlywedge (b \curlywedge c) = a \curlywedge b = a,$$

hence transitivity holds.

By commutativity and idempotence $a \curlywedge b \preceq a, b$ and if $c \preceq a, b$, that is $c \curlywedge a = c$ and $c \curlywedge b = c$, then $c \curlywedge (a \curlywedge b) = (c \curlywedge a) \curlywedge b = c \curlywedge b = c$, that is $c \preceq a \curlywedge b$. This shows that $\inf(a, b) = a \curlywedge b$. Similarly $a \curlyvee b = \sup(a, b)$. □

Because of this equivalence, from now we will identify the relational notion of lattice (that is an order admitting sups and infs) and the algebraic notion of an $\mathcal{L}_{\mathrm{LTC}}$-structure satisfying (4.4)–(4.6). This equivalence shows that the same class of objects can be axiomatized using distinct languages. The axiomatization in the language $\mathcal{L}_{\mathrm{LTC}}$ is an equational theory, hence by Proposition 4.12 the family of lattices is closed by substructures, homomorphic images, and products. On the other hand in the language $\mathcal{L}_{\mathrm{ORDR}}$ there is neither equational nor universal axiomatization for lattices, since a subset of a lattice is an ordered set, but not necessarily a lattice. Part (c) of Proposition 4.14 shows that the two operations $\curlywedge$ and $\curlyvee$ are interdependent: if $(A, \curlyvee, \curlywedge_1)$ and $(A, \curlyvee, \curlywedge_2)$ are lattices, then $\curlywedge_1$ agrees with $\curlywedge_2$. Similarly, if $(A, \curlyvee_1, \curlywedge)$ and $(A, \curlyvee_2, \curlywedge)$ are lattice, then $\curlyvee_1$ agrees with $\curlyvee_2$.

A **sublattice** of a lattice $(L, \leq)$ is an $L' \subseteq L$ such that $\sup(a, b)$, $\inf(a, b)$ computed in L belong to L', for all $a, b \in L'$—this is more than requiring that L' with the induced order is a lattice. In other words: a sublattice is an $\mathcal{L}_{\mathrm{LTC}}$-substructure.

The operations $\curlywedge$ and $\curlyvee$ are monotone, that is if $x \leq x'$ and $y \leq y'$, then $x \curlywedge y \leq x' \curlywedge y'$ and $x \curlyvee y \leq x' \curlyvee y'$. Therefore $x \curlywedge y \leq x \curlywedge (y \curlyvee z)$ and $x \curlywedge z \leq x \curlywedge (y \curlyvee z)$, so that $(x \curlywedge y) \curlyvee (x \curlywedge z) \leq x \curlywedge (y \curlyvee z)$. Similarly $x \leq (x \curlyvee y) \curlywedge (x \curlyvee z)$ and $y \curlywedge z \leq (x \curlyvee y) \curlywedge (x \curlyvee z)$, and hence $x \curlyvee (y \curlywedge z) \leq (x \curlyvee y) \curlywedge (x \curlyvee z)$. A lattice is **distributive** if these inequalities can be replaced by equalities, that is if it satisfies the statements

$$\forall x, y, z \, ((x \curlyvee y) \curlywedge z \eqcirc (x \curlywedge z) \curlyvee (y \curlywedge z)) \tag{4.7a}$$

$$\forall x, y, z \, ((x \curlywedge y) \curlyvee z \eqcirc (x \curlyvee z) \curlywedge (y \curlyvee z)) \tag{4.7b}$$

Every family $\mathcal{S}$ of subsets of a given set, closed under intersections and unions is a distributive lattice, and by Exercises 7.96 and 15.12 all distributive lattices are isomorphic to such an $\mathcal{S}$.

Not every lattice is distributive. For example the five element lattices $\mathcal{M}_3$ and $\mathcal{N}_5$ in Figure 7 on page 78 are the first examples of non-distributive lattices. Another example of a non-distributive lattice is the family of subspaces of a vector space of dimension ≥ 2. This last example suggests the following definition: a lattice is **modular** if it satisfies the next two sentences, called the **modular law**

$$\forall x, y, z \, ((x \curlywedge y) \curlyvee (x \curlywedge z) \eqcirc x \curlywedge (y \curlyvee (x \curlywedge z))) \tag{4.8a}$$

$$\forall x, y, z \, ((x \curlyvee y) \curlywedge (x \curlyvee z) \eqcirc x \curlyvee (y \curlywedge (x \curlyvee z))) \,. \tag{4.8b}$$

Every distributive lattice is modular, but not conversely: the lattice $\mathcal{N}_5$ is not modular, while $\mathcal{M}_3$ is modular, but not distributive (Exercise 4.69).

The following result characterizes distributive and modular lattices—for a proof see [**BS81**, pp. 14–15] or [**Ber12**, pp. 26–27].

Theorem 4.15. (a) *A lattice is modular if and only if it does not contain* $\mathcal{N}_5$ *as a sublattice.*

(b) *A lattice is distributive if and only if it contains neither* $\mathcal{N}_5$ *nor* $\mathcal{M}_3$ *as sublattice.*

The fourth lattice of Figure 7 contains $\mathcal{N}_5$ as a sublattice, so it is not modular, and hence not distributive.

Remark 4.16. By Exercise (4.68) a lattice is modular if it satisfies at least one of the two conditions (4.8); similarly, in order to check that a lattice is distributive it is enough to check one of the two conditions (4.7). These conditions can be further weakened: a lattice is distributive if it satisfies either one of

$$\forall x, y, z\big((x \curlyvee y) \curlywedge (x \curlyvee z) \leq x \curlyvee (y \curlywedge z)\big)$$
$$\forall x, y, z\big(x \curlywedge (y \curlyvee z) \leq (x \curlywedge y) \curlyvee (x \curlywedge z)\big).$$

Similarly the definition of modularity can be weakened to either one of

$$\forall x, y, z\,((x \curlywedge y) \curlyvee (x \curlywedge z) \leq x \curlywedge (y \curlyvee (x \curlywedge z)))$$
$$\forall x, y, z\,(z \leq x \Rightarrow x \curlywedge (y \curlyvee z) \leq (x \curlywedge y) \curlyvee z)\,.$$

The axioms for lattices, the modular law, the distributive properties are equations, hence they are preserved by taking substructures and homomorphic images, and products (Proposition 4.12).

A **Boolean algebra** B is a distributive lattice with distinguished elements $\mathbf{0}$ and $\mathbf{1}$, and a unary operation $b \mapsto b^*$ such that $b \curlywedge b^* = \mathbf{0}$ and $b \curlyvee b^* = \mathbf{1}$, and $b \curlywedge \mathbf{1} = b$ and $b \curlyvee \mathbf{0} = b$, for all $b \in B$. Boolean algebras are finitely axiomatizable in the language $\mathcal{L}_{\mathrm{Boole}}$ extending $\mathcal{L}_{\mathrm{Ltc}}$ with a unary function symbol * and two constant symbols $\mathbf{0}$ and $\mathbf{1}$. Recall that in any lattice, and hence in any Boolean algebra, the order is defined by $b \leq c \Leftrightarrow b \curlywedge c = b \Leftrightarrow b \curlyvee c = c$, so that $\mathbf{0}$ is the minimum and $\mathbf{1}$ is the maximum. A Boolean algebra is non-degenerate if it has at least two elements—equivalently if it satisfies $\mathbf{0} \neq \mathbf{1}$.

The element b^* is the **complement** of b, and it is the unique element c in the Boolean algebra such that $b \curlywedge c = \mathbf{0}$ and $b \curlyvee c = \mathbf{1}$. In fact this is true in any distributive lattice.

Lemma 4.17. *Let* x, y, z *be elements of a distributive lattice with minimum* $\mathbf{0}$ *and maximum* $\mathbf{1}$*, such that* $x \curlywedge y = x \curlywedge z = \mathbf{0}$ *and* $x \curlyvee y = x \curlyvee z = \mathbf{1}$*. Then* $y = z$*.*

Proof. $y = \mathbf{1} \curlywedge y = (x \curlyvee z) \curlywedge y = (x \curlywedge y) \curlyvee (z \curlywedge y) = \mathbf{0} \curlyvee (y \curlywedge z) = y \curlywedge z$, whence $y \leq z$. Swapping y and z the other inequality $z \leq y$ is obtained. □

Lemma 4.18. *In a Boolean algebra the following properties hold:*

(a) $x \curlywedge y = \mathbf{0} \Leftrightarrow x \leq y^*$;

(b) $(x \curlywedge y)^* = x^* \curlyvee y^*$ *and* $(x \curlyvee y)^* = x^* \curlywedge y^*$ *(De Morgan's laws);*

(c) $x \leq y \Leftrightarrow y^* \leq x^*$;

(d) $x \curlywedge y \leq z \Leftrightarrow x \leq z \curlyvee y^*$.

Proof. (a) Suppose $x \curlywedge y = \mathbf{0}$. Then

$$x = x \curlywedge (y \curlyvee y^*) = (x \curlywedge y) \curlyvee (x \curlywedge y^*) = \mathbf{0} \curlyvee (x \curlywedge y^*) = x \curlywedge y^*$$

that is $x \leq y^*$. Conversely, suppose $x \leq y^*$. Then $x \curlywedge y \leq y$ and $x \curlywedge y \leq x \leq y^*$ and hence $x \curlywedge y \leq y \curlywedge y^* = \mathbf{0}$, that is $x \curlywedge y = \mathbf{0}$.

(b) By distributivity

$$(x^* \curlyvee y^*) \curlywedge (x \curlywedge y) = (x^* \curlywedge (x \curlywedge y)) \curlyvee (y^* \curlywedge (x \curlywedge y)) = \mathbf{0}$$
$$(x^* \curlyvee y^*) \curlyvee (x \curlywedge y) = (x^* \curlyvee y^* \curlyvee x) \curlywedge (x^* \curlyvee y^* \curlyvee y) = \mathbf{1}$$

so $(x \curlywedge y)^* = x^* \curlyvee y^*$ by Lemma 4.17. The other identity $(x \curlyvee y)^* = x^* \curlywedge y^*$ follows by duality.

(c) $x \leq y \Leftrightarrow x \curlywedge y = x \Leftrightarrow x^* \curlyvee y^* = (x \curlywedge y)^* = x^* \Leftrightarrow y^* \leq x^*$.

(d) Suppose $x \curlywedge y \leq z$: then $x = x \curlywedge (y \curlyvee y^*) = (x \curlywedge y) \curlyvee (x \curlywedge y^*) \leq z \curlyvee y^*$. Conversely, if $x \leq z \curlyvee y^*$ then $x \curlywedge y \leq (z \curlyvee y^*) \curlywedge y = (z \curlywedge y) \curlyvee (y^* \curlywedge y) = z \curlywedge y \leq z$. □

Example 4.19. An **algebra of sets** is a non-empty $\mathcal{A} \subseteq \mathscr{P}(X)$ such that $\mathcal{A}$ is closed under complements (if $A \in \mathcal{A}$ then $A^{\complement} = X \setminus A \in \mathcal{A}$) and closed under unions or intersections (and hence under both operations). Such $\mathcal{A}$ is a Boolean algebra with $\mathbf{0} = \emptyset$ and $\mathbf{1} = X$ and the operations of union, intersection, and complements. In particular $\mathscr{P}(X)$ is a Boolean algebra, and it is non-degenerate when $X \neq \emptyset$.

Stone's Theorem 14.19 says that every Boolean algebra is isomorphic to an algebra of sets.

As the axioms Boolean algebras are equations, they are preserved by taking substructures and homomorphic images, and products (Proposition 4.12).

An **atom** of a Boolean algebra B is a minimal element of $B \setminus \{\mathbf{0}\}$, that is an $a \in B \setminus \{\mathbf{0}\}$ such that there are no $\mathbf{0} < b < a$. An algebra B is **atomic** if for every $b > \mathbf{0}$ there is an atom $a \leq b$; the algebra B is **atomless** if it has no atoms.

The degenerate algebra $\mathscr{P}(\emptyset)$ is both atomic and atomless. If $X \neq \emptyset$ then $\mathscr{P}(X)$ is atomic, and the singletons are the atoms. There are infinite atomless Boolean algebras (Example 7.45(a)) and there are non-degenerate algebras that are neither atomic, nor atomless.

4.F. Increasing unions. Fix a language $\mathcal{L}$ which, for notational simplicity will be assumed to have only a binary relation symbol R and a binary function symbol $*$. Let $(I, \leq)$ be a linearly ordered set, and suppose $\mathcal{M}_i = (M_i, R_i, *_i)$ $(i \in I)$ are $\mathcal{L}$-structures such that $\mathcal{M}_i$ is a substructure of $\mathcal{M}_j$ for all $i \leq j$. Let $\mathcal{M}_\infty = \bigcup_{i \in I} \mathcal{M}_i$ be the $\mathcal{L}$-structure with universe $M_\infty = \bigcup_{i \in I} M_i$ defined as follows

$$\begin{aligned} x_1 \; R_\infty \; x_2 &\Leftrightarrow \exists i[x_1, x_2 \in M_i \wedge x_1 \; R_i \; x_2] \\ &\Leftrightarrow \forall i[x_1, x_2 \in M_i \Rightarrow x_1 \; R_i \; x_2] \\ x_1 *_\infty x_2 = y &\Leftrightarrow \exists i[x_1, x_2, y \in M_i \wedge x_1 *_i x_2 = y] \\ &\Leftrightarrow \forall i[x_1, x_2, y \in M_i \Rightarrow x_1 *_i x_2 = y]. \end{aligned}$$

Proposition 4.20. *Suppose $\mathcal{M}_i$ with $i \in I$ are as above, $\mathcal{M}_i \vDash \sigma$, and σ is a $\forall\exists$-sentence. Then $\mathcal{M}_\infty \vDash \sigma$.*

Proof. Say σ is $\forall x_1, \dots x_n \exists y_1 \dots y_m \theta$ with θ quantifier-free, and suppose $\mathcal{M}_i \vDash \sigma$ for all $i \in I$. We must show that for all $a_1, \dots, a_n \in M_\infty$ there are $b_1, \dots, b_m \in M_\infty$ such that $\mathcal{M}_\infty \vDash \theta[\vec{a}, \vec{b}]$. Fix $a_1, \dots, a_n \in M_\infty$ and choose $i \in I$ such that $a_1, \dots, a_n \in M_i$. As $\mathcal{M}_i \vDash \sigma$ there are $b_1, \dots, b_m \in M_i$ such that $\mathcal{M}_i \vDash \theta[\vec{a}, \vec{b}]$ so that $\mathcal{M}_\infty \vDash \theta[\vec{a}, \vec{b}]$. □

Corollary 4.21. *If a theory is axiomatized by $\forall\exists$-sentences, then it is preserved under increasing unions.*

In particular, the increasing union of fields, of dense linear orders, etc. is a field, a dense linear order, etc. Proposition 4.20 and Corollary 4.21 do not extend to $\exists\forall$-sentences. For example $\mathcal{M}_n = (\{0, \dots, n\}, \leq)$ satisfies $\exists x \forall y \, (y \leq x)$, but $\bigcup_{n \in \mathbb{N}} \mathcal{M}_n = (\mathbb{N}, \leq)$ does not.

Corollary 4.21 admits a converse: if a first-order theory is preserved under increasing unions, then it is axiomatizable by $\forall\exists$-sentences.

Example 4.22. The product of two groups G, H is usually called the **direct sum** of the two groups, and it is usually denoted by $G \oplus H$. There are two injective morphisms $i_G \colon G \to G \oplus H$ and $i_H \colon H \to G \oplus H$ defined by $i_G(x) = (x, 1_H)$ and $i_H(y) = (1_G, y)$. In particular, modulo identifying G with its isomorphic copy in $G \oplus H$, we may assume that G is a subgroup of $G \oplus H$.

The **direct sum** of the groups G_n is

$$\textstyle\bigoplus_n G_n = \{s \in \bigtimes_n G_n \mid \{n \in \mathbb{N} \mid s(n) \neq 1_{G_n}\} \text{ is finite}\}$$

with the operations defined component-wise, and can be construed as an increasing union of groups

$$G_0 \subseteq G_0 \oplus G_1 \subseteq G_0 \oplus G_1 \oplus G_2 \subseteq \dots$$

where the inclusions are modulo the identification above.

Remarks 4.23. (a) The direct sum construction applies to rings as well, or more generally to models of any equational theory T (so that product is defined) and such that if $\mathcal{M}, \mathcal{N}$ are models of T, then there is an embedding of $\mathcal{M}$ into $\mathcal{M} \times \mathcal{N}$. For example if R_n is the ring $\mathbb{Z}$ for all n, then the direct sum $\bigoplus_n R_n$ is $\mathbb{Z}[X]$.

(b) While a direct sum can be seen as an increasing union, the two notions are distinct: $\bigcup_{n>0} \mathbb{Z}[1/n] = \mathbb{Q}$, while $\bigoplus_{n>0} \mathbb{Z}[1/n]$ is not divisible (Exercise 4.81).

Example 4.24. For any linear order L let L^+ be the linear order extending L obtained by adding a new minimum, a new maximum, and adding a point between two consecutive elements of L. Therefore if $L = \{x_1 < x_2 < \cdots < x_n\}$ is finite, then $L^+ = \{y_1 < x_1 < y_2 < x_2 \cdots < x_n < y_{n+1}\}$ is also finite. Let

$$L_0 \subset L_1 \subset L_2 \subset \ldots$$

be the finite linear orders defined by L_0 a singleton, and $L_{n+1} = (L_n)^+$. As $<_n$ the ordering on L_n is extended by $<_m$ the ordering on L_m, when $m > n$, then all these orderings are extended by $<_\infty$ on $L_\infty = \bigcup_n L_n$. For this reason we forgo the subscript and use the symbol $<$ to denote anyone of these orderings. Observe that for all n

$$\forall x, y \in L_n\, (x < y \Rightarrow \exists z \in L_{n+1}\, (x < z \wedge z < y))$$
$$\exists y, z \in L_{n+1}\, \forall x \in L_n\, (y < x \wedge x < z).$$

so $(L_\infty, <)$ is a dense linear order without minimum or maximum. Moreover L_∞ is countable, being a countable union of finite sets (Theorem 14.31). Theorem 13.32 shows that any countable dense linear order without endpoints is isomorphic to the rationals. Therefore $\mathbb{Q}$ can be seen as a countable increasing union of finite linear orders.

4.G. Elementary embeddings and completeness.

Definition 4.25. (i) Let $\mathcal{N} \subseteq \mathcal{M}$ be $\mathcal{L}$-structures. We say that $\mathcal{N}$ is an **elementary substructure of** $\mathcal{M}$ if for all formulæ $\varphi(x_1, \ldots, x_n)$ and all $a_1, \ldots, a_n \in N$

$$\mathcal{M} \vDash \varphi[a_1, \ldots, a_n] \text{ if and only if } \mathcal{N} \vDash \varphi[a_1, \ldots, a_n].$$

Equivalently: $\mathbf{T}^{\mathcal{N}}_{\varphi} = \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\ldots,x_n)} \cap N^n$ for all $\varphi(x_1, \ldots, x_n)$.

(ii) If $f \colon \mathcal{N} \to \mathcal{M}$ is an embedding and $\operatorname{ran}(f)$ is an elementary substructure, we will say that f is an **elementary embedding** and that $\mathcal{N}$ **elementarily embeds into** $\mathcal{M}$.

If $\mathcal{N}$ elementarily embeds into $\mathcal{M}$, then $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent. An isomorphism is an elementary embedding, therefore isomorphic structures are elementarily equivalent. The converse does not hold since, as we shall see later, there are elementarily equivalent structures of different cardinalities. If $F\colon \mathcal{N} \to \mathcal{M}$ is a morphism such that

$$\mathcal{N} \vDash \varphi[a_1, \dots, a_n] \text{ if and only if } \mathcal{M} \vDash \varphi[F(a_1), \dots, F(a_n)].$$

for all formulæ φ and all $a_1, \dots, a_n \in N$, then F is injective since it must preserve the formula $x \neq y$, and hence it is an elementary embedding.

Next we look at three criteria—one for elementary substructures, one for two structures being elementarily equivalent, and one for completeness of theories.

4.G.1. *A criterion for elementary substructures.* The next result is known as the **Tarski-Vaught criterion**.

Theorem 4.26. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure and let N be a subset of M, the universe of $\mathcal{M}$. The following are equivalent:*

(a) *N is the universe of an elementary substructure of $\mathcal{M}$,*

(b) *for every formula $\varphi(y, x_1, \dots, x_n)$ and every $a_1, \dots, a_n \in N$*

$$\mathcal{M} \vDash \exists y \varphi[\vec{a}] \Leftrightarrow \exists a_0 \in N \, (\mathcal{M} \vDash \varphi[a_0, a_1, \dots, a_n]) \,.$$

Proof. (a) $\Rightarrow$ (b): Suppose N is the universe of $\mathcal{N}$ an elementary substructure of $\mathcal{M}$, and that $\mathcal{M} \vDash \exists y \varphi[a_1, \dots, a_n]$. By elementarity there is $a_0 \in N$ such that $\mathcal{N} \vDash \varphi[a_0, a_1, \dots, a_n]$, and hence $\mathcal{M} \vDash \varphi[a_0, a_1, \dots, a_n]$.

(b) $\Rightarrow$ (a): First of all let us show that N is the universe of $\mathcal{N}$ a substructure of $\mathcal{M}$. The relations $R^{\mathcal{N}}$ are defined by restricting the $R^{\mathcal{M}}$ to N, so we only need to show that $c^{\mathcal{M}} \in N$ for every constant symbol c, and that N is closed under every operation $f^{\mathcal{M}}$, with f a function symbol. To prove this consider the formulæ $\exists y(y \mathrel{=} c)$ and $\exists y(y \mathrel{=} f(x_1, \dots, x_n))$ and apply (b).

Next, by induction on the height of ψ we prove that

$$\mathcal{N} \vDash \psi[a_1, \dots, a_n] \Leftrightarrow \mathcal{M} \vDash \psi[a_1, \dots, a_n]. \tag{4.9}$$

If ψ is atomic, then (4.9) holds by definition of substructure. If ψ is either $\neg\psi_1$ or $\psi_1 \vee \psi_2$, then (4.9) holds by inductive assumption and by definition of the satisfaction relation. Therefore we may assume that ψ is $\exists y \varphi$:

$$\begin{aligned} \mathcal{N} \vDash \exists y \varphi[a_1, \dots, a_n] &\Leftrightarrow \exists a_0 \in N \, (\mathcal{N} \vDash \varphi[a_0, a_1, \dots, a_n]) \\ &\Leftrightarrow \exists a_0 \in N \, (\mathcal{M} \vDash \varphi[a_0, a_1, \dots, a_n]) \\ &\Leftrightarrow \mathcal{M} \vDash \exists y \varphi[a_1, \dots, a_n]. \end{aligned}$$ □

Corollary 4.27. *If $\mathcal{N} \subseteq \mathcal{M}$ then the following are equivalent:*

- *$\mathcal{N}$ is an elementary substructure of $\mathcal{M}$,*
- *for any $\varphi(y, x_1, \dots, x_n)$ and any $a_1, \dots, a_n \in N$*

$$\mathcal{M} \vDash \exists y \varphi[a_1, \dots, a_n] \Leftrightarrow \exists a_0 \in N \, (\mathcal{M} \vDash \varphi[a_0, a_1, \dots, a_n]) \,.$$

Corollary 4.28. *If $F\colon \mathcal{N} \to \mathcal{M}$ is an embedding, then the following are equivalent:*

- *F is an elementary embedding*
- *for any $\varphi(y, x_1, \dots, x_n)$ and any $a_0, a_1, \dots, a_n \in N$*

$$\mathcal{M} \vDash \exists y \varphi[F(a_1), \dots, F(a_n)] \Leftrightarrow \exists a_0 \in N\, (\mathcal{M} \vDash \varphi[F(a_0), F(a_1), \dots, F(a_n)])\,.$$

Proposition 4.29. *If $\mathcal{M}_n$ are $\mathcal{L}$-structures such that $\mathcal{M}_n$ is an elementary substructure of $\mathcal{M}_m$ when $n < m$, then each $\mathcal{M}_i$ is an elementary substructure of $\mathcal{M}_\infty \overset{\text{def}}{=} \bigcup_{n \in \mathbb{N}} \mathcal{M}_n$.*

Proof. We prove by induction on the complexity of $\varphi(x_1, \dots, x_n)$ that

$$(4.10)\ \forall i \in \mathbb{N}\, \forall a_1, \dots, a_n \in M_i \left(\mathcal{M}_i \vDash \varphi[a_1, \dots, a_n] \Leftrightarrow \mathcal{M}_\infty \vDash \varphi[a_1, \dots, a_n]\right)$$

The argument is an elaboration of the proof of the Tarski-Vaught criterion. If φ is atomic, the result follows from the definition of substructure, and if φ is $\neg\psi$ or $\psi \odot \chi$ with $\odot$ a binary connective, then the result follows at once from the inductive assumption.

Assume that φ is $\exists y \psi$, fix $i \in \mathbb{N}$ and $a_1, \dots, a_n \in M_i$. If $\mathcal{M}_i \vDash \varphi[\vec{a}]$ then $\mathcal{M}_i \vDash \psi[b, \vec{a}]$ for some $b \in M_i$, so that $M_\infty \vDash \psi[b, \vec{a}]$ by inductive assumption, and hence $\mathcal{M}_\infty \vDash \varphi[\vec{a}]$. Conversely, suppose $\mathcal{M}_\infty \vDash \varphi[\vec{a}]$, and let $b \in M_\infty$ be such that $\mathcal{M}_\infty \vDash \psi[b, \vec{a}]$. Let $j \geq i$ be such that $b \in M_j$ so that by inductive assumption

$$\mathcal{M}_j \vDash \psi[b, \vec{a}] \quad \text{if and only if} \quad \mathcal{M}_\infty \vDash \psi[b, \vec{a}]$$

Therefore $\mathcal{M}_j \vDash \varphi[\vec{a}]$ and hence $\mathcal{M}_i \vDash \varphi[\vec{a}]$ since $\mathcal{M}_i$ is an elementary substructure of $\mathcal{M}_j$.

If φ is $\forall y \psi$, then the result follows from the fact that φ is equivalent to $\neg\exists y \neg\psi$ and the paragraph above. More precisely, by inductive assumption (4.10) holds for the formula ψ, and hence also for $\neg\psi$, by the properties of the $\vDash$ relation. Therefore

$$\begin{aligned} \mathcal{M}_i \vDash \forall y \psi[\vec{a}] \quad &\text{if and only if} \quad \mathcal{M}_i \nvDash \exists y \neg\psi[\vec{a}] \\ &\text{if and only if} \quad \mathcal{M}_\infty \nvDash \exists y \neg\psi[\vec{a}] \\ &\text{if and only if} \quad \mathcal{M}_\infty \vDash \forall y \psi[\vec{a}]. \end{aligned}$$

This concludes the proof. □

4.G.2. *A criterion elementarity.* We present a criterion to determine whether two $\mathcal{L}$-structures are elementary equivalent. This criterion applies to relational languages with at most finitely many constant symbols, but in view of Section 4.C this is not a serious drawback. So let's fix $\mathcal{L}$ with an arbitrary quantity of relation symbols and finitely many constant symbols $c_0, \dots, c_{m-1}$, with the understanding that $m = 0$ means that the language is relational.

Let $\mathcal{A} = (A, \dots)$ and $\mathcal{B} = (B, \dots)$ be two $\mathcal{L}$-structures with $\mathcal{L}$ a relational language, and assume for simplicity that $A \cap B = \emptyset$. A **partial isomorphism** from $\mathcal{A}$ to $\mathcal{B}$ is an isomorphism $p \colon \mathcal{A}' \to \mathcal{B}'$ where $\mathcal{A}'$ is a finite substructure of $\mathcal{A}$ and $\mathcal{B}'$ is a finite substructure of $\mathcal{B}$. Note that $p(c_i^{\mathcal{A}}) = c_i^{\mathcal{B}}$ for every $i < m$.

For $n \geq 1$ the **Ehrenfeucht-Fraïsse game** $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$ is a game lasting n rounds in which two players **I** and **II** take turns and choose elements $x_0, y_0, \dots, x_{n-1}, y_{n-1}$ in $A \cup B$

I	x_0		x_1		$\cdots$	x_{n-1}	
II		y_0		y_1	$\cdots$		y_{n-1}

with player **I** moving first in each round. There are three rules:

(1) x_i and y_i must belong to distinct structures, that is
$$\forall i < n \; (x_i \in A \Leftrightarrow y_i \in B)\,;$$

(2) if **I** chooses an x_k that was already played, say $x_k \in \{x_i, y_i\}$, then **II** plays $y_k \in \{x_i, y_i\}$, so that $\{x_i, y_i\} = \{x_k, y_k\}$;

(3) if **I** plays a constant in one of the two structures, then **II** must play the same constant in the other structure.

Letting $a_i \in A$ and $b_i \in B$ be such that $\{x_i, y_i\} = \{a_i, b_i\}$, at the end of the match we have a function
$$p \colon \{c_0^{\mathcal{A}}, \dots, c_{m-1}^{\mathcal{A}}, a_0, \dots, a_{n-1}\} \to \{c_0^{\mathcal{B}}, \dots, c_{m-1}^{\mathcal{B}}, b_0, \dots, b_{n-1}\}$$
such that $p(c_i^{\mathcal{A}}) = c_i^{\mathcal{B}}$ for $i < m$ and $p(a_i) = b_i$ for $i < n$. We decree that **II** wins this match of $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$ if p is a partial isomorphism from $\mathcal{A}$ to $\mathcal{B}$, otherwise **I** wins. A **winning strategy** for **II** is a protocol that guarantees **II**'s victory, no matter what **I** plays; similarly, a winning strategy for **I** is a protocol guaranteeing victory against any play of **II**.

The Ehrenfeucht-Fraïsse game is an example of a two-persons, perfect information (each player knows the moves played so far), zero-sum game (every match ends with the victory of exactly one player).

In the next examples $\mathcal{L}$ is the language for orders with just one binary relation symbol $\leq$.

Example 4.30. Let $\mathcal{A} = (\mathbb{Z}, \leq)$ and let $\mathcal{B} = (\mathbb{Q}, \leq)$. Then **I** wins $\mathrm{EF}_3(\mathcal{A}, \mathcal{B})$ by playing $a_0 = 0$ and $a_1 = 1$ so that **II** must respond $b_0 < b_1$ in $\mathbb{Q}$, and in the third and final round **I** plays $b_2 = \frac{1}{2}(b_0 + b_1)$ so that no matter what $a_2 \in \mathbb{Z}$ is played by **II**, the map $a_i \mapsto b_i$ $(i \leq 2)$ is not increasing.

Example 4.31. Let $\mathcal{A} = (\mathbb{N}, \leq)$ and let $\mathcal{B} = (\mathbb{N} \uplus \mathbb{Z}, \preceq)$, the disjoint union of the natural numbers and the integers, with the ordering $\preceq$ that lists all elements of $\mathbb{N}$ and then those of $\mathbb{Z}$.[18] The two players cooperatively construct a function $a_i \mapsto b_i$ $(i < n)$, and **II** wins if this map is increasing, and we will prove that **II** has a winning strategy.

We will show that given a partial isomorphism p (i.e. a finite increasing map), if p is regular enough then it can be further extended to a partial isomorphism. The notion of regularity is based on the definition of *distance*:

- if $a, a' \in \mathbb{N}$, the universe of $\mathcal{A}$, then $d_{\mathcal{A}}(a, a') = |a - a'|$;
- if $b, b' \in \mathbb{N} \uplus \mathbb{Z}$, the universe of $\mathcal{B}$, then $d_{\mathcal{B}}(b, b') = |b - b'|$ if both of them belong to $\mathbb{N}$ or to $\mathbb{Z}$, and it is ∞ otherwise.

Before we state the actual strategy, let us see what we need to assume on the partial isomorphism played so far. Suppose we are at round $k < n$ and **I** plays a_k between $a_i < a_j$ with $i, j < k$. Then **II** must reply with b_k between $b_i < b_j$. Moreover if $k + 1 < n$ and $a_k = a_i + 1$, then $b_k = b_i + 1$ since otherwise **I** could play b_{k+1} between b_i and b_k leaving no room for **II** to answer. Similarly, if $a_k + 1 = a_i$ then $b_k + 1 = b_j$. This argument can be generalized: if $k + 2^m < n$ and $d_{\mathcal{A}}(a_k, a_i) \leq 2^m$ or $d_{\mathcal{A}}(a_k, a_j) \leq 2^m$, then $d_{\mathcal{B}}(b_k, b_i) = d_{\mathcal{A}}(a_k, a_i)$ or $d_{\mathcal{B}}(b_k, b_j) = d_{\mathcal{A}}(a_k, a_j)$.

Here is the crucial definition: an increasing map $p\colon \{a_0, \dots, a_{k-1}\} \to \{b_0, \dots, b_{k-1}\}$, $a_i \mapsto b_i$, is (n, k)**-regular** if for all $-1 \leq i < j < k$

$$d_{\mathcal{A}}(a_i, a_j) \leq 2^{n-j} \Leftrightarrow d_{\mathcal{B}}(b_i, b_j) \leq 2^{n-j}, \tag{4.11a}$$

$$d_{\mathcal{A}}(a_i, a_j) \leq 2^{n-j} \Rightarrow d_{\mathcal{A}}(a_i, a_j) = d_{\mathcal{B}}(b_i, b_j), \tag{4.11b}$$

where $a_{-1} = 0_{\mathcal{A}}$ (that is the minimum of $\mathbb{N}$) and $b_{-1} = 0_{\mathcal{B}}$ (that is the minimum of $\mathbb{N} \uplus \mathbb{Z}$). Let p be as above and assume it is (n, k)-regular, and that $k < n$. Suppose **I** plays a_k in $\mathcal{A}$. Then

- either $a_k < \min(a_0, \dots, a_{k-1})$,
- or there are $i, j < k$ such that $a_i < a_k < a_j$ but it is not the case that $a_i < a_h < a_j$ for some other $h < k$,
- or else $a_k > \max(a_0, \dots, a_{k-1})$.

Conditions (4.11) guarantees that **II** has enough room to play b_k such that $b_k < \min(b_0, \dots, b_{k-1})$, or else $b_i < b_k < b_j$, or else $b_k > \max(b_0, \dots, b_{k-1})$, so that the map $\tilde{p} \overset{\text{def}}{=} p \cup \{(a_k, b_k)\}$ is $(n, k+1)$-regular. If instead **I** plays b_k in $\mathcal{B}$ then by adapting the argument above one shows that **II** has enough room to play a suitable a_k in $\mathcal{A}$ so that $\tilde{p}$ is $(n, k+1)$-regular. Therefore after the n-th round an (n, n)-nice map $\{a_0, \dots, a_{n-1}\} \to \{b_0, \dots, b_n\}$, $a_i \mapsto b_i$ is obtained. As this map is increasing then **II** wins the game.

[18] The ordered set $\mathcal{B}$ is denoted in Section 13 as $\mathbb{N} + \mathbb{Z}$.

Certain games last forever: the Ehrenfeucht-Fraïsse game $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$ lasts infinitely many moves, with **I** and **II** cooperatively constructing a map $a_i \mapsto b_i$ between infinite substructures $\mathcal{A}' = \{a_i \mid i \in \mathbb{N}\}$ and $\mathcal{B}' = \{b_i \mid i \in \mathbb{N}\}$, and **II** wins just in case this map is an isomorphism.

Example 4.32. Player **II** has a winning strategy for $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$ where $\mathcal{A} = (A, \leq)$ and $\mathcal{B} = (B, \preceq)$ are dense linear orders without endpoints.

The result follows from the fact that any is a partial isomorphism p from $\mathcal{A}$ to $\mathcal{B}$ can be extended to a partial isomorphism p' such that $a \in \operatorname{dom} p'$ and $b \in \operatorname{ran} p'$ for any given $a \in A$ and $b \in B$. In fact suppose **I** plays $a \in A$ then:

- if a is smaller than the minimum of $\operatorname{dom} p$ then **II** can answer with an element smaller than $\operatorname{ran} p$ (as $\mathcal{B}$ has no minimum);
- if a is larger than the maximum of $\operatorname{dom} p$ then **II** can answer with an element larger than $\operatorname{ran} p$ (as $\mathcal{B}$ has no maximum);
- if a is between a_i and a_j, then using the fact that $\mathcal{B}$ is a dense linear order, **II** plays an element between b_i and b_j.

The case when **I** plays $b \in B$ is similar.

If **II** has a winning strategy for $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$ then it has a winning strategy for $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$ for any n, but not conversely.

Example 4.33. Player **I** has a winning strategy in $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$ where $\mathcal{A}, \mathcal{B}$ are as in Example 4.31.

Say **I** plays an element $b_0 \in \mathbb{Z}$ in the structure $\mathcal{B}$. Then **II** must answer some $a_0 \in \mathbb{N}$ in the structure $\mathcal{A}$. If **I** plays $b_k = b_0 - k$ for $k > 0$, then after a_0-many rounds **II** will reach a certain loss.

Finally, let us show how Ehrenfeucht-Fraïsse games are related to elementary equivalence.

Definition 4.34. Let $\mathcal{L}$ be an arbitrary language. The **quantifier-rank** of an $\mathcal{L}$-formula φ is defined as follows:

- if φ is atomic, then $\mathrm{qr}(\varphi) = 0$;
- if φ is $\neg\psi$, then $\mathrm{qr}(\varphi) = \mathrm{qr}(\psi)$;
- if φ is $\psi \odot \chi$, then $\mathrm{qr}(\varphi) = \max(\mathrm{qr}(\psi), \mathrm{qr}(\chi))$;
- if φ is $\exists x\psi$ or $\forall x\psi$, then $\mathrm{qr}(\varphi) = \mathrm{qr}(\psi) + 1$.

The quantifier rank is a measure of complexity of formulæ: $\mathrm{qr}(\varphi) = 0$ just in case φ is quantifier-free, $\mathrm{qr}(\varphi) = 1$ just in case φ is Boolean combination of formulæ that are either quantifier-free or else of the form $\exists x\psi$ or $\forall x\psi$, with ψ quantifier-free, and so on.

Theorem 4.35. *Let $\mathcal{A}$, $\mathcal{B}$ be $\mathcal{L}$-structures, with $\mathcal{L}$ a language without function symbols and with finitely many constant symbols. For each $n \in \mathbb{N}$ the following are equivalent:*

(a) *$\mathcal{A} \vDash \sigma$ if and only if $\mathcal{B} \vDash \sigma$, for all sentences σ such that $\mathrm{qr}(\sigma) \leq n$;*

(b) ***II** has winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$.*

If a is an element of a $\mathcal{L}$-structure $\mathcal{A}$, then $(\mathcal{A}, a)$ is a $\mathcal{L} \cup \{\mathring{a}\}$-structure, where $\mathring{a}$ is a new constant symbol that is interpreted as a in this new structure. Thus if $\varphi(x)$ is a formula with one free variable, then a belongs to the truth set of $\varphi(x)$ for the structure $\mathcal{A}$ if and only if $(\mathcal{A}, a)$ satisfies the sentence $\varphi\llparenthesis\mathring{a}/x\rrparenthesis$ obtained from $\varphi(x)$ by replacing x with $\mathring{a}$:

$$\mathcal{A} \vDash \varphi[a] \text{ if and only if } (\mathcal{A}, a) \vDash \varphi\llparenthesis\mathring{a}/x\rrparenthesis.$$

Proof of Theorem 4.35.

LATER

□

Corollary 4.36. *Let $\mathcal{A}$, $\mathcal{B}$ be $\mathcal{L}$-structures, with $\mathcal{L}$ a relational language. Then $\mathcal{A}$ and $\mathcal{B}$ are elementary equivalent if and only if **II** has winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$, for any $n \in \mathbb{N}$.*

Therefore $(\mathbb{Q}, \leq)$ and $(\mathbb{R}, \leq)$ are elementary equivalent by Example 4.32, and so are $(\mathbb{N}, \leq)$ and $(\mathbb{N} \uplus \mathbb{Z}, \preceq)$ by Example 4.31.

4.G.3. *A criterion for completeness.* Two structures have the same size if there is a bijection between their universes. In particular, isomorphic structures have the same size. In Chapter VII (Theorem 31.36) we will prove the following criterion for the completeness of a theory.

Theorem 4.37. *Let T be a satisfiable theory in a language with at most countably many non-logical symbols. Suppose*

- *either there is exactly one model of T up to isomorphism,*
- *or else every model of T is infinite, and there is a model $\mathcal{M}$ of T such that every model $\mathcal{N}$ of T of the same size as $\mathcal{M}$ is isomorphic to $\mathcal{M}$.*

Then T is a complete theory.

Example 4.38. Consider the language $\mathcal{L}$ with no non-logical symbols: its models are the non-empty sets. If $T_\emptyset$ is the $\mathcal{L}$-theory with no axioms, then $T_\emptyset$ is satisfiable, since it is satisfied by any non-empty set, but it is not complete, since neither the sentence “there are exactly n elements” $\boldsymbol{\varepsilon}_n$ of page 18, nor its negation are logical consequences of $T_\emptyset$. By Theorem 4.37 the theories $T_n = \{\boldsymbol{\varepsilon}_n\}$ and $T_\infty = \{\boldsymbol{\varepsilon}_{\geq n} \mid n > 0\}$ are complete. (For T_∞ note that any two countable models are isomorphic.) The theories T_n ($n = 1, 2, \dots, \infty$) are the only complete theories extending $T_\emptyset$ (Exercise 4.91).

If T is a complete theory that has a finite model of size n, then $T \models \boldsymbol{\varepsilon}_n$ and hence every model of T is finite of size n. Thus the theories of (semi)groups (abelian or not), of rings, of fields, ... are not complete.

Example 4.39. Recall that T_{FLDS} is the theory of fields in the language $\mathcal{L}_{\mathrm{RINGS}}$. If we add the sentence $p1 = 0$ (p a prime) we obtain the theory F_p of the fields of characteristic p, while if we add sentences $p1 \neq 0$ (for all primes p) we obtain F_0 the theory of fields of characteristic zero.

The theory of algebraically closed fields is

$$\mathrm{ACF} = T_{\mathrm{FLDS}} \cup \{\varphi_n \mid n \geq 1\}$$

where φ_n says that every polynomial of degree n has a root

$$(\varphi_n) \qquad \forall a_0, \dots, a_n \, (a_n \neq 0 \Rightarrow \exists x \, (a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 = 0)).$$

The theory ACF is not complete, since the characteristic of the field is not determined by these axioms. Let

$$\mathrm{ACF}_p = \mathrm{ACF} \cup \{p1 = 0\}$$

be the theory of algebraically closed fields of characteristic p, and let

$$\mathrm{ACF}_0 = \mathrm{ACF} \cup \{n1 \neq 0 \mid n \geq 2\}$$

be the theory of algebraically closed fields of characteristic zero.

Theorem 4.40. *The theories* ACF_0 *and* ACF_p *are complete, and these are the only complete theories extending* ACF*.*

Sketch of the proof. Any two uncountable, algebraically closed fields of the same size and same characteristic have transcendence bases of the same size, and hence they are isomorphic—this uses a few facts about cardinalities that will be proved in full generality in Section 20. □

4.H. Definable sets. A subset A of M^n is **definable without parameters** if it is the truth set of a formula φ and a finite list of variables $x_1, \dots, x_n$, that is if $A = \mathbf{T}^{\mathcal{M}}_{\varphi(x_1,\dots,x_n)}$. When A is a singleton $\{(a_1, \dots, a_n)\}$ we say that $(a_1, \dots, a_n)$ is definable. The integer n is called the dimension of the definable set A.

We say that $A \subseteq M^n$ is **definable with parameters** $p_1, \dots, p_k \in M$ if there is φ and variables $(x_1, \dots, x_n, y_1, \dots, y_k)$ such that

$$A = \{(a_1, \dots, a_n) \in M^n \mid (a_1, \dots, a_n, p_1, \dots, p_k) \in \mathbf{T}^{M}_{\varphi(x_1,\dots,x_n,y_1,\dots,y_k)}\}.$$

In other words: A is the section of $\mathbf{T}^{M}_{\varphi(x_1,\dots,x_n,y_1,\dots,y_k)}$ given by $(p_1, \dots, p_k)$.

A function $f\colon X \to M$ with $X \subseteq M^n$ is definable (with or without parameters) if its graph $\mathrm{Gr}(f)$ is definable. Every $a \in M$ is definable with parameter a, via formula $x_1 \doteq y_1$. In order to avoid trivialities, when dealing with elements (i.e. singletons) the definability is always understood to be *without* parameters. Every set which is definable without parameters can be also defined with parameters $p_1, \dots, p_k$—just take the conjunction of the formula defining the set with a valid formula with free variables $y_1, \dots, y_k$, for example $\bigwedge_{1\leq i\leq k} y_i \doteq y_i$. Thus the notion of definable set with parameters extends the notion of definable set without parameters. Conversely, if $A \subseteq M^n$ is definable via $\varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ and parameters $p_1, \dots, p_k$, and if every p_i is definable via $\psi_i(y_i)$, then A is definable without parameters via the formula

$$\exists y_1, \dots, y_k \bigl(\bigwedge_{1\leq i\leq k} \psi_i(y_i) \wedge \varphi(x_1, \dots, x_n, y_1, \dots, y_k)\bigr)$$

or equivalently via the formula

$$\forall y_1, \dots, y_k \bigl(\bigwedge_{1\leq i\leq k} \psi_i(y_i) \Rightarrow \varphi(x_1, \dots, x_n, y_1, \dots, y_k)\bigr).$$

Therefore the notions of definability with or without parameters agree in structures where every element is definable, such as the natural numbers (Section 11.A).

The family of definable sets in $\mathcal{M}$ (with or without parameters), of fixed dimension n always contains the empty set (defined either by $\bigwedge_{1\leq i\leq n} x_i \not\doteq x_i$ or by $\bigvee_{1\leq i\leq n} x_i \not\doteq x_i$), the set M^n (defined by $\bigwedge_{1\leq i\leq n} x_i \doteq x_i$ or by $\bigvee_{1\leq i\leq n} x_i \doteq x_i$) and it is closed under complements, intersections, unions, and differences: if $A, B \subseteq M^n$, are defined by the formulæ $\varphi(x_1, \dots, x_n)$ and $\psi(x_1, \dots, x_n)$ then

- $M^n \setminus A$ is defined by $\neg\varphi$,
- $A \cap B$ is defined by $\varphi \wedge \psi$,
- $A \cup B$ is defined by $\varphi \vee \psi$,
- $A \setminus B$ defined by $\varphi \wedge \neg\psi$.

Therefore the family of definable sets in $\mathcal{M}$ (with or without parameters), of fixed dimension n is an algebra of subsets of M^n, where:

Definition 4.41. An **algebra of subsets** of a given set X is an $\mathcal{A} \subseteq \mathscr{P}(X)$ such that $X, \emptyset \in \mathcal{A}$, and closed under intersections unions, and differences.

Remark 4.42. A subset $A \subseteq M^n$ definable with parameters $p_1, \dots, p_k$ can be identified with a $\hat{A} \subseteq M^{n+m}$ definable with the same parameters—for example if A is defined by $\varphi(x_1, \dots, x_n, y_1, \dots, y_k)$ and parameters $p_1, \dots, p_k$, then $\hat{A} = A \times M^m$, is defined by

$$\varphi(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m}, y_1, \dots, y_k)$$

and parameters $p_1, \dots, p_k$. Moreover the function $A \mapsto \hat{A}$ preserves[19] the usual set-theoretic operation of intersection, union, complement, ... so the collection of definable sets of dimension n can be seen as a subfamily of the subsets of dimension $m > n$.

The family of definable sets becomes more complex as the dimension grows—as we shall see in Section 11.A, the definable subsets of dimension 1 of $(\mathbb{N}, S)$ where S is the successor operation, are exactly the finite and cofinite subsets, while the diagonal $\{(n, n) \mid n \in \mathbb{N}\}$ is an infinite definable subset of dimension 2, whose complement is also infinite.

In general it is much easier to verify that a set $A \subseteq M^n$ is definable rather than proving the opposite: in the first case a formula φ whose truth set is A must be found, while in the second case we must prove that *no* formula φ would do. An often efficient method to prove the non-definability of a set is based on the notion of **automorphism** of a structure, that is an isomorphism of the structure onto itself. The set of all automorphisms of $\mathcal{M}$

$$\mathrm{Aut}(\mathcal{M})$$

is a group under composition. Every structure $\mathcal{M}$ has at least one automorphism—the identity function id_M—and if this is the only automorphism, i.e. if $\mathrm{Aut}(\mathcal{M})$ is the trivial group, we shall say that $\mathcal{M}$ is **rigid**. By Proposition 4.6(e), if $A \subseteq M^n$ is definable, then it is mapped into itself by every automorphism. Thus in order to prove that a set $A \subseteq M^n$ is not definable it is sufficient to find an automorphism that does not map A onto itself. If there is an automorphism f such that $f[A] \neq A$ and $f(p_i) = p_i$, for $i = 1, \dots, k$, it follows that A is not definable with parameters $p_1, \dots, p_k$. For example, $\{\mathrm{i}, -\mathrm{i}\}$ is definable in the complex field by the formula $x \cdot x + 1 = 0$, but neither the imaginary unit nor its conjugate are definable, since $z \mapsto \overline{z}$ is an automorphism.

Remarks 4.43. (a) A set invariant under automorphisms need not be definable. (A set $A \subseteq M^n$ is **invariant under automorphisms** if $\vec{a} \in A$ implies that $F(\vec{a}) \in A$, for every automorphism F of $\mathcal{M}$.) For example the only automorphism of the natural numbers with the successor operations is the identity (Exercise 4.76) and therefore every subset of $\mathbb{N}$ is invariant under automorphisms. The definable subsets are as many as the formulæ of the language containing the symbols 0 and S and, as we shall see in Chapter VII, there are countably many of them, while the subsets of $\mathbb{N}$ are many more. A more interesting example is given by multiplication versus divisibility: every automorphism of $(\mathbb{N}, |)$ is also an automorphism of $(\mathbb{N}, \cdot)$ (Exercise 11.46) yet multiplication is not definable from divisibility (Exercise 12.30).

[19] A map like this is called a homomorphism of Boolean algebras, see Section 7.F.3.

(b) If $\mathcal{M}$ is rigid and $\mathcal{M} \cong \mathcal{N}$, then also $\mathcal{N}$ is rigid and the isomorphism between $\mathcal{M}$ and $\mathcal{N}$ is unique, since if $F, G \colon \mathcal{M} \to \mathcal{N}$ are isomorphisms then $G^{-1} \circ F$ is an automorphism of M and hence it is the identity. Therefore if $\mathscr{C}$ is a collection of isomorphic $\mathcal{L}$-structures, and if one of them is rigid (equivalently: they are all rigid), then the structures in $\mathscr{C}$ are canonically isomorphic, and hence they can be completely identified.

4.I. Interpretability in structures. Fix a field $\Bbbk$. The set $\mathrm{GL}_2(\Bbbk)$ of invertible 2×2 matrices on $\Bbbk$ can be identified with the subset of $\Bbbk^4$ defined by $\{(x_{11}, x_{12}, x_{21}, x_{22}) \mid x_{11} \cdot x_{22} \neq x_{12} \cdot x_{21}\}$, and the matrix-multiplication operation can be seen as a binary operation on $\Bbbk^4$. Thus the group $\mathrm{GL}_2(\Bbbk)$ can be defined in the field $\Bbbk$, and we shall say that the structure $(\mathrm{GL}_2(\Bbbk), \cdot)$ is definably interpretable in the structure $(\Bbbk, +, \cdot, 0, 1)$. More generally, an $\mathcal{L}$-structure $\mathcal{M}$ is **definably interpretable** into an $\mathcal{L}'$-structure $\mathcal{M}'$ if there is an isomorphism $F \colon \mathcal{M} \to \mathcal{N}$ such that N, the universe of $\mathcal{N}$, is a definable subset (of suitable dimension) of $\mathcal{M}'$ and if all relations, functions, constants of $\mathcal{N}$ can be defined in $\mathcal{M}'$. (The k-ary operations of $\mathcal{N}$ can be seen as $k+1$-ary relations on N.)

A further extension of the notion of definable interpretation is obtained by encoding the structure $\mathcal{M}$ as a quotient of $\mathcal{M}'$. More precisely we require that N be of the form X/E where X definable subset (of suitable dimension) of $\mathcal{M}'$ and E is a definable equivalence relation on X. In this case we say that $\mathcal{M}$ is **definably interpretable in a quotient of** $\mathcal{M}'$. When $E = \mathrm{id}_M$ we fall-back in the previous definition.

For example consider the projective space of dimension n over a field $\Bbbk$

$$\Bbbk\mathbb{P}^n \overset{\text{def}}{=} (\Bbbk^{n+1} \setminus \{\mathbf{0}\})/E$$

where $\mathbf{x} \mathrel{E} \mathbf{y} \Leftrightarrow \exists \lambda \in \Bbbk \setminus \{0\} \, (\lambda \mathbf{x} = \mathbf{y})$ is the collinearity relation on $\Bbbk^{n+1}$. If $f \in \Bbbk[X_0, \ldots, X_n]$ is a homogeneous polynomial of degree d, i.e. $f(\lambda \mathbf{x}) = \lambda^d f(\mathbf{x})$ for all $\mathbf{x} \in \Bbbk^{n+1}$ and $\lambda \in \Bbbk$, the projective variety defined by f is

$$V = \{[\mathbf{x}] \in \Bbbk\mathbb{P}^n \mid f(\mathbf{x}) = 0\}.$$

Thus the structure $(\Bbbk\mathbb{P}^n, V)$ is definably interpretable with parameters[20] in $\Bbbk$.

4.I.1. *Coding arithmetic with sequences*.* Recall (Example 3.24) that $\mathcal{L}_{\mathrm{CONC}}$ is the language with a binary function symbol $*$ and three constant symbols $\mathbf{0}, \mathbf{1}, \varepsilon$. If A be a set with at least two elements a, b, then $A^{\mathbb{N}}$, the set of all finite sequences from A, can be construed as an $\mathcal{L}_{\mathrm{CONC}}$-structure $\mathcal{A} = (A^{<\mathbb{N}}, {}^\frown, a, b, \langle\rangle)$. At first sight $\mathcal{A}$ looks a bit dull, with few definable subsets. The goal of this section is to show that the opposite is true, as $(\mathbb{N}, +, \cdot)$ is interpretable in $\mathcal{A}$.

[20] The parameters are the coefficients of f.

For the sake of legibility the symbol $*$ will often be suppressed, so when t, u are $\mathcal{L}_{\textsc{Conc}}$-terms we write tu rather than $t * u$. Following the Convention stipulated on page 25, t^n is the term obtained by repeated application of $*$ to the term t, with the understanding that t^0 is the constant ε.

The first step is to find a definable subset of $A^{<\mathbb{N}}$ that plays the role of $\mathbb{N}$. The formula

$$(\varphi_{\mathbb{N}}(x)) \qquad\qquad \forall y, z\,(x \neq y\mathbf{0}z)$$

defines the set $N \overset{\text{def}}{=} \{b^{(n)} \mid n \in \mathbb{N}\}$ of all strings in which a does not occur. Each $b^{(n)} \in N$ is the value of the closed term $\mathbf{1}^n$ in $\mathcal{A}$ and the correspondence $\mathbb{N} \to N$, $n \mapsto b^{(n)}$ is a bijection. Observe that N is closed under concatenation and that $b^{(n)}{}^\frown b^{(m)} = b^{(n+m)}$. Therefore addition on N is just the concatenation operation.

The real issue is to find a formula $\varphi_\times(x, y, z)$ that defines multiplication on N. The formulæ

$$\exists u\,\exists v\,(u * x * v = y)$$
$$\exists v\,(x * v = y)$$
$$\exists u\,(u * x = y)$$

define the orderings $x \sqsubseteq y$, $x \sqsubseteq_{\mathrm{i}} y$ and $x \sqsubseteq_{\mathrm{f}} y$ (see Definition 3.16), so we can freely use these symbols in the formulæ below. Given $n, m > 0$, the closed term

$$t = \mathbf{00101}^m\mathbf{001}^2\mathbf{01}^{2m}\mathbf{001}^3\mathbf{01}^{3m}\mathbf{00}\ldots\mathbf{001}^n\mathbf{01}^{nm}\mathbf{00}$$

encodes the computation of $n \cdot m$ in the following sense:

- the sequence $\mathbf{00101}^m\mathbf{0}$ is the initial segment of t;
- the term $\mathbf{000}$ does not occur in t, that is t satisfies $\varphi_1(w)$: $\neg\exists u, v\,(w = u\mathbf{000}v)$;
- terms of the form $\mathbf{001}^i\mathbf{00}$ do not occur in t, that is t satisfies $\varphi_2(w)$: $\neg\exists u(\varphi_{\mathbb{N}}(u) \wedge \mathbf{00}u\mathbf{00} \sqsubseteq w)$;
- if $\mathbf{01}^k\mathbf{001}^i\mathbf{0}$ occurs in t and $i \neq n$, then right after it we have $\mathbf{1}^{k+m}\mathbf{001}^{i+1}\mathbf{0}$, where m is retrieved from the initial part of t; thus t satisfies $\varphi_3(w)$:

$$\begin{aligned}&\forall u, s, z, v[\varphi_{\mathbb{N}}(u) \wedge \varphi_{\mathbb{N}}(s) \wedge \varphi_{\mathbb{N}}(t) \wedge \varepsilon \neq u \wedge \varepsilon \neq s \wedge \varepsilon \neq z\\ &\quad \wedge \mathbf{0010}u\mathbf{00} \sqsubseteq_{\mathrm{i}} w \wedge v\mathbf{0}s\mathbf{00}z\mathbf{0} \sqsubseteq w \wedge u \neq z \Rightarrow v\mathbf{0}s\mathbf{00}z\mathbf{0}su\mathbf{00}z\mathbf{10} \sqsubseteq w]\end{aligned}$$

- the sequence $\mathbf{01}^n\mathbf{01}^{n\cdot m}\mathbf{00}$ is a final segment of w.

Thus the formula $\varphi_\times(x, y, z)$

$$\begin{aligned}&\varphi_{\mathbb{N}}(x) \wedge \varphi_{\mathbb{N}}(y) \wedge \varphi_{\mathbb{N}}(z) \wedge \big[((x = \varepsilon \vee y = \varepsilon) \wedge z = \varepsilon)\\ &\qquad \vee \exists w\,\big(\mathbf{0010}y\mathbf{0} \sqsubseteq_{\mathrm{i}} w \wedge \varphi_1(w) \wedge \varphi_2(w) \wedge \varphi_3(w) \wedge \mathbf{0}x\mathbf{0}z\mathbf{00} \sqsubseteq_{\mathrm{f}} w\big)\big]\end{aligned}$$

defines multiplication on N in the sense that for all $n, m, k \in \mathbb{N}$

$$\mathcal{A} \vDash \varphi_\times[b^{(n)}, b^{(m)}, b^{(k)}] \quad \text{if and only if} \quad k = n \cdot m.$$

Therefore we have shown that:

Theorem 4.44. $(\mathbb{N}, +, \cdot)$ *is definably interpretable in* $\mathcal{A}$.

4.J. Definability in groups. In order to study the first-order theory of groups, we can use $\mathcal{L}_{\text{GRPS}}$ seen on page 53 and consisting of two function symbols $\cdot$ and $^{-1}$ and a constant symbol 1, but the choice of language is far from being unique. If the symbol for inverses is removed, the language $\mathcal{L}_{\text{MND}}$ is obtained; a structure for this language is a monoid if it satisfies (3.10a) and (3.10b), and it is a group if it satisfies also $\forall x \exists y\, (x \cdot y \mathrel{=} 1 \wedge y \cdot x \mathrel{=} 1)$. For the sake of frugality, we could eschew using the constant 1, limiting ourselves to the language for semigroups $\mathcal{L}_{\text{SGRPS}}$ that has only one symbol $\cdot$ for a binary operation (Exercise 4.84). When dealing with abelian groups it is customary to use additive notation and the language $\mathcal{L}_{\text{ABGR}}$ (see page 55).

In this section G denotes an arbitrary group, and 1_G is its identity element. Let us see some examples subsets of G^n that are definable without parameters, using $\mathcal{L}_{\text{GRPS}}$, $\mathcal{L}_{\text{MND}}$, or $\mathcal{L}_{\text{SGRPS}}$.

- The trivial subgroup $\{1_G\}$ is defined by $x \mathrel{=} x \cdot x$ or by $x \mathrel{=} 1$.
- The **center** $C(G)$ is defined by $\forall y (y \cdot x \mathrel{=} x \cdot y)$. More generally, if $A \subseteq G$ is definable with parameters $p_1, \dots, p_n$, then its **centralizer** $C_G(A) \overset{\text{def}}{=} \{g \in G \mid \forall x \in A\, (g \cdot x = x \cdot g)\}$ is definable with parameters $p_1, \dots, p_n$.
- The graph of the inverse map $g \mapsto g^{-1}$ is defined by either one of the following formulæ: $y \cdot x \mathrel{=} (y \cdot x) \cdot (y \cdot x)$, $x \cdot y \mathrel{=} 1$, or $y \mathrel{=} x^{-1}$.
- The conjugacy relation is defined by $\exists z (z \cdot x \mathrel{=} y \cdot z)$, or by $\exists z (z \cdot x \cdot z^{-1} \mathrel{=} y)$.

In fact all of the above notions are **uniformly definable**, that is they are defined using a single formula that works for every group.

4.J.1. *Torsion.* An element $g \in G$ has **torsion** if $g^n = 1_G$ for some $n > 0$ and the smallest such n is called the **order** of g and it is denoted by $o(g)$. Since $o(g) = 1 \Leftrightarrow g = 1_G$, when we say that "$G$ has an element with torsion" we mean that there is $g \in G$ such that $o(g) = n > 1$. If g in **torsionless**, i.e. it has no torsion, we write $o(g) = \infty$, and the subgroup generated by g is isomorphic to $(\mathbb{Z}, +)$.

A **torsion group** is a group in which every element has torsion; if instead the only torsion element is 1_G then the group is said to be **torsion-free** or **torsionless**. Torsion-free groups are axiomatized by $T_{\text{GRPS}} \cup \{\tau_n \mid n \geq 1\}$, with

$$(\tau_n) \qquad \forall x\, (x \neq 1 \Rightarrow x^n \neq 1).$$

For $n \geq 1$ the set

$$\mathrm{Tor}_n(G) = \{g \in G \mid o(g) = n\}$$

is defined by $x^n \mathrel{\dot=} 1 \wedge \bigwedge_{1<k<n} x^k \neq 1$, and

$$\mathrm{Tor}(G) = \textstyle\bigcup_{n\geq 1} \mathrm{Tor}_n(G)$$

is the set of all elements of G that have torsion. It is easy to check that $\mathrm{Tor}(G)$ is a subgroup, when G is abelian.

Because of the quantification on the integers, the expression stating that x has torsion, $\exists n > 1\, (x^n \mathrel{\dot=} 1)$ is only a pseudo-formula. If we replaced $\exists n > 1$ with a disjunction of the form $\bigl(x^2 \mathrel{\dot=} 1\bigr) \vee \bigl(x^3 \mathrel{\dot=} 1\bigr) \vee \ldots$ an infinite string of symbols is obtained, and such object cannot be a formula. So we may ask: is $\mathrm{Tor}(G)$ a definable subset of G? If G is torsion then $\mathrm{Tor}(G) = G$, while if G is torsion-free then $\mathrm{Tor}(G) = \{1_G\}$, so in these cases $\mathrm{Tor}(G)$ is definable without parameters. So the question above should be stated as: is $\mathrm{Tor}(G)$ a *uniformly* definable subset of G? Corollary 4.56 shows that the answer is negative.

4.J.2. *Divisibility.* The **n-divisible part** ($n \geq 1$) of a group G is the set $\mathrm{Div}_n(G)$ of all elements of the form g^n, and it is defined by the formula $\exists y\, (x \mathrel{\dot=} y^n)$. The **divisible part** of G, in symbols $\mathrm{Div}(G)$, is the intersection of all its n-divisible parts. When $(G, +)$ is an abelian group its n-divisible part

$$nG = \{ng \mid g \in G\}$$

is a subgroup called the **n-divisible subgroup**, and the divisible part is called the **divisible subgroup**. Finally we say that a group is **n-divisible** if it coincides with its n-divisible part; similarly a group is **divisible** if it coincides with its divisible part. Divisible groups are axiomatized by $T_{\mathrm{GRPS}} \cup \{\delta_n \mid n \geq 2\}$ with

$$(\delta_n) \qquad \forall x\, \exists y\, (y^n \mathrel{\dot=} x).$$

(If the additive notation is used then δ_n becomes $\forall x\, \exists y\, (ny \mathrel{\dot=} x)$.)

The expression $\forall n > 0\, \exists y \bigl(ny \mathrel{\dot=} x\bigr)$ is not a formula, hence it cannot be used to define the divisible part of a group. So we may ask: is the divisible part definable in the group G? This is certainly the case if G is divisible, or if the divisible part is $\{1_G\}$, so the question must be restated as: is $\mathrm{Div}(G)$ a *uniformly* definable subset of G? The answer is negative by Corollary 4.56.

Examples of n-divisible abelian groups are

$$\mathbb{Z}[1/n] = \{x \in \mathbb{Q} \mid \exists k (n^k x \in \mathbb{Z})\}$$

and $\mathbb{Z}[1/n]/\mathbb{Z}$, that can be identified with a subgroup of the multiplicative group $\{z \in \mathbb{C} \mid |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$, while

$$\mathbb{Q} = \textstyle\bigcup_{n\geq 1} \mathbb{Z}[1/n], \quad \mathbb{R}, \quad \mathbb{Q}/\mathbb{Z}, \quad \mathbb{R}/\mathbb{Z}$$

are divisible and abelian. The group $\mathbb{Z}$ is not n-divisible for any n, and its divisible subgroup is $\{0\}$, while $\mathbb{Z} \times \mathbb{Q}$ is not divisible, but its divisible subgroup is $\{0\} \times \mathbb{Q}$.

Example 4.45. Any torsion-free, divisible abelian group G is a vector space over $\mathbb{Q}$ and its dimension as a vector space is called the **rank** of G (Exercise 4.83). Two uncountable vector spaces over $\mathbb{Q}$ of the same size are isomorphic (see Section 18.D.1 for details). Therefore $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, and $(\mathbb{Q}^n, +)$ for $n \geq 1$, are all elementarily equivalent, and the theory of torsion-free, divisible abelian groups is complete.

4.K. The Compactness Theorem. A set of sentences Σ is **finitely satisfiable** if every finite $\Sigma_0 \subseteq \Sigma$ is satisfiable. Every satisfiable set of sentences is finitely satisfiable, and the **Compactness Theorem for first-order logic** asserts that the converse is true.

Theorem 4.46. *Let Σ be a set of $\mathcal{L}$-sentences. If Σ is finitely satisfiable, then Σ is satisfiable.*

This result is one of the cornerstones of mathematical logic, and will be proved in Section 15. The proof for infinite languages $\mathcal{L}$ requires (a consequence of) the axiom of choice, a set-theoretic principle that will be introduced in Section 14.

Corollary 4.47. *Let Σ be a set of $\mathcal{L}$-sentences and let τ be an $\mathcal{L}$-sentence. If $\Sigma \models \tau$, then there is a finite $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \tau$.*

Proof. Suppose $\Sigma \models \tau$, so that $\Sigma \cup \{\neg\tau\}$ is unsatisfiable by Proposition 3.30. By compactness there is a finite $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \cup \{\neg\tau\}$ is unsatisfiable, and hence $\Sigma_0 \models \tau$ again by Proposition 3.30. □

The next result is most useful.

Theorem 4.48. *Suppose Σ is a set of $\mathcal{L}$-sentences with arbitrarily large finite models. Then Σ has an infinite model.*

Proof. Otherwise $\Sigma \cup \{\boldsymbol{\varepsilon}_{\geq k} \mid k \geq 1\}$ would be unsatisfiable, and hence by compactness there would be an $n \geq 1$ such that $\Sigma \cup \{\boldsymbol{\varepsilon}_{\geq k} \mid 1 \leq k \leq n\}$ would be unsatisfiable, against our assumption that Σ has a model of size $\geq n$. □

4.K.1. *Finitely axiomatizable theories and classes.* A theory is said to be **finitely axiomatizable** if it has a finite set of axioms. More generally, given theories $T' \subseteq T$ in a language $\mathcal{L}$, we say that T is **finitely axiomatizable modulo** T' if there is a finite set Σ of $\mathcal{L}$-sentences such that $T' \cup \Sigma$ is an axiom system for T. Thus T is finitely axiomatizable if and only if it is finitely axiomatizable modulo T', where T' is a theory consisting of valid sentences, e.g. $T' = \emptyset$. The following result is most useful for proving that a given theory is not finitely axiomatizable.

Theorem 4.49. *Let T be an $\mathcal{L}$-theory and let $\{\sigma_n \mid n \in \mathbb{N}\} \cup T'$ be a system of axioms for it. Suppose that for every n there is an $m > n$ such that $\{\sigma_0, \dots, \sigma_n\} \cup T' \not\models \sigma_m$. Then T is not finitely axiomatizable modulo T'.*

Proof. Towards a contradiction, suppose that $\{\tau_0, \dots, \tau_n\} \cup T'$ is a set of axioms for T, and let $\tau = \bigwedge_{i \leq n} \tau_i$. As $\{\sigma_n \mid n \in \mathbb{N}\} \cup T' \models \tau$, by Corollary 4.47 there is a finite set $I \subseteq \mathbb{N}$ such that $\{\sigma_n \mid n \in I\} \cup T' \models \tau$. By assumption there is a large enough m such that $\{\sigma_n \mid n \in I\} \cup T' \not\models \sigma_m$, and this contradicts the fact that $\{\tau\} \cup T' \models \sigma_n$ for all n. □

Corollary 4.50. *If or every n there is $m > n$ such that $\{\sigma_0, \dots, \sigma_n\} \not\models \sigma_m$ then $\{\sigma_n \mid n \in \mathbb{N}\}$ is not finitely axiomatizable.*

Two sets of sentences Σ and Δ are **logically equivalent** if and only if they axiomatize each other, that is

$$\Sigma \models \sigma \quad \text{if and only if} \quad \Delta \models \sigma$$

for every sentence σ. Then Δ is a set of axioms for Σ, and conversely. Call Σ an **independent system of sentences** if none of its members is logical consequence of the other sentences, that is if $\Sigma \setminus \{\sigma\} \not\models \sigma$, for every $\sigma \in \Sigma$. Every finite set of sentences Σ contains an independent set of axioms Δ, but such Δ is far from being unique. If Σ is countable, then it has an independent set of axioms Δ, but Δ might not be a subset of Σ (Exercise 4.89).

The collection of all models of T is

$$\mathrm{Mod}(T) = \{\mathcal{M} \mid \mathcal{M} \text{ is an } \mathcal{L}\text{-structure such that } \mathcal{M} \vDash T\}.$$

Thus $\mathrm{Mod}(T) = \emptyset$ if and only if T is unsatisfiable and $\mathrm{Mod}(T)$ is the collection of all $\mathcal{L}$-structures if and only if T consists of valid sentences. Given a class $\mathscr{C}$ of $\mathcal{L}$-structures, we can ask whether there is some theory T in the language $\mathcal{L}$ such that $\mathscr{C} = \mathrm{Mod}(T)$. By Proposition 4.6(e) if $\mathcal{M} \in \mathrm{Mod}(T)$ and $\mathcal{N} \cong \mathcal{M}$, then $\mathcal{N} \in \mathrm{Mod}(T)$, and hence the problem is meaningful just in case $\mathscr{C}$ is closed under isomorphisms.

Definition 4.51. A class of $\mathcal{L}$-structures $\mathscr{C}$ is **axiomatizable** or **elementary** if $\mathscr{C} = \mathrm{Mod}(T)$ for some theory T; if T can be taken to be finite (or equivalently: finitely axiomatizable), then $\mathscr{C}$ is **finitely axiomatizable** or **basic elementary**. If $\mathscr{C}' = \mathrm{Mod}(T')$ then $\mathscr{C} \subset \mathscr{C}'$ is **finitely axiomatizable modulo** $\mathscr{C}'$ if $\mathscr{C} = \mathrm{Mod}(T' \cup \Sigma)$ for some finite set of axioms Σ.

The finite set Σ of sentences in the definition above can be replaced by its conjunction $\bigwedge \Sigma$, so if $\mathscr{C}_i = \mathrm{Mod}(T' \cup \{\sigma_i\})$ is finitely axiomatizable modulo $\mathscr{C}' = \mathrm{Mod}(T')$, then $\mathscr{C}_0 \cap \mathscr{C}_1$, $\mathscr{C}_0 \cup \mathscr{C}_1$, and $\mathscr{C}' \setminus \mathscr{C}_i$ are finitely axiomatized modulo $\mathscr{C}'$ via the sentences $\sigma_0 \wedge \sigma_1$, $\sigma_0 \vee \sigma_1$, and $\neg\sigma_i$, respectively. In other words: the family of all *finitely* axiomatizable classes is closed under taking intersections, unions and complements. For the axiomatizable classes, we have that

- $\mathrm{Mod}(T_0) \cap \mathrm{Mod}(T_1) = \mathrm{Mod}(T_0 \cup T_1)$, so the intersection of two axiomatizable classes is axiomatizable;
- the union of two axiomatizable classes is axiomatizable, if the language $\mathcal{L}$ has countably many non-logical symbols (Exercise 31.58 in Chapter VII),
- the complement of an axiomatizable class $\mathscr{C}$ is axiomatizable if and only if it is finitely axiomatizable, and so is $\mathscr{C}$ (Theorem 4.52).

If $\mathscr{C}$ is a class of $\mathcal{L}$-structures such as: the non-empty sets, the ordered sets, the groups, the rings, etc., then $\mathscr{C}$ is finitely axiomatized. Adding the sentences $\varepsilon_{\geq n}$ we obtain an axiomatization for the class $\mathscr{C}' \subseteq \mathscr{C}$ of all: infinite sets, infinite ordered sets, infinite groups, infinite rings, etc., and by Theorem 4.49 $\mathscr{C}'$ is axiomatizable, but not finitely axiomatizable. Finally the class $\mathscr{C} \setminus \mathscr{C}'$ of all: finite non-empty sets, finite ordered sets, finite groups, finite rings, etc., is not axiomatizable by Theorem 4.48. This is a particular instance of a general result.

Theorem 4.52. *Suppose $\mathscr{C}$ is an axiomatizable class, and that $\mathscr{C}_0 \cup \mathscr{C}_1 = \mathscr{C}$ and $\mathscr{C}_0 \cap \mathscr{C}_1 = \emptyset$. If $\mathscr{C}_0$ and $\mathscr{C}_1$ are axiomatizable, then they are finitely axiomatizable modulo $\mathscr{C}$.*

Proof. Let T be a set of axioms for $\mathscr{C}$, and let Σ_i be a set of axioms for $\mathscr{C}_i$, for $i = 0, 1$. Then $T \cup \Sigma_0 \cup \Sigma_1$ is unsatisfiable, so by compactness there are finite $\Sigma'_i \subseteq \Sigma_i$ such that $T \cup \Sigma'_0 \cup \Sigma'_1$ is unsatisfiable. Therefore $\mathscr{C} \supseteq \mathrm{Mod}(T \cup \Sigma'_i) \supseteq \mathrm{Mod}(T \cup \Sigma_i)$ and $\mathrm{Mod}(T \cup \Sigma'_0), \mathrm{Mod}(T \cup \Sigma'_1)$ partition $\mathscr{C}$, and therefore $\mathrm{Mod}(T \cup \Sigma'_i) = \mathrm{Mod}(T \cup \Sigma_i) = \mathscr{C}_i$. □

Theorem 4.53. *Let $\mathscr{C}' \subseteq \mathscr{C}$ be axiomatizable classes, and suppose that $\mathscr{C}'$ is not finitely axiomatizable modulo $\mathscr{C}$. Then $\mathscr{C} \setminus \mathscr{C}'$ is not axiomatizable.*

Proof. Apply Theorem 4.52 to $\mathscr{C}_0 = \mathscr{C}'$ and $\mathscr{C}_1 = \mathscr{C} \setminus \mathscr{C}'$. □

4.K.2. *Some examples.* Let $\mathcal{L}$ be the language with no logical symbols, so that the $\mathcal{L}$-structures are just the non-empty sets. Then $\{\varepsilon_{\geq n} \mid n \geq 1\}$ is the **theory of infinite sets**. Since any finite number of sentences in this theory has a finite model, it follows that this theory is not finitely axiomatizable.

Similarly, suppose $\mathcal{L}$ is any first-order language and T is any $\mathcal{L}$-theory that has arbitrarily large finite models. Then $T' = T \cup \{\varepsilon_{\geq n} \mid n \geq 1\}$ is the theory of all infinite models of T, and it is not finitely axiomatizable. Equivalently, letting $\mathscr{C} = \mathrm{Mod}(T)$ and $\mathscr{C}' = \mathrm{Mod}(T')$, then $\mathscr{C}'$ is not finitely axiomatizable modulo $\mathscr{C}$, while $\mathscr{C} \setminus \mathscr{C}'$, the class of all finite models of T, is not axiomatizable.

Corollary 4.54. *The classes of all infinite groups, infinite rings, infinite fields, infinite orders, ... are axiomatizable, but not finitely so. Therefore the classes of all finite groups, finite rings, finite fields, finite orders, ... are not axiomatizable.*

Theorem 4.55. *The class of torsion-free abelian groups is axiomatizable, but not finitely axiomatizable.*

The class of divisible abelian groups is axiomatizable, but not finitely axiomatizable, and hence the class of non-divisible groups is not axiomatizable.

Proof. Let T_{AbGr} be the set of axioms for abelian groups. The class of torsion-free abelian groups is axiomatized by $T_{\mathrm{AbGr}} \cup \{\tau_n \mid n \geq 1\}$, so by Theorem 4.49 it is enough to check no finite list of τ_ns suffices. Given $n_1, \dots, n_k$ take a prime number $p > n_1, \dots, n_k$ and consider the group $\mathbb{Z}(p)$: this is a torsion group that satisfies $\tau_{n_1} \wedge \dots \wedge \tau_{n_k}$.

The class of all divisible groups is axiomatized by $T_{\mathrm{AbGr}} \cup \{\delta_n \mid n \geq 2\}$, so it is enough to check no finite list of δ_ns suffices. Given n let p be a sufficiently large prime, say $n! < p$, so that $\mathbb{Z}[1/n!]$ is k-divisible, for all $k \leq n$, but it is not p-divisible. □

Corollary 4.56. *The set of torsion elements and the divisible part are not uniformly definable over class of all groups, that is to say: there are no formulæ* $\varphi_{\mathrm{Tor}}(x)$ *and* $\varphi_{\mathrm{Div}}(x)$ *that define* $\mathrm{Tor}(G)$ *and* $\mathrm{Div}(G)$ *for any group* G.

Proof. Towards a contradiction suppose $\varphi_{\mathrm{Tor}}(x)$ defines $\mathrm{Tor}(G)$ for all G. Then $\mathrm{Mod}(T_{\mathrm{Grps}} \cup \{\forall x\, \varphi_{\mathrm{Tor}}(x)\})$ would be the class of all torsion groups, against Theorem 4.55.

The case for $\varphi_{\mathrm{Div}}(x)$ is similar. □

Recall from Example 4.39 that $\mathrm{F}_0, \mathrm{F}_p$ are the theories of fields of characteristic zero and p, respectively; ACF is the theory of all algebraically closed fields, while $\mathrm{ACF}_0, \mathrm{ACF}_p$ are the theories of all algebraically closed fields of characteristic zero or p.

The theory F_p is finitely axiomatized, while F_0 has infinitely many axioms $n1 \neq 0$: given any finite list of these axioms we can choose a large enough prime p so that $\mathbb{Z}(p)$ satisfies all these finitely many axioms, but does not satisfy $p1 \neq 0$. Therefore F_0 is not finitely axiomatizable.

The theory ACF has infinitely many axioms. By standard results in algebra it is possible to construct a non-algebraically closed field (of any prescribed characteristic) satisfying finitely many of these axioms. Therefore none of ACF, ACF_0, ACF_p is finitely axiomatizable.

Recapping:

Theorem 4.57. *The classes of all algebraically closed fields* Mod(ACF) *and of all fields of characteristic zero* $\mathrm{Mod}(\mathrm{F}_0)$ *are not finitely axiomatizable.*

The class $\mathrm{Mod}(\mathrm{ACF}_0)$ *of all algebraically closed fields of characteristic zero is not finitely axiomatizable modulo either* Mod(ACF) *or* $\mathrm{Mod}(\mathrm{F}_0)$*.*

Many axiomatizable classes of infinite structures are not finitely axiomatizable. On the other hand there are finitely axiomatizable classes with only infinite structures, for example: dense linear orders, atomless Boolean algebras, non-commutative division rings (Wedderburn's Theorem), ... In the next sections we shall see more examples of classes of structures which are finitely axiomatizable, and also examples of classes that are axiomatizable, but not finitely so, and examples of classes that are not axiomatizable at all. Just like for definability, it is much easier to show that a class is (finitely) axiomatizable, rather than proving the opposite. Sometimes the problem of (finite) axiomatizability of a class of structures depends on the language. The class of bipartite graphs is axiomatizable, but not finitely so, in the language of graphs (Exercise 10.12 in Chapter III), while the same class is finitely axiomatizable in a suitable extended language. A similar situation happens for the class of abelian torsion-free groups (Example 9.6(d) and Exercise 32.13). Another interesting example is the class of **homogeneous linear orders**, that is linear orders such that for any pair of elements a, b there is an automorphism F (that is an increasing bijection) such that $F(a) = b$. By Exercises 4.90 and 32.15 homogeneous linear orders are not axiomatizable in the language containing only $<$, but they are finitely axiomatizable in a suitably extended language.

4.L. Some applications of compactness.

Theorem 4.58. *Let* $(G, \cdot)$ *be a group such that* $\forall n \geq 2\, \exists g \in G\, (o(g) \geq n)$*. There is a group* H *which is elementarily equivalent to* G *and such that* $\exists h \in H\, (o(h) = \infty)$*.*

Proof. Let $\mathcal{L}$ be the language extending $\mathcal{L}_{\mathrm{SGRPS}}$ by adding a new constant symbol c. An $\mathcal{L}$-structure $(H, \cdot, h)$ consists of a non-empty set H with a binary operation $\cdot$ and a chosen element h. If $(H, \cdot, h)$ is a model of

$$\Sigma = \mathrm{Th}(G) \cup \{c^{n+1} \neq 1 \mid n \in \mathbb{N}\}$$

then $(H, \cdot) \vDash \mathrm{Th}(G)$ so it is a group elementarily equivalent to $(G, \cdot)$. Moreover the element h must satisfy $h^{n+1} \neq 1_H$ for all n so it is torsionless. Therefore it is enough to prove that Σ is satisfiable. By compactness it is enough to prove that every finite $\Sigma_0 \subseteq \Sigma$ is satisfiable. Given Σ_0 choose N large enough so that if $c^{n+1} \neq 1$ belongs to Σ_0 then $n < N$. So it is enough to show that $\Delta \overset{\text{def}}{=} \mathrm{Th}(G) \cup \{c^{n+1} \neq 1 \mid n < N\} \supseteq \Sigma_0$ is satisfiable. But $(G, \cdot, \bar{g}) \vDash \Delta$, where $\bar{g} \in G$ is an element of order $> N$. This proves the theorem. □

The strategy of the proof of Theorem 4.58 is more important than the statement, so let us summarize it. Given a theory T with a model $\mathcal{M} = (M, \dots)$, one expands the language by adding new symbols (in this case a constant c) and extends T to a new theory $\Sigma = T \cup \{\sigma_n \mid n \in \mathbb{N}\}$ whose satisfiability would prove the result. (In our case T is $\mathrm{Th}(G)$, $\mathcal{M} = (G, \cdot)$, and σ_n is $c^{n+1} \neq 1$.) By the compactness theorem it is enough to show that $T \cup \{\sigma_n \mid n \in I\}$ is satisfiable, for any finite $I \subseteq \mathbb{N}$. For each I one choses an appropriate element $\bar{a}_I \in M$ so that the expanded structure $\mathcal{M}_I = (M, \dots, \bar{a}_I)$ is a model of $T \cup \{\sigma_n \mid n \in I\}$, proving the result.

An ordered field is **Archimedean** if it satisfies **Archimedes' principle**

$$\forall x \exists n \in \mathbb{N} \big(0 < x \Rightarrow x < n1\big).$$

If K is a non-Archimedean ordered field, an element $\xi \in K$ is said to be infinite positive if $n1 < \xi$ for all n. Its opposite $\eta = -\xi$ satisfies $\eta < -n1$ for all n, and it is an infinite negative element. The inverse ε of an infinite (positive or negative) element is called an infinitesimal and satisfies $\varepsilon \neq 0$ and $-1 < n\varepsilon < 1$ for all n.

The field $\mathbb{R}$ and its subfields are Archimedean, as Archimedes' property is preserved by taking substructures. Observe that the definition of the Archimedean property is not a first-order formula, it is only a pseudo-formula.

Theorem 4.59. *Every field is elementarily equivalent to a non-Archimedean one. Therefore the Archimedean property is not first-order.*

Proof. Let $(F, +, \cdot, 0_F, 1_F, <)$ be an ordered field. Let c be a new constant symbol and consider the theory

$$\Sigma = \mathrm{Th}(F) \cup \{n1 < c \mid n \in \mathbb{N}\}.$$

If $(K, +, \cdot, 0_K, 1_K, \bar{k}) \vDash \Sigma$ then $(K, +, \cdot, 0_K, 1_K)$ is a non-Archimedean field (witnessed by the element $\bar{k}$) elementary equivalent to $(F, +, \cdot, 0_F, 1_F, <)$. □

With further work it is possible to construct a non-Archimedean field ${}^*\mathbb{R}$ such that $\mathbb{R}$ elementarily embeds into it, and any $f \colon \mathbb{R}^n \to \mathbb{R}$ can be extended to a ${}^*f \colon {}^*\mathbb{R}^n \to {}^*\mathbb{R}$. In this context it is possible to develop mathematical analysis using infinite and infinitesimal "numbers". This is the starting point of an important branch of mathematical logic known as **non-standard analysis**.

4.L.1. *Complex variables.* Recall (Example 4.39) that ACF_p and ACF_0, the theory of algebraically closed fields of characteristic p (a prime number) or zero, are complete theories. Using this one can prove an interesting result in complex analysis.

Theorem 4.60 (Ax)**.** *Every injective polynomial function $f\colon \mathbb{C}^n \to \mathbb{C}^n$ is surjective.*

By a polynomial function $f = (f_1, \dots, f_n)\colon R^n \to R^n$ where R is a rng, we mean n polynomials in n variables $f_i \in R[X_1, \dots, X_n]$ for $i = 1, \dots, n$. The degree of f is $\max(\deg(f_1), \dots, \deg(f_n))$. It is a trivial, but tedious matter to check that for all $n, d > 0$ there is a $\forall\exists$-sentence $\sigma_{n,d}$ of $\mathcal{L}_{\text{RNGS}}$ such that for each R commutative ring, $R \vDash \sigma_{n,d}$ if and only if

every injective polynomial function $R^n \to R^n$ of degree $\leq d$ is surjective.

Observe that if R is finite, then so is R^n, so $R \vDash \sigma_{n,d}$ as any injective function $R^n \to R^n$ must be surjective.

Ax's theorem amounts to prove that for all $n, d > 0$, $\mathbb{C} \vDash \sigma_{n,d}$; equivalently $\mathrm{ACF}_0 \models \sigma_{n,d}$. Towards a contradiction and using the completeness of ACF_0, suppose $\mathrm{ACF}_0 \models \neg\sigma_{\bar{n},\bar{d}}$, for some $\bar{n}, \bar{d} > 0$. By compactness, there is N such that

$$\Sigma \overset{\text{def}}{=} \mathrm{ACF} \cup \{k1 \neq 0 \mid k \leq N\} \models \neg\sigma_{\bar{n},\bar{d}}.$$

If $\mathbb{F}$ is an algebraically closed field of characteristic $p > N$, then $\mathbb{F} \vDash \Sigma$, so $\mathbb{F} \vDash \neg\sigma_{\bar{n},\bar{d}}$. Therefore a contradiction is attained, and hence Theorem 4.60 will be proved, once we show the following result.

Theorem 4.61. $\mathrm{ACF}_p \models \sigma_{n,d}$ *for all* $n, d > 0$ *and all primes* p.

Proof. Fix n, d, p. The theory ACF_p is complete, so it is enough to prove that $\overline{\mathbb{Z}(p)}$, the algebraic closure of $\mathbb{Z}(p)$, satisfies $\sigma_{n,d}$. As $\overline{\mathbb{Z}(p)} = \bigcup_{k\in\mathbb{N}} \mathbb{F}_k$ is the increasing union of finite fields $\mathbb{F}_k$, then each $\mathbb{F}_k$ satisfies $\sigma_{n,d}$, and so does $\overline{\mathbb{Z}(p)}$ by Proposition 4.20. □

Exercises

Exercise 4.62. Let $(P, \preceq)$ and $(Q, \trianglelefteq)$ be orders and let $f\colon P \to Q$. Show that:

(i) $f\colon (P, \preceq) \to (Q, \trianglelefteq)$ is an embedding (in the sense of structures) if and only if $\forall x, y \in P\ (x \preceq y \Leftrightarrow f(x) \trianglelefteq f(y))$,

(ii) if f is an embedding, then it is increasing,

(iii) the implication in (ii) cannot be reversed,

(iv) if $(P, \preceq)$ is total and f monotone then $\forall x, y \in P\, (f(x) \lhd f(y) \Rightarrow x \prec y)$,

(v) if $(P, \preceq)$ is total and f increasing then $\forall x, y \in P\, (x \preceq y \Leftrightarrow f(x) \unlhd f(y))$,

(vi) the assumption "$(P, \preceq)$ is total" in (v) cannot be removed.

Exercise 4.63. Check that:

(i) if $F\colon M \to N$ is a morphism of structures, then $\operatorname{ran}(F)$ is a substructure of N, and $F\colon M \to \operatorname{ran}(F)$ is a morphism of structures;

(ii) if $\mathcal{L}$ does not contain relation symbols, then a bijective morphism $F\colon M \to N$ is an isomorphism;

(iii) M embeds into N if and only if M is isomorphic to a substructure of N;

(iv) if $F\colon M \to N$ is bijective and (A′), (B) and (C) on page 70 hold, then F is an isomorphism.

Exercise 4.64. Use the notation of Example 3.35.

(i) Verify that the following sets are definable in M: $g[M \setminus f^{-1}[P]]$, $f^{-1}[P] \setminus g[Q]$, $f[P] \mathbin{\triangle} f[Q]$.

(ii) Find a sentence σ such that $M \vDash \sigma$ if and only if $f[P] \cup g[P] \subseteq f^{-1}[P] \cap g^{-1}[Q]$.

Exercise 4.65. Show that the covering relation (see page 46) is definable from the ordering relation $\leq$.

Exercise 4.66. A **semi-lattice-algebra** is a commutative semigroup $(S, \cdot)$ satisfying the idempotence property, that is $\forall x\, (x \cdot x = x)$.

(i) Show that if $(L, \leq)$ is an upper semi-lattice, then $(L, \curlyvee)$ is a semi-lattice-algebra. Similarly, if $(L, \leq)$ is a lower semi-lattice, then $(L, \curlywedge)$ is a semi-lattice-algebra.

(ii) In semi-lattice-algebra $(S, \cdot)$ we define the relations $\leq_\curlyvee$ and $\leq_\curlywedge$ on L by letting $a \leq_\curlyvee b \Leftrightarrow a \cdot b = b$ and $a \leq_\curlywedge b \Leftrightarrow a \cdot b = a$. Show that $(L, \leq_\curlyvee)$ is an upper semi-lattice and $(L, \leq_\curlywedge)$ is a lower semi-lattice, and that $(L, \leq_\curlyvee)$ and $(L, \leq_\curlywedge)$ are dual to each other. Moreover $\sup_{\leq_\curlyvee}(a, b) = a \cdot b = \inf_{\leq_\curlywedge}(a, b)$.

Exercise 4.67. (i) Show that in a finite linear order every element is definable and hence every subset is definable without parameters.

(ii) Consider the ordered sets $\mathcal{M}_3$ and $\mathcal{N}_5$ of figure 7 on page 78, and find their definable elements and their subsets that are definable without parameters.

(iii) If L is a finite linear order of size $n \geq 1$ then the order $L \times L$ has n definable elements.

Exercise 4.68. Show that in every lattice the following sentences hold:

$$\begin{aligned}
&\forall x, y, z\,((x \curlywedge y) \curlyvee z \leq (x \curlyvee z) \curlywedge (y \curlyvee z))\\
&\forall x, y, z\,((x \curlywedge z) \curlyvee (y \curlywedge z) \leq (x \curlyvee y) \curlywedge z)\\
&\forall x, y, z\,((x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z))\\
&\qquad\qquad \Leftrightarrow \forall x, y, z\,((x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z))\\
&\forall x, y, z\,(z \leq x \Rightarrow (x \curlywedge y) \curlyvee z \leq x \curlywedge (y \curlyvee z))\\
&\forall x, y, z\,((x \curlywedge y) \curlyvee (x \curlywedge z) = x \curlywedge (y \curlyvee (x \curlywedge z)))\\
&\qquad\qquad \Leftrightarrow \forall x, y, z\,(z \leq x \Rightarrow x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee z)\\
&\qquad\qquad \Leftrightarrow \forall x, y, z\,((x \curlyvee y) \curlywedge (x \curlyvee z) = x \curlyvee (y \curlywedge (x \curlyvee z))).
\end{aligned}$$

Exercise 4.69. Show that:

(i) Every distributive lattice is modular.

(ii) The lattice $\mathcal{N}_5$ is not modular, while the lattice $\mathcal{M}_3$ is modular, but not distributive.

Exercise 4.70. Show that $(x \curlywedge y) \curlyvee (y \curlywedge z) \curlyvee (x \curlywedge z) = (x \curlyvee y) \curlywedge (y \curlyvee z) \curlywedge (x \curlyvee z)$ holds in any distributive lattice.

Exercise 4.71. Suppose R_i is a binary relation on $X_i \neq \emptyset$ with $i = 0, 1$. Let $R_0 \otimes R_1$ be the binary relation on $X_0 \times X_1$ defined by

$$(x_0, x_1)\ R_0 \otimes R_1\ (x'_0, x'_1) \Leftrightarrow x_0\ R_0\ x'_0 \wedge x_1\ R_1\ x'_1$$

so that $(X_0 \times X_1, R_0 \otimes R_1)$ is the product of the two structures (X_0, R_0) and (X_1, R_1). Show that

- R_0, R_1 are reflexive if and only if $R_0 \otimes R_1$ is reflexive;
- if R_0, R_1 are symmetric then $R_0 \otimes R_1$ is symmetric. Conversely if $R_0 \otimes R_1$ is symmetric and $R_{1-i} \neq \emptyset$ then R_i is symmetric;
- if R_0, R_1 are transitive then $R_0 \otimes R_1$ is transitive. Conversely if $R_0 \otimes R_1$ is transitive and $\operatorname{dom}(R_{1-i}) \cap \operatorname{ran}(R_{1-i}) \neq \emptyset$ then R_i is transitive;
- R_0, R_1 are preorders if and only if $R_0 \otimes R_1$ is a preorder;
- R_0, R_1 are equivalence relations if and only if $R_0 \otimes R_1$ is an equivalence relation;
- if R_0, R_1 are antisymmetric then $R_0 \otimes R_1$ is antisymmetric. Conversely if $R_0 \otimes R_1$ is antisymmetric and R_{1-i} is not irreflexive then R_i is antisymmetric;
- R_0, R_1 are orders if and only if $R_0 \otimes R_1$ is an order;
- R_0, R_1 are upward/downward directed orders if and only if $R_0 \otimes R_1$ is an upward/downward directed order.

Exercise 4.72. For each pair of structures

$$(\mathbb{R}_+, \cdot), \quad (\mathbb{Q}_+, \cdot), \quad (\mathbb{R} \setminus \{0\}, \cdot), \quad (\mathbb{Q} \setminus \{0\}, \cdot), \quad (\mathbb{R}, +), \quad (\mathbb{Q}, +)$$

determine whether they are isomorphic, or one embeds into the other. Repeat the argument for: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N} \setminus \{0\}, \cdot)$.

Exercise 4.73. Show that $(\mathbb{R}_+, \cdot)$, $(\mathbb{Q}_+, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ are pairwise elementarily inequivalent.

Exercise 4.74. Show that:

(i) If $f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is such that $f(a + c, b + d) = f(a, b) + f(c, d)$ for all $a, b, c, d \in \mathbb{N}$, then $f(0, 0) = 0$ and $f(0, m) = f(n, 0) = nm$ where $n = f(0, 1)$ and $m = f(1, 0)$. In particular, f is not injective, and hence $(\mathbb{N} \times \mathbb{N}, +)$ does not embed into $(\mathbb{N}, +)$.

(ii) $(\mathbb{Z}_+, \cdot)$ is isomorphic to $(\mathbb{N}[X], +)$. Conclude that $(\mathbb{Z}_+ \times \mathbb{Z}_+, \cdot)$ is isomorphic to $(\mathbb{Z}_+, \cdot)$, where multiplication on $\mathbb{Z}_+ \times \mathbb{Z}_+$ is defined componentwise, that is $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$.

(iii) There is no injective function $f \colon \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ such that for all $a, b, c, d \in \mathbb{Z}_+$

$$f(a, b \cdot d) = f(a, b) \cdot f(a, d) \quad \text{or} \quad f(a \cdot c, b) = f(a, b) \cdot f(c, b).$$

Exercise 4.75. Let M be an $\mathcal{L}$-structure and $p_1, \dots, p_k \in M$. Show that

(i) if $f_1, \dots, f_n$ are partial functions from M^m to M and g is a partial functions from M^n to M, and are definable in M with parameters $p_1, \dots, p_k$, then the partial function h from M^m to M defined by $h(\vec{x}) = g(f_1(\vec{x}), \dots, f_n(\vec{x}))$ is definable with parameters $p_1, \dots, p_k$;

(ii) if f is a partial injective function from M into itself, and it is definable with parameters $p_1, \dots, p_k$, then so is the partial function f^{-1}.

Exercise 4.76. Show that:

(i) Every element is definable in $(\mathbb{N}, +)$.

(ii) Every element is definable in $(\mathbb{Z}, +, \cdot)$.

(iii) Every element is definable in $(\mathbb{Q}, +, \cdot)$.

(iv) $(\mathbb{N}, S)$, $(\mathbb{N}, +)$, $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are rigid structures.

(v) 0 is the only definable element in the structure $(\mathbb{Z}, +)$.

(vi) Neither $\mathbb{N}$ nor $<$ are definable without parameters in $(\mathbb{Z}, +)$ and in $(\mathbb{R}, +)$.

Exercise 4.77. Show that the following sets are definable in $(\mathbb{N}, |)$, where $|$ is the divisibility relation:

(i) $\{0\}$ and $\{1\}$;

(ii) $\{n \mid n \text{ is not prime}\}$;

(iii) $\{p^n \mid p \text{ is prime and } n > 0\}$;

(iv) $\{p^2 \mid p \text{ is prime}\}$;

(v) $\{pq \mid p \text{ and } q \text{ are distinct primes}\}$;

(vi) $\{(n, m) \in \mathbb{N}^2 \mid n \perp m\}$, where $n \perp m$ means that n and m are coprime;

(vii) $\{(n, m, k) \in \mathbb{N}^3 \mid k = \mathrm{lcm}(n, m)\}$, where $\mathrm{lcm}(n, m)$ is the least common multiple of n and m;

(viii) $\{(n, m, k) \in \mathbb{N}^3 \mid k = \gcd(n, m)\}$, where $\gcd(n, m)$ is the greatest common divisor of n and m.

Exercise 4.78. Show that the complex field and the group $\{z \in \mathbb{C} \mid |z| = 1\}$ are definably interpretable in $(\mathbb{R}; +, \cdot)$.

Exercise 4.79. Let H be a subgroup of a group G. The **normalizer of** H **in** G is $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. Show that if H is definable with parameters $p_1, \dots, p_n$, then also $N_G(H)$ is definable with the same parameters.

Exercise 4.80. Let $G = \{z \in \mathbb{C} \mid |z| = 1\}$. Show that:

(i) $f \colon (\mathbb{R}+) \to (G, \cdot)$, $f(x) = \mathrm{e}^{2\pi \mathrm{i} x}$, is a surjective homomorphism and $\ker f = \mathbb{Z}$;

(ii) $\mathrm{Tor}(G) = \{\mathrm{e}^{2\pi \mathrm{i} x} \mid x \in \mathbb{Q}\}$, the group of all roots of unity;

(iii) G is an infinite abelian group that has torsion elements with arbitrarily large order, and has elements without torsion;

(iv) there are distinct $z, w \in G \setminus \mathrm{Tor}(G)$ such that $zw \in \mathrm{Tor}(G)$. Therefore the set of all torsionless elements together with 1_G is not a subgroup.

Exercise 4.81. Let $G = \bigoplus_{n>0} \mathbb{Z}[1/n]$. Show that $G \cong \bigoplus_{n>0} \mathbb{Z}$ and that $mG \cong G$ and $\bigcap_{m \geq 1} mG = \{0_G\}$.

Exercise 4.82. Let $n > 1$. Show that in $\mathbb{Z}/n\mathbb{Z}$ every subgroup is definable without parameters. What are the definable elements of $\mathbb{Z}/n\mathbb{Z}$?

Exercise 4.83. Show that:

(i) the divisible torsion-free abelian groups are exactly the vector spaces over $\mathbb{Q}$, and that homomorphisms between divisible torsion-free abelian groups is a linear map between the corresponding spaces;

(ii) if G is a divisible torsion-free abelian group, then the only subsets that are definable without parameters are $\emptyset$, G, $\{0_G\}$, and $G \setminus \{0_G\}$. [Hint: a linearly independent set of vectors can be extended to a basis.[21]] In particular, 0_G is the unique definable element;

[21] This fact requires the axiom of choice.

(iii) each group $\mathbb{Z}/n\mathbb{Z}$ is definable in $\mathbb{R}/\mathbb{Z}$, with the identifications $\mathbb{Z}/n\mathbb{Z} \cong \{\mathrm{e}^{2\mathrm{i}\pi k/n} \mid 0 \leq k < n\}$ and $\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} \mid |z| = 1\}$,

(iv) Let $x \in G \setminus \{0_G\}$ where G is an abelian n-divisible group. Show that if G is ordered, then there is a unique $y \in G$ such that $ny = x$. Show with a counterexample that the result does not hold if G is not orderable.

Exercise 4.84. (i) Show that a semigroup $(S, \cdot)$ is a group if and only if there is an $e \in S$ which is a **left identity**, that is $e \cdot x = x$ for all $x \in S$, and for every $x \in S$ there is $y \in S$ which is a **left inverse with respect to** e, that is $y \cdot x = e$. Similarly, if we assume a right identity and right inverses.

(ii) If S has at least two elements and satisfies $\forall x, y\, (x \cdot y = x)$ then $(S, \cdot)$ is an example of a semigroup with a left identity, every element has a right inverse, but it is not a group.

(iii) Find an axiom system for groups, and for torsion-free groups, in the language $\mathcal{L}_{\mathrm{SGRPS}}$.

Exercise 4.85. Let B and C be Boolean algebras, with B not atomless and C not atomic. Show that the Boolean algebra $B \times C$ is neither atomic nor atomless.

Exercise 4.86. (i) Consider the following classes of $\mathcal{L}_{\mathrm{GRPS}}$-structures:

- For $n \geq 2$, $\mathscr{C}_{\leq n}$ and $\mathscr{C}_{\geq n}$ are the collections of all groups such that each element (other than the identity) has order $\leq n$ and $\geq n$ respectively. Thus $\mathscr{C}_n = \mathscr{C}_{\leq n} \cap \mathscr{C}_{\geq n}$ is the collections of all groups such that each element (other than the identity) has order n,
- $\mathscr{C}_{<\omega}$ is the collection of all groups such that each element has finite order,
- $\mathscr{C}_\infty$ is the collection of all groups such that each element (other than the identity) has infinite order.

For each of the classes $\mathscr{C}_{\leq n}$, $\mathscr{C}_{\geq n}$, $\mathscr{C}_n$, $\bigcup_{2 \leq n} \mathscr{C}_n$, $\mathscr{C}_{<\omega}$, and $\mathscr{C}_\infty$ determine whether it is an axiomatizable class, and in the affirmative case whether it is finitely axiomatizable.

(ii) The conjugacy class of $g \in G$ is $\{h^{-1}gh \mid h \in G\}$, and the conjugacy class of 1_G is $\{1_G\}$, and it is said to be trivial. The size of conjugacy classes depends on the group: in the abelian case every conjugacy class is a singleton, but if the group is not abelian they can be quite large. For example, if $n \geq 5$ then the least size of a non-trivial conjugacy class of S_n is $\binom{n}{2}$.

Consider the following classes of $\mathcal{L}_{\mathrm{GRPS}}$-structures:

- for $n \geq 2$ the class $\mathscr{C}_{\geq n}$ is the collection of all groups such that each non-trivial conjugacy class has size $\geq n$,

- $\mathscr{C}_{<\omega}$ the collection of all groups such that each conjugacy class is finite,
- $\mathscr{C}_{\infty}$ the collection of all groups such that each non-trivial conjugacy class is infinite,
- $\mathscr{C}^{\geq n}$ is the collection of all groups with at least n conjugacy classes,
- $\mathscr{C}^{<\omega}$ the collection of all groups with finitely many conjugacy classes,
- $\mathscr{C}^{\infty}$ the collection of all groups with infinitely many conjugacy classes.

Note that $\bigcup_{2\leq n}\mathscr{C}_{\geq n}\subset\mathscr{C}_{<\omega}$ but $\bigcup_{2\leq n}\mathscr{C}^{n}=\mathscr{C}^{<\omega}$. For each of the classes $\mathscr{C}_{\geq n}$, $\bigcup_{2\leq n}\mathscr{C}_{\geq n}$, $\mathscr{C}_{<\omega}$, $\mathscr{C}_{\infty}$, $\mathscr{C}^{\geq n}$, $\mathscr{C}^{<\omega}$, and $\mathscr{C}^{\infty}$ determine whether it is an axiomatizable class, and in the affirmative case whether it is finitely axiomatizable.

Exercise 4.87. Let $\mathcal{L}$ be the language with a binary relation symbol. By a minor abuse of notation, call an $\mathcal{L}$-structure (X,R) an equivalence relation if R is an equivalence relation on X. Consider the following classes of $\mathcal{L}$-structures:

- $\mathscr{C}_{n}$: all equivalence relations whose equivalence classes have size n,
- $\mathscr{C}_{<\omega}$: all equivalence relations whose equivalence classes are finite,
- $\mathscr{C}_{\infty}$: all equivalence relations whose equivalence classes are infinite,
- $\mathscr{C}^{n}$: all equivalence relations with exactly n equivalence classes,
- $\mathscr{C}^{<\omega}$: all equivalence relations with finitely many equivalence classes,
- $\mathscr{C}^{\infty}$: all equivalence relations with infinitely many equivalence classes.

Note that $\bigcup_{n}\mathscr{C}_{n}\subset\mathscr{C}_{<\omega}$ but $\bigcup_{n}\mathscr{C}^{n}=\mathscr{C}^{<\omega}$. For each of the classes $\mathscr{C}_{n}$, $\bigcup_{n}\mathscr{C}_{n}$, $\mathscr{C}_{<\omega}$, $\mathscr{C}_{\infty}$, $\mathscr{C}^{n}$, $\mathscr{C}^{<\omega}$, and $\mathscr{C}^{\infty}$ determine whether it is an axiomatizable class, and in the affirmative case whether it is finitely axiomatizable.

Exercise 4.88. (i) Show that both the class of all atomic Boolean algebras, and the class of all atomless Boolean algebras, are finitely axiomatizable in $\mathcal{L}_{\textsc{Boole}}$.

(ii) Let $\mathscr{C}_{\leq n}$ be the class of all Boolean algebras with at most n many atoms, and let $\mathscr{C}_{\geq n}$ be the class of all Boolean algebras with at least n many atoms. Let also $\mathscr{C}_{<\omega}=\bigcup_{n}\mathscr{C}_{\leq n}$ be the class of all Boolean algebras with finitely many atoms, and let $\mathscr{C}_{\infty}$ be the class of all Boolean algebras with infinitely many atoms. For each class determine whether it is axiomatizable, and in the affirmative case whether it is finitely axiomatizable.

Exercise 4.89. Let Σ be a set of sentences. Show that:

(i) If $\sigma\in\Sigma$ and σ is valid, then Σ and $\Sigma\setminus\{\sigma\}$ are logically equivalent.

(ii) If Σ is finite there is $\Delta\subseteq\Sigma$ which is independent and logically equivalent to Σ.

(iii) Suppose $\Sigma = \{\sigma_n \mid n \in \mathbb{N}\}$ and that $\sigma_{n+1} \models \sigma_n$, but $\sigma_n \not\models \sigma_{n+1}$, for all $n \in \mathbb{N}$. Then
- Σ is not finitely axiomatizable,
- Σ has no independent subset of size ≥ 2,
- $\Delta = \{\tau_n \mid n \in \mathbb{N}\}$ is a set of axioms for Σ, and $\Delta \setminus \{\tau_n\} \not\models \tau_n$ for all $n \geq 1$, where τ_0 is σ_0 and τ_{n+1} is $\bigwedge_{i \leq n} \sigma_i \Rightarrow \sigma_{n+1}$.

(iv) If Σ is countable, then it has a countable, independent set of axioms.

Exercise 4.90. Recall that a linear order L is homogeneous if for any pair of points a, b there is an automorphism $F_{ab} \colon L \to L$ sending a to b. Show that homogeneous linear orders are finitely axiomatizable in a language with $\leq$ and a 4-ary predicate $F(a, b, x, y)$.

Exercise 4.91. Following the notation of Example 4.38, show that the theories T_n ($n \in \mathbb{N}$) and T_∞ are the only complete extensions of $T_\emptyset$.

Exercise 4.92. Prove Theorem 4.46 from Corollary 4.47.

Exercise 4.93. Let $\Bbbk$ be a field and $n > 1$. Show that the following structures are definably interpretable in $\Bbbk$:

(i) the ring $M_{n,n}(\Bbbk)$ of all $n \times n$ matrices;

(ii) the groups $\mathrm{GL}_n(\Bbbk)$ of all invertible $n \times n$ matrices, and $\mathrm{SL}_n(\Bbbk)$ of all $n \times n$ matrices with determinant 1;

(iii) the set of all nilpotent $n \times n$ matrices, i.e. those $A \in M_{n,n}(\Bbbk)$ such that $A^m = \mathbf{0}$ for some $m \in \mathbb{N}$, and the set of all diagonalizable $n \times n$ matrices.

Show that the groups $\mathrm{PGL}_n(\Bbbk) \overset{\text{def}}{=} \mathrm{GL}_n(\Bbbk)/C(\mathrm{GL}_n(\Bbbk))$, and $\mathrm{PSL}_n(\Bbbk) \overset{\text{def}}{=} \mathrm{SL}_n(\Bbbk)/C(\mathrm{SL}_n(\Bbbk))$, where C is the center, are definably interpretable in a quotient of $\Bbbk$.

Exercise 4.94. Suppose $A \subseteq \mathbb{R}^n$ is definable with parameters $p_1, \dots, p_k \in \mathbb{R}$, in the field $(\mathbb{R}, +, \cdot, 0, 1)$. Show that $\mathrm{Cl}(A)$ and $\mathrm{Int}(A)$, the closure and the interior of A, are definable with the same parameters.

Exercise 4.95. Let $\Bbbk$ be an infinite field, let $G = \{\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) \mid x, y \in \Bbbk \wedge x \neq 0\}$, and let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} b & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $b \in \Bbbk \setminus \{0, 1\}$. Show that:

(i) G is a group under matrix multiplication;

(ii) the centralizers of A and B are $C_G(A) = \{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \mid x \in \Bbbk\}$ and $C_G(B) = \{\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) \mid x \in \Bbbk \setminus \{0\}\}$, and that $C_G(B)$ acts on $C_G(A)$ by conjugation:

$$\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & y/x \\ 0 & 1 \end{smallmatrix}\right);$$

(iii) the map $j \colon C_G(A) \setminus \{I\} \to C_G(B)$, $j(M) = N \Leftrightarrow N^{-1}MN = A$ where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, is well-defined and $j\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$;

(iv) the operation $*\colon C_G(A) \times C_G(A) \to C_G(A)$,

$$M * N = \begin{cases} j(N)M\left(j(N)\right)^{-1} & \text{if } N \neq I \\ I & \text{otherwise} \end{cases}$$

is well-defined, commutative and associative, and it is definable in G using the parameters A and B;

(v) $(\Bbbk, +, \cdot, 0, 1)$ is isomorphic to $(C_G(A), \cdot, *, I, A)$. Conclude that the field $\Bbbk$ is definably interpretable in the group G.

Notes and remarks

The first axiomatizations of groups (abelian or otherwise) via a single equation as described in Remark 4.11, were isolated by Tarski in 1938, and Higman and Neumann in 1952—see [**MS96**] for an interesting survey of these classical results and more recent developments. Exercise 4.95 is taken from [**Mar02**].

5. Derivations

In the previous pages we have seen as mathematical logic can be used to formalize mathematical statements, and how to make rigorous the notion that a sentence σ is true in a structure $\mathcal{M}$. In this section we will tap another aspect of logic, namely the study of the underpinnings of mathematical proofs. More precisely we are going to define the notion of **derivation**, which is the precise mathematical counterpart of the concept of proof. If we restrict to proofs of identities we have the **equational calculus**; if we focus on proofs that are based only on connectives we have the **propositional calculus**; if we allow also quantifiers we obtain the **predicate calculus**.

A formula A can be derived from Γ, in symbols $\Gamma \vdash \mathrm{A}$, if there is a finite sequence $\mathrm{P}_1, \dots, \mathrm{P}_n$ of formulæ such that $\mathrm{P}_n = \mathrm{A}$ and each P_i either is in Γ or else it is a **logical axiom**, or else it is obtained from earlier P_js using some **rules**.[22] (A logical axiom is a statement of a specific form that can used to build derivations.) We write $\Gamma, \mathrm{B} \vdash \mathrm{A}$ rather than $\Gamma \cup \{\mathrm{B}\} \vdash \mathrm{A}$, and write $\mathrm{B}_1, \dots, \mathrm{B}_n \vdash \mathrm{A}$ instead of $\{\mathrm{B}_1, \dots, \mathrm{B}_n\} \vdash \mathrm{A}$.

The simplest system for derivations is the equational calculus. It is suitable for first order languages without predicate symbols, formulæ are equations $s = t$ for some terms s, t, and the only rule is the high-school rule of substituting equal quantities inside equal terms.

[22] Capital roman letters like A, B, ... range over formulæ (or propositions), and Γ, Δ, ... range over (possibly empty) sets of formulæ.

In order to deal with formulæ with connectives and quantifiers we need to introduce suitable rules. The main goal of this section is to devise a fixed, finite set of rules and logical axioms for connectives and quantifiers. We first deal with the propositional logic (i.e. we only use connectives, no quantifiers are allowed), and then move to first-order logic.

5.A. Equational calculus. This logical calculus is meant to derive identities from other identities, so it is suitable for equational theories (Definition 4.10). Fix a language $\mathcal{L}$ without predicate symbols. The identity $s \doteq t$ can be derived from a set of identities Γ is there is a finite sequence $\alpha_0, \ldots, \alpha_n$ of identities such that α_n is $s \doteq t$, and each α_k for $k \leq n$ is either a **premise**, that is an identity in Γ or a logical axiom, or else it can be derived from earlier α_js by means of rules of inference: symmetry and transitivity for equality, and Leibniz' principle of indiscernibility of identicals

$$\frac{s \doteq t}{t \doteq s} \qquad \frac{s \doteq t \qquad t \doteq u}{s \doteq u} \qquad \frac{s_1 \doteq t_1 \qquad \cdots \qquad s_n \doteq t_n}{f(s_1, \ldots, s_n) \doteq f(t_1, \ldots, t_n)}$$

for any n-ary function symbol f of $\mathcal{L}$, and the substitution rule:

$$\frac{s \doteq t}{s[u_1/x_1, \ldots, u_n/x_n] \doteq t[u_1/x_1, \ldots, u_n/x_n]} .$$

The only logical axiom is $v_0 \doteq v_0$, where v_0 is the first variable in our official list of variables (see page 23).

Recall that if $\mathcal{A}$ is an $\mathcal{L}$-structure, an identity α is true in $\mathcal{A}$ if its universal closure holds in $\mathcal{A}$. It is immediate to check that if α is obtained by an inference rule from identities that are true in $\mathcal{A}$, then also α is true in $\mathcal{A}$, and since $v_0 \doteq v_0$ is true in any structure, we have the following result.

Theorem 5.1. *If* $\Gamma \vdash s \doteq t$ *then* $\Gamma \models s \doteq t$.

The result above says that the rules of equational calculus are sound, i.e. they yield true statements if applied to true statements. For this reason the result above is known as the Soundness Theorem for the equational calculus. The converse of Theorem 5.1 is the Completeness Theorem for the equational calculus.

Theorem 5.2. *If* $\Gamma \models s \doteq t$ *then* $\Gamma \vdash s \doteq t$.

Let us see two examples to illustrate derivations in the equality calculus.

Example 5.3. Let $\mathcal{L}_{\mathrm{SGRPS}}$ be the language with a binary function symbol $\cdot$. We claim that

$$(x \cdot y) \cdot z \doteq y \vdash x \doteq y.$$

Thus if $*$ is a binary operation on a nonempty set A such that $(a * b) * c = b$ for all $a, b, c \in A$, then A is a singleton.

Here is the derivation of $x = y$ from $(x \cdot y) \cdot z = y$: it is a list with three columns, the first one for the counter, the second for the identities, the third for the justification of the line in question: **p** stands for *premise* that is either a formula in Γ or else the logical axiom $v_0 = v_0$, $\mathbf{sym}(k)$ means that the current line is obtained from line k using *symmetry* of equality, $\mathbf{trn}(k, j)$ means that the the identity $s = u$ in the current line is obtained from the identities $s = t$ in line k and $t = u$ in line j using *transitivity* of equality, $\mathbf{ind}(k, j)$ means that the identity in this line is is obtained via using the *indiscernibility* of identicals, that is the identity in the current line is $s \cdot t = u \cdot v$ and $s = u$ is on line on line k and $t = v$ is on line j while $\mathbf{ind}(k)$ means that the identity in this line is $s^{-1} = t^{-1}$ where the equality in line k is $s = t$, and $\mathbf{sbs}(k)_{[t_1/x_1,\dots,t_m/x_m]}$ means that the line is obtained from the identity in line k by substituting $x_1, \dots, x_m$ with $t_1, \dots, t_m$. It goes without saying that if on line n we write $\mathbf{sym}(k)$, $\mathbf{trn}(k, j)$, $\mathbf{ind}(k, j)$ or $\mathbf{sbs}(k)_{[t_1/x_1,\dots,t_m/x_m]}$ then $j, k < n$.

1	$(x \cdot y) \cdot z = y$	$\mathbf{p}$
2	$(x \cdot x) \cdot z = x$	$\mathbf{sbs}(1)_{[x/y]}$
3	$((x \cdot x) \cdot z) \cdot y = z$	$\mathbf{sbs}(1)_{[x \cdot x/x, z/y, y/z]}$
4	$v_0 = v_0$	$\mathbf{p}$
5	$y = y$	$\mathbf{sbs}(4)_{[y/v_0]}$
6	$((x \cdot x) \cdot z) \cdot y = x \cdot y$	$\mathbf{ind}(2, 5)$
7	$x \cdot y = ((x \cdot x) \cdot z) \cdot y$	$\mathbf{sym}(6)$
8	$x \cdot y = z$	$\mathbf{trn}(7, 3)$
9	$x \cdot y = x$	$\mathbf{sbs}(8)_{[x/z]}$
10	$x \cdot y = y$	$\mathbf{sbs}(8)_{[y/z]}$
11	$x = x \cdot y$	$\mathbf{sym}(9)$
12	$x = y$	$\mathbf{trn}(11, 10)$

The derivation above is replete with trivial steps that most mathematicians would skip. For example common sense would suggest that $x \cdot y = z$ on line 8 should follow directly from lines 3 and 6. One way to avoid this is to relax the rule **trn** by allowing $s = t$ to be derived from any chain of identities that link the term s to the term t. Another rule that can be safely extended is **ind**: from $s = t$ we can infer $s \cdot u = t \cdot u$ or $u \cdot s = u \cdot t$ for any term u. These “relaxed” rules are called **derived rules**, that is auxiliary rules that can be derived from the official rules, aimed at simplifying derivations. Another pedantry is the step from line 4 to 5, and the solution is to declare any identity of the form $t = t$ should be taken to be an axiom.

Example 5.4. Let $\mathcal{L}_{\mathrm{GRPS}}$ be the language for groups with a binary function symbol $\cdot$, a unary function symbol $^{-1}$, and a constant symbol e. Let us show that $\Gamma \vdash (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$, where Γ is the set of the identities

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad x \cdot e = x \quad e \cdot x = x \quad x \cdot x^{-1} = e \quad x^{-1} \cdot x = e$$

1	$(xy)z \eqcirc x(yz)$	$\mathbf{p}$
2	$xe \eqcirc x$	$\mathbf{p}$
3	$ex \eqcirc x$	$\mathbf{p}$
4	$xx^{-1} \eqcirc e$	$\mathbf{p}$
5	$x^{-1}x \eqcirc e$	$\mathbf{p}$
6	$(xy)(y^{-1}x^{-1}) \eqcirc x(y(y^{-1}x^{-1}))$	$\mathbf{sbs}(1)_{[y^{-1}x^{-1}/z]}$
7	$(yy^{-1})x^{-1} \eqcirc y(y^{-1}x^{-1})$	$\mathbf{sbs}(1)_{[y/x, y^{-1}/y, x^{-1}/z]}$
8	$yy^{-1} \eqcirc e$	$\mathbf{sbs}(4)_{[y/x]}$
9	$x^{-1} \eqcirc x^{-1}$	$\mathbf{p}$
10	$(yy^{-1})x^{-1} \eqcirc ex^{-1}$	$\mathbf{ind}(9, 11)$
11	$ex^{-1} \eqcirc x^{-1}$	$\mathbf{sbs}(3)_{[x^{-1}/x]}$
12	$y(y^{-1}x^{-1}) \eqcirc x^{-1}$	$\mathbf{trn}(7, 10, 11)$
13	$x(y(y^{-1}x^{-1})) \eqcirc xx^{-1}$	$\mathbf{ind}(12)$
14	$(xy)(y^{-1}x^{-1}) \eqcirc e$	$\mathbf{trn}(6, 4, 13)$
15	$(xy)^{-1}((xy)(y^{-1}x^{-1})) \eqcirc (xy)^{-1}e$	$\mathbf{ind}(14)$
16	$(xy)^{-1}e \eqcirc (xy)^{-1}$	$\mathbf{sbs}(2)_{[(xy)^{-1}/x]}$
17	$((xy)^{-1}(xy))(y^{-1}x^{-1}) \eqcirc (xy)^{-1}((xy)(y^{-1}x^{-1}))$	$\mathbf{sbs}(1)_{[(xy)^{-1}/x, xy/y, y^{-1}x^{-1}/z]}$
18	$((xy)^{-1}(xy))(y^{-1}x^{-1}) \eqcirc (xy)^{-1}$	$\mathbf{trn}(15, 16, 17)$
19	$(xy)^{-1}(xy) \eqcirc e$	$\mathbf{sbs}(5)_{[xy/x]}$
20	$((xy)^{-1}(xy))(y^{-1}x^{-1}) \eqcirc e(y^{-1}x^{-1})$	$\mathbf{ind}(19)$
21	$e(y^{-1}x^{-1}) \eqcirc y^{-1}x^{-1}$	$\mathbf{sbs}(3)_{[y^{-1}x^{-1}/x]}$
22	$y^{-1}x^{-1} \eqcirc (xy)^{-1}$	$\mathbf{trn}(18, 20, 21)$

Figure 8. The derivation of Example 5.4.

that axiomatize the theory of groups. By associativity $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) \eqcirc x \cdot (y \cdot (y^{-1} \cdot x^{-1})) \eqcirc x \cdot ((y \cdot y^{-1}) \cdot x^{-1})$, and as $y \cdot y^{-1} \eqcirc x \cdot x^{-1} \eqcirc e$ and $e \cdot x^{-1} \eqcirc x^{-1}$, then $x \cdot ((y \cdot y^{-1}) \cdot x^{-1}) \eqcirc x \cdot (e \cdot x^{-1}) \eqcirc x \cdot x^{-1} \eqcirc e$. Therefore

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) \eqcirc e.$$

Multiplying on the left by $(x \cdot y)^{-1}$ the identity above $(x \cdot y)^{-1} \cdot ((x \cdot y) \cdot (y^{-1} \cdot x^{-1})) \eqcirc (x \cdot y)^{-1} \cdot e \eqcirc (x \cdot y)^{-1}$, and by associativity $(x \cdot y)^{-1} \cdot ((x \cdot y) \cdot (y^{-1} \cdot x^{-1})) \eqcirc ((x \cdot y)^{-1} \cdot (x \cdot y)) \cdot (y^{-1} \cdot x^{-1}) \eqcirc e \cdot (y^{-1} \cdot x^{-1}) \eqcirc (y^{-1} \cdot x^{-1})$. Therefore $(x \cdot y)^{-1} \eqcirc y^{-1} \cdot x^{-1}$. This argument can be converted in a full-fledged derivation, as in Figure 8, where in order to enhance readability, the symbol $\cdot$ is dropped and ts stands for $t \cdot s$.

5.B. Natural deduction for propositional logic. In order to study propositional logic, we start from a set L of symbols called **letters**, denoted by a, b, c, ... By applying the connectives to the propositional letters we obtain the **propositions on** L, denoted by A, B, C, ...

The calculus of natural deduction is a good framework for formalizing mathematical proofs. There are no logical axioms, only logical rules. Any proposition derived from $\Gamma = \emptyset$ is a tautology (Theorem 5.12) and conversely every tautology can be derived from no premise (Theorem 5.24)—the first result say that the rules for connectives are *sound*, that is they do not prove questionable facts, the second result says that they are *complete*, that is they are powerful enough to prove any true fact.

5.B.1. *Rules.* Following the notation in Section 2.A, an introduction and an elimination rule are formulated for each connective ¬, ∧, ∨, ⇒. The rules for ∧ and ∨ are

$$(\mathbf{I}_\wedge)\ \frac{\Gamma \vdash \mathrm{A} \qquad \Gamma \vdash \mathrm{B}}{\Gamma \vdash \mathrm{A} \wedge \mathrm{B}} \qquad (\mathbf{E}_{\wedge \ell})\ \frac{\Gamma \vdash \mathrm{A} \wedge \mathrm{B}}{\Gamma \vdash \mathrm{A}} \qquad (\mathbf{E}_{\wedge r})\ \frac{\Gamma \vdash \mathrm{A} \wedge \mathrm{B}}{\Gamma \vdash \mathrm{B}}$$

$$(\mathbf{I}_{\vee \ell})\ \frac{\Gamma \vdash \mathrm{A}}{\Gamma \vdash \mathrm{B} \vee \mathrm{A}} \qquad (\mathbf{I}_{\vee r})\ \frac{\Gamma \vdash \mathrm{A}}{\Gamma \vdash \mathrm{A} \vee \mathrm{B}} \qquad (\mathbf{E}_\vee)\ \frac{\Gamma \vdash \mathrm{A} \vee \mathrm{B} \qquad \Gamma \vdash \neg \mathrm{A}}{\Gamma \vdash \mathrm{B}}$$

The meaning of these rules is clear—for example $\mathbf{I}_\wedge$ says that if A and B can be derived from Γ, then so does A ∧ B. Using the rules for ∧ one can prove that $\mathrm{A} \wedge \mathrm{B} \vdash \mathrm{B} \wedge \mathrm{A}$: if A ∧ B is a premise, then we obtain A and B using $\mathbf{E}_\wedge$, so that B ∧ A follows from $\mathbf{I}_\wedge$, in symbols

$$\mathrm{A} \wedge \mathrm{B},\ \mathrm{A},\ \mathrm{B},\ \mathrm{B} \wedge \mathrm{A}.$$

A more informative method to convey this is to write derivations as a list with three columns, the first one for the counter, the second for the formulæ, the third for the justification of the line in question:

$$\begin{array}{lll} 1 & \mathrm{A} \wedge \mathrm{B} & \mathbf{p} \\ 2 & \mathrm{A} & \mathbf{E}_{\wedge \ell}(1) \\ 3 & \mathrm{B} & \mathbf{E}_{\wedge r}(1) \\ 4 & \mathrm{B} \wedge \mathrm{A} & \mathbf{I}_\wedge(3,2) \end{array} \tag{5.1}$$

Here and below **p** stands for **premise** i.e. a formula in Γ, and the numbers in the justification points to the lines where the rule is applied, for example $\mathbf{I}_\wedge(3,2)$ requires to take the conjunction of the proposition in line 3 with the proposition in line 2.

The rules for ⇒ and ¬ are:

$$(\mathbf{I}_\Rightarrow)\ \frac{\Gamma, \mathrm{A} \vdash \mathrm{B}}{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B}}\ , \qquad (\mathbf{E}_\Rightarrow)\ \frac{\Gamma \vdash \mathrm{A} \qquad \Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B}}{\Gamma \vdash \mathrm{B}}\ ,$$

$$(\mathbf{I}_\neg)\ \frac{\Gamma, \mathrm{A} \vdash \bot}{\Gamma \vdash \neg \mathrm{A}}\ , \qquad (\mathbf{E}_\neg)\ \frac{\Gamma, \neg \mathrm{A} \vdash \bot}{\Gamma \vdash \mathrm{A}}\ ,$$

where ⊥ denotes any formula of the form B ∧ ¬B. Rule $\mathbf{E}_\Rightarrow$ is usually called *Modus ponens.*

This concludes the list of our rules for the connectives.

Remarks 5.5. (a) We could also introduce suitable rules for the bi-implication

$$(\mathbf{I}_\Leftrightarrow)\ \frac{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B} \qquad \Gamma \vdash \mathrm{B} \Rightarrow \mathrm{A}}{\Gamma \vdash \mathrm{A} \Leftrightarrow \mathrm{B}}\ ,$$

$$(\mathbf{E}_{\Leftrightarrow \ell})\ \frac{\Gamma \vdash \mathrm{A} \Leftrightarrow \mathrm{B}}{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B}} \qquad (\mathbf{E}_{\Leftrightarrow r})\ \frac{\Gamma \vdash \mathrm{A} \Leftrightarrow \mathrm{B}}{\Gamma \vdash \mathrm{B} \Rightarrow \mathrm{A}}$$

and similarly for the exclusive disjunction, but this this would add an extra layer of complexity in the later proofs. For this reason it is best to think of $\mathrm{A} \Leftrightarrow \mathrm{B}$ and $\mathrm{A} \veebar \mathrm{B}$ as abbreviations for $(\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{B} \Rightarrow \mathrm{A})$ and $\neg\mathrm{A} \Leftrightarrow \mathrm{B}$, respectively.

(b) In order to keep the notation to a minimum, we will drop ℓ and r in the rules $\mathbf{E}_{\wedge}$ and $\mathbf{I}_{\vee}$.

We postpone the official definition of derivation to Section 5.C.1, but in the meanwhile let us notice the following:

Proposition 5.6. (a) *If* $\Gamma \vdash \mathrm{A}$ *and* $\Gamma' \supseteq \Gamma$ *then* $\Gamma' \vdash \mathrm{A}$.

(b) *If* $\Gamma \vdash \mathrm{A}$ *and* $\Gamma', \mathrm{A} \vdash \mathrm{B}$ *then* $\Gamma \cup \Gamma' \vdash \mathrm{B}$.

Let us see some examples of derivations.

Since $\mathrm{A}, \mathrm{B} \vdash \mathrm{A}$, then $\mathrm{A} \vdash \mathrm{B} \Rightarrow \mathrm{A}$ by $\mathbf{I}_{\Rightarrow}$. This simple derivation can be written as

$$\begin{array}{rll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \mid \mathrm{B} & \mathbf{a} \\
3 & \mid \mathrm{A} & \mathbf{i}(1) \\
4 & \mathrm{B} \Rightarrow \mathrm{A} & \mathbf{I}_{\Rightarrow}(1)
\end{array} \tag{5.2}$$

The vertical bar in the middle column delimits a **sub-derivation**—the **a** in the third column says that B is the **assumption** of the sub-derivation. A line of a sub-derivation is alive as long as the sub-derivation hasn't ended, but after that it will be considered **dead**—a line cannot be revitalized. Thus lines 2 and 3 will be dead at line 4. Therefore $\mathbf{I}_{\Rightarrow}(j)$ on line $k+1$ justifies the implication $\mathrm{P}_j \Rightarrow \mathrm{P}_k$ and witnesses that the sub-derivation on lines from j to k is dead, while $\mathbf{i}(k)$ means that we are importing line k inside this sub-derivation, and $\mathbf{i}$ is the **importing rule**—it is mandatory for the imported statement to appear in a line that is still alive.

Remark 5.7. It is possible for a proposition to occur at distinct lines $j < k$ with only one of the two occurrences defunct at a later time, so "being alive" is a property of a *line* of a derivation, not of the propositions involved.

Similarly one can prove that $\vdash \mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A})$:

$$\begin{array}{rll}
1 & \mid \mathrm{A} & \mathbf{a} \\
2 & \mid \mid \mathrm{B} & \mathbf{a} \\
3 & \mid \mid \mathrm{A} & \mathbf{i}(1) \\
4 & \mid \mathrm{B} \Rightarrow \mathrm{A} & \mathbf{I}_{\Rightarrow}(2) \\
5 & \mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A}) & \mathbf{I}_{\Rightarrow}(1)
\end{array} \tag{5.3}$$

In the derivation (5.3) lines 1 and 4 die at stage 5, lines 2 and 3 die at stage 4, so at the end the only surviving line is 5.

The number d_k of vertical bars in the kth line is the **depth** of such line; the depth of a derivation is the maximum depth of any of its lines. In (5.3)

$d_2 = d_3 = 2$, $d_1 = d_4 = 1$ and $d_5 = 0$, so the depth of this derivation is 2. The depth of derivation (5.1) is 0.

5.B.2. *Derived rules.* Derivations can be cumbersome, but they can be streamlined by means of auxiliary rules, as we have seen in Section 5.A. As these auxiliary rules can be derived from the official rules, we could dispense of them altogether, if we wish so, at the price of making our derivations more involved.

- The **contrapositive rules**

(**ctr**)
$$\frac{\Gamma \vdash \neg \mathrm{B} \Rightarrow \neg \mathrm{A}}{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B}} \quad \text{and} \quad \frac{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B}}{\Gamma \vdash \neg \mathrm{B} \Rightarrow \neg \mathrm{A}}$$

follow from $\neg \mathrm{B} \Rightarrow \neg \mathrm{A} \vdash \mathrm{A} \Rightarrow \mathrm{B}$ and $\mathrm{A} \Rightarrow \mathrm{B} \vdash \neg \mathrm{B} \Rightarrow \neg \mathrm{A}$. The first derivation is

$$\begin{array}{lll}
1 & \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{p} \\
2 & \mid \mathrm{A} & \mathbf{a} \\
3 & \mid \mid \neg \mathrm{B} & \mathbf{a} \\
4 & \mid \mid \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{i}(1) \\
5 & \mid \mid \neg \mathrm{A} & \mathbf{E}_{\Rightarrow}(3,4) \\
6 & \mid \mid \mathrm{A} & \mathbf{i}(2) \\
7 & \mid \mid \mathrm{A} \wedge \neg \mathrm{A} & \mathbf{I}_{\wedge}(6,5) \\
8 & \mid \mathrm{B} & \mathbf{E}_{\neg}(3) \\
9 & \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{I}_{\Rightarrow}(2)
\end{array} \tag{5.4}$$

The other derivation is proved in a similar way.

Let us see with example how **ctr** can be applied. To prove $\mathrm{A}, \neg \mathrm{B} \Rightarrow \neg \mathrm{A} \vdash \mathrm{B}$ argue:

$$\begin{array}{lll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{p} \\
3 & \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{ctr}(2) \\
4 & \mathrm{B} & \mathbf{E}_{\Rightarrow}(1,3)
\end{array}$$

If we wished to avoid the contrapositive rule, we would have written

$$\begin{array}{lll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{p} \\
3 & \mid \mathrm{A} & \mathbf{a} \\
4 & \mid \mid \neg \mathrm{B} & \mathbf{a} \\
5 & \mid \mid \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{i}(2) \\
6 & \mid \mid \neg \mathrm{A} & \mathbf{E}_{\Rightarrow}(4,5) \\
7 & \mid \mid \mathrm{A} & \mathbf{i}(3) \\
8 & \mid \mid \mathrm{A} \wedge \neg \mathrm{A} & \mathbf{I}_{\wedge}(7,6) \\
9 & \mid \mathrm{B} & \mathbf{E}_{\neg}(4) \\
10 & \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{I}_{\Rightarrow}(3) \\
11 & \mathrm{B} & \mathbf{E}_{\Rightarrow}(1,10)
\end{array}
\qquad \text{or} \qquad
\begin{array}{lll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{p} \\
3 & \mid \neg \mathrm{B} & \mathbf{a} \\
4 & \mid \neg \mathrm{B} \Rightarrow \neg \mathrm{A} & \mathbf{i}(2) \\
5 & \mid \neg \mathrm{A} & \mathbf{E}_{\Rightarrow}(3,4) \\
6 & \mid \mathrm{A} & \mathbf{i}(1) \\
7 & \mid \mathrm{A} \wedge \neg \mathrm{A} & \mathbf{I}_{\wedge}(7,6) \\
8 & \mathrm{B} & \mathbf{E}_{\neg}(4)
\end{array}$$

where the derivation of the left is obtained by replacing the contrapositive rule with its derivation, while the one on the right, although more succinct, is still twice as long as the original one.

- The **proof-by-cases** rule—seen in Example 2.8—says that

$$\frac{\Gamma, \mathrm{B} \vdash \mathrm{A} \qquad \Gamma, \neg\mathrm{B} \vdash \mathrm{A}}{\Gamma \vdash \mathrm{A}}$$

  Thus if A follows from both Γ, B and $\Gamma, \neg\mathrm{B}$ then it follows from Γ alone—proposition B is called the **conditional assumption**. It is justified as follows. Taking Γ as premises, assume $\neg\mathrm{A}$ towards a contradiction. Assume B. Since $\Gamma, \mathrm{B} \vdash \mathrm{A}$ then $\Gamma, \mathrm{B}, \neg\mathrm{A}$ yields a contradiction, so $\Gamma, \neg\mathrm{A} \vdash \neg\mathrm{B}$. As $\Gamma, \neg\mathrm{B} \vdash \mathrm{A}$, then $\Gamma, \neg\mathrm{A}$ yields a contradiction, so $\Gamma \vdash \mathrm{A}$.

- The rule

$$\frac{\Gamma, \mathrm{B} \vdash \mathrm{A} \qquad \Gamma, \mathrm{C} \vdash \mathrm{A}}{\Gamma \vdash \mathrm{B} \vee \mathrm{C} \Rightarrow \mathrm{A}} \tag{5.5}$$

  follows from the proof-by-cases rule, with B as conditional assumption.

- The **transitivity rule for implication** ($\mathbf{tr}_{\Rightarrow}$) is

$$\frac{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{B} \qquad \Gamma \vdash \mathrm{B} \Rightarrow \mathrm{C}}{\Gamma \vdash \mathrm{A} \Rightarrow \mathrm{C}}$$

  and follows from $\mathrm{A} \Rightarrow \mathrm{B}, \mathrm{B} \Rightarrow \mathrm{C} \vdash \mathrm{A} \Rightarrow \mathrm{C}$:

$$\begin{array}{rll}
1 & \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{p} \\
2 & \mathrm{B} \Rightarrow \mathrm{C} & \mathbf{p} \\
3 & \mid \mathrm{A} & \mathbf{a} \\
4 & \mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{i}(1) \\
5 & \mid \mathrm{B} & \mathbf{E}_{\Rightarrow}(3,4) \\
6 & \mid \mathrm{B} \Rightarrow \mathrm{C} & \mathbf{i}(2) \\
7 & \mid \mathrm{C} & \mathbf{E}_{\Rightarrow}(5,6) \\
8 & \mathrm{A} \Rightarrow \mathrm{C} & \mathbf{I}_{\Rightarrow}(3)
\end{array} \tag{5.6}$$

- Anything can be proved from a proposition and its negation:

$$(\bot) \quad \frac{\Gamma \vdash \mathrm{A} \qquad \Gamma \vdash \neg\mathrm{A}}{\Gamma \vdash \mathrm{B}} \tag{5.7}$$

  To verify this start from Γ and, towards a contradiction, suppose $\neg\mathrm{B}$; since $\Gamma, \neg\mathrm{B}$ proves both A and $\neg\mathrm{A}$, then $\neg\mathrm{B}$ is rejected and B holds.

Exercise 5.48 lists several other useful auxiliary rules—associativity of $\wedge$ and $\vee$, distributivity of $\wedge$ and $\vee$, De Morgan's rules, the double negation rule, ..., which are commonplace in mathematical proofs. For example, the distributivity of $\wedge$ with respect to $\vee$ is used to verify the distributivity of intersection with respect to union, i.e. that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. In fact it is enough to verify that $x \in A \wedge (x \in B \vee x \in C) \Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$, which follows from such a rule—just write $\mathrm{A}, \mathrm{B}, \mathrm{C}$ in place of $x \in A$, $x \in B$ and $x \in C$.

5.B.3. *More derivations.*

Example 5.8. $\vdash (\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$, since

$$\begin{array}{rll}
1 & \mid \mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C}) & \mathbf{a} \\
2 & \mid\mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
3 & \mid\mid\mid \mathrm{A} & \mathbf{a} \\
4 & \mid\mid\mid \mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C}) & \mathbf{i}(1) \\
5 & \mid\mid\mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{i}(2) \\
6 & \mid\mid\mid \mathrm{B} \Rightarrow \mathrm{C} & \mathbf{E}_{\Rightarrow}(3,4) \\
7 & \mid\mid\mid \mathrm{C} & \mathbf{tr}_{\Rightarrow}(5,6) \\
8 & \mid\mid \mathrm{A} \Rightarrow \mathrm{C} & \mathbf{I}_{\Rightarrow}(3) \\
9 & \mid (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}) & \mathbf{I}_{\Rightarrow}(2) \\
10 & (\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}) & \mathbf{I}_{\Rightarrow}(1)
\end{array}$$

Example 5.9. $\vdash \mathrm{A} \Rightarrow \neg\neg\mathrm{A}$ and $\vdash \neg\neg\mathrm{A} \Rightarrow \mathrm{A}$ follow by $\mathrm{A} \vdash \neg\neg\mathrm{A}$ and $\neg\neg\mathrm{A} \vdash \mathrm{A}$ and $\mathbf{I}_{\Rightarrow}$:

$$\begin{array}{rll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \mid \neg\mathrm{A} & \mathbf{a} \\
3 & \mid \mathrm{A} & \mathbf{i}(1) \\
4 & \neg\neg\mathrm{A} & \mathbf{I}_{\neg}(2)
\end{array}
\qquad
\begin{array}{rll}
1 & \neg\neg\mathrm{A} & \mathbf{p} \\
2 & \mid \neg\mathrm{A} & \mathbf{a} \\
3 & \mid \neg\neg\mathrm{A} & \mathbf{i}(1) \\
4 & \mathrm{A} & \mathbf{E}_{\neg}(2)
\end{array}$$

Example 5.10. $\vdash \neg\mathrm{A} \Rightarrow (\mathrm{A} \Rightarrow \mathrm{B})$ and $\vdash \mathrm{A} \Rightarrow (\neg\mathrm{B} \Rightarrow \neg(\mathrm{A} \Rightarrow \mathrm{B}))$, since

$$\begin{array}{rll}
1 & \mid \neg\mathrm{A} & \mathbf{a} \\
2 & \mid\mid \mathrm{A} & \mathbf{a} \\
3 & \mid\mid \neg\mathrm{A} & \mathbf{i}(1) \\
4 & \mid\mid \mathrm{B} & \bot(2,3) \\
5 & \mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{I}_{\Rightarrow}(2) \\
6 & \neg\mathrm{A} \Rightarrow (\mathrm{A} \Rightarrow \mathrm{B}) & \mathbf{I}_{\Rightarrow}(1)
\end{array}
\qquad
\begin{array}{rll}
1 & \mid \mathrm{A} & \mathbf{a} \\
2 & \mid\mid \neg\mathrm{B} & \mathbf{a} \\
3 & \mid\mid\mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
4 & \mid\mid\mid \mathrm{A} & \mathbf{i}(1) \\
5 & \mid\mid\mid \mathrm{B} & \mathbf{E}_{\Rightarrow}(4,3) \\
6 & \mid\mid\mid \neg\mathrm{B} & \mathbf{i}(2) \\
7 & \mid\mid\mid \mathrm{B} \land \neg\mathrm{B} & \mathbf{I}_{\land}(5,6) \\
8 & \mid\mid \neg(\mathrm{A} \Rightarrow \mathrm{B}) & \mathbf{I}_{\neg}(3) \\
9 & \mid \neg\mathrm{B} \Rightarrow \neg(\mathrm{A} \Rightarrow \mathrm{B}) & \mathbf{I}_{\Rightarrow}(2) \\
10 & \mathrm{A} \Rightarrow (\neg\mathrm{B} \Rightarrow \neg(\mathrm{A} \Rightarrow \mathrm{B})) & \mathbf{I}_{\Rightarrow}(1)
\end{array}$$

where $\bot$ is the rule (5.7).

Example 5.11. $\vdash (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\neg\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B})$, since by the proof-by-cases rule using A as conditional assumption we have:

$$\begin{array}{rll}
1 & \mathrm{A} & \mathbf{p} \\
2 & \mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
3 & \mid \mathrm{A} & \mathbf{i}(1) \\
4 & \mid \mathrm{B} & \mathbf{E}_{\Rightarrow}(3,2) \\
5 & \mid\mid \neg\mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
6 & \mid\mid \mathrm{B} & \mathbf{i}(4) \\
7 & \mid (\neg\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B} & \mathbf{I}_{\Rightarrow}(5) \\
8 & (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\neg\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B}) & \mathbf{I}_{\Rightarrow}(2)
\end{array}$$

and

$$\begin{array}{lll}
1 & \neg\mathrm{A} & \mathbf{p} \\
2 & \mid \mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
3 & \mid \mid \neg\mathrm{A} \Rightarrow \mathrm{B} & \mathbf{a} \\
4 & \mid \mid \neg\mathrm{A} & \mathbf{i}(1) \\
5 & \mid \mid \mathrm{B} & \mathbf{E}_{\Rightarrow}(4,3) \\
6 & \mid (\neg\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B} & \mathbf{I}_{\Rightarrow}(3) \\
7 & (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B}) & \mathbf{I}_{\Rightarrow}(2)
\end{array}$$

5.C. Soundness. In this section we prove that the rules of natural deduction for propositional calculus are *sound*, that is they yield correct results. Recall from Section 3.C.1 that a valuation is a function $v\colon \mathrm{Prop}(L) \to \{0,1\}$, from the set of all propositions built from a set of letters L, to the truth values 0 and 1. Any valuation is completely determined by its restriction to L, so it is customary to define v on L and canonically extend it to $\mathrm{Prop}(L)$. If Γ is a set of propositions, with a minor abuse of notation we write $v(\Gamma) = 1$ to mean that $v(\mathrm{P}) = 1$ for all $\mathrm{P} \in \Gamma$. Recall also that A is tautological consequence of Γ if $v(\mathrm{A}) = 1$ for all valuations v such that $v(\Gamma) = 1$.

Theorem 5.12. *If* $\Gamma \vdash \mathrm{A}$*, then* A *is a tautological consequence of* Γ.

In particular:

Corollary 5.13. *If* $\vdash \mathrm{A}$*, then* A *is a tautology.*

If $\Gamma \vdash \mathrm{A}$ and Γ is finite (which can always be assumed by Theorem 5.17), then $\vdash \bigwedge\Gamma \Rightarrow \mathrm{A}$, so if $\bigwedge\Gamma \Rightarrow \mathrm{A}$ is a tautology, then A is tautological consequence of Γ. Therefore Corollary 5.13 implies Theorem 5.12. The converse of these results are also true—every tautology can be derived—but a direct proof using natural deduction is a bit involved. In the next section a different kind of logical calculus is introduced, one that will easily yield the desired result.

In order to appreciate the hurdles that we need overcome towards proving soundness for natural deduction, let us consider some specific cases.[23]

Suppose first $\mathrm{P}_1, \dots, \mathrm{P}_n$ is a derivation of $\Gamma \vdash \mathrm{A}$ of depth $d = 0$, that is there are no sub-derivations. We claim that:

$$(*) \qquad \text{If } v(\Gamma) = 1, \text{ then } v(\mathrm{P}_i) = 1 \text{ for all } 1 \leq i \leq n.$$

Since $\mathrm{P}_n = \mathrm{A}$, then $(*)$ yields that A is tautological consequence of Γ. To prove $(*)$ we argue by induction on $i \leq n$. Suppose $v(\Gamma) = 1$. If $\mathrm{P}_i \in \Gamma$ then $v(\mathrm{P}_i) = 1$ by choice of v, so we may assume that P_i is obtained from earlier P_js by means of $\mathbf{I}_\wedge, \mathbf{E}_\wedge, \mathbf{I}_\vee, \mathbf{E}_\vee, \mathbf{E}_\Rightarrow$. (The rules $\mathbf{I}_\neg, \mathbf{E}_\neg, \mathbf{I}_\Rightarrow$ entail the use of sub-derivations, so they are not allowed here.) Suppose, for example, that

[23] The reader is encouraged to verify that the statement of Theorem 5.12 holds for the derivations seen so far.

on line i rule $\mathbf{I}_\wedge$ was used, that is $\mathrm{P}_i = \mathrm{P}_j \wedge \mathrm{P}_k$ with $j, k < i$; by induction assumption $v(\mathrm{P}_j) = v(\mathrm{P}_k) = 1$, so $v(\mathrm{P}_i) = 1$. The case of the other rules is similar.

Note that $(*)$ fails for the derivations with depth 1—for example in the derivation (5.2) of $\mathrm{A} \vdash \mathrm{B} \Rightarrow \mathrm{A}$, consider a valuation such that $v(\mathrm{A}) = 1$ and $v(\mathrm{B}) = 0$. The correct genaralization of $(*)$ to derivations of depth 1 is

$(**)$ Suppose $v(\Gamma) = 1$. If line i has depth 0, then $v(\mathrm{P}_i) = 1$; if line i it has depth 1 and $v(\mathrm{P}_j) = 1$, where j is the first line of the sub-derivation reaching line i, then $v(\mathrm{P}_i) = 1$.

As the last line of a derivation has depth 0, then $(**)$ yields Theorem 5.12 for derivations of depth 1. The proof of $(**)$ is similar to that of $(*)$. Let us see a specific example.

Example 5.14. Let $\mathrm{P}_1, \ldots, \mathrm{P}_8$ be the derivation of $\mathrm{A} \Rightarrow \mathrm{B}, \mathrm{B} \Rightarrow \mathrm{C} \vdash \mathrm{A} \Rightarrow \mathrm{C}$ displayed on (5.6) on page 119. Suppose $v(\mathrm{A} \Rightarrow \mathrm{B}) = v(\mathrm{B} \Rightarrow \mathrm{C}) = 1$. As $\mathrm{P}_1, \mathrm{P}_2$ are premises, then $v(\mathrm{P}_1) = v(\mathrm{P}_2) = 1$. Since P_3 (that is: A) is an assumption, from now until line 7 we may assume that $v(\mathrm{A}) = 1$; as $\mathrm{P}_4 = \mathrm{P}_1$ and $\mathrm{P}_6 = \mathrm{P}_2$, then $v(\mathrm{P}_4) = v(\mathrm{P}_6) = 1$, and hence $v(\mathrm{P}_5) = v(\mathrm{P}_7) = 1$. Finally, consider line 8, where $\mathrm{A} \Rightarrow \mathrm{C}$ is inferred from lines 3 and 7 via $\mathbf{I}_\Rightarrow$. If $v(\mathrm{A}) = 1$ then $v(\mathrm{C}) = v(\mathrm{P}_7) = 1$, so $v(\mathrm{A} \Rightarrow \mathrm{C}) = 1$, and if $v(\mathrm{A}) = 0$, then $v(\mathrm{A} \Rightarrow \mathrm{C}) = 1$. Therefore $v(\mathrm{P}_8) = 1$ in any case.

The proof of Theorem 5.12 follows from a suitable generalization of $(*)$ and $(**)$ to all derivations.

5.C.1. *A proof of Theorem 5.12*.* Before plunging into the details of the proof, we must first give a precise definition of what is a derivation. Definition 5.15 below is a bit intimidating, but it is just collecting what we have said so far about derivations.

Definition 5.15. A **justified derivation** from Γ is a finite list

$$(\mathrm{P}_1, \mathbf{j}_1, d_1, D_1), \ldots, (\mathrm{P}_n, \mathbf{j}_n, d_n, D_n)$$

where the P_ks are propositions, $d_k \in \mathbb{N}$ is the depth of line k, D_k is the set of dead lines at stage k, and $\mathbf{j}_k$ is a justification, i.e. one of the following labels: $\mathbf{p}$, $\mathbf{a}$, $\mathbf{i}(m)$, or an introduction/elimination rule for the connectives. For any $1 \leq k \leq n$ we require that:

(1) $D_1 = \emptyset$,

(2) $|d_k - d_{k-1}| \leq 1$, where $d_0 = d_n = 0$,

(3) if $d_{k-1} \leq d_k$, then $D_k = D_{k-1}$,

(4) if $d_{k-1} > d_k$, then

$$D_k = D_{k-1} \cup \{k^*, \ldots, k-1\}, \tag{5.8}$$

where k^* is least m such that $d_m = d_{k-1}$, and $d_i = d_{k-1}$ for all $m \leq i \leq k-1$,

(5) if $\mathbf{j}_k = \mathbf{p}$, then $\mathrm{P}_k \in \Gamma$,

(6) $d_k = d_{k-1} + 1$ if and only if $\mathbf{j}_k = \mathbf{a}$,

(7) if $\mathbf{j}_k = \mathbf{i}(k')$, then $1 \leq k' < k$ and $k' \notin D_k$, and $d_{k'} < d_k$,

(8) if $\mathbf{j}_k$ is one of $\mathbf{I}_{\wedge}(j,h)$, $\mathbf{E}_{\wedge\ell}(j)$, $\mathbf{E}_{\wedge r}(j)$, $\mathbf{I}_{\vee\ell}(j)$, $\mathbf{I}_{\vee r}(j)$, $\mathbf{E}_{\vee}(j,h)$, or $\mathbf{E}_{\Rightarrow}(j,h)$, then
- $d_k = d_{k-1}$,
- $j, h \in \{1, \dots, k-1\} \setminus D_k$,
- $d_h = d_j = d_k$;

(9) if $\mathbf{j}_k$ is one of $\mathbf{I}_{\Rightarrow}(j)$, $\mathbf{I}_{\neg}(j)$, $\mathbf{E}_{\neg}(j)$, then $d_k = d_{k-1} - 1$, and $j = k^*$ following the notation of (5.8). Moreover
- if $\mathbf{j}_k = \mathbf{I}_{\Rightarrow}(j)$, then $\mathrm{P}_k = \mathrm{P}_j \Rightarrow \mathrm{P}_{k-1}$,
- if $\mathbf{j}_k = \mathbf{I}_{\neg}(j)$, then $\mathrm{P}_k = \neg\mathrm{P}_j$,
- if $\mathbf{j}_k = \mathbf{E}_{\neg}(j)$, then $\neg\mathrm{P}_k = \mathrm{P}_j$.

An **unjustified derivation** (or simply: a **derivation**) from Γ is a sequence of propositions $\mathrm{P}_1, \dots, \mathrm{P}_n$ that admit a **justification**, that is sequence $(\mathbf{j}_1, d_1, D_1), \dots, (\mathbf{j}_n, d_n, D_n)$ so that $(\mathrm{P}_1, \mathbf{j}_1, d_1, D_1), \dots, (\mathrm{P}_n, \mathbf{j}_n, d_n, D_n)$ is a justified derivation from Γ.

A proposition A **derives** from Γ, in symbols $\Gamma \vdash \mathrm{A}$, if there is a derivation $\mathrm{P}_1, \dots, \mathrm{P}_n$ from Γ such that $\mathrm{A} = \mathrm{P}_n$.

Remarks 5.16. (a) The sets D_ks can be retrieved from the d_ks, which in turn can be retrieved from the $\mathbf{j}_k$s, but the $\mathbf{j}_k$s cannot be retrieved from the P_ks. Therefore a justification can (and form now on: will) be identified with the sequence $\mathbf{j}_1, \dots, \mathbf{j}_n$, and a justified derivation can be defined as a sequence of pairs $(\mathrm{P}_1, \mathbf{j}_1), \dots, (\mathrm{P}_n, \mathbf{j}_n,)$ satisfying the conditions above.

(b) If $(\mathrm{P}_1, \mathbf{j}_1, d_1, D_1), \dots, (\mathrm{P}_n, \mathbf{j}_n, d_n, D_n)$ is a derivation from Γ and $k < n$, then $(\mathrm{P}_1, \mathbf{j}_1, d_1, D_1), \dots, (\mathrm{P}_k, \mathbf{j}_k, d_k, D_k)$ is a derivation from Γ if and only if $d_k = 0$.

If $\Gamma \vdash \mathrm{A}$ and $\Gamma \subseteq \Gamma'$, then the same derivation witnesses that $\Gamma' \vdash \mathrm{A}$. Conversely if $\Gamma \vdash \mathrm{A}$, then $\Gamma_0 \vdash \mathrm{A}$ for some finite $\Gamma_0 \subseteq \Gamma$ since finitely many premises can occur in a derivation. Therefore we have proved the following:

Theorem 5.17. $\Gamma \vdash \mathrm{A}$ *if and only if* $\Gamma_0 \vdash \mathrm{A}$ *for some finite* $\Gamma_0 \subseteq \Gamma$.

Given a derivation of length n, for each $k \leq n$ let A_k be the set of all lines $\leq k$ in which assumptions have appeared and that are not yet dead:

$$A_k = \{m \mid 1 \leq m \leq k \wedge \mathbf{j}_m = \mathbf{a}\} \setminus D_k. \tag{5.9}$$

For example in the derivation (5.4)on page 118 $A_0 = A_9 = \emptyset$, $A_2 = A_8 = \{2\}$ and $A_3 = \cdots = A_7 = \{2, 3\}$.

Lemma 5.18. *Using the notation of Definition 5.15:*

(a) $D_k \subseteq \{1, \dots, k-1\}$*, so* $k \notin D_k$*.*

(b) *If* $1 \le k' \le k \le n$ *then* $D_{k'} \subseteq D_k$ *and* $D_k \cap \{1, \dots, k'\} = D_{k'}$*.*

(c) *If* $m + 1 = \max A_{k-1}$ *and* $d_k < d_{k-1}$*, then* $A_m = A_k$*.*

(d) $|A_k| = d_k$*.*

Proof. (a) and (b) are proved by induction using clauses (3) and (4).

(c). If $m + 1 = \max A_{k-1}$ and $d_k + 1 = d_{k-1}$ then $D_k = D_{k-1} \cup \{m + 1, \dots, k - 1\}$ so by parts (a) and (b)

$$\begin{aligned} A_k &= \{i \le k \mid \mathbf{j}_i = \mathbf{a}\} \setminus D_k \\ &= \{i \le m \mid \mathbf{j}_i = \mathbf{a}\} \setminus D_k \\ &= \{i \le m \mid \mathbf{j}_i = \mathbf{a}\} \setminus D_m \\ &= A_m. \end{aligned}$$

(d). By clause (6) and part (c)

$$\begin{aligned} d_k = d_{k-1} + 1 &\Leftrightarrow \mathbf{j}_k = \mathbf{a} \Leftrightarrow A_k = A_{k-1} \cup \{k\} \\ d_k = d_{k-1} &\Leftrightarrow A_k = A_{k-1} \\ d_k = d_{k-1} - 1 &\Leftrightarrow A_k = A_{k-1} \setminus \{\max A_{k-1}\}. \end{aligned}$$

Therefore if $d_k = |A_{k-1}|$ then $d_k = |A_k|$ and since $d_0 = 0$ and $A_0 = \emptyset$ the result follows by induction. □

Recall that $\Gamma \models \mathrm{P}$ means that P is a tautological consequence of Γ (Example 3.26).

Theorem 5.19. *If* $(\mathrm{P}_1, \mathbf{j}_1, d_1, D_1), \dots, (\mathrm{P}_n, \mathbf{j}_n, d_n, D_n)$ *is a justified derivation from* Γ*, then* $\Gamma \models \bigwedge_{i \in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_k$*, where* A_k *is as in* (5.9)*.*

Remark 5.20. If $A_k = \emptyset$ then $\bigwedge_{i \in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_k$ is P_k. The condition above could have been stated more easily as P_k is tautological consequence of $\Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$, but the current formulation is useful for Theorem 5.40 later on.

Proof. We proceed by induction on $k \le n$, and consider the various possibility for what $\mathbf{j}_k$ can be. The result follows vacuously if there is no valuation that gives truth value 1 to all propositions in $\Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$, so let's assume otherwise.

If $\mathbf{j}_k$ is $\mathbf{p}$ or $\mathbf{a}$, then $\mathrm{P}_k \in \Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$, and the result follows at once.

If $\mathbf{j}_k$ is $\mathbf{i}(j)$ then $j \notin D_k$, and $j < k$. By inductive assumption P_j is a tautological consequence of $\Gamma \cup \{\mathrm{P}_i \mid i \in A_j\}$, and since $\mathrm{P}_j = \mathrm{P}_k$ and $A_j \subseteq A_k$ the result follows at once.

Thus $\mathbf{j}_k$ must be an application of a rule for connectives, as in cases (8) and (9) of Definition 5.15.

If $\mathbf{j}_k$ is one of $\mathbf{I}_\wedge(j,h)$, $\mathbf{E}_{\wedge\ell}(j)$, $\mathbf{E}_{\wedge r}(j)$, $\mathbf{I}_{\vee\ell}(j,h)$, $\mathbf{I}_{\vee r}(j,h)$, $\mathbf{E}_\vee(j,h)$, or $\mathbf{E}_\Rightarrow(j,h)$, with $j,h < k$, then P_k is a tautological consequence of $\mathrm{P}_j, \mathrm{P}_h$, and since $d_j = d_h = d_k$ we have that $A_j = A_h = A_k$. By inductive $\Gamma \models \bigwedge_{i\in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_j$ and $\Gamma \models \bigwedge_{i\in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_h$, so the result follows.

Thus we may assume that $\mathbf{j}_k$ is one of $\mathbf{I}_\Rightarrow(j)$, $\mathbf{I}_\neg(j)$, $\mathbf{E}_\neg(j)$. Then there is a sub-derivation from line $m < k-1$ to line $k-1$ of depth d_k+1 that proves P_k, and

$$A_m = A_{k-1} = A_k \cup \{m\}. \tag{5.10}$$

- If $\mathbf{j}_k = \mathbf{E}_\neg(m)$, then $\mathrm{P}_k = \neg\mathrm{P}_m$ and $\mathrm{P}_{k-1} = \mathrm{B} \wedge \neg\mathrm{B}$ for some B. By inductive assumption $\Gamma \models \bigwedge_{i\in A_{k-1}} \mathrm{P}_i \Rightarrow \mathrm{P}_{k-1}$. If v is any valuation satisfying $\Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$ then since $v(\mathrm{P}_{k-1}) = 0$ and by (5.10) $v(\mathrm{P}_m) = 0$, that is $v(\mathrm{P}_k) = 1$. In other words $\Gamma \models \bigwedge_{i\in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_k$.
- The case when $\mathbf{j}_k = \mathbf{I}_\neg(m)$ is similar.
- Finally suppose $\mathbf{j}_k = \mathbf{I}_\Rightarrow(m)$, so that $\mathrm{P}_k = \mathrm{P}_m \Rightarrow \mathrm{P}_{k-1}$. By inductive assumption $\Gamma \models \bigwedge_{i\in A_{k-1}} \mathrm{P}_i \Rightarrow \mathrm{P}_{k-1}$. If v is any valuation satisfying $\Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$, then $v(\mathrm{P}_m \Rightarrow \mathrm{P}_{k-1}) = 1$ by (5.10). Therefore $\Gamma \models \bigwedge_{i\in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_k$.

The proof is complete. □

As the last line n of a derivation has depth 0, then $A_n = \emptyset$ so Theorem 5.12 holds.

5.D. Hilbert-style propositional calculus. Hilbert and Ackerman introduced a logical calculus—completely equivalent to natural deduction of Section 5.B—consisting of a few selected tautologies called **logical axioms** and one logical rule, *Modus Ponens* (MP) of page 9, which is just the elimination rule for implication. There are many variants of this calculus, depending on the choice of the logical axioms, and for this reason we speak of **Hilbert-style calculi**. In some sense, natural deduction is the best choice for modelling mathematical proofs and writing down specific derivations, while a Hilbert-style calculus is the best choice for proving facts *about* derivations.

Convention. Since there are two competing notions of derivation—natural deduction vs. Hilbert-style—we write $\vdash^{\mathrm{ND}}$ and $\vdash^{\mathrm{H}}$ to tell them apart. Once we prove that the two notions yield the same results, we can forget about these decorations.

We take $\neg$ and $\Rightarrow$ as basic connectives, and define the other ones in term of these. In particular $\mathrm{A} \vee \mathrm{B}$, $\mathrm{A} \wedge \mathrm{B}$ are shorthand for $\neg \mathrm{A} \Rightarrow \mathrm{B}$ and $\neg(\mathrm{A} \Rightarrow \neg \mathrm{B})$, and $\mathrm{A} \Leftrightarrow \mathrm{B}$ is $(\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{B} \Rightarrow \mathrm{A})$. The axioms are

A1: $\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A})$,

A2: $(\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$,

A3: $\mathrm{A} \Rightarrow \neg\neg \mathrm{A}$,

A4: $\neg \mathrm{A} \Rightarrow (\mathrm{A} \Rightarrow \mathrm{B})$,

A5: $\mathrm{A} \Rightarrow (\neg \mathrm{B} \Rightarrow \neg(\mathrm{A} \Rightarrow \mathrm{B}))$,

A6: $(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\neg \mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B})$.

These are *axiom schemata*, since $\mathrm{A}, \mathrm{B}, \mathrm{C}$ stand for any proposition, and by Section 5.B.3 they are provable in the calculus of natural deduction.

A **(Hilbert-style) derivation from** Γ is a finite list $\mathrm{P}_1, \dots, \mathrm{P}_n$ such that each P_i is either in Γ, or else it is an axiom, or else it follows from earlier P_js via MP, and in this case we say that P_n is derivable from Γ, in symbols $\Gamma \vdash^{\mathrm{H}} \mathrm{P}_n$. An initial segment of a Hilbert-style derivation is still a derivation, so proofs by induction on the length of a derivation are considerably easier than similar proofs in the context for natural deduction. For example it is straightforward to check that

(5.11) if $\Gamma \vdash^{\mathrm{H}} \mathrm{A}$, then A is tautological consequence of Γ.

By (5.3) and Section 5.B.3, the logical axioms are derivable using the calculus of natural deduction, and since MP is $\mathbf{E}_{\Rightarrow}$, it follows at once that

(5.12) if $\Gamma \vdash^{\mathrm{H}} \mathrm{A}$, then $\Gamma \vdash^{\mathrm{ND}} \mathrm{A}$.

Lemma 5.21. (a) $\vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{A}$,

(b) *If* $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{B}$ *and* $\Gamma \vdash^{\mathrm{H}} \neg \mathrm{A} \Rightarrow \mathrm{B}$ *then* $\Gamma \vdash^{\mathrm{H}} \mathrm{B}$.

Proof. (a) For notational ease we write B for $\mathrm{A} \Rightarrow \mathrm{A}$:

1	$(\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A})) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{A}))$	**A2**
2	$\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A})$	**A1**
3	$(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{A})$	MP(1,2)
4	$\mathrm{A} \Rightarrow (\mathrm{A} \Rightarrow \mathrm{A})$, i.e. $\mathrm{A} \Rightarrow \mathrm{B}$	**A1**
5	$\mathrm{A} \Rightarrow \mathrm{A}$	MP(3,4)

(b) Say $\mathrm{P}_1, \dots, \mathrm{P}_n$ and $\mathrm{P}_{n+1}, \dots, \mathrm{P}_{n+m}$ are derivations from Γ where P_n is $\mathrm{A} \Rightarrow \mathrm{B}$ and P_{n+m} is $\neg \mathrm{A} \Rightarrow \mathrm{B}$. By **A6**

$$\mathrm{P}_1,\ \dots,\ \mathrm{P}_{n+m},\ (\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\neg \mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B}),\ (\neg \mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{B},\ \mathrm{B}$$

is a derivation witnessing that $\Gamma \vdash^{\mathrm{H}} \mathrm{B}$. □

The proof above exemplifies everything that is annoying with the Hilbert-style calculi—not only proofs are considerably longer than their analogs in natural deduction, they lack any clear motivation. And although $\vdash^{\mathrm{H}}$-derivations are easy to check, they are hard to devise.

The next result shows how to prove the $\mathbf{I}_{\Rightarrow}$-rule.

Theorem 5.22. *If* $\Gamma, \mathrm{A} \vdash^{\mathrm{H}} \mathrm{B}$ *then* $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{B}$.

Proof. Suppose $\mathrm{P}_1, \ldots, \mathrm{P}_n$ witnesses $\Gamma, \mathrm{A} \vdash^{\mathrm{H}} \mathrm{B}$, with $\mathrm{P}_n = \mathrm{B}$. We prove by induction on $1 \leq i \leq n$ that $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{P}_i$. We take cases:

- If P_i is in Γ, then $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{P}_i$ since

$$\begin{array}{lll} 1 & \mathrm{P}_i \Rightarrow (\mathrm{A} \Rightarrow \mathrm{P}_i) & \mathbf{A1} \\ 2 & \mathrm{P}_i & \mathbf{p} \\ 3 & \mathrm{A} \Rightarrow \mathrm{P}_i & \mathrm{MP}(1,2) \end{array}$$

- If P_i is A then $\vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{P}_i$ by part (a) of Lemma 5.21.
- If P_i follows by MP from P_m and P_k, where $m, k < i$ and P_k is $\mathrm{P}_m \Rightarrow \mathrm{P}_i$, then by inductive assumption $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{P}_m$ and $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow (\mathrm{P}_m \Rightarrow \mathrm{P}_i)$. As $(\mathrm{A} \Rightarrow (\mathrm{P}_m \Rightarrow \mathrm{P}_i)) \Rightarrow ((\mathrm{A} \Rightarrow \mathrm{P}_m) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{P}_i))$ is an axiom **A2**, then $\Gamma \vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{P}_i$ follows from two applications of MP. □

By MP, if $\vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{B}$ then $\mathrm{A} \vdash^{\mathrm{H}} \mathrm{B}$, and hence

$$\vdash^{\mathrm{H}} \mathrm{A} \Rightarrow \mathrm{B} \text{ if and only if } \mathrm{A} \vdash^{\mathrm{H}} \mathrm{B}.$$

If $v \colon \{\mathrm{a}_1, \ldots, \mathrm{a}_n\} \to \{0, 1\}$ and $\mathrm{A} \in \mathrm{Prop}(\{\mathrm{a}_1, \ldots, \mathrm{a}_n\})$, define

$$\mathrm{A}^v = \begin{cases} \mathrm{A} & \text{if } v(\mathrm{A}) = 1, \\ \neg\mathrm{A} & \text{if } v(\mathrm{A}) = 0. \end{cases}$$

Lemma 5.23. *If* A *is a proposition whose letters are among* $\{\mathrm{a}_1, \ldots, \mathrm{a}_n\}$ *and* $v \colon \{\mathrm{a}_1, \ldots, \mathrm{a}_n\} \to \{0, 1\}$*, then* $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash^{\mathrm{H}} \mathrm{A}^v$.

Proof. By induction on the number k of connectives of A. If $k = 0$, then $\mathrm{A} = \mathrm{a}_i$ for some i, and hence $\mathrm{a}_i \vdash \mathrm{a}_i$ and $\neg\mathrm{a}_i \vdash \neg\mathrm{a}_i$. Thus we may assume that $k > 0$ and that the result holds for all B with fewer connectives.

Suppose A is $\neg$B. Then by inductive assumption $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{B}^v$. If $\mathrm{B}^v = \neg\mathrm{B} = \mathrm{A}$, then $v(\mathrm{B}) = 0$, so $v(\mathrm{A}) = 1$ and $\mathrm{A} = \mathrm{A}^v$, and hence $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{A}^v$. If $\mathrm{B}^v = \mathrm{B}$ then $v(\mathrm{B}) = 1$ so $v(\mathrm{A}) = 0$ and $\mathrm{A}^v = \neg\mathrm{A} = \neg\neg\mathrm{B}$. Since $\mathrm{B} \Rightarrow \neg\neg\mathrm{B}$ is an axiom **A3**, then $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \neg\neg\mathrm{B}$, that is $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{A}^v$.

Suppose A is $\mathrm{B} \Rightarrow \mathrm{C}$. Then $(*)$ $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{B}^v$, and $(\star)$ $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{C}^v$ by inductive assumption.

- If $v(\mathrm{B}) = 0$ then $v(\mathrm{A}) = 1$ so $\mathrm{B}^v = \neg\mathrm{B}$ and $\mathrm{A}^v = \mathrm{A}$ is $\mathrm{B} \Rightarrow \mathrm{C}$. As $\neg\mathrm{B} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})$ is an axiom **A4** then $(*)$ together with MP yields $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{B} \Rightarrow \mathrm{C}$, that is $\mathrm{a}_1^v, \ldots, \mathrm{a}_n^v \vdash \mathrm{A}^v$.

- If $v(\mathrm{C}) = 1$ then $v(\mathrm{A}) = 1$, so $\mathrm{C}^v = \mathrm{C}$ and $\mathrm{A}^v = \mathrm{A}$. As $\mathrm{C} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})$ is an axiom **A1**, then $(\star)$ together with MP yields $\mathrm{a}_1^v, \dots, \mathrm{a}_n^v \vdash \mathrm{B} \Rightarrow \mathrm{C}$, that is $\mathrm{a}_1^v, \dots, \mathrm{a}_n^v \vdash \mathrm{A}^v$.
- If $v(\mathrm{B}) = 1$ and $v(\mathrm{C}) = 0$ then $v(\mathrm{A}) = 0$, so that $\mathrm{A}^v = \neg(\mathrm{B} \Rightarrow \mathrm{C})$, $\mathrm{B}^v = \mathrm{B}$, and $\mathrm{C}^v = \neg\mathrm{C}$. As $\mathrm{B} \Rightarrow (\neg\mathrm{C} \Rightarrow \neg(\mathrm{B} \Rightarrow \mathrm{C}))$ is an axiom **A5**, then $(*)$, $(\star)$ and MP yield that $\mathrm{a}_1^v, \dots, \mathrm{a}_n^v \vdash \neg(\mathrm{B} \Rightarrow \mathrm{C})$, that is $\mathrm{a}_1^v, \dots, \mathrm{a}_n^v \vdash \mathrm{A}^v$. □

Theorem 5.24 (Post). *If* A *is a tautology, then* $\vdash^{\mathrm{H}}$ A*, and hence* $\vdash^{\mathrm{ND}}$ A.

Proof. Say $\mathrm{a}_1, \dots, \mathrm{a}_n$ are the letters occurring in A. We prove by induction on $0 \leq k \leq n$ that $\mathrm{a}_1^v, \dots, \mathrm{a}_{n-k}^v \vdash \mathrm{A}$ for any $v \colon \{\mathrm{a}_1, \dots, \mathrm{a}_{n-k}\} \to \{0, 1\}$. The case $k = 0$ is Lemma 5.23. If the result holds for some k and $v \colon \{\mathrm{a}_1, \dots, \mathrm{a}_{n-k-1}\} \to \{0, 1\}$ then

$$\mathrm{a}_1^v, \dots, \mathrm{a}_{n-k-1}^v, \mathrm{a}_{n-k} \vdash^{\mathrm{H}} \mathrm{A} \quad \text{and} \quad \mathrm{a}_1^v, \dots, \mathrm{a}_{n-k-1}^v, \neg\mathrm{a}_{n-k} \vdash^{\mathrm{H}} \mathrm{A},$$

so by Theorem 5.22

$$\mathrm{a}_1^v, \dots, \mathrm{a}_{n-k-1}^v \vdash^{\mathrm{H}} \mathrm{a}_{n-k} \Rightarrow \mathrm{A} \quad \text{and} \quad \mathrm{a}_1^v, \dots, \mathrm{a}_{n-k-1}^v \vdash^{\mathrm{H}} \neg\mathrm{a}_{n-k} \Rightarrow \mathrm{A}.$$

Therefore $\mathrm{a}_1^v, \dots, \mathrm{a}_{n-k-1}^v \vdash^{\mathrm{H}} \mathrm{A}$ by part (b) of Lemma 5.21. Therefore the result holds for $k + 1$. Note that when $k = n$ this says $\vdash^{\mathrm{H}}$ A. □

Theorem 5.24 is called the **completeness theorem for propositional calculus**—it asserts that the logical rules are *complete*, i.e. they are powerful enough to derive any result proved semantically using truth tables. By Theorems 5.12 and 5.24, for any set of propositions Σ,

$$\Sigma \vdash \mathrm{A} \text{ if and only if A is a tautological consequence of } \Sigma.$$

Definition 5.25. Fix a non-empty set S of propositional letters. A set $\Sigma \subseteq \mathrm{Prop}(S)$ is

- **consistent** if no propositional contradiction can be derived from Σ,
- **satisfiable** if it has a model, that is[24] there is a valuation $v \colon S \to 0, 1$ such that $v(\mathrm{A}) = 1$ for all $\mathrm{A} \in \Sigma$.

If Σ is **inconsistent**, i.e. it is not consistent, then every proposition can be derived from Σ, and conversely. Therefore

$$\Sigma \text{ is consistent if and only if } \{\mathrm{P} \in \mathrm{Prop}(S) \mid \Sigma \vdash \mathrm{P}\} \neq \mathrm{Prop}(S).$$

If $\Sigma \vdash \mathrm{P}$ then $\Sigma_0 \vdash \mathrm{P}$ for some finite $\Sigma_0 \subseteq \Sigma$, so Σ is consistent if and only if every finite $\Sigma_0 \subseteq \Sigma$ is consistent. If $\Sigma_0 = \{\mathrm{Q}_0, \dots, \mathrm{Q}_n\}$ then $\Sigma_0 \vdash \mathrm{P}$ if and only if $\mathrm{Q}_0 \Rightarrow \dots \Rightarrow \mathrm{Q}_n \Rightarrow \mathrm{P}$ is a tautology. Thus, if Σ is satisfiable then Σ is consistent.

[24] See Example 3.26

Conversely, suppose Σ is consistent. Assume, for the time being, that Σ is finite. If $\Sigma = \{Q_1, \dots, Q_n\}$ then by induction on $n \geq 0$ we prove that Σ is satisfiable. In fact if $n = 0$ then Σ is empty so it is trivially satisfiable. If $n > 0$ then $\{Q_1, \dots, Q_{n-1}\}$ is also consistent, so it is satisfiable by inductive assumption. If, towards a contradiction, $\{Q_1, \dots, Q_n\}$ were not satisfiable, then $v(Q_n) = 0$ for every v model of $\{Q_1, \dots, Q_{n-1}\}$, and hence $Q_1 \Rightarrow \dots \Rightarrow Q_{n-1} \Rightarrow \neg Q_n$ would be a tautology. This would yield $Q_1, \dots, Q_{n-1} \vdash \neg Q_n$ by the Completeness Theorem 5.24, and hence the inconsistency of $\{Q_1, \dots, Q_n\}$ would follow, against our assumption. Suppose now Γ is infinite: by the argument above Σ is finitely satisfiable, so Σ is satisfiable by the Compactness Theorem 4.46. Therefore we have proved:

Theorem 5.26. $\Sigma \subseteq \mathrm{Prop}(S)$ *is satisfiable if and only if it is consistent.*

5.E. Shoenfield's system*. We now look at a proof system based on the connectives $\neg, \vee$ as presented in Shoenfield's textbook [**?**]. All other connectives are defined in terms of $\neg$ and $\vee$, for example (recalling Convention 3.A) $A_1 \Rightarrow \dots \Rightarrow A_n \Rightarrow B$ and $A_1 \wedge \dots \wedge A_n \Rightarrow B$ stand for $\neg A_1 \vee \dots \vee \neg A_n \vee B$.

There is only one type of axiom, $\neg A \vee A$, and there are four inference rules:

$$\frac{A \vee B \vee C}{(A \vee B) \vee C} \qquad \frac{A \vee A}{A} \qquad \frac{A}{B \vee A} \qquad \frac{A \vee B \qquad \neg A \vee C}{B \vee C}$$

called: **associativity**, **contraction**, **expansion**, and **cut**. (Note that the expansion rule is just $\mathbf{I}_{\vee\ell}$ from Section 5.B.) An **S-derivation from** Γ is a finite list $A_1, \dots, A_n$ such that each A_i is either in Γ, or else it is an axiom (i.e. of the form $\neg B \vee B$), or else it follows from earlier A_js via one of the four rules. Write $\Gamma \vdash^S A$ if there is an S-derivation $A_1, \dots, A_n$ from Γ such that A_n is A. As usual when Γ is empty we write $\vdash^S A$.

Proposition 5.27. *The commutativity rule* $\dfrac{A \vee B}{B \vee A}$ *and* MP $\dfrac{A \qquad \neg A \vee B}{B}$ *hold.*

Proof. Suppose $A \vee B$: as $\neg A \vee A$ is an axiom then $\vdash B \vee A$ by the cut rule. Thus the commutative rule holds.

For MP argue as follows. Given A then $B \vee A$ by expansion, and hence $A \vee B$ by commutativity. If $\neg A \vee B$ holds, then $B \vee B$ by the cut rule, and therefore $\vdash B$ by the contraction rule. □

Corollary 5.28. *The rule of tautological consequence holds: for all $n \geq 1$ if* A_1, *…*, A_n *and* $\neg A_1 \vee \dots \vee \neg A_n \vee B$ *hold, then* B *holds. In symbols:*

$$\frac{A_1, \quad A_2, \quad \dots \quad A_n \qquad \neg A_1 \vee \dots \vee \neg A_n \vee B}{B}$$

Proof. By induction on n. When $n = 1$ it is just MP. Assuming the result is true for some $n \geq 1$, and suppose we are given $\mathrm{A}_1, \mathrm{A}_2, \dots, \mathrm{A}_{n+1}$, and $\neg\mathrm{A}_1 \vee \neg\mathrm{A}_2 \cdots \vee \neg\mathrm{A}_{n+1} \vee \mathrm{B}$, then $\neg\mathrm{A}_2 \cdots \vee \neg\mathrm{A}_{n+1} \vee \mathrm{B}$ follows by MP, and therefore B by inductive assumption. □

Proposition 5.29. *If* $\mathrm{A}_1, \dots, \mathrm{A}_n$ *is a derivation from* Γ*, then each* A_i *is a tautological consequence of* Γ.

Proof. If $\mathrm{A}_i \in \Gamma$ then the result holds by *fiat*, so we may assume otherwise. Therefore $i > 1$ and we may assume that the result holds for A_j with $j < i$. Proposition A_i is obtained from earlier A_js by means of one of our four rules, and since all these rules preserve tautological consequence, the result holds by induction. □

In particular, if $\vdash^{\mathrm{S}} \mathrm{A}$ then A is a tautology. Conversely,

Theorem 5.30. *If* A *is a tautology then* $\vdash^{\mathrm{S}} \mathrm{A}$.

Corollary 5.31. $\mathrm{A}_1, \dots, \mathrm{A}_n \vdash^{\mathrm{S}} \mathrm{A}$ *if and only if* $\vdash^{\mathrm{S}} \neg\mathrm{A}_1 \vee \dots \neg\mathrm{A}_n \vee \mathrm{A}$.

Proof. If $\mathrm{A}_1, \dots, \mathrm{A}_n \vdash^{\mathrm{S}} \mathrm{A}$ then by Proposition 5.29 A is tautological consequence of $\mathrm{A}_1, \dots, \mathrm{A}_n$, so $\neg\mathrm{A}_1 \vee \dots \neg\mathrm{A}_n \vee \mathrm{A}$ is a tautology, and hence $\vdash^{\mathrm{S}} \neg\mathrm{A}_1 \vee \dots \neg\mathrm{A}_n \vee \mathrm{A}$.

Conversely, if $\vdash^{\mathrm{S}} \neg\mathrm{A}_1 \vee \dots \neg\mathrm{A}_n \vee \mathrm{A}$ then by repeated applications of MP we successively derive

$$\begin{aligned}
&\mathrm{A}_1, \dots, \mathrm{A}_n \vdash^{\mathrm{S}} \neg\mathrm{A}_2 \vee \dots \vee \neg\mathrm{A}_n \vee \mathrm{A} \\
&\mathrm{A}_1, \dots, \mathrm{A}_n \vdash^{\mathrm{S}} \neg\mathrm{A}_3 \vee \dots \vee \neg\mathrm{A}_n \vee \mathrm{A} \\
&\qquad\qquad\vdots \\
&\mathrm{A}_1, \dots, \mathrm{A}_n \vdash^{\mathrm{S}} \mathrm{A}
\end{aligned}$$

which is what we had to prove. □

Therefore in order to derive a result we can either use Shoenfield's system, or the Hilbert-system of Section 5.D or the system of Natural Deduction from Section 5.B, that is

$$\Gamma \vdash^{\mathrm{S}} \mathrm{A} \quad \text{if and only if} \quad \Gamma \vdash^{\mathrm{H}} \mathrm{A} \quad \text{if and only if} \quad \Gamma \vdash^{\mathrm{ND}} \mathrm{A}.$$

Before proving Theorem 5.30 we need some preliminary results. For the sake of brevity write $\vdash$ for $\vdash^{\mathrm{S}}$.

Lemma 5.32. *The double negation rule* $\dfrac{\mathrm{A} \vee \mathrm{B}}{\neg\neg\mathrm{A} \vee \mathrm{B}}$ *holds.*

Proof. The proposition $\neg\neg\mathrm{A} \vee \neg\mathrm{A}$ holds, being an axiom, so by commutativity we get $\neg\mathrm{A} \vee \neg\neg\mathrm{A}$. As $\mathrm{A} \vee \mathrm{B}$ holds by assumption we get $\mathrm{B} \vee \neg\neg\mathrm{A}$ by cut, and hence $\neg\neg\mathrm{A} \vee \mathrm{B}$ by commutativity. □

Lemma 5.33. *For $1 \leq i < j \leq n$ the rule* $\dfrac{\mathrm{A}_i \vee \mathrm{A}_j}{\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n}$ *holds.*

Proof. We proceed by induction on n. If $n = 2$ there is nothing to prove, so we may suppose that $n \geq 3$. Assume $\mathrm{A}_i \vee \mathrm{A}_j$ towards proving $\mathrm{A}_1 \vee \mathrm{A}_2 \vee \mathrm{B}$, where $\mathrm{B} = \mathrm{A}_3 \vee \cdots \vee \mathrm{A}_n$.

If $i \geq 2$, then A_j occurs in B so by inductive assumption $\mathrm{A}_2 \vee \mathrm{B}$ holds, and hence $\mathrm{A}_1 \vee \mathrm{A}_2 \vee \mathrm{B}$ by expansion.

If $i = 1$ and $j \geq 3$, then $\mathrm{A}_1 \vee \mathrm{B}$ holds by inductive assumption, so $\mathrm{B} \vee \mathrm{A}_1$ by commutativity, and hence $\mathrm{A}_2 \vee \mathrm{B} \vee \mathrm{A}_1$ by the expansion rule. By associativity and commutativity $\mathrm{A}_1 \vee \mathrm{A}_2 \vee \mathrm{B}$ holds, which is what we had to prove.

If $i = 1$ and $j = 2$, then $\mathrm{A}_1 \vee \mathrm{A}_2$ holds by assumption, so by the expansion rule and commutativity $(\mathrm{A}_1 \vee \mathrm{A}_2) \vee \mathrm{B}_2$ holds. Therefore $\mathrm{A}_1 \vee \mathrm{A}_2 \vee \mathrm{B}_2$ holds by associativity. □

Lemma 5.34. *If $n, m \geq 1$ and $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$, then the rule* $\dfrac{\mathrm{A}_{i_1} \vee \cdots \vee \mathrm{A}_{i_m}}{\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n}$ *holds.*

Proof. By induction on m.

If $m = 1$ then letting $i = i_1$ we have that $(\mathrm{A}_{i+1} \vee \cdots \vee \mathrm{A}_n) \vee \mathrm{A}_i$ by the expansion rule so that $\mathrm{A}_i \vee \mathrm{A}_{i+1} \vee \cdots \vee \mathrm{A}_n$ by commutativity. The result follows by repeated applications of the expansion rule.

If $m = 2$ we distinguish two cases: if $i_1 = i_2$ by applying the contraction rule we fall back in the $m = 1$ case, and if $i_1 \neq i_2$ we may assume by commutativity that $i_1 < i_2$ and apply Proposition 5.33.

Suppose $m \geq 3$ and that $\mathrm{A}_{i_1} \vee \cdots \vee \mathrm{A}_{i_m}$ holds. For notational ease let $\mathrm{A} = \mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n$. By associativity $(\mathrm{A}_{i_1} \vee \mathrm{A}_{i_2}) \vee \mathrm{A}_{i_3} \vee \cdots \vee \mathrm{A}_{i_m}$ holds, and since this is a disjunction of $m - 1$ propositions, then by inductive assumption $(\mathrm{A}_{i_1} \vee \mathrm{A}_{i_2}) \vee \mathrm{A}$ holds. Commutativity and associativity imply that $(\mathrm{A} \vee \mathrm{A}_{i_1}) \vee \mathrm{A}_{i_2}$ holds, and since this is a disjunction of two propositions we have $(\mathrm{A} \vee \mathrm{A}_{i_1}) \vee \mathrm{A}$ by case $m = 2$. By commutativity and associativity $(\mathrm{A} \vee \mathrm{A}) \vee \mathrm{A}_{i_1}$ so by commutativity $\mathrm{A}_{i_1} \vee (\mathrm{A} \vee \mathrm{A})$, which is a disjunction of two propositions. From the case $m = 1$ we obtain $\mathrm{A} \vee (\mathrm{A} \vee \mathrm{A})$ and hence $(\mathrm{A} \vee \mathrm{A}) \vee (\mathrm{A} \vee \mathrm{A})$ by expansion and associativity. Applying contraction twice we obtain A. □

Lemma 5.35. *The rule* $\dfrac{\neg\mathrm{A} \vee \mathrm{C} \qquad \neg\mathrm{B} \vee \mathrm{C}}{\neg(\mathrm{A} \vee \mathrm{B}) \vee \mathrm{C}}$ *holds.*

Proof. The proposition $\neg(\mathrm{A} \vee \mathrm{B}) \vee \mathrm{A} \vee \mathrm{B}$ holds, being an axiom, so by commutativity we get $\mathrm{A} \vee \mathrm{B} \vee \neg(\mathrm{A} \vee \mathrm{B})$. As $\neg\mathrm{A} \vee \mathrm{C}$ holds by assumption we get $(\mathrm{B} \vee \neg(\mathrm{A} \vee \mathrm{B})) \vee \mathrm{C}$ by cut, and hence $\mathrm{C} \vee \mathrm{B} \vee \neg(\mathrm{A} \vee \mathrm{B})$ by commutativity. By Proposition 5.34 $\mathrm{B} \vee \mathrm{C} \vee \neg(\mathrm{A} \vee \mathrm{B})$ holds, and since $\neg\mathrm{B} \vee \mathrm{C}$ holds by assumption, we obtain $(\mathrm{C} \vee \neg(\mathrm{A} \vee \mathrm{B})) \vee \mathrm{C}$ by cut. Therefore $\mathrm{C} \vee \mathrm{C} \vee \neg(\mathrm{A} \vee \mathrm{B})$ by commutativity, and hence $\neg(\mathrm{A} \vee \mathrm{B}) \vee \mathrm{C}$ by Proposition 5.34. □

Call $\mathrm{A} \in \mathrm{Prop}(L)$ a **literal** if it is either a propositional letter or else the negation of a propositional letter.

Proposition 5.36. *Suppose* $\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n$ *is a tautology and that every* A_i *is a literal. Then there are* $i \neq j$ *such that* A_i *is the negation of* A_j.

Proof. Suppose there are no i, j as above. Let $v \colon L \to 2$ be the valuation $v(\mathrm{a}) = 1 \Leftrightarrow \neg\mathrm{a}$ is A_i, for some $i = 1, \ldots, n$. Then $v(\mathrm{A}_i) = 0$ for all i and hence $v(\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n) = 0$. □

Lemma 5.37. *Let* $n \geq 2$. *If* $\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n$ *is a tautology, then* $\vdash \mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n$.

Proof. We prove the result by induction on the pseudo-length of $\mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n$, that is the number

$$N = \mathrm{lh}(\mathrm{A}_1) + \cdots + \mathrm{lh}(\mathrm{A}_n).$$

By Proposition 5.36 we may assume that some A_i is not a literal. By Proposition 5.34 for all $1 \leq i \leq n$

$$\vdash \mathrm{A}_1 \vee \cdots \vee \mathrm{A}_n \quad \text{if and only if} \quad \vdash \mathrm{A}_i \vee \cdots \vee \mathrm{A}_n \vee \mathrm{A}_1 \vee \cdots \vee \mathrm{A}_{i-1}$$

so we may assume that A_1 is not a literal. Thus A_1 could be of the form $\mathrm{B} \vee \mathrm{C}$, or $\neg\neg\mathrm{B}$, or $\neg(\mathrm{B} \vee \mathrm{C})$.

If A_1 is $\mathrm{B} \vee \mathrm{C}$, then $\mathrm{B} \vee \mathrm{C} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ is a tautology, and since its pseudo-length is $N - 1$, by inductive assumption $\vdash \mathrm{B} \vee \mathrm{C} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$, and therefore $\vdash (\mathrm{B} \vee \mathrm{C}) \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ by associativity.

If A_1 is $\neg\neg\mathrm{B}$ then $\mathrm{B} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ is a tautology with pseudo-length $N - 2$ so by inductive assumption $\vdash \mathrm{B} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$. Therefore $\vdash \mathrm{A}_1 \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ by the double negation rule.

If A is $\neg(\mathrm{B} \vee \mathrm{C})$, then $\neg\mathrm{B} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ and $\neg\mathrm{C} \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$ are tautologies of pseudo-length $< N$, so by inductive assumption they can be derived. By Lemma 5.35 $\vdash \neg(\mathrm{B} \vee \mathrm{C}) \vee \mathrm{A}_2 \vee \cdots \vee \mathrm{A}_n$, which is what we had to prove. □

We can now prove Theorem 5.30.

Proof of Theorem 5.30. If A is a tautology, then so is $\mathrm{A} \vee \mathrm{A}$ so $\vdash \mathrm{A} \vee \mathrm{A}$ by Lemma 5.37 so $\vdash \mathrm{A}$ by contraction. □

5.F. Predicate calculus using natural deduction. Natural deduction for first-order logic has the rules for the connectives from Section 5.B, an introduction and an elimination rule for quantifiers, and a few axioms for equality. The resulting system is called **predicate calculus**. As for propositional calculus, derivations are organized in sub-derivations and the notion of depth and a line being alive/dead is as before. Since we are dealing with first-order logic, we abandon upper case roman letters $\mathrm{A}, \mathrm{B}, \mathrm{C}, \dots$ used for propositions in favour of the lower case Greek letters $\varphi, \psi, \chi, \dots$ for formulæ, while $\Gamma, \Delta, \dots$ are sets of formulæ. The rules are:

$$(\mathbf{I}_\exists)\ \frac{\varphi(\!|t/x|\!)}{\exists x\, \varphi}$$

$$(\mathbf{E}_\exists)\ \frac{\exists x\, \varphi}{\varphi(\!|c/x|\!)}\ , \quad c \text{ a new constant, starting a sub-derivation}$$

$$(\mathbf{I}_\forall)\ \frac{\varphi}{\forall x\, \varphi}\ , \quad x \text{ does not occur free in any assumption alive at this stage}$$

$$(\mathbf{E}_\forall)\ \frac{\forall x\, \varphi}{\varphi(\!|t/x|\!)}\ , \quad t \text{ a term.}$$

The adjective *new* in $\mathbf{E}_\exists$ means that c does not belong to the language $\mathcal{L}$ we are currently using. Note that the term t in $\mathbf{I}_\exists$ and in $\mathbf{E}_\forall$ could be x itself, so in that case $\varphi(\!|t/x|\!)$ is just φ. The rules $\mathbf{I}_\exists$ and $\mathbf{E}_\forall$ are obvious, while the other two need some explanation.

- $\mathbf{E}_\exists$ captures a basic pattern in proofs: once we get to an existential formula $\exists x\, \varphi$, it is customary to fix a witness c satisfying φ and proceed with the argument, so that at the end of the proof no mention of this c is present. Whenever $\mathbf{E}_\exists$ is applied a new sub-derivation begins, increasing the depth of the derivation; this sub-derivation can be terminated once we reach a formula φ in which c does not occur, and φ is exported to the next line with justification **e**.
- $\mathbf{I}_\forall$ is the rule of generalization since it allows to infer $\forall x\, \varphi$ from φ. The requirement for its applicability can be stated more formally as follows. If $\mathbf{I}_\forall$ is to be applied to $\varphi(x)$ on line n yielding $\forall x \varphi$ on line $n+1$, we must consider every line $k \leq n$ that are still alive at this stage and which are the beginning of sub-derivation: for any such k we must check that x does not occur free in that formula. Failure to comply with the requirement above might lead to incorrect proofs.

Example 5.38. Suppose c is a constant symbol of our language, then

$$\begin{array}{lll} 1 & x \doteq c & \mathbf{p} \\ 2 & \forall x\,(x \doteq c) & \mathbf{I}_\forall(1) \end{array}$$

witnesses that $x \doteq c \vdash \forall x\,(x \doteq c)$. In fact, a straightforward elaboration of this argument shows that $\varphi(x) \vdash \forall x\, \varphi(x)$ for any $\varphi(x)$.

On the other hand

$$\begin{array}{lll} 1 & \multicolumn{1}{|l}{x = c} & \mathbf{a} \\ 2 & \multicolumn{1}{|l}{\forall x\,(x = c)} & \mathbf{I}_{\forall}(1)\ \lightning \\ 3 & x = c \Rightarrow \forall x\,(x = c) & \mathbf{I}_{\Rightarrow}(1,2) \end{array}$$

is not a derivation because of an incorrect application of $\mathbf{I}_{\forall}$ on line 1, as a sub-derivation starts on that line and x is free in the formula of that line. If the above were a derivation, it would prove that $\vdash x = c \Rightarrow \forall x\,(x = c)$, and by the argument above we could prove that $\vdash \forall x\,(x = c \Rightarrow \forall x\,(x = c))$, which is not a valid sentence, since it fails in any model with more than one element.

Example 5.38 highlights a subtle point in the predicate calculus. Although $\vdash \varphi \Rightarrow \psi$ yields $\varphi \vdash \psi$ by means of $\mathbf{E}_{\Rightarrow}$, the converse does not hold: from $\varphi \vdash \psi$ we cannot infer that $\vdash \varphi \Rightarrow \psi$, so Theorem 5.22 from Section 5.D fails. The correct version of that result in our context is Theorem 5.44.

The next example illustrates the usage of the rule $\mathbf{I}_{\exists}$.

Example 5.39. $\vdash \varphi\llparenthesis t/x \rrparenthesis \Rightarrow \exists x\, \varphi$, since

$$\begin{array}{lll} 1 & \multicolumn{1}{|l}{\varphi\llparenthesis t/x \rrparenthesis} & \mathbf{a} \\ 2 & \multicolumn{1}{|l}{\exists x\, \varphi} & \mathbf{I}_{\exists}(1) \\ 3 & \varphi\llparenthesis t/x \rrparenthesis \Rightarrow \exists x\, \varphi & \mathbf{I}_{\Rightarrow}(1,2) \end{array}$$

In order to complete our presentation of predicate calculus we must define the **axioms for equality**:

EQ1: $x = x$,

EQ2: $x = y \Rightarrow y = x$,

EQ3: $x = y \wedge y = z \Rightarrow x = z$,

EQ4: $(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$

EQ5: $(x_1 = y_1 \wedge \cdots \wedge x_n = y_n \wedge P(x_1, \ldots, x_n)) \Rightarrow P(y_1, \ldots, y_n)$

where f is a function symbol, and P is a relation symbol. The axioms for equality can be used inside a derivation just like premises.

Given Γ a set of $\mathcal{L}$-formulæ and φ an $\mathcal{L}$-formula, a **derivation of** φ **from** Γ is a finite sequence $\psi_1, \ldots, \psi_n$ of $\mathcal{L}$-formulæ such that each ψ_i is either an element of Γ, or it is an axiom of equality, or it is obtained by one of the introduction/elimination rules described above. We write

$$\Gamma \vdash_{\mathcal{L}} \varphi$$

to say that there is a derivation of φ from Γ, but the subscript $\mathcal{L}$ will be suppressed, when it is clear from the context. Proposition 5.6 holds for predicate calculus, as well, so

- if $\Gamma \vdash \varphi$ and $\Gamma' \supseteq \Gamma$ then $\Gamma' \vdash \varphi$, and

- if $\Gamma \vdash \varphi$ and $\Gamma', \varphi \vdash \psi$ then $\Gamma \cup \Gamma' \vdash \psi$.

Of course it is possible to use the derived rules of Section 5.B.2 for propositional calculus, as well as some specific ones for the quantifiers that will be presented in Section 5.F.2.

The rules are **sound** that is only valid formulæ can be derived, and are **complete** that is any valid sentence can be derived.

Theorem 5.40 (Soundness)**.** *Let* $\Gamma \cup \{\varphi\}$ *be a set of* $\mathcal{L}$*-formulæ. If* $\Gamma \vdash \varphi$ *then* $\Gamma \models \varphi$*.*

The proof of Theorem 5.40 is an elaboration of that of Theorem 5.12, and is contained in Section 5.F.1 below. The reverse implication $\Sigma \models \varphi \Rightarrow \Sigma \vdash \varphi$ i.e. *completeness* will be proved in Chapter VII.

Warning. The word "complete" has two distinct meanings in logic, and this unfortunate situation may cause some confusion. The completeness of some logical calculus refers to the fact that the logical rules are powerful enough to derive any result proved by means of models. It does not say that the set of all sentences that are true in every structure is a *complete theory*, as Example 4.38 shows.

5.F.1. *Proof of the Soundness Theorem 5.40*.* The notation of the proof of Theorem 5.12 will be adopted in what follows. First of all we need to extend Definition 5.15 to first-order logic. A justified derivation from Γ is a finite list

$$(\varphi_1, \mathbf{j}_1, d_1, D_1, \mathbf{c}_1), \dots, (\varphi_n, \mathbf{j}_n, d_n, D_n, \mathbf{c}_n)$$

where

- $\mathbf{c}_k = \langle c_1, c_2, \dots \rangle$ is a (possibly empty) finite string of new constant symbols, that is c_i is a constant symbol that does not belong to $\mathcal{L} \cup \{c_1, \dots, c_{i-1}\}$, the language $\mathcal{L}$ with the symbols $c_1, \dots, c_{i-1}$ added for all $1 \leq i \leq \operatorname{lh} \mathbf{c}_k$. Set $\mathcal{L}(\mathbf{c}_k) = \mathcal{L} \cup \{c_1, \dots, c_m\}$ where $\mathbf{c}_k = \langle c_1, \dots, c_m \rangle$;
- φ_k is a $\mathcal{L}(\mathbf{c}_k)$-formula;
- $\mathbf{j}_k$ is one of the following labels: $\mathbf{p}$, $\mathbf{a}$, $\mathbf{i}$, an introduction/elimination rule for the connectives, or an introduction/elimination rule for the quantifiers, or the export rule $\mathbf{e}$;
- $d_k \in \mathbb{N}$ and $D_k \subseteq \{1, \dots, k-1\}$;

Clauses (1)–(9) are stated with φ_k in place of P_k, but (6) is modified as

(6) $d_k = d_{k-1} + 1$ if and only if $\mathbf{j}_k \in \{\mathbf{a}, \mathbf{E}_\exists\}$.

Besides clauses (1)–(9) we require that:

(10) $\mathbf{c}_1 = \mathbf{c}_n = \langle\rangle$ be the empty string;

(11) if $\mathbf{j}_k \in \{\mathbf{I}_\exists, \mathbf{E}_\forall, \mathbf{I}_\forall\}$ then

- $\mathbf{c}_k = \mathbf{c}_{k-1}$,
- $d_k = d_{k-1}$ and hence $D_k = D_{k-1}$ by clause (3);

(12) if $\mathbf{j}_k = \mathbf{I}_\exists$ then φ_k is of the form $\exists x\, \psi$ and φ_{k-1} is $\psi(\!|t/x|\!)$ with t an $\mathcal{L}(\mathbf{c}_{k-1})$-term,

(13) if $\mathbf{j}_k = \mathbf{E}_\forall$ then φ_{k-1} is of the form $\forall x\, \psi$ and φ_k is $\psi(\!|t/x|\!)$, with t an $\mathcal{L}(\mathbf{c}_{k-1})$-term,

(14) if $\mathbf{j}_k = \mathbf{I}_\forall$ then φ_k is $\forall x\, \psi$ and φ_{k-1} is ψ and x does not occur free in any of the assumptions alive at line k, that is x is not free in any φ_m with $m \in A_k$;

(15) if $\mathbf{j}_k = \mathbf{E}_\exists$ then:
- $d_k = d_{k-1} + 1$ and hence $D_k = D_{k-1}$ by condition (3),
- $\mathbf{c}_k$ is obtained by extending $\mathbf{c}_{k-1}$ with a new constant symbol $\bar{c}$, that is if $\mathbf{c}_{k-1} = \langle c_1, \dots, c_m \rangle$ then $\mathbf{c}_k = \langle c_1, \dots, c_m, \bar{c} \rangle$;
- φ_k is $\psi(\!|\bar{c}/x|\!)$ and φ_{k-1} is $\exists x\, \psi$;

(16) if $\mathbf{j}_k = \mathbf{e}$ then:
- $k^* = m + 1 < k - 1$,
- φ_m is of the form $\exists x\, \psi$
- φ_{m+1} is $\psi(\!|\bar{c}/x|\!)$ and $\mathbf{j}_{m+1} = \mathbf{E}_\exists$
- $d_m = d_k$ and $d_{m+1} = d_{k-1} = d_k + 1$ and hence $D_k \supset D_{k-1}$ by clause (4),
- $\mathbf{c}_m = \mathbf{c}_k$ and $\mathbf{c}_{m+1} = \mathbf{c}_{k-1} = \mathbf{c}_k{}^\frown\langle \bar{c} \rangle$,
- φ_k is φ_{k-1} and $\bar{c}$ does not occur in φ_{k-1}.

Suppose $\Gamma \vdash \varphi$ and let $(\varphi_1, \mathbf{j}_1, d_1, D_1, \mathbf{c}_1), \dots, (\varphi_n, \mathbf{j}_n, d_n, D_n, \mathbf{c}_n)$ be a justified derivation of φ from Γ, so that φ_n is φ. As in Theorem 5.19 we show that for all $k \leq n$

$$\Gamma \models \bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k \tag{5.13}$$

where A_k is the set defined in (5.9), so that when $A_n = \emptyset$ this yields $\Gamma \models \varphi$ as required. The formula $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$ belongs to the language $\mathcal{L}(\mathbf{c}_k)$, so (5.13) amounts to say that: for any $\mathcal{L}(\mathbf{c}_k)$-structure $\mathcal{B}$, if $\mathcal{B} \vDash \Gamma$ (that is $\mathcal{B}$ satisfies the universal closure of any formula in Γ), if the free variables of $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$ are among $x_1, \dots, x_p$ and $b_1, \dots, b_p$ are elements of $\mathcal{B}$ such that $\mathcal{B} \vDash \varphi_i[b_1, \dots, b_p]$ for all $i \in A_k$, then $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$. So suppose that

> the free variables of $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$ are among $x_1, \dots, x_p$,
> that $b_1, \dots, b_p$ are elements of $\mathcal{B}$, an $\mathcal{L}(\mathbf{c}_k)$-structure, and
> that $\mathcal{B} \vDash \varphi_i[b_1, \dots, b_p]$

towards proving $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$.

If $\mathbf{j}_k \in \{\mathbf{p}, \mathbf{a}, \mathbf{i}, \mathbf{I}_\neg, \mathbf{E}_\neg, \mathbf{I}_\wedge, \mathbf{E}_\wedge, \mathbf{I}_\vee, \mathbf{E}_\vee, \mathbf{I}_\Rightarrow, \mathbf{E}_\Rightarrow\}$ the argument is the same as in the proof of Theorem 5.19, except for minor changes. For example suppose $\mathbf{j}_k = \mathbf{I}_\Rightarrow(m)$, with $m < k$. Then φ_k is $\varphi_m \Rightarrow \varphi_{k-1}$. Let $\mathcal{B}$ be an $\mathcal{L}(\mathbf{c}_k)$-structure. By inductive assumption $\Gamma \models \bigwedge_{i \in A_{k-1}} \varphi_i \Rightarrow \varphi_{k-1}$. If v is any valuation satisfying $\Gamma \cup \{\mathrm{P}_i \mid i \in A_k\}$, then $v(\mathrm{P}_m \Rightarrow \mathrm{P}_{k-1}) = 1$ by (5.10). Therefore $\Gamma \models \bigwedge_{i \in A_k} \mathrm{P}_i \Rightarrow \mathrm{P}_k$.

Therefore it is enough to consider when $\mathbf{j}_k \in \{\mathbf{I}_\exists, \mathbf{E}_\exists, \mathbf{I}_\forall, \mathbf{E}_\forall, \mathbf{e}\}$. Let us summarize a few facts:

- if $\mathbf{j}_k \in \{\mathbf{I}_\exists, \mathbf{E}_\forall, \mathbf{I}_\forall\}$ then by (11) $d_k = d_{k-1}$ and hence $A_k = A_{k-1}$,
- if $\mathbf{j}_k = \mathbf{E}_\exists$, then $d_k = d_{k-1} + 1$ and $A_k = A_{k-1} \cup \{k\}$,
- if $\mathbf{j}_k = \mathbf{e}$, then, with the notation of (16), $d_{k-1} = d_k + 1$, $A_m = A_k$ and $A_{m+1} = A_{k-1} = A_k \cup \{m+1\}$.

Suppose $\mathbf{j}_k = \mathbf{I}_\exists$. Then φ_{k-1} is $\psi(\!|t/x|\!)$ and φ_k is $\exists x \psi$. As $A_k = A_{k-1}$, the free variables of $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$ are the same of $\bigwedge_{i \in A_{k-1}} \varphi_i \Rightarrow \varphi_{k-1}$. By inductive assumption $\mathcal{B} \vDash \varphi_{k-1}[b_1, \dots, b_p]$, so $t^{\mathcal{B}}[b_1, \dots, b_p]$ witnesses that $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$ as required.

Suppose $\mathbf{j}_k = \mathbf{E}_\forall$. Then φ_{k-1} is $\forall x \psi$ and φ_k is $\psi(\!|t/x|\!)$. As $A_k = A_{k-1}$, the free variables of $\bigwedge_{i \in A_{k-1}} \varphi_i \Rightarrow \varphi_{k-1}$ occur free in $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$. By inductive assumption $\mathcal{B} \vDash \varphi_{k-1}[b_1, \dots, b_p]$, and therefore $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$ as required.

Suppose $\mathbf{j}_k = \mathbf{I}_\forall$. Then φ_k is $\forall x \varphi_{k-1}$ and x does not occur free in any φ_i where $i \in A_k = A_{k-1}$. The free variables of $\bigwedge_{i \in A_{k-1}} \varphi_i \Rightarrow \varphi_{k-1}$ are among $x, x_1, \dots, x_p$. Let b be an arbitrary element of $\mathcal{B}$. By case assumption $\mathcal{B} \vDash \bigwedge_{i \in A_{k-1}} \varphi_i[b_1, \dots, b_p]$, so $\mathcal{B} \vDash \bigwedge_{i \in A_{k-1}} \varphi_i[b, b_1, \dots, b_p]$, and hence by inductive assumption $\mathcal{B} \vDash \varphi_{k-1}[b, b_1, \dots, b_p]$. Therefore $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$.

Suppose $\mathbf{j}_k = \mathbf{E}_\exists$. Then φ_{k-1} is $\exists x \psi$ and φ_k is $\psi(\!|c/x|\!)$. As $k \in A_k$, the formula $\bigwedge_{i \in A_k} \varphi_i \Rightarrow \varphi_k$ is a tautology, and since $\mathcal{B} \vDash \bigwedge_{i \in A_k} \varphi_i[b_1, \dots, b_p]$ then $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$, as required.

Lastly, suppose $\mathbf{j}_k = \mathbf{e}$. Then φ_k is φ_{k-1} and $\bar{c}$ does not occur in it. By case assumption

$$\forall i \in A_k = A_m \ (\mathcal{B} \vDash \varphi_i[b_1, \dots, b_p]) \,. \tag{5.14}$$

Th free variables of $\bigwedge_{i \in A_m} \varphi_i \Rightarrow \varphi_m$ are those of $\bigwedge_{i \in A_{m+1}} \varphi_i$, and they are among the $x_1, \dots, x_p$. By inductive assumption $\mathcal{B} \vDash \varphi_m[b_1, \dots, b_p]$, so there is an element $\bar{b}$ of $\mathcal{B}$ such that

$$(\mathcal{B}, \bar{b}) \vDash \varphi_{m+1}[b_1, \dots, b_p] \tag{5.15}$$

where $(\mathcal{B}, \bar{b})$ is the $\mathcal{L}(\mathbf{c}_{m+1})$-structure obtained from $\mathcal{B}$ by interpreting the constant symbol $\bar{c}$ with $\bar{b}$. By (5.14) and (5.15) it follows that $(\mathcal{B}, \bar{b}) \vDash \bigwedge_{i \in A_{m+1}} \varphi_i[b_1, \dots, b_p]$, and since $A_{m+1} = A_{k-1}$ and by inductive assumption we have that $(\mathcal{B}, \bar{b}) \vDash \varphi_{k-1}[b_1, \dots, b_p]$. As φ_k, that is φ_{k-1}, is an $\mathcal{L}(\mathbf{c}_k)$-formula, it follows that $\mathcal{B} \vDash \varphi_k[b_1, \dots, b_p]$, as required.

The proof of the Soundness Theorem 5.40 is complete.

5.F.2. *Some derived rules for predicate calculus.*

- The rule of **tautological consequence** (**taut**) asserts that if $\Gamma \vdash \psi_1, \dots, \Gamma \vdash \psi_n$ and if φ is tautological consequence of $\psi_1, \dots, \psi_n$, then $\Gamma \vdash \varphi$. In fact $\psi_1 \Rightarrow \dots \Rightarrow \psi_n \Rightarrow \varphi$ is provable, since it is a tautology (Theorem 5.24) so this rule follows from repeated applications of the $\mathbf{E}_{\Rightarrow}$.
- The rules ($\mathbf{exch}_{\exists/\forall}$) for **exchanging the quantifiers**

$$\frac{\forall x\, \varphi}{\neg\exists x\, \neg\varphi}\,, \qquad \frac{\neg\exists x\, \neg\varphi}{\forall x\, \varphi}\,, \qquad \frac{\exists x\, \varphi}{\neg\forall x\, \neg\varphi}\,, \qquad \frac{\neg\forall x\, \neg\varphi}{\exists x\, \varphi}\,,$$

state that either quantifier can be defined from the other one. The first two instances follow from $\vdash \forall x\, \varphi \Rightarrow \neg\exists x\, \neg\varphi$ and $\vdash \neg\exists x\, \neg\varphi \Rightarrow \forall x\, \varphi$:

$$\begin{array}{lll}
1 & \vert\ \forall x\, \varphi & \mathbf{a} \\
2 & \vert\ \vert\ \exists x\, \neg\varphi & \mathbf{a} \\
3 & \vert\ \vert\ \vert\ \neg\varphi \llparenthesis c/x \rrparenthesis & \mathbf{E}_{\exists}(3) \\
4 & \vert\ \vert\ \vert\ \forall x\, \varphi & \mathbf{i}(1) \\
5 & \vert\ \vert\ \vert\ \varphi \llparenthesis c/x \rrparenthesis & \mathbf{E}_{\forall}(4) \\
6 & \vert\ \vert\ \vert\ \forall x\, \varphi \wedge \neg\forall x\, \varphi & \bot(3,5) \\
7 & \vert\ \vert\ \forall x\, \varphi \wedge \neg\forall x\, \varphi & \mathbf{e} \\
8 & \vert\ \neg\exists x\, \neg\varphi & \mathbf{I}_{\neg}(2) \\
9 & \forall x\, \varphi \Rightarrow \neg\exists x\, \neg\varphi & \mathbf{I}_{\Rightarrow}(1,8)
\end{array}
\qquad
\begin{array}{lll}
1 & \vert\ \neg\exists x\, \neg\varphi & \mathbf{a} \\
2 & \vert\ \vert\ \neg\varphi & \mathbf{a} \\
3 & \vert\ \vert\ \exists x\, \neg\varphi & \mathbf{I}_{\exists}(2) \\
4 & \vert\ \vert\ \neg\exists x\, \neg\varphi & \mathbf{i}(1) \\
5 & \vert\ \vert\ \exists x\, \neg\varphi \wedge \neg\exists x\, \neg\varphi & \mathbf{I}_{\wedge}(3,4) \\
6 & \vert\ \varphi & \mathbf{E}_{\neg}(2) \\
7 & \vert\ \forall x\, \varphi & \mathbf{I}_{\forall}(6) \\
8 & \neg\exists x\, \neg\varphi \Rightarrow \forall x\, \varphi & \mathbf{I}_{\Rightarrow}(1,7)
\end{array}$$

while the third and fourth instance follow from the first two with $\neg\varphi$ in place of φ and the double negation rule (Exercise 5.50).

- The **instantiation rules**

$$\frac{\forall x_1 \dots \forall x_n\, \varphi}{\varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis}\,, \qquad \frac{\varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis}{\exists x_1 \dots \exists x_n\, \varphi}\,,$$

follow from

$$\begin{aligned} &\vdash \forall x_1 \dots \forall x_n\, \varphi \Rightarrow \varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis, \\ &\vdash \varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis \Rightarrow \exists x_1 \dots \exists x_n\, \varphi. \end{aligned} \tag{5.16}$$

By ($\mathbf{exch}_{\exists/\forall}$) and the contrapositive rule, it is enough to prove the second derivation. By Example 5.39

$$\exists x_{i+1} \dots \exists x_n \varphi \llparenthesis t_1/x_1, \dots, t_i/x_i \rrparenthesis \Rightarrow \exists x_i \exists x_{i+1} \dots \exists x_n \varphi \llparenthesis t_1/x_1, \dots, t_{i-1}/x_{i-1} \rrparenthesis$$

is valid, with the understanding that when $i = n$, this means that

$$\vdash \varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis \Rightarrow \exists x_n \varphi \llparenthesis t_1/x_1, \dots, t_{n-1}/x_{n-1} \rrparenthesis.$$

By transitivity of implication $\vdash \varphi \llparenthesis t_1/x_1, \dots, t_n/x_n \rrparenthesis \Rightarrow \exists x_1 \dots \exists x_n\, \varphi$ follows. In particular

$$\vdash \forall x_1 \dots \forall x_n\, \varphi \Rightarrow \exists x_1 \dots \exists x_n\, \varphi. \tag{5.17}$$

- The **swapping of quantifiers rule** $\dfrac{\Gamma \vdash \exists x\, \forall y\, \varphi}{\Gamma \vdash \forall y\, \exists x\, \varphi}$, follows from $\vdash \exists x\, \forall y\, \varphi \Rightarrow \forall y\, \exists x\, \varphi$. Consider these:

$$\begin{array}{lll}
1 & \mid\ \exists x\, \forall y\, \varphi & \mathbf{a} \\
2 & \mid\ \mid\ \forall y\, \varphi(\!|c/x|\!) & \mathbf{E}_{\exists}(1) \\
3 & \mid\ \mid\ \varphi(\!|c/x|\!) & \mathbf{E}_{\forall}(2) \\
4 & \mid\ \mid\ \exists x\, \varphi & \mathbf{I}_{\exists}(3) \\
5 & \mid\ \exists x\, \varphi & \mathbf{e} \\
6 & \mid\ \forall y\, \exists x\, \varphi & \mathbf{I}_{\forall}(5) \\
7 & \exists x\, \forall y\, \varphi \Rightarrow \forall y\, \exists x\, \varphi & \mathbf{I}_{\Rightarrow}(1,6)
\end{array}
\qquad
\begin{array}{llll}
1 & \mid\ \forall y\, \exists x\, \varphi & \mathbf{a} & \\
2 & \mid\ \exists x\, \varphi & \mathbf{E}_{\forall}(1) & \\
3 & \mid\ \mid\ \varphi(\!|c/x|\!) & \mathbf{E}_{\exists}(2) & \\
4 & \mid\ \mid\ \forall y\, \varphi(\!|c/x|\!) & \mathbf{I}_{\forall}(3) & ? \\
5 & \mid\ \mid\ \exists x\, \forall y\, \varphi & \mathbf{I}_{\exists}(4) & \\
6 & \mid\ \exists x\, \forall y\, \varphi & \mathbf{e} & \\
7 & \forall y\, \exists x\, \varphi \Rightarrow \exists x\, \forall y\, \varphi & \mathbf{I}_{\Rightarrow}(1,6) &
\end{array}$$

The one on the left is a derivation of $\vdash \exists x\, \forall y\, \varphi \Rightarrow \forall y\, \exists x\, \varphi$, while the one on the right *might not be a derivation*: the application of $\mathbf{I}_{\forall}$ on line 4 could be illegal since y might occur free in φ. In case y is not free in φ, it is a derivation of $\forall y\, \exists x\, \varphi \Rightarrow \exists x\, \forall y\, \varphi$. (In this case $\forall y\, \exists x\, \varphi$, $\exists x\, \forall y\, \varphi$, and $\exists x\, \varphi$ assert the same fact.)

- The **equivalence rules** are

$$\frac{\varphi \Leftrightarrow \psi}{\forall x\, \varphi \Leftrightarrow \forall x\, \psi}, \qquad \frac{\varphi \Leftrightarrow \psi}{\exists x\, \varphi \Leftrightarrow \exists x\, \psi}.$$

The first one follows from $\varphi \Rightarrow \psi \vdash \forall x \varphi \Rightarrow \forall x \psi$:

$$\begin{array}{lll}
1 & \varphi \Rightarrow \psi & \mathbf{p} \\
2 & \forall x(\varphi \Rightarrow \psi) & \mathbf{I}_{\forall}(1) \\
3 & \mid\ \forall x \varphi & \mathbf{a} \\
4 & \mid\ \mid\ \neg \forall x \psi & \mathbf{a} \\
5 & \mid\ \mid\ \exists x \neg \psi & \mathbf{exch}_{\exists/\forall} \\
6 & \mid\ \mid\ \mid\ \neg \psi(\!|c/x|\!) & \mathbf{E}_{\exists}(5) \\
7 & \mid\ \mid\ \mid\ \forall x(\varphi \Rightarrow \psi) & \mathbf{i}(2) \\
8 & \mid\ \mid\ \mid\ \varphi(\!|c/x|\!) \Rightarrow \psi(\!|c/x|\!) & \mathbf{E}_{\forall}(7) \\
9 & \mid\ \mid\ \mid\ \neg \varphi(\!|c/x|\!) & \mathbf{taut}(6,8) \\
10 & \mid\ \mid\ \mid\ \forall x \varphi & \mathbf{i}(1) \\
11 & \mid\ \mid\ \mid\ \varphi(\!|c/x|\!) & \mathbf{E}_{\forall} \\
12 & \mid\ \mid\ \mid\ \forall x \psi & \bot(11,9) \\
13 & \mid\ \mid\ \forall x \psi & \mathbf{e} \\
14 & \mid\ \mid\ \forall x \psi \wedge \neg \forall x \psi & \mathbf{I}_{\wedge}(13,4) \\
15 & \mid\ \forall x \psi & \mathbf{E}_{\neg}(4) \\
16 & \forall x \varphi \Rightarrow \forall x \psi & \mathbf{I}_{\Rightarrow}(1,15)
\end{array}$$

The second rule follows from the first and $(\mathbf{exch}_{\exists/\forall})$.

Remark 5.41. If $\Gamma \vdash \varphi \Leftrightarrow \psi$, then by the equivalence rule $\Gamma \vdash \neg \exists x \varphi \Leftrightarrow \forall x \neg \psi$, so the rule $(\mathbf{exch}_{\exists/\forall})$ can be extended accordingly. For example $\vdash \neg \exists x(\varphi \wedge \psi) \Leftrightarrow \forall x(\varphi \Rightarrow \neg \psi)$.

5.F.3. *Results about derivations.*

Proposition 5.42. (a) *Suppose* $\Gamma \vdash \varphi \Rightarrow \psi$.

- *If x does not occur free in φ, then* $\Gamma \vdash \varphi \Rightarrow \forall x\, \psi$.
- *If x does not occur free in ψ, then* $\Gamma \vdash \exists x\, \varphi \Rightarrow \psi$.

(b) *If* $\Gamma \vdash \varphi$*, then* $\Gamma \vdash \forall x\, \varphi$*. Therefore* $\Gamma \vdash \varphi$ *if and only if* $\Gamma \vdash \varphi^{\forall}$*, where* $\varphi^{\forall}$ *is the universal closure of* φ*.*

(c) $\Gamma, \psi \vdash \varphi$ *if and only if* $\Gamma, \forall x\, \psi \vdash \forall x\, \varphi$*.*

(d) *If* $\Gamma \vdash \varphi$*, then* $\Gamma \vdash \varphi(\!|t_1/x_1, \dots, t_n/x_n|\!)$*.*

(e) *If* $\Gamma \vdash \varphi \Rightarrow \psi$*, then* $\Gamma \vdash \exists x\, \varphi \Rightarrow \exists x\, \psi$ *and* $\Gamma \vdash \forall x\, \varphi \Rightarrow \forall x\, \psi$*.*

Proof. (a) Assume φ and suppose x does not occur free in φ: as $\varphi \Rightarrow \psi$ follows from Γ, then so does ψ, so by applying $\mathbf{I}_{\forall}$ we get $\forall x\, \psi$. This application of $\mathbf{I}_{\forall}$ is legal, as by assumption x is not free in φ.

The other result follows by the contrapositive rule.

(b) Suppose $\Gamma \vdash \varphi$. As $\exists x\, \neg\varphi \Rightarrow \varphi$ is a tautological consequence of φ then $\Gamma \vdash \exists x\, \neg\varphi \Rightarrow \varphi$. By part (a) $\Gamma \vdash \exists x\, \neg\varphi \Rightarrow \forall x\, \varphi$, and since $\forall x\, \varphi$ is a tautological consequence of $\exists x\, \neg\varphi \Rightarrow \forall x\, \varphi$ then $\Gamma \vdash \forall x\, \varphi$. By repeated applications of this argument, $\Gamma \vdash \varphi$ implies $\Gamma \vdash \varphi^{\forall}$. The converse direction follows from (5.16).

(c) Let $\chi_1, \dots, \chi_n$ be a derivation of $\Gamma, \psi \vdash \varphi$. Without loss of generality we may assume that χ_1 is ψ with justification $\mathbf{p}$. Then $\chi_0, \dots, \chi_{n+1}$ is a derivation of $\Gamma, \forall x\, \psi \vdash \forall x\, \varphi$, where

- χ_0 is $\forall x\, \varphi$ with justification $\mathbf{p}$,
- the justification of χ_1 is changed from $\mathbf{p}$ to $\mathbf{E}_{\forall}(0)$,
- χ_{n+1} is $\forall x\, \varphi$ with justification $\mathbf{I}_{\forall}(n)$.

The application of $\mathbf{I}_{\forall}(n)$ is legal, since the depth of line n in the derivation is 0, so it does not depend on any assumption.

Conversely, suppose $\chi_1, \dots, \chi_n$ is a derivation of $\Gamma, \forall x\, \psi \vdash \forall x\, \varphi$, where χ_1 is $\forall x\, \psi$ with justification $\mathbf{p}$. Then $\chi_0, \dots, \chi_{n+1}$ is a derivation of $\Gamma, \psi \vdash \varphi$, where

- χ_0 is φ with justification $\mathbf{p}$,
- the justification of χ_1 is changed from $\mathbf{p}$ to $\mathbf{I}_{\forall}(0)$,
- χ_{n+1} is φ with justification $\mathbf{E}_{\forall}(n)$.

(d) Suppose $\Gamma \vdash \varphi$. By part (b) $\Gamma \vdash \varphi^{\forall}$, so $\Gamma \vdash \varphi(\!|t_1/x_1, \dots, t_n/x_n|\!)$ follows from (5.16).

(e) Suppose $\Gamma \vdash \varphi \Rightarrow \psi$. By (5.16) again, $\vdash \psi \Rightarrow \exists x\, \psi$, so $\Gamma \vdash \varphi \Rightarrow \exists x\, \psi$, and hence $\Gamma \vdash \exists x\, \varphi \Rightarrow \exists x\, \psi$ by part (a). The result with the universal quantifiers follows from the contrapositive rule. □

Part (b) of Proposition 5.42 explains a common pattern in mathematical proofs: in order to prove the universal closure of φ it is enough to prove φ itself.

By Proposition 5.42(d) the axioms for equality with arbitrary terms instead of variables are derivable:

EQ1⁺: $t = t$,

EQ2⁺: $t = s \Rightarrow s = t$,

EQ3⁺: $t = s \wedge s = u \Rightarrow t = u$,

EQ4⁺: $(t_1 = s_1 \wedge \cdots \wedge t_n = s_n) \Rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$

EQ5⁺: $(t_1 = s_1 \wedge \cdots \wedge t_n = s_n \wedge P(t_1, \ldots, t_n)) \Rightarrow P(s_1, \ldots, s_n)$.

The next result is called the equality theorem.

Theorem 5.43. *If the terms $t_1, \ldots, t_n$ and $s_1, \ldots, s_n$ are substitutable for $x_1, \ldots, x_n$ in φ, then*

$$\vdash t_1 = s_1 \wedge \cdots \wedge t_n = s_n \;\Rightarrow\; (\varphi(\!|t_1/x_1, \ldots, t_n/x_n|\!) \Leftrightarrow \varphi(\!|s_1/x_1, \ldots, s_n/x_n|\!))\,.$$

Proof. Suppose first φ is atomic. By **EQ2⁺** it is enough to prove that

$$\vdash t_1 = s_1 \wedge \cdots \wedge t_n = s_n \wedge \varphi(\!|t_1/x_1, \ldots, t_n/x_n|\!) \;\Rightarrow\; \varphi(\!|s_1/x_1, \ldots, s_n/x_n|\!).$$

If φ is $x_1 = x_2$ then we must prove that

$$\vdash t_1 = s_1 \wedge t_2 = s_2 \wedge t_1 = t_2 \Rightarrow s_1 = s_2$$

which follows from **EQ3⁺**. If φ is $u(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)$ with u, v terms, then we must prove that

$$\begin{aligned}\vdash t_1 = s_1 \wedge \cdots \wedge t_n = s_n \wedge u(t_1, \ldots, t_n) = v(t_1, \ldots, t_n)&\\ \Rightarrow u(s_1, \ldots, s_n) = v(s_1, \ldots, s_n),&\end{aligned}$$

which follows from **EQ4⁺** and transitivity. If φ is $P(x_1, \ldots, x_n)$ apply **EQ5⁺**. Thus the result holds for any atomic φ.

We now proceed by induction on the height of φ. First of all notice that

$$(\mathrm{A} \Leftrightarrow \mathrm{B}) \Rightarrow (\neg\mathrm{A} \Leftrightarrow \neg\mathrm{B}),$$
$$(\mathrm{A}_1 \Leftrightarrow \mathrm{B}_1) \wedge (\mathrm{A}_2 \Leftrightarrow \mathrm{B}_2) \Rightarrow ((\mathrm{A}_1 \odot \mathrm{A}_2) \Leftrightarrow (\mathrm{B}_1 \odot \mathrm{B}_2))$$

are tautologies, where $\odot$ is any binary connective. Therefore if φ is either $\neg\psi$ or else $\psi \odot \chi$, the result follows at once by the inductive assumption. Finally if φ is either $\exists y\, \psi$ or else $\forall y\, \psi$, then the result follows from the inductive assumption and the equivalence rule. □

As we observed after Example 5.38, if $\Gamma \vdash \varphi \Rightarrow \psi$ then $\Gamma, \varphi \vdash \psi$ by MP. Conversely suppose $\chi_1, \ldots, \chi_n$ is a derivation of $\Gamma \cup \{\varphi\} \vdash \psi$. In order to prove $\Gamma \vdash \varphi \Rightarrow \psi$, one would start with assuming φ, starting thus a sub-derivation, then write $\chi_1, \ldots, \chi_n$, the derivation for $\Gamma \cup \{\varphi\} \vdash \psi$, and then finish by closing the sub-derivation using the $\mathbf{I}_{\Rightarrow}$ rule. The problem is that there might be a line $1 \leq k \leq n$ in the derivation of $\Gamma \cup \{\varphi\} \vdash \psi$ where

$\mathbf{I}_\forall$ is applied to a variable that occurs free in φ, spoiling our plan. Therefore the version of Theorem 5.22 for first-order logic is:

Theorem 5.44. *Suppose that there is a derivation of $\Gamma \cup \{\varphi\} \vdash \psi$ and suppose that in such derivation all applications of $\mathbf{I}_\forall$, if any, do not involve variables that occur free in φ. Then $\Gamma \vdash \varphi \Rightarrow \psi$.*

In particular, if φ is a sentence and $\Gamma \cup \{\varphi\} \vdash \psi$ then $\Gamma \vdash \varphi \Rightarrow \psi$.

In mathematics, when proving $\forall x\, \varphi$ one usually argues as follows: take a generic element $\bar{x}$ and show that φ holds for that $\bar{x}$; as $\bar{x}$ is arbitrary, one obtains $\forall x\, \varphi(x)$. The next result justifies the correctness of this argumentation.

Theorem 5.45. *Suppose Γ is a set of $\mathcal{L}$-formulæ and φ is an $\mathcal{L}$-formula. If c is a constant not in $\mathcal{L}$, then*

$$\Gamma \vdash_{\mathcal{L}} \forall x\, \varphi \quad \textit{if and only if} \quad \Gamma \vdash_{\mathcal{L}\cup\{c\}} \varphi\llparenthesis c/x\rrparenthesis.$$

Proof. If $\Gamma \vdash_{\mathcal{L}} \forall x\, \varphi$ then $\Gamma \vdash_{\mathcal{L}\cup\{c\}} \forall x\, \varphi$, and hence $\Gamma \vdash_{\mathcal{L}\cup\{c\}} \varphi\llparenthesis c/x\rrparenthesis$ by (5.17).

Conversely suppose $\psi_1, \dots, \psi_n$ witnesses that $\Gamma \vdash_{\mathcal{L}\cup\{c\}} \varphi$, and let y be a variable that doesn't occur in any ψ_i. Each ψ_i is an $\mathcal{L}\cup\{c\}$-formula, and it is easy to check that $\psi_i\llparenthesis y/c\rrparenthesis$ is an $\mathcal{L}$-formula. For notational ease, write $\bar{\psi}_i$ for $\psi_i\llparenthesis y/c\rrparenthesis$. Observe that if ψ_i is in Γ or is an axiom for equality, then $\bar{\psi}_i$ is ψ_i, and that $\bar{\psi}_n$ is $(\varphi\llparenthesis c/x\rrparenthesis)\llparenthesis y/c\rrparenthesis$, that is $\varphi\llparenthesis y/c\rrparenthesis$. Then $\bar{\psi}_1, \dots, \bar{\psi}_n$ is an $\mathcal{L}$-derivation witnessing $\Gamma \vdash_{\mathcal{L}} \varphi\llparenthesis y/x\rrparenthesis$. Next we apply Proposition 5.42: by part (d) $\Gamma \vdash_{\mathcal{L}} (\varphi\llparenthesis y/x\rrparenthesis)\llparenthesis x/y\rrparenthesis$, that is $\Gamma \vdash_{\mathcal{L}} \varphi$, and hence $\Gamma \vdash_{\mathcal{L}} \forall x\, \varphi$ by part (b). □

5.G. From informal proofs to derivations. Let us sketch how to translate a simple informal proof into a derivation.

Example 5.46. Suppose R is a transitive, symmetric relation on a set X such that $\forall x \in X\, \exists y \in X \;\; x \mathrel{R} y$. Then R is an equivalence relation on X.

We want to show that $\Gamma \vdash \forall x\, (x \mathrel{R} x)$, where Γ is the set made up of the three sentences: $\forall x, y, z\, (x \mathrel{R} y \land y \mathrel{R} z \Rightarrow x \mathrel{R} z)$, $\forall x, y\, (x \mathrel{R} y \Rightarrow y \mathrel{R} x)$, $\forall x\, \exists y\, (x \mathrel{R} y)$. The semantic argument runs as follows. Given an element $c \in X$, by hypothesis there is $d \in X$ such that $c \mathrel{R} d$, and hence $d \mathrel{R} c$. As R is transitive, from $c \mathrel{R} d$ and $d \mathrel{R} c$ we obtain $c \mathrel{R} c$. Being c arbitrary we infer $\forall x\, (x \mathrel{R} x)$. So if $\mathcal{L}$ is the language with R as a binary predicate, and c is a constant symbol that does not belong to $\mathcal{L}$, then by Theorem 5.45 it is enough to prove that $\Gamma \vdash_{\mathcal{L}\cup\{c\}} c \mathrel{R} c$, as in Figure 9.

To be continued

$$\begin{array}{rll}
1 & \forall x\,\exists y\,(x\;R\;y) & \mathbf{p} \\
2 & \forall x,y\,(x\;R\;y \Rightarrow y\;R\;x) & \mathbf{p} \\
3 & \forall x,y,z\,(x\;R\;y \wedge y\;R\;z \Rightarrow x\;R\;z) & \mathbf{p} \\
4 & \exists y\,(c\;R\;y) & \mathbf{E}_{\forall}(1) \\
5 & \big|\; c\;R\;d & \mathbf{E}_{\exists}(4) \\
6 & \big|\; \forall x,y\,(x\;R\;y \Rightarrow y\;R\;x) & \mathbf{i}(2) \\
7 & \big|\; \forall y\,(c\;R\;y \Rightarrow y\;R\;c) & \mathbf{E}_{\forall}(6) \\
8 & \big|\; c\;R\;d \Rightarrow d\;R\;c & \mathbf{E}_{\forall}(7) \\
9 & \big|\; d\;R\;c & \mathbf{E}_{\Rightarrow}(5,8) \\
10 & \big|\; c\;R\;d \wedge d\;R\;c & \mathbf{I}_{\wedge}(5,9) \\
11 & \big|\; \forall x,y,z\,(x\;R\;y \wedge y\;R\;z \Rightarrow x\;R\;z) & \mathbf{i}(3) \\
12 & \big|\; \forall y,z\,(c\;R\;y \wedge y\;R\;z \Rightarrow c\;R\;z) & \mathbf{E}_{\forall}(10) \\
13 & \big|\; \forall z\,(c\;R\;d \wedge d\;R\;z \Rightarrow c\;R\;z) & \mathbf{E}_{\forall}(11) \\
14 & \big|\; c\;R\;d \wedge d\;R\;c \Rightarrow c\;R\;c & \mathbf{E}_{\forall}(12) \\
15 & \big|\; c\;R\;c & \mathbf{E}_{\Rightarrow}(13,5) \\
16 & c\;R\;c & \mathbf{e}
\end{array}$$

Figure 9. A derivation used in Example 5.46.

5.H. A Hilbert-style calculus for first-order logic. It is possible to develop a Hilbert-style calculus for first-order logic. In order to keep the notational complexity to a minimum, we present a system where the premises, the axioms, and the theorems are *sentences*. In other words when we write $\Gamma \vdash^{\mathrm{H}} \varphi$ we are assuming that all formulæ in Γ are sentences, φ is a sentence, and every formula in this derivation is a sentence as well.

The official connectives are $\neg$ and $\Rightarrow$, all the other connectives are defined accordingly. A **logical axiom** is a sentence of which is the universal closure of a formula of the form

- $\varphi \Rightarrow \forall x\,\varphi$, where x does not occur free in φ,
- $\varphi(\!|t_1/x_1,\dots,t_n/x_n|\!) \Rightarrow \exists x_1 \dots \exists x_n \varphi$, where $t_1,\dots,t_n$ are closed terms,
- $\forall x\,\neg\varphi \Rightarrow \neg\exists x\,\varphi$,
- $\forall x\,(\varphi \Rightarrow \psi) \Rightarrow (\forall x\,\varphi \Rightarrow \forall x\,\psi)$,
- an axiom for equality **EQ1**–**EQ5**,
- a tautology for propositional calculus.

Then $\Gamma \vdash^{\mathrm{H}} \varphi$ just in case there is a finite list $\psi_1,\dots,\psi_n$ of sentences such that each ψ_i is either a logical axiom, or else it belongs to Γ, or else it is obtained from the earlier ψ_is using the *Modus Ponens* (MP).

The last clause in the definition of logical axiom drastically simplifies derivations, but at the same time makes the proofs and arguments in Section 5.D utterly irrelevant.

Every axiom of this system is provable using natural deduction, and hence $\Gamma \vdash^{\mathrm{H}} \varphi$ implies that $\Gamma \vdash \varphi$. It will be proved in Chapter VII that if

$\Gamma \vdash^{\mathrm{H}} \varphi$ then $\Gamma \models \varphi$ (Soundness Theorem 33.4), and, conversely, if every model satisfying Γ is a model of φ then $\Gamma \vdash \varphi$ (Completeness Theorem 34.3).

Remark 5.47. The fact that the only logical rule is the MP has the amusing consequence that propositional logic governs derivations in first-order logic. Validities in propositional logic can be established using the method of truth tables, while derivations in first-order logic (arising from the formalization of proofs in mathematics) tend to be quite complex, so a word of explanation is in order.

If Γ is a *finite* set of propositions over a set of letters L, then $\Gamma \vdash \mathrm{A}$ if and only if $\bigwedge \Gamma \Rightarrow \mathrm{A}$ is a tautology, and this that can be established in a mechanical way. When Γ is infinite, $\Gamma \vdash \mathrm{A}$ just in case there is a finite $\Gamma_0 \subseteq \Gamma$ such that $\bigwedge \Gamma_0 \Rightarrow \mathrm{A}$ is a tautology, but there is no simple way to find out which Γ_0 would do the job.

If $\Gamma \cup \{\varphi\}$ is a set of $\mathcal{L}$-sentences, $\Gamma \vdash \varphi$ just in case φ can be derived using propositional logic from $\Gamma \cup \Lambda$, where Λ is the set of all logical axioms for $\mathcal{L}$. Observe that Λ is infinite, even if Γ is finite (or even empty!), so the task of deciding whether $\Gamma \vdash \varphi$ cannot be solved in a mechanical way.

Exercises

Exercise 5.48. Prove the following logical rules of propositional calculus using natural deduction.

(i) The double negation rules $\mathrm{A} \vdash \neg\neg\mathrm{A}$ and $\neg\neg\mathrm{A} \vdash \mathrm{A}$.

(ii) De Morgan's laws: $\vdash \neg(\mathrm{A} \vee \mathrm{B}) \Leftrightarrow \neg\mathrm{A} \wedge \neg\mathrm{B}$ and $\vdash \neg(\mathrm{A} \wedge \mathrm{B}) \Leftrightarrow \neg\mathrm{A} \vee \neg\mathrm{B}$.

(iii) The distributivity rules for $\wedge$ and $\vee$: $\vdash \mathrm{A} \wedge (\mathrm{B} \vee \mathrm{C}) \Leftrightarrow (\mathrm{A} \wedge \mathrm{B}) \vee (\mathrm{A} \wedge \mathrm{C})$ and $\vdash \mathrm{A} \vee (\mathrm{B} \wedge \mathrm{C}) \Leftrightarrow (\mathrm{A} \vee \mathrm{B}) \wedge (\mathrm{A} \vee \mathrm{C})$.

(iv) Associativity and commutativity of $\vee$ and $\wedge$:

$$\begin{array}{ll} \vdash \mathrm{A} \vee (\mathrm{B} \vee \mathrm{C}) \Leftrightarrow (\mathrm{A} \vee \mathrm{B}) \vee \mathrm{C} & \qquad \vdash \mathrm{A} \vee \mathrm{B} \Leftrightarrow \mathrm{B} \vee \mathrm{A} \\ \vdash \mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C}) \Leftrightarrow (\mathrm{A} \wedge \mathrm{B}) \wedge \mathrm{C} & \qquad \vdash \mathrm{A} \wedge \mathrm{B} \Leftrightarrow \mathrm{B} \wedge \mathrm{A}. \end{array}$$

(v) $\vdash (\mathrm{A} \Rightarrow \mathrm{B}) \Leftrightarrow (\neg\mathrm{A} \vee \mathrm{B})$.

(vi) $\vdash (\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Leftrightarrow ((\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{C})$.

Exercise 5.49. Prove the following tautologies using the calculus of natural deduction.

(i) $(\mathrm{A} \Rightarrow \mathrm{B}) \vee (\mathrm{B} \Rightarrow \mathrm{A})$ (Dummet's law).

(ii) $((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{A}) \Rightarrow \mathrm{A}$ (Peirce's law).

(iii) $(\neg\mathrm{B} \Rightarrow \neg\mathrm{A}) \Rightarrow ((\neg\mathrm{B} \Rightarrow \mathrm{A}) \Rightarrow \mathrm{B})$.

(iv) $(\mathrm{C} \Rightarrow \mathrm{A}) \Rightarrow [(\mathrm{C} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{C} \Rightarrow (\mathrm{A} \wedge \mathrm{B})]$.

(v) $(\mathrm{A} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{A} \vee \mathrm{B}) \Rightarrow \mathrm{C}$.

(vi) $(\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\mathrm{B} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$.

(vii) $((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \mathrm{C}) \Rightarrow ((\mathrm{C} \Rightarrow \mathrm{A}) \Rightarrow (\mathrm{D} \Rightarrow \mathrm{A}))$.

Exercise 5.50. Prove the validity of the following formulæ using the calculus of natural deduction.

(i) $\exists x\varphi \Leftrightarrow \neg\forall x\neg\varphi$ (this is half of the rule $\mathbf{exch}_{\exists/\forall}$).

(ii) Assuming x does not occur free in ψ:
- $\forall x(\varphi \Rightarrow \psi) \Leftrightarrow (\exists x\varphi \Rightarrow \psi)$,
- $(\psi \Rightarrow \forall x\varphi) \Leftrightarrow \forall x(\psi \Rightarrow \varphi)$,
- $(\psi \Rightarrow \exists x\varphi) \Leftrightarrow \exists x(\psi \Rightarrow \varphi)$,
- $(\forall x\varphi \Rightarrow \psi) \Leftrightarrow \exists x(\varphi \Rightarrow \psi)$.

(iii) $\exists x\,(\varphi \Rightarrow \forall x\,\varphi)$. (This is Example 2.5.)

(iv) $\exists x\,\exists y\,\varphi \Leftrightarrow \exists y\,\exists x\,\varphi$ and $\forall x\,\forall y\,\varphi \Leftrightarrow \forall y\,\forall x\,\varphi$.

(v) $\forall x\,\varphi \wedge \forall x\,\psi \Leftrightarrow \forall x\,(\varphi \wedge \psi)$ and $\exists x\,(\varphi \vee \psi) \Leftrightarrow \exists x\,\varphi \vee \exists x\,\psi$.

(vi) $\forall x\,\varphi \vee \forall x\,\psi \Rightarrow \forall x\,(\varphi \vee \psi)$ and, dually, $\exists x\,(\varphi \wedge \psi) \Leftrightarrow \exists x\,\varphi \wedge \exists x\,\psi$.

(vii) $\forall x\,(\varphi \Rightarrow \psi) \Rightarrow (\forall x\,\varphi \Rightarrow \forall x\,\psi)$.

(viii) $\exists x(\varphi \wedge \forall y(\varphi\llparenthesis y/x\rrparenthesis \Rightarrow y = x)) \Leftrightarrow (\exists x\,\varphi \wedge \forall x\forall y(\varphi \wedge \varphi\llparenthesis y/x\rrparenthesis \Rightarrow x = y))$ and $\exists x(\varphi \wedge \forall y(\varphi\llparenthesis y/x\rrparenthesis \Rightarrow y = x)) \Leftrightarrow \exists x\forall y(\varphi\llparenthesis y/x\rrparenthesis \Leftrightarrow x = y)$. Thus the three formulations of $\exists!$ on page 16 are equivalent.

Exercise 5.51. Using natural deduction, show that if there are m distinct elements that satisfy $\varphi(x)$, then there are n distinct elements that satisfy $\varphi(x)$, with $1 \leq n \leq m$.

Exercise 5.52. Show that the axioms **EQ2** and **EQ3** (i.e. symmetry and transitivity of $=$) can be replaced by $x_1 = y_1 \wedge x_2 = y_2 \wedge x_1 = x_2 \Rightarrow y_1 = y_2$.

Notes and remarks

The approach to natural deduction presented here is due to Frederic Fitch and it is exposed in detail in [**BPBE11**]. There are as many versions of Hilbert-style calculi, as there are books in logic; the one presented here is (a modification of) the one in [**Men15**].

6. What is mathematical logic?

It would have probably been wiser to place a section with a title like this at the end of the book, when the reader—hopefully—has mastered the basics of the subject. And even then a title like this might still look a bit over the top, since the goal of this textbook is not presenting all of mathematical logic (a patently hopeless endeavour), but only to cover the basics of those areas that, according to the author's opinion, are closer to other parts of mathematics. Maybe this section should be entitled *What is that part of mathematical logic covered in this book?* or something like that.... In any case, the desire to give an eagle's eye view of what will be covered in detail in the next sections is too compelling.

Mathematical logic originated with the attempts to give mathematically precise answers to general questions such as:

(1) *What is a proof?*

(2) *What is an effective procedure?*

(3) *What does it mean that a certain statement is true?*

(4) *What is a set?*

(5) *Is logic a part of mathematics, or is it a discipline that comes before mathematics?*

The attempts to answer to these questions have generated a large body of mathematical theories.

6.A. Proof theory. The notion of derivation has syntactical flavour, while the usual mathematical reasoning is based on the notion of logical consequence (see page 56), and this is a semantic concept, i.e. it talks about models. The formal, syntactical notion of proof (encoded by the definition of derivation) and the semantic one (following common mathematical practice) are tightly connected. If $\Sigma \vdash \sigma$ then every model of Σ is a model of σ (soundness Theorem 33.4) and, conversely, if every model satisfying Σ is also a model of σ then $\Sigma \vdash \sigma$ (completeness Theorem 34.3). Therefore derivations are the formal counterpart of the intuitive notion of proof—σ is provable (in the usual sense) from Σ, if and only if σ can be derived from Σ, in symbols $\Sigma \vdash \sigma$.

A system of axioms Σ is **consistent** if it does not derive every formula, that is if it cannot derive a formula and its negation. If Σ has a model, then it is consistent, since a structure cannot satisfy both a sentence and its negation. The converse also holds (model existence Theorem 34.4): if Σ is consistent, then it has a model.

6.B. Computability. Every effective function belongs to a set of functions known as the **computable functions**. Since every computable function is effective, we shall use the terms "effective" and "computable" interchangeably. A set $A \subseteq \mathbb{N}$ is **decidable** or **computable** if its characteristic function is computable. To check that n belongs to $\operatorname{ran}(f)$, with $f \colon \mathbb{N} \to \mathbb{N}$ a computable function, it is enough to compute $f(0), f(1), \ldots$: if n appears in this list, then we will be able to asses in a finite number of steps that $n \in \operatorname{ran}(f)$, if instead n does not appear, we must perform an infinite number of computations in order to be sure that $n \notin \operatorname{ran}(f)$. A set of the form $\operatorname{ran}(f)$ with f computable is **semi-decidable** or **computably enumerable**. Every computable set is computably enumerable, but not conversely. The computably enumerable subsets of $\mathbb{N}$ are exactly the **Diophantine sets**, i.e. those of the form $\mathbb{N} \cap \{f(n_1, \dots, n_k) \mid n_1, \dots, n_k \in \mathbb{Z}\}$ with f a polynomial in k variables and coefficients in $\mathbb{Z}$.

If we consider a language with finitely many non-logical symbols—almost every first-order language considered so far is of this kind—it is possible to associate to each formula and, more generally, to any string of formulæ, a natural number. If Σ is a computable set of axioms, then the set of all derivations from Σ is computable. In other words: it is a routine task to check whether or not a given string of formulæ is a derivation, while if Σ is *sufficiently strong*, then the set of theorems of Σ is computably enumerable, but not computable. The expression "sufficiently strong" means that Σ proves certain elementary facts on natural numbers—for example, **Peano arithmetic** (see Section 12.D in Chapter III) would do. A further extension of these ideas leads to the celebrated Gödel's **First Incompleteness Theorem**:[25] every sufficiently strong, computable, and consistent system of axioms Σ is **incomplete**, that is there is a statement σ such that $\Sigma \nvdash \sigma$ and $\Sigma \nvdash \neg\sigma$.

6.C. Models. In mathematical logic, terms and formulæ of a language $\mathcal{L}$ are full fledged mathematical objects (just like natural numbers, graphs, vector spaces, ...). On the other hand, in common mathematical practice (pseudo-)formulæ don't have a real mathematical *status*, their role is to describe properties of structures, that are the true point of interest for all mathematicians not working in logic. Thus one of the first, and foremost, obstacles met at the beginning of the study of mathematical logic is to accept the fact that formulæ and structures are both objects worth studying. This shift in perspective allows not only to study all formulæ that are true in a given structure, or in a class of structures, like it happens in algebra, but it also allows the opposite route: starting with a set of sentences and consider the structures that satisfy this given set. Model theory, that is the study of the mutual relationship between formulæ and structures of the same language, already begun in Sections 3 and 9 will be investigated in a systematic way in Chapter VII. We shall see that the study of models of first-order theories can solve problems arising in other parts of mathematics, and sheds new light on well-known objects. For example, we shall construct structures $(M, +, \cdot, <)$ which are elementarily equivalent (but not isomorphic) to $(\mathbb{N}, +, \cdot, <)$. These

[25] The incompleteness theorems are among the deepest results in mathematical logic and will be proved in Chapter VIII.

structures are called non-standard models of arithmetic, and are essential to fully appreciate the Gödel incompleteness theorem.

Finally, observe that in the preceding pages we have explained what it means for a sentence of $\mathcal{L}$ to be true in a structure $\mathcal{M}$, that is there is a map

$$\mathcal{L}\text{-sentences} \times \mathcal{L}\text{-structures} \to \{0, 1\}$$

assigning value 1 to $(\sigma, \mathcal{M})$ if and only if $\mathcal{M} \vDash \sigma$. Under closer scrutiny, the definition above is not very satisfying since we were a bit too cavalier when moving from the formal language $\mathcal{L}$ to the informal language where mathematical facts are stated. To convince oneself of the need for an adequate formalization of the notions of satisfaction and definability, it is enough to consider the following argument, known as **Berry's paradox**: let n be the smallest natural number that it is not definable with less than 1000 symbols. But the sentence above has less than 1000 symbols, and hence it defines n. In Chapter VII we shall rigorously formalize the satisfaction relation, and Berry's paradox will vanish in thin air.

Peano arithmetic and set theory are theories where it is possible to construct statements that can be neither proved nor refuted from the given theory. On the other hand, there are examples of mathematically interesting first-order theories that are not subject to the incompleteness phenomenon. For example, ACF_0 the theory of algebraically closed fields of characteristic zero (Example 4.39) is complete, thus it is the theory of $(\mathbb{C}, +, \cdot)$ by Proposition 3.32. Every complete theory T, in a computable language is **decidable**, that is there is an algorithm that decides wether a given statement is provable or not from T, and the study of complete decidable theories is one of the central topics in model theory. The theory of $(\mathbb{N}, +, \cdot)$ is complete, but undecidable, and so it is not computably axiomatizable. Whenever $(\mathbb{N}, +, \cdot)$ is definably interpretable in a structure, it follows that such structure is undecidable.

6.D. Sets. Set theory is ubiquitous in mathematics—the objects studied in algebra, analysis, geometry, are construed as sets with some additional structure. In Section 13 of Chapter IV and more extensively in Chapter VI we will show how to reconstruct in set theoretic terms the fundamental objects of mathematics—natural numbers, real numbers, measure theory, etc. Because of this foundational aspect, we will study set theory in Chapter V.

Besides being a handy and useful language for mathematics, set theory has a life of its own, focusing on the analysis of the notion of infinity, with problems, techniques, specific methods, that make it one of the most fascinating parts of mathematical logic. Before plunging into these topics, note that set theory can be formalized as a first-order theory—in fact such formalization is needed, since Russell in 1901 showed that naïve set theory is inconsistent. At the beginning of the twentieth century, several (essentially equivalent) axiomatizations of the notion of set have been introduced, and in Chapter V we will develop set theory as a first-order theory.

Let's go back at the notion of infinity. Cantor, the creator of set theory, had the revolutionary idea that sizes of infinite sets can be compared using bijections. In particular, the kind of infinity of the real line is larger than the kind of infinity of the natural numbers (Theorem 13.22). Cantor conjectured that there was no intermediate kind of infinity, that is every infinite subset of the real line is either in bijection with the natural numbers, or with the line itself, and this conjecture was called the **Continuum Hypothesis** (CH). In 1938 Gödel showed that the Continuum Hypothesis cannot be disproved from the axioms of set theory, and in 1963 Cohen showed that it is neither provable. Therefore axiomatic set theory is incomplete, and the Continuum Hypothesis is an example of such incompleteness. In the last few decades a large number of questions, some of which originated in other areas of mathematics, have been shown to be independent.

6.E. Metamathematics. In this book, set theory is taken as the bedrock upon which other mathematical objects are built. In particular, logical notions such as language, derivation, structure, truth, ..., are formalized within axiomatic set theory. Here we focus on the Zermelo-Frænkel axiom system ZF, possibly augmented with the axiom of choice ZFC, but a similar argument applies to the other axiomatizations of set theory, such as NGB or MK. Being a first-order theory, ZF should be presented after Chapter VII where the results on first-order theories are proved. We reach a paradoxical situation: we need set theory to define the concept of structure of first-order language (in order to define the notion of validity of a formula), and yet we must use a first-order language to rigorously develop the notion of set, i.e. the theory ZF. More generally: if logic is a part of mathematics, how can it be the foundation of all of mathematics (and hence of itself)? This vicious circle, reminiscent of chicken-or-egg dilemma, is just apparent. Let's see how it can be solved.

6.E.1. *Syntax.* Consider a first-order language $\mathcal{L}$ with a finite number of non-logical symbols (i.e. relation, function, and constant symbols)—all examples in Sections 3 and 9 are of this kind, and so is $\mathcal{L}_{\in}$, the language having only one binary relation symbol $\in$. Terms and formulæ of $\mathcal{L}$ are concrete objects, symbols that we write on the blackboard or on a piece of paper, so we can check in a mechanical way if a given string is a formula of $\mathcal{L}$. Suppose Σ is an effective set of sentences of $\mathcal{L}$, that is such that it is possible to establish in a mechanical way whether an $\mathcal{L}$-sentence σ belongs to Σ. For brevity's sake we say that $\mathcal{L}$ and Σ as above are **effective**. All examples of axiom systems encountered in Sections 3 and 9, as well as the axiom systems for set theory that will be seen in Chapter V, are examples of effective theories. As explained in Section 6.A a **derivation of σ from Σ** is a finite string of formulæ of $\mathcal{L}$, each of which is a logical axiom, or it is in Σ, or it is obtained from the preceding formulæ by means of a logical rule, and the notion "being a derivation from Σ" is effective. In other words: given a sequence $\varphi_0, \ldots, \varphi_n$ of formulæ of $\mathcal{L}$, it is possible to determine in a mechanical way whether this is a derivation from Σ.[26]

The formulæ of $\mathcal{L}_\in$ as well as the derivations in this language are *pre-set-theoretic* entities, concrete objects that are needed in order to be able to speak about arbitrary sets. The mathematical environment where these constructive arguments on formulæ are carried out is called **metatheory** or **metamathematics**. If we were to try formulate a bold analogy with computer science, we could say that metamathematics is to mathematics as compilers are to general programs.

We shall say that Σ is **consistent** if it is not possible to derive from it *any* formula or, equivalently, if no logically false formula can be derived from it, such as, for example, $\exists x(x \neq x)$. Thus asserting the consistency of Σ is a universal statement, and can be seen as an optimistic prediction: we shall never be able to derive a contradiction from Σ. Conversely, to conclude that Σ is inconsistent (i.e. it is not consistent) we must exhibit a derivation of a contradiction from Σ.

6.E.2. *Semantics.* The notions of structure, model, morphism, ... are all set-theoretical and hence live inside ZF, but they do not belong to the the metatheory. Conversely, all arguments carried out in the metatheory can be coded within a sufficiently strong theory, such as, for example, ZF. In particular, the notions of derivation and consistency can be coded within set theory, thus ZF can formalize (and prove) both the Completeness Theorem 34.3

> *Let T be a first-order theory in a language $\mathcal{L}$ and let σ be an $\mathcal{L}$-statement. Then $T \models \sigma$ if and only if $T \vdash \sigma$.*

and the Model Existence Theorem 34.4

> *A consistent first-order theory is satisfiable.*

These two results apply to *all* first-order theories, not just the effective ones.

6.E.3. *Coding of syntax.* If $\mathcal{L}$ and Σ are effective, then they are representable using natural numbers inside set theory. Every formula φ is coded via a natural numbers $\ulcorner \varphi \urcorner$, while Σ is coded by a computable set of natural numbers $\ulcorner \Sigma \urcorner$. Thus a derivation from Σ can be coded as a finite sequence of natural numbers, which in turns can be coded by a single natural number.

[26] When we claim to have proved a theorem, we are essentially saying (modulo a translation in the language $\mathcal{L}_\in$) that a certain statement σ can be derived form the axion of set theory.

If in the metatheory it has been shown that

$$\Sigma \vdash \sigma \tag{6.1}$$

then the fact that such derivation exists is provable inside ZF, and we can write

$$\mathsf{ZF} \vdash \exists n\, (n \text{ codes a proof of } \sigma \text{ from } \Sigma). \tag{6.2}$$

Thus (6.2) follows from (6.1). The converse implication, however, is problematic: to prove formula (6.1) an *explicit derivation* $\varphi_0, \dots, \varphi_n$ of σ must be provided, while to prove (6.2) it is enough to show that *there exists some derivation* of σ from Σ; for example it is enough to reach a contradiction in ZF from the assumption that no such derivation exist. The situation is similar to what happens in number theory when one proves a statements of the form $\exists n\, \varphi(n)$ with φ a computable property: if the proof uses constructive arguments, then we can (hope to) explicitly write down a number n that has property φ, but if abstract methods were used in the proof, then, in general, we have no clue on what n might be. The problem can be stated as follows. We have a theory T and a formula $\varphi(x)$, where x ranges over the natural numbers, such that membership for the set I defined by it is effective. Suppose $\mathsf{T} \vdash \exists x \varphi(x)$ yet in the metatheory we verify that $I = \emptyset$, and hence T proves that $\neg\varphi(0)$, $\neg\varphi(1)$, $\neg\varphi(2)$, ... Such T is a deranged theory, since it asserts the existence of a natural number that cannot be found in the real world, yet it need not be inconsistent. A theory T for which this phenomenon *does not* occur, is called **Σ_1-sound**. If we assume that ZF is Σ_1-sound (and this is a very reasonable assumption) then (6.2) implies (6.1).

Gödel's **Second Incompleteness Theorem** says that no effective, consistent, sufficiently strong theory proves its own consistency. Sufficiently strong entails that such theory can encode the syntax of an effective language, so ZF is sufficiently strong. Moreover, the vast body of mathematical results proved in set theory suggests that ZF is free from contradictions. Thus, by Gödel's theorem, $\mathsf{ZF} \nvdash \mathrm{Con}_{\mathsf{ZF}}$.

The interplay between theory and metatheory is one of logic's most fascinating facets, and will be studied in Chapter VIII.

Chapter II

Orders, Boolean algebras and computations

7. Orders, lattices, and Boolean algebras

7.A. Orders. An $\mathcal{L}_{\mathrm{ORDR}}$-structure, where $\mathcal{L}_{\mathrm{ORDR}}$ is the language containing a binary relation symbol $\leq$, is a pair $(P, \leq_P)$ with $\leq_P$ a binary relation on P. Recall that $(P, \leq_P)$ is an order if it satisfies

- $\forall x\,(x \leq x)$,
- $\forall x, y\,(x \leq y \wedge y \leq x \Rightarrow x = y)$,
- $\forall x, y, z\,(x \leq y \wedge y \leq z \Rightarrow x \leq z)$,

and $(P, \leq_P)$ is a total i.e. linear order if moreover it satisfies $\forall x, y\,(x \leq y \vee y \leq x)$. If antisymmetry is dropped we have a preorder or quasi-order. Observe that a subset of a (total) order is a (total) ordered, as the axioms used to define it are $\forall$-sentences. If $(P, \leq)$ is an ordered set and $A \subseteq P$,

$$\mathrm{pred}(x, A; \leq) = \{y \in A \mid y < x\}$$

is the set of all predecessors of x that lie in A—thus $\mathrm{pred}(x) = \mathrm{pred}(x, P; \leq)$ is the set of all predecessors of x. The **dual** of an $\mathcal{L}_{\mathrm{ORDR}}$-structure $\mathcal{P} = (P, \leq)$ is the $\mathcal{L}_{\mathrm{ORDR}}$-structure

$$\mathcal{P}^{\Delta} = (P, \geq)$$

where $\geq$ is the inverse of $\leq$, that is $a \geq b \Leftrightarrow b \leq a$. Clearly $\mathcal{P}^{\Delta\Delta} = \mathcal{P}$. The **dual of formula** φ of $\mathcal{L}_{\mathrm{ORDR}}$ is φ^{Δ} obtained by replacing in φ every atomic sub-formula of the form '$x \leq y$' with '$y \leq x$'. Formally the dual of a formula is defined inductively by

- $(x = y)^{\Delta}$ is $x = y$,
- $(x \leq y)^{\Delta}$ is $y \leq x$,
- $(\neg\varphi)^{\Delta}$ is $\neg(\varphi^{\Delta})$,
- $(\varphi \odot \psi)^{\Delta}$ is $\varphi^{\Delta} \odot \psi^{\Delta}$,
- $(\mathsf{Q}x\varphi)^{\Delta}$ is $\mathsf{Q}x\varphi^{\Delta}$,

where $\odot$ is a binary connective and Q is a quantifier. By induction on the height of φ it is shown that $\mathbf{T}^{\mathcal{P}}_{\varphi(x_1,\dots,x_n)} = \mathbf{T}^{\mathcal{P}^{\Delta}}_{\varphi^{\Delta}(x_1,\dots,x_n)}$, and hence

$$\mathcal{P} \vDash \sigma \quad \text{if and only if} \quad \mathcal{P}^{\Delta} \vDash \sigma^{\Delta}$$

for every sentence σ. A formula is **self-dual** if it is (logically equivalent to) its dual. The sentences that axiomatize the class of orders (the reflexive, antisymmetric and transitive properties) are self-dual, hence $\mathcal{P}$ is a (pre-) order if and only if $\mathcal{P}^{\Delta}$ is a (pre-)order. To recap:

Duality principle for (pre-)orders. *If $\mathcal{P}$ is a (pre-)order and σ is a sentence of $\mathcal{L}_{POrdr}$ then*

$$\mathcal{P} \vDash \sigma \quad \textit{if and only if} \quad \mathcal{P}^{\Delta} \vDash \sigma^{\Delta}.$$

In particular: σ is logical consequence of the axioms for (pre-)orders if and only if so is σ^{Δ}.

Given an order $(P, \leq)$ and $\emptyset \neq X \subseteq P$, we will say that an element $m \in X$ is **maximum** in X if $a \leq m$ for all $a \in X$; if the condition is weakened to "there is no $a \in X$ such that $m < a$" the notion of **maximal** element in X is obtained. When $X = P$ we speak of maximum and maximal element. By the antisymmetric property a maximum of a set X (if it exists) is unique, and it is denoted by $\max X$, and it is the unique element satisfying the formula $\forall y\,(y \leq x)$ in the structure $(X, \leq)$. An element is **minimum** or **minimal** if it is maximum or maximal in the dual order.

Remark 7.1. The duality principle for orders can be used to cut the number of verifications in half, but attention must be payed in order to avoid misunderstandings. ***The duality principle does not assert that***:

- if an ordered set satisfies σ then it satisfies also σ^{Δ}—there are ordered sets that have minimum but not maximum (and conversely) so that they satisfy $\exists x \forall y\,(x \leq y)$ but not $\exists x \forall y\,(y \leq x)$;
- an ordered set satisfies every self-dual sentence—any order without maximum or minimum does not satisfy the self-dual sentence $\exists x \forall y\,(x \leq y) \wedge \exists x \forall y\,(y \leq x)$.

Proposition 7.2. *A finite non-empty ordered set has minimal and maximal elements.*

Proof. Let $(A, \leq)$ be a finite non-empty ordered set, say $A = \{a_0, \dots, a_n\}$. Towards a contradiction, suppose $(A, \leq)$ has no maximal elements. As a_0 is not maximal, there must be $k_1 \leq n$ such that $a_0 < a_{k_0}$; as a_{k_1} is not maximal, there must be $k_2 \leq n$ such that $a_{k_1} < a_{k_2}$; and so on. Arguing this way we would construct infinitely many elements $a_0 < a_{k_0} < \dots$ of A against our finiteness assumption.

The proof that $(A, \leq)$ has minimal elements is obtained by taking the dual order. □

Remark 7.3. The proof of the preceding result uses a couple of obvious facts that will be proved in detail later on. The first is that the k_is is defined inductively—in order to define k_{i+1} we must have first defined k_i. (These definitions will be considered in Section 12.B.) The second fact is that $\mathbb{N}$ does not inject into a finite set (Dirichlet's pigeonhole principle—Theorem 13.15).

Proposition 7.4. *Any ordering $\leq$ on a finite sets A can be extended to a linear ordering $\preceq$ on A, that is $\forall x, y \in A\,(x \leq y \Rightarrow x \preceq y)$.*

Proof. Proceed by induction on n the number of elements of A. If $n \leq 1$ the result is trivial, so we may assume that $n \geq 2$. By Proposition 7.2 let $\bar{a} \in A$ be minimal: by inductive assumption there is a linear order $\leq^*$ on $A \setminus \{\bar{a}\}$ extending $\leq$ on $A \setminus \{\bar{a}\}$. Then

$$x \preceq y \Leftrightarrow \begin{cases} x \leq^* y \text{ and } x, y \in A \setminus \{\bar{a}\} \\ x = \bar{a} \end{cases}$$

is a linear ordering on A extending $\leq$. □

In Chapter VI we shall see that Proposition 7.4 holds for infinite sets as well (Theorem 14.22.)

Proposition 7.5. *Two finite linear orders of the same size are isomorphic, and the isomorphism is unique.*

Proof. Let us prove by induction on n that two finite linear orders $(P, \leq_P)$ and $(Q, \leq_Q)$ of size n are isomorphic, and the isomorphism is unique. If $n = 0$ then $P = Q = \emptyset$ and there is nothing to prove. Suppose P and Q have size $n+1$. By Proposition 7.2 there are maxima $\bar{p} \in P$ and $\bar{q} \in Q$, so by inductive assumption there is a unique isomorphism $\bar{f} \colon (P \setminus \{\bar{p}\}, \leq_P) \to (Q \setminus \{\bar{q}\}, \leq_Q)$, so $f \colon P \to Q$ defined by

$$f(p) = \begin{cases} \bar{f}(p) & \text{if } p \neq \bar{p}, \\ \bar{q} & \text{if } p = \bar{p}, \end{cases}$$

is an isomorphism. Uniqueness of f follows from the observation that any isomorphism maps $\bar{p}$ to $\bar{q}$. □

If $(P, \leq)$ is a preorder, $Q \subseteq P$ is an **initial segment** or **lower set** or **down-set** of P if $x \in Q \wedge y \leq x \Rightarrow y \in Q$. For example,

$$\downarrow Q = \{y \in P \mid \exists x \in Q(y \leq x)\}$$

is a lower set, for all $Q \subseteq P$; in fact Q is a lower set if and only if $\downarrow Q = Q$. When Q is a singleton $\{x\}$ we shall write $\downarrow x$ instead of $\downarrow\{x\}$. Note that $\downarrow x = \operatorname{pred}(x) \cup \{x\}$. The collection of all lower sets of the preorder P is

$$\operatorname{Down}(P)$$

and it is an ordered set under inclusion, with maximum P and minimum $\emptyset$. If P is an order (i.e. antisymmetry holds), the map

$$P \to \operatorname{Down}(P), \qquad x \mapsto \downarrow x \tag{7.1}$$

is an embedding, and hence:

Proposition 7.6. *Every order $(P, \leq)$ is embeddable in $(\mathscr{P}(P), \subseteq)$.*

We say that $Q \subseteq P$ is a **final segment** or **upper set** or **up-set** if it is a lower set of the dual preorder P^{Δ}, and

$$\uparrow Q = \{y \in P \mid \exists x \in Q(x \leq y)\}$$

is the set $\downarrow Q$ computed in P^{Δ}. The collection of all upper subsets of P is denoted by $\operatorname{Up}(P)$, and it is ordered under inclusion. Since

$$\begin{aligned} \operatorname{Down}(P)^{\Delta} &\to \operatorname{Up}(P), & Q &\mapsto P \setminus Q \\ \operatorname{Up}(P) &\to \operatorname{Down}(P^{\Delta}), & Q &\mapsto Q \end{aligned}$$

are isomorphisms, then

$$\operatorname{Down}(P)^{\Delta} \cong \operatorname{Down}(P^{\Delta}) \quad \text{and} \quad \operatorname{Up}(P)^{\Delta} \cong \operatorname{Up}(P^{\Delta}).$$

The families $\operatorname{Down}(P)$ and $\operatorname{Up}(P)$ are topologies on P, known as the **downward** and **upward topology** respectively. The family $\{\downarrow p \mid p \in P\}$ a basis for $\operatorname{Down}(P)$ and $\{\uparrow p \mid p \in P\}$ is a basis for $\operatorname{Up}(P)$.

Lemma 7.7. *Suppose P, Q are preordered sets and $f \colon P \to Q$. The following are equivalent:*

(a) *f is monotone;*

(b) *f is continuous, when P, Q are endowed with the downward topology;*

(c) *f is continuous, when P, Q are endowed with the upward topology.*

Proof. Suppose f is monotone. As $f^{-1}[\downarrow q]$ is a down-set for any $q \in Q$, the preimage of a basic open set is open, so f is continuous. Conversely suppose f is continuous and that $p_1 \leq_P p_2$. As p_2 belongs to the open set $f^{-1}[\downarrow f(p_2)]$ then $p_1 \in \downarrow p_2 \subseteq f^{-1}[\downarrow f(p_2)]$, so $f(p_1) \in \downarrow f(p_2)$, that is $f(p_1) \leq_Q f(p_2)$. Therefore we have proved that (a)⇔(b).

The proof of (a)$\Leftrightarrow$(c) is completely analogous. □

An **upper bound** for a subset X of P is an element $a \in P$ such that $\forall x \in X\,(x \leq a)$ and $X^{\blacktriangledown}$ is the set of all upper bounds of X. A subset X with an upper bound, that is such that $X^{\blacktriangledown} \neq \emptyset$ is **bounded above**. If $a = \min X^{\blacktriangledown}$ we say that a is the **least upper bound** of X. The definitions of $X^{\blacktriangle}$, **lower bound**, **subset bounded from below**, **greatest lower bound** are obtained by "dualizing" the definitions above. By the antisymmetric property, the least upper bound of $X = \{p_i \mid i \in I\}$ (if it exists) is unique and will be denoted by

$$\sup X = \sup_{i\in I} p_i \quad \text{or} \quad \bigcurlyvee X = \bigcurlyvee_{i\in I} p_i .$$

Recall from Section 4.E that $\sup(a, b)$ is denoted by $a \curlyvee b$. Similarly, the greatest lower bound of $X = \{p_i \mid i \in I\} \subseteq P$ is unique (if it exists) and is denoted by

$$\inf X = \inf_{i\in I} p_i \quad \text{or} \quad \bigcurlywedge X = \bigcurlywedge_{i\in I} p_i$$

and $\inf(a, b)$ is denoted by $a \curlywedge b$.

In a lattice the maximum and the minimum (if they exist) are denoted by $\mathbf{1}$ and $\mathbf{0}$,[1] and in this case we say it is a **bounded lattice**. In the case of linear orders the maximum and minimum are called **end-points**. A lattice $(L, \leq)$ is **complete** if $\bigcurlyvee X$ exists for every $X \subseteq L$; equivalently, by Lemma 7.8 below, if $\bigcurlywedge X$ exists for every $X \subseteq L$. If $X = \{a_1, \dots, a_n\}$, then $\bigcurlyvee X = a_1 \curlyvee \dots \curlyvee a_n$ and $\bigcurlywedge X = a_1 \curlywedge \dots \curlywedge a_n$ exist and are well defined, hence every finite lattice complete. A complete lattice L is bounded, since $\mathbf{1} = \bigcurlyvee L$ and $\mathbf{0} = \bigcurlywedge \emptyset$. Recall that $X^{\blacktriangledown} = \{y \in L \mid \forall x \in X\,(x \leq y)\}$ is the set of all upper bounds of X, and that $X^{\blacktriangle} = \{y \in L \mid \forall x \in X\,(y \leq x)\}$ is the set of all lower bounds of X. If we only require the existence of $\bigcurlyvee X$ when X is bounded from above, i.e. $X^{\blacktriangledown} \neq \emptyset$ (equivalently: $\bigcurlywedge X$ exists if X is bounded from below, i.e. $X^{\blacktriangle} \neq \emptyset$), then we say that the lattice is **Dedekind-complete**. The definition of (Dedekind-)complete lattice is not first-order, because of the quantification over arbitrary subsets.

If L is a complete lattice, a **complete sublattice** is an $L' \subseteq L$ such that $\bigcurlyvee X, \bigcurlywedge X \in L'$ for all $X \subseteq L'$. Requiring that $L' \subseteq L$ be a complete sublattice is more than being a sublattice and at the same time being a complete lattice, as we require that for any $X \subseteq L'$, the values $\bigcurlyvee X$ and $\bigcurlywedge X$ computed in L or in L' agree.

Lemma 7.8. *For any order $(P, \leq)$ the following are equivalent:*

(1) $\bigcurlyvee X$ exists, for every $X \subseteq P$,

(2) $\bigcurlywedge X$ exists, for every $X \subseteq P$;

[1] Some books use $\top$ and $\perp$ for the maximum and minimum, but we will try to avoid this notation since the symbol $\perp$ is already use for the incompatibility relation—see Section 7.J.2.

and also the following are equivalent

(3) $\bigcurlyvee X$ *exists, for every* $\emptyset \neq X \subseteq P$ *bounded from above,*

(4) $\bigcurlywedge X$ *exists, for every* $\emptyset \neq X \subseteq P$ *bounded from below.*

Proof. Suppose (1) holds. Fix $X \subseteq P$. By assumption $\bigcurlyvee X^{\blacktriangle}$ exists, and let $\bar{a}$ be this element. Since any $x \in X$ is an upper bound of the set $X^{\blacktriangle}$, it follows that $\bar{a} \leq x$, hence $\bar{a}$ is a lower bound of X, and it is the largest such, that is $\bar{a} = \bigcurlywedge X$. This shows that (1)⇒(2). The other implication is similar so we have that (1)⇔(2).

The proof that (3)⇔(4) is left to the reader. □

Corollary 7.9. *Any ordered set satisfying* (1) *or* (2) *of Lemma 7.8 is a complete lattice; any ordered set satisfying* (3) *or* (4) *of Lemma 7.8 is a Dedekind-complete lattice.*

Examples 7.10. (a) A family $\mathcal{S} \subseteq \mathscr{P}(X)$ closed under intersections and unions, ordered by $\subseteq$ is a **lattice of sets**, with $A \curlywedge B = A \cap B$ and $A \curlyvee B = A \cup B$. If $\emptyset, X \in \mathcal{S}$ and $\mathcal{S}$ is closed under arbitrary unions and intersections, then $\bigcurlyvee_{i \in I} A_i = \bigcup_{i \in I} A_i$ and $\bigcurlywedge_{i \in I} A_i = \bigcap_{i \in I} A_i$, and we will speak of a **complete lattice of sets**. In particular: $(\mathscr{P}(X), \subseteq)$ and $(\mathrm{Down}(P), \subseteq)$, with $(P, \preceq)$ an ordered set, are complete lattices of sets. Note that $\mathcal{S} \subseteq \mathscr{P}(X)$ is a (complete) lattice of sets if and only if it is a (complete) sublattice of $\mathscr{P}(X)$.

(b) If $\mathcal{S} \subseteq \mathscr{P}(X)$ is closed under arbitrary intersections, then $\mathcal{S}$ ordered by $\subseteq$ is a bounded lattice with $A \curlywedge B = A \cap B$ and $A \curlyvee B = \bigcap_{C \supseteq A \cup B} C$. Moreover, if $\{A_i \mid i \in I\} \subseteq \mathcal{S}$ then $\bigcurlywedge_{i \in I} A_i = \bigcap_{i \in I} A_i$, so $\mathcal{S}$ is a complete lattice, but in general it is not a lattice of sets. Similarly, if $\mathcal{S} \subseteq \mathscr{P}(X)$ is closed under arbitrary unions and $\emptyset \in \mathcal{S}$, then $\mathcal{S}$ is a complete lattice, but not necessarily a lattice of sets.

Monotone functions on complete lattices have fixed points.

Theorem 7.11. *Let* $(L, \leq)$ *be a complete lattice, let* $f \colon L \to L$ *be monotone, and let* $L' = \{x \in L \mid f(x) = x\}$. *Then*

(a) $\sup\{x \in L \mid x \leq f(x)\}$ *and* $\inf\{x \in L \mid f(x) \leq x\}$ *are, respectively, the largest and the smallest fixed points of* f*, and hence* $L' \neq \emptyset$.

(b) L' *with the induced order is a complete lattice.*[2]

Proof. (a) Let $A = \{x \in L \mid x \leq f(x)\}$ and let $\bar{a} = \sup A$. If $x \in A$, then $x \leq \bar{a}$ and $x \leq f(x)$, whence $x \leq f(x) \leq f(\bar{a})$. Therefore $f(\bar{a})$ is an upper bound for A. It follows that $\bar{a} \leq f(\bar{a})$, whence $f(\bar{a}) \leq f(f(\bar{a}))$ as f is monotone. Thus $f(\bar{a}) \in A$, hence $f(\bar{a}) \leq \bar{a}$. Therefore $\bar{a} = f(\bar{a}) \in L'$. Since

[2] But L' is not necessarily a sublattice of L.

$L' \subseteq A$, it follows that $\bar{a}$ is the largest fixed point of f. By a similar argument, $\inf\{x \in L \mid f(x) \leq x\}$ is the smallest fixed point of f.

(b) In order to prove that $(L', \leq)$ is a complete lattice, by Lemma 7.8 it is enough to show that $\curlyvee_{L'} X$ exists, for any $X \supseteq L'$. So fix $X \subseteq L'$ and let a be the supremum of X as computed in L. If $x \in X$ then $x \leq a$ so $x = f(x) \leq f(a)$, hence $f(a) \in X^{\blacktriangledown}$, and therefore $a \leq f(a)$. Since $M = {\uparrow}a$ is a complete lattice and $f \restriction M \colon M \to M$, there is a least fixed point a' for $f \restriction M$. Therefore $a' \in L'$ and since $a \leq a'$, then $a' \in X^{\blacktriangledown}$. If $b \in L'$ is an upper bound for X, then $a \leq b$, so $b \in M$, hence $a' \leq b$. Therefore a' is the least upper bound of X as computed in L'. □

By Proposition 7.6 every order P can be embedded into a complete lattice, but $\mathscr{P}(P)$ need not be the smallest complete lattice L such that there is an embedding $j \colon P \to L$. Smallest here means that for any embedding $j' \colon P \to L'$ there is a unique monotone $h \colon L \to L'$ such that $h \circ j = j'$ and $h(x \curlywedge_L y) = h(x) \curlywedge_{L'} h(y)$ for all $x, y \in L$. If L' is also least, then there is $h' \colon L' \to L$ such that $h' \circ j' = j$ so that $h \circ h' \circ j' = j'$, and since $\mathrm{id}_{L'} \circ j' = j'$ then by uniqueness $h \circ h' = \mathrm{id}_{L'}$; similarly $h' \circ h = \mathrm{id}_L$ and hence $L \cong L'$. Thus the least complete lattice into which P can be embedded is unique up to isomorphism, and it is called the **Dedekind-McNeille completion** of P, denoted by $\mathbf{DM}(P)$.

Let $f \colon P \to Q$ be monotone. We say that f **preserves sups** if $f(\curlyvee_P A) = \curlyvee_Q f[A]$ whenever $\curlyvee_P A$ and $\curlyvee_Q f[A]$ exist for $A \subseteq P$; the definition of f **preserves infs** is analogous.

Theorem 7.12. *For any order P the family*

$$\mathbf{DM}(P) = \{A \subseteq P \mid A^{\blacktriangledown\blacktriangle} = A\}$$

ordered by inclusion is a complete lattice, and the map $i \colon P \to \mathbf{DM}(P)$, $i(p) = {\downarrow}p$ is an embedding of orders that preserves sups and infs.

Moreover, if L is a complete lattice and $j \colon P \to L$ is an embedding that preserves sups and infs, then there is a unique embedding $h \colon \mathbf{DM}(P) \to L$ that preserves sups and infs and such that $h \circ i = j$.

As the power-set of a finite set is finite, and every finite lattice is complete, we have:

Corollary 7.13. *Suppose P is a finite order. Then $\mathbf{DM}(P)$ is finite as well, and if P is a lattice, then $P \cong \mathbf{DM}(P)$.*

The proof of Theorem 7.12 is postponed after Theorem 7.30. By Exercise 7.72, if P is a linear order then so is $\mathbf{DM}(P)$, and if P has no endpoints, then $\emptyset, P$ are the minimum and maximum of $\mathbf{DM}(P)$, and if p is the supremum of $\operatorname{pred} p = \{q \in P \mid q < p\} = {\downarrow}p \setminus \{p\}$ then $(\operatorname{pred} p)^{\blacktriangledown\blacktriangle} = {\downarrow}p$. The linear order $\mathbf{DM}(P) \setminus \{\emptyset, P\}$ is Dedekind-complete, and it is the **Dedekind completion** of the linear order P. The Dedekind completion of $\mathbb{Q}$ is $\mathbb{R}$—a real number is (or better: can be construed as) a **Dedekind cut**, that is: a non-empty proper initial segment of $\mathbb{Q}$ that has no maximum:

$$\mathbb{R} = \{x \subset \mathbb{Q} \mid \emptyset \neq x \wedge {\downarrow}x = x \wedge \forall p \in x \, \exists y \in x \, (p < q)\}.$$

7.A.1. *Induction systems*.* A function $m \colon \mathscr{P}(A) \to \mathscr{P}(A)$ is an **operator on** A. We say m is **monotone** if $X \subseteq Y \subseteq A \Rightarrow m(X) \subseteq m(Y)$, and that m is **progressive** if $X \subseteq m(X)$. In other words, an operator is monotone/progressive if it is a monotone/progressive map with respect to inclusion. As $\mathscr{P}(A)$ is a complete lattice, by Theorem 7.11 any monotone operator has a fixed point, that is a set $X \subseteq A$ such that $X = m(X)$. If m is monotone, then $X \mapsto X \cup m(X)$ is monotone and progressive, and the least fixed point containing X is $\bigcup_{n \in \mathbb{N}} X_n$, where $X_0 = X$ and $X_{n+1} = X_n \cup m(X_n)$.

Any family $\mathcal{F}$ of operations on A yields a monotone operator

$$m(X) = \{f(a_1, \dots, a_k) \mid a_1, \dots, a_k \in X \wedge f \in \mathcal{F} \wedge k \text{ is the arity of } f\},$$

so the smallest subset of A, closed under every $f \in \mathcal{F}$ and containing X is

$$\operatorname{Cl}_{\mathcal{F}} X = \bigcup_{n \in \mathbb{N}} X_n$$

where $X_0 = X$ and $X_{n+1} = X_n \cup m(X_n)$. Moreover

$$\operatorname{Cl}_{\mathcal{F}} = \bigcup \{\operatorname{Cl}_{\mathcal{G}} Y \mid Y \subseteq X, \mathcal{G} \subseteq \mathcal{F}, \text{ with } Y, \mathcal{G} \text{ finite}\}.$$

One inclusion holds as $\operatorname{Cl}_{\mathcal{G}} Y \subseteq \operatorname{Cl}_{\mathcal{F}} X$ for any $\mathcal{G} \subseteq \mathcal{F}$ and $Y \subseteq X$. For the other inclusion we prove by induction on n that if $z \in X_n$ then $z \in \operatorname{Cl}_{\mathcal{G}} Y$ for some finite $Y \subseteq X$ and $\mathcal{G} \subseteq \mathcal{F}$. If $z \in X_0 = X$ take $\mathcal{G} = \emptyset$ and $Y = \{z\}$. If $z \in X_{n+1} \setminus X_0$ then $z = f(w_1, \dots, w_k)$ with $w_1, \dots, w_k \in X_n$ and $f \in \mathcal{F}$, so by inductive assumption there are finite $\mathcal{G}_1, \dots \mathcal{G}_k \subseteq \mathcal{F}$ and $Y_1, \dots, Y_k \subseteq X$ such that $w_i \in \operatorname{Cl}_{\mathcal{G}_i} Y_i$ for $1 \leq i \leq k$, and hence $z \in \operatorname{Cl}_{\mathcal{G}} Y$ where $\mathcal{G} = \mathcal{G}_1 \cup \dots \cup \mathcal{G}_k \cup \{f\}$ and $Y = Y_1 \cup \dots \cup Y_k$.

The ideas above are important enough to deserve a proper name.

Definition 7.14. An **induction system** is a triple $\mathcal{X} = (A, \mathcal{F}, X)$ where $\mathcal{F}$ is a set of operations on A and $X \subseteq A$; the sets $(X_n)_{n \in \mathbb{N}}$ are the **canonical sequence** of the system; the **closure** of $\mathcal{X}$ is $\overline{\mathcal{X}} = \operatorname{Cl}_{\mathcal{F}} X$.

Example 7.15. The subgroup H of a group G generated by a subset X is the intersection of all subgroups of G containing X, but can also be defined as the closure of the induction system $(G, \{\cdot, {}^{-1}\}, X \cup \{1_G\})$.

More generally, if M is a structure in a language $\mathcal{L}$ and $X \subseteq M$, the substructure generated by X is the intersection of all substructures of M

containing X or, equivalently, it is the closure of the induction system $(M, \{f^M \mid f \text{ function symbol of } \mathcal{L}\}, X \cup \{c^M \mid c \text{ constants of } \mathcal{L}\})$.

Example 7.16. Let $\mathcal{L}$ be a first-order language, and let Func and Const be the sets of all function and constant symbols. Then $(\mathrm{Term}, \mathrm{Func}, \mathrm{Const})$ and $(\mathrm{Term}, \mathrm{Func}, \mathrm{Const} \cup \{x_1, \dots, x_n\})$ are induction systems, and their closure are the set of all closed terms ClTerm, and the set of all terms whose variables are among $\{x_1, \dots, x_n\}$.

Similarly, if Fml, AtFml, QFFml are the sets of all formulæ, all atomic formulæ, all quantifier-free formulæ, respectively, and if $\mathcal{C}$ is the set of all connectives and $\mathcal{Q} = \{\forall x, \exists x \mid x \text{ is a variable}\}$, then $(\mathrm{Fml}, \mathcal{C}, \mathrm{AtFml})$ and $(\mathrm{Fml}, \mathcal{C} \cup \mathcal{Q}, \mathrm{QFFml})$ are induction systems, and their closure are QFFml and the set of all formulæ in prenex normal form, respectively.

Example 7.17. Let $f(n) = 2n$, and $g(n) = m$ if $n = 3m + 1$ is even and $g(n) = 0$ otherwise, and let $C \subseteq \mathbb{N}$ be the closure of the inductive system $(\mathbb{N}, \{f, g\}, \{0, 1\})$. In other words, $n \in C$ just in case there is a suitable sequence of compositions of f and g that starting from 1 yields n. Equivalently $n \geq 2$ belongs to C if the following algorithm applied to n yields 1 in a finite number of steps: if a number is even, divide it by 2, if it is odd multiply it by 3 and add 1. The received opinion is that $C = \mathbb{N}$, that is to say: given any $n \geq 2$ the above algorithm will yield 1 in a finite number of steps—this is known as **Collatz's conjecture** and it is an open problem in mathematics.

7.B. Residuated maps, Galois connections, and closure functions*.

Lemma 7.18. *Suppose that P, Q are ordered sets, and that $f \colon P \to Q$ and $g \colon Q \to P$ are monotone and such that $g \circ f \geq \mathrm{id}_P$ and $f \circ g \leq \mathrm{id}_Q$. Then*

$$\forall p \in P\, \forall q \in Q\ (f(p) \leq q \Leftrightarrow g(q) \geq p)\,, \tag{7.2a}$$

$$\forall q \in Q\ \bigl(g(q) = \max f^{-1}[\downarrow q]\bigr)\,. \tag{7.2b}$$

Proof. If $f(p) \leq q$ then $p \leq g(f(p)) \leq g(q)$; conversely, if $p \leq g(q)$ then $f(p) \leq f(g(q)) \leq q$. So (7.2a) holds.

Note that $p \in f^{-1}[{\downarrow}q] \Leftrightarrow f(p) \leq q \Leftrightarrow p \leq g(q) \Leftrightarrow p \in {\downarrow}g(q)$, where the second equivalence is by (7.2a). Then $f^{-1}[{\downarrow}q] = {\downarrow}g(q)$, and hence (7.2b) holds. □

Proposition 7.19. *If P, Q are ordered sets and $f \colon P \to Q$, then the following are equivalent:*

(a) *$f^{-1}[{\downarrow}q]$ is a principal down-set, for all $q \in Q$;*

(b) *f is monotone and there is a monotone $g \colon Q \to P$ such that $g \circ f \geq \mathrm{id}_P$ and $f \circ g \leq \mathrm{id}_Q$.*

Proof. Endow P and Q with the downward topology. If (a) holds then the preimage of a basic open set is basic open, so f is continuous, and therefore monotone. For each $q \in Q$ there is a $p \in P$ such that $\downarrow p = f^{-1}[\downarrow q]$, and by antisymmetry this p is unique, and we call it $g(q)$. If $q_1 \leq q_2$ then $f^{-1}[\downarrow q_1] \subseteq f^{-1}[\downarrow q_2]$, so g is monotone. Now $g(q) \in \downarrow g(q) = \downarrow p = f^{-1}[\downarrow q]$ so $f(g(q)) \leq q$, for all $q \in Q$. Also $p \in f^{-1}[\downarrow f(p)] = \downarrow g(f(p))$, so $p \leq g(f(p))$. Thus (b) holds.

The direction (b)⇒(a) follows at once from (7.2b) in Lemma 7.18. □

Lemma 7.20. *Suppose P, Q are ordered sets, and $f\colon P \to Q$ is monotone. Then there is at most one monotone $g\colon Q \to P$ such that $g \circ f \geq \mathrm{id}_P$ and $f \circ g \leq \mathrm{id}_Q$.*

Proof. Suppose $g_1, g_2\colon Q \to P$ are such that $g_i \circ f \geq \mathrm{id}_P$ and $f \circ g_i \leq \mathrm{id}_Q$, for $i = 1, 2$. Then $g_1 = \mathrm{id}_P \circ g_1 \leq (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) \leq g_2 \circ \mathrm{id}_Q = g_2$. By symmetry $g_2 \leq g_1$. □

A function $f\colon P \to Q$ between ordered sets satisfying either of the equivalent conditions of Proposition 7.19 is said to be **residuated**, and the unique function g is called the **residual** of f, and it is denoted by f^*.

Lemma 7.21. *If $f\colon P \to Q$ is residuated, then $f \circ f^* \circ f = f$ and $f^* \circ f \circ f^* = f^*$, and hence the maps $F\colon P \to P$, $F = f^* \circ f$ and $G\colon Q \to Q$, $G = f \circ f^*$, are idempotent.*

Proof. For any $p \in P$ we have that $f^* \circ f(p) \geq p$, and hence $f \circ f^* \circ f(p) = f(f^* \circ f(p)) \geq f(p)$. Since $f \circ f^*(q) \leq q$, for all $q \in Q$, then $f \circ f^* \circ f(p) = f \circ f^*(f(p)) \leq f(p)$, so equality holds. The proof of the other identity is similar, and the result on F and G is immediate. □

The results above can be dualized in the obvious way: if P, Q are ordered sets then

- if $f\colon P \to Q$ and $g\colon Q \to P$ are monotone and $g \circ f \leq \mathrm{id}_P$ and $f \circ g \geq \mathrm{id}_Q$, then

$$\forall p \in P\, \forall q \in Q\ (f(p) \geq q \Leftrightarrow g(q) \leq p)\,, \tag{7.3a}$$

$$\forall q \in Q\ \big(g(q) = \min f^{-1}[\downarrow q]\big)\,. \tag{7.3b}$$

- for any $f\colon P \to Q$ there is at most one monotone $g\colon Q \to P$ such that $g \circ f \leq \mathrm{id}_P$ and $f \circ g \geq \mathrm{id}_Q$.
- for any $f\colon P \to Q$ the following are equivalent:
  - $f^{-1}[\uparrow q]$ is a principal up-set, for all $q \in Q$;
  - f is monotone and there is a unique monotone $g\colon Q \to P$ such that $g \circ f \leq \mathrm{id}_P$ and $f \circ g \geq \mathrm{id}_Q$.

Example 7.22. Let X be a topological space, let P be the collection of all open sets, and let Q be the collection of all closed sets. The map $P \to Q$, $U \mapsto \operatorname{Cl} U$ is residuated with residual $Q \to P$, $C \mapsto \operatorname{Int} C$. Therefore $\operatorname{Int}\operatorname{Cl} U \supseteq U$ for any open set U, $\operatorname{Cl}\operatorname{Int} C \subseteq C$ for any closed set C, and $\operatorname{Int}\operatorname{Cl}\operatorname{Int} Y = \operatorname{Int} Y$ and $\operatorname{Cl}\operatorname{Int}\operatorname{Cl} Y = \operatorname{Cl} Y$ for all $Y \subseteq X$. Moreover $\operatorname{Int} \circ \operatorname{Cl} \colon P \to P$ and $\operatorname{Cl} \circ \operatorname{Int} \colon Q \to Q$ are idempotent.

If $f \colon P \to Q$ is residuated, then $f^* \colon Q \to P$ need not be residuated. However, by duality, $f \colon P \to Q$ is residuated with residual $g \colon Q \to P$ if and only if $g \colon Q^\Delta \to P^\Delta$ is residuated with residual $f \colon P^\Delta \to Q^\Delta$. Thus f and f^* can be defined one from the other. It is customary to call f^* the **left adjoint** of f, and f the **right adjoint** of f^*—the reason for this terminology will be explained in Section 22.

Definition 7.23. If $f \colon P \to Q$ and $g \colon Q \to P$ are *antitone* maps between ordered sets such that $f \circ g \geq \mathrm{id}_Q$ and $g \circ f \geq \mathrm{id}_P$, then the pair (f, g) is a **Galois connection between P and Q**.

If $f \colon P \to Q$ is residuated, then (f, f^*) is a Galois connection between P and Q^Δ; conversely, if (f, g) is a Galois connection between P and Q then $f \colon P \to Q^\Delta$ is residuated with residual $g \colon Q^\Delta \to P$. Therefore Galois connections and residuated maps are equivalent techniques for studying ordered sets. Each approach has its merits: residuated maps can be composed so that if $f \colon P \to Q$ and $g \colon Q \to R$ are residuated then so is $g \circ f \colon P \to R$ (Exercise 7.75), while Galois connections are symmetric, meaning that (f, g) is a Galois connection between P and Q if and only if (g, f) is a Galois connection between Q and P. In view of the equivalence between residuated maps and Galois connections, Lemma 7.21 becomes:

Lemma 7.24. *If (f, g) is a Galois connection between P and Q, then $f \circ g \circ f = f$ and $g \circ f \circ g = g$.*

Galois connections abound in mathematics. The next example, upon which the notion is modelled, and giving the name to this subject, comes from Galois theory in algebra.

Example 7.25. If $K \subseteq L$ are fields and $\mathrm{Gal}(L : K)$ is the set of all automorphisms of L that are the identity on K, let P be the set of all subgroups of $\mathrm{Gal}(L : K)$ and let Q be the set of all subfields of L containing K. Then $(\mathcal{F}, \mathcal{G})$ is a Galois connection between P and Q, where $\mathcal{F}(G) = \{x \in L \mid \forall g \in G\, (g(x) = x)\}$ and $\mathcal{G}(F) = \mathrm{Gal}(L : F)$.

Example 7.26. If K is an algebraically closed field and $n \geq 1$ let $P = \mathscr{P}(K^n)$ and let Q be the set of all ideals of $K[X_1, \dots, X_n]$. For $A \subseteq K^n$ let $I(A)$ be the ideal of all polynomials that vanish on A, and for $\mathfrak{a}$ an ideal of $K[X_1, \dots, X_n]$, let $Z(\mathfrak{a})$ be the set of all common zeroes of the polynomials in $\mathfrak{a}$. This gives a Galois connection between the set of all ideals of $K[X_1, \dots, X_n]$ and $\mathscr{P}(K^n)$.

Example 7.27. Let $(P, \leq)$ be an ordered set. The functions $A \mapsto A^{\blacktriangledown}$ and $A \mapsto A^{\blacktriangle}$ form a Galois connection between $\mathscr{P}(P)$ and itself.

First of all they are both antitone maps. In order to show that $A \subseteq A^{\blacktriangledown\blacktriangle}$ fix $a \in A$. If $b \in A^{\blacktriangledown}$ then $b \leq a$, so $a \in A^{\blacktriangledown\blacktriangle}$. The other inclusion $A \subseteq A^{\blacktriangle\blacktriangledown}$ is proved similarly.

A **closure function** on an ordered set P is a monotone function $f\colon P \to P$ which is progressive and idempotent, that is such that $f \circ f = f$. If progressiveness is replaced by its dual requirement, that is $\forall x(f(x) \leq x)$, we say that f is an **interior function**. A closure/interior operator on X is a closure/interior function on $\mathscr{P}(X)$ ordered by inclusion.

Example 7.28. The operations of closure/interior in a topological space X are examples of closure/interior functions on X. If $\mathcal{F}$ is a family of operations on a set X, then $\mathrm{Cl}_{\mathcal{F}}$ is a closure function on X.

If $f\colon P \to Q$ is residuated with residual $f^*\colon Q \to P$, then $f^* \circ f\colon P \to P$ is a closure function and $f \circ f^*\colon Q \to Q$ is an interior function. Equivalently: if (f, g) is a Galois connection between P and Q, then $g \circ f\colon P \to P$ and $f \circ g\colon Q \to Q$ are closure functions. Every closure function arises this way: if $c\colon P \to P$ is a closure function then there is an ordered set Q and functions f and g such that (f, g) is a Galois connection between P and Q and $c = g \circ f$ [**Bly05**, Theorem 1.7 p. 10].

Proposition 7.29. *Let i and c be an interior and closure functions on the order P. Then $i \circ c$ is a closure function on* $\operatorname{ran} i$*, and $c \circ i$ is an interior function on* $\operatorname{ran} c$.

Proof. Monotonicity of $i \circ c$ is clear, so let us prove that it is progressive and idempotent on $\operatorname{ran} i$. Fix $x \in \operatorname{ran} i$. We have that $c(x) \geq x$ so $i(c(x)) \geq i(x) = x$. Thus $i \circ c$ is progressive, and hence $(i \circ c) \circ (i \circ c)(x) \geq (i \circ c)(x)$. Also $i(c(x)) \leq c(x)$ so $c(i(c(x))) \leq c(c(x)) = c(x)$, and hence $(i \circ c) \circ (i \circ c)(x) \leq (i \circ c)(x)$. Thus $i \circ c$ is idempotent.

The result on $c \circ i$ follows by duality. □

Theorem 7.30. *Let L be a complete lattice, let $f\colon L \to L$ and $M = \operatorname{ran} f$. If f is a closure function, then M, with the ordering induced by L, is a complete lattice, and*

$$\forall A \subseteq M \left(\bigwedge\nolimits_M A = \bigwedge\nolimits_L A \quad \textit{and} \quad \bigvee\nolimits_M A = f(\bigvee\nolimits_L A) \right).$$

Dually, if f is an interior function then M is a complete lattice and $\bigwedge_M A = f(\bigwedge_L A)$ and $\bigvee_M A = \bigvee_L A$.

Proof. Suppose f is a closure function. Since $f \circ f = f$, then M is the set of all fixed points of f, so it is a complete lattice by part (b) of Theorem 7.11. Fix $A \subseteq M$, and note that $\curlywedge_M A \leq \curlywedge A$ and $\curlyvee A \leq \curlyvee_M A$.

Claim 7.30.1. *$\curlywedge A \in M$, and hence $\curlywedge_M A = \curlywedge A$.*

Proof. Let $a = \curlywedge A$. For each $x \in A$ we have that $a \leq x$ and hence $f(a) \leq f(x) = x$, so that $f(a)$ is an upper bound of A, and therefore $f(a) \leq a$. By progressiveness $a \leq f(a)$ so $a = f(a) \in M$ as required. □

Let $a = \curlyvee A$ and $a' = \curlyvee_M A$: we must show that $f(a) = a'$. As $a \leq a'$ and $a' \in M$, then $a \leq f(a) \leq f(a') = a'$. As $f(a) \in M$ is an upper bound of A, then $f(a) = a'$ as required.

The case of the interior function follows from duality. □

We are now ready to prove Theorem 7.12:

Proof. As $f\colon \mathscr{P}(P) \to \mathscr{P}(P)$, $A \mapsto A^{\blacktriangledown\blacktriangle}$ is a closure operator, then $\mathbf{DM}(P)$ is a sub-order of $\mathscr{P}(P)$, and it is a complete lattice with the operations $\curlywedge \mathcal{A} = \bigcap \mathcal{A}$ and $\curlyvee \mathcal{A} = (\bigcup \mathcal{A})^{\blacktriangledown\blacktriangle}$ for all $\mathcal{A} \subseteq \mathbf{DM}(P)$.

Next we prove that $i\colon P \to \mathbf{DM}(P)$ is an embedding of orders that preserves infs and sups. Observe that $i(x) = {\downarrow} x = \{x\}^{\blacktriangle} = \{x\}^{\blacktriangledown\blacktriangle}$ for all $x \in P$, so

$$x \leq y \Leftrightarrow \{x\}^{\blacktriangledown} \supseteq \{y\}^{\blacktriangledown} \Leftrightarrow \{x\}^{\blacktriangledown\blacktriangle} \subseteq \{y\}^{\blacktriangledown\blacktriangle}$$

and hence i is an embedding. If $a = \curlywedge_P A$ then

$$\begin{aligned} i(a) = \{a\}^{\blacktriangle} &= \textstyle\bigcap_{x\in A}\{x\}^{\blacktriangle} \\ &= \curlywedge_{\mathscr{P}(P)} \{\{x\}^{\blacktriangle} \mid x \in A\} \\ &= \inf_{\mathbf{DM}(P)} \{\{x\}^{\blacktriangle} \mid x \in A\} && \text{by Theorem 7.30} \\ &= \inf_{\mathbf{DM}(P)} i[A] \end{aligned}$$

so i preserves infs. If $b = \curlyvee_P A$ then $y \geq b \Leftrightarrow \forall x \in A\,(y \in \{x\}^{\blacktriangledown} = \{x\}^{\blacktriangledown\blacktriangle\blacktriangledown})$ by Example 7.27 and Lemma 7.24, so

$$\{b\}^{\blacktriangledown} = \bigcap_{x\in A} \{x\}^{\blacktriangledown\blacktriangle\blacktriangledown} = (\bigcup_{x\in A} \{x\}^{\blacktriangledown\blacktriangle})^{\blacktriangledown}$$

the last equality following from the identity $\bigcap_{i\in I} A_i^{\blacktriangledown} = (\bigcup_{i\in I} A_i)^{\blacktriangledown}$—see Exercise 7.71. Therefore

$$\begin{aligned} i(b) = \{b\}^{\blacktriangledown\blacktriangle} &= (\textstyle\bigcup_{x\in A} \{x\}^{\blacktriangledown\blacktriangle})^{\blacktriangledown\blacktriangle} \\ &= f(\curlyvee_{\mathscr{P}(P)}\{\{x\}^{\blacktriangledown\blacktriangle} \mid x \in A\}) \\ &= \curlyvee_{\mathbf{DM}(P)}\{i(x) \mid x \in A\} && \text{by Theorem 7.30} \end{aligned}$$

so i preserves sups as well.

Now we prove the minimality of $\mathbf{DM}(P)$. Let L be a complete lattice and $j \colon P \to L$ an embedding that preserves sups and infs. For $A \in \mathbf{DM}(P)$ set

$$h(A) = \curlyvee_L j[A].$$

Let us check that $f \colon \mathbf{DM}(P) \to L$ is an embedding. It is clear that h is monotone, so suppose $h(A) \leq h(B)$ towards proving that $A \subseteq B$. For $x \in A$ we have $j(x) \leq h(A) \leq h(B) = \curlyvee_L j[B]$ so given $y \in B^{\blacktriangle}$ we have that $j(x) \leq j(y)$, and hence $x \leq y$. Therefore $x \in B^{\blacktriangle\blacktriangledown} = B$ for all $x \in A$, which is what we had to prove.

Next we check that h preserves sups, and hence preserves infs by Exercise 7.70. Let $\mathcal{A} \subseteq \mathbf{DM}(P)$ and let $\bar{A} = \bigcup \mathcal{A} = \curlyvee_{\mathbf{DM}(P)} \mathcal{A} \in \mathbf{DM}(P)$. Then

$$\begin{aligned} &\curlyvee_L h[\mathcal{A}] = \curlyvee_L \{h(B) \mid B \in \mathcal{A}\} = \curlyvee_L \{\curlyvee_L j[B] \mid B \in \mathcal{A}\} \\ &= \curlyvee_L \{\curlyvee_L j(x) \mid \exists B \in \mathcal{A}\, (x \in B)\} = \curlyvee_L j[\bigcup \mathcal{A}] = h(\bar{A}) = h(\curlyvee_{\mathbf{DM}(P)} \mathcal{A}). \end{aligned}$$

The function h commutes with i and j, since for all $x \in P$

$$h(i(x)) = h(\{x\}^{\blacktriangle\blacktriangledown}) = h(\{x\}^{\blacktriangledown}) = \sup_L j[\{x\}^{\blacktriangledown}] = j(x)$$

by monotonicity of j.

Finally we prove the uniqueness of h. As $A = \bigcup_{x \in A} i(x) = \bigcup i[A]$ for all $A \in \mathbf{DM}(P)$, if $h' \colon \mathbf{DM}(P) \to L$ is any embedding that preserves sups and such that $h' \circ i = j$, then

$$h'(A) = h(\bigcup i[A]) = \curlyvee_L h \circ i[A] = \curlyvee_L j[A] = h(A). \qquad \square$$

7.C. Lattices. The **dual of a term** t of $\mathcal{L}_{\text{LTC}}$ is the term t^{Δ} obtained by swapping the symbols $\curlyvee$ and $\curlywedge$. The **dual of a formula** φ is the formula φ^{Δ} obtained by replacing each term with its dual. The **dual of a structure** $\mathcal{A} = (A, \curlyvee, \curlywedge)$ is the $\mathcal{L}_{\text{LTC}}$-structure $\mathcal{A}^{\Delta} = (A, \sqcup, \sqcap)$ where $\sqcup = \curlywedge$ and $\sqcap = \curlyvee$. The dual of the dual is the original structure, that is $\mathcal{A}^{\Delta\Delta} = \mathcal{A}$. If $\mathcal{A}$ is an $\mathcal{L}_{\text{LTC}}$-structure and σ is a sentence, then

$$\mathcal{A} \vDash \sigma \quad \text{if and only if} \quad \mathcal{A}^{\Delta} \vDash \sigma^{\Delta}.$$

Since the axioms for lattice are self-dual, the dual of a lattice is a lattice. The following result is the analogue of the duality for orders.

Duality principle for lattices. *If $\mathcal{A}$ is a lattice and σ is an $\mathcal{L}_{\text{LTC}}$-sentence, then*

$$\mathcal{A} \vDash \sigma \quad \textit{if and only if} \quad \mathcal{A}^{\Delta} \vDash \sigma^{\Delta}.$$

In particular: σ is logical consequence of the axioms of lattices if and only if so is σ^{Δ}.

Remark 7.31. The duality principles for lattices should not be misunderstood. By Exercise 4.68 the *sentences*

$$\forall x, y, z \left[(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z)\right], \qquad \forall x, y, z \left[(x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)\right]$$

are logically equivalent modulo the axioms for lattices, but this does not hold for the *formulæ*

$$(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z), \qquad (x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)$$

(see Remark 3.36(a)). For example, in the fourth lattice of Figure 7 $(a \curlyvee b) \curlywedge c = (a \curlywedge c) \curlyvee (b \curlywedge c)$ but $(a \curlywedge b) \curlyvee c \neq (a \curlyvee c) \curlywedge (b \curlyvee c)$.

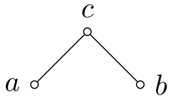
7.D. Distributive lattices. The axioms for modular and distributive lattices are self-dual, hence the dual of a distributive/modular lattice is of the same kind, hence the duality principle generalizes to the realm of distributive and modular lattices: if σ is a sentence a $\mathcal{L}_{\mathrm{LTC}}$ holding in every modular/distributive lattice, then also the dual sentence σ^{Δ} holds in every modular/distributive lattice.

7.D.1. *Free lattices.* By Theorem 7.12 any ordered set P can be embedded in a minimal complete lattice $\mathbf{DM}(P)$. The dual question would be: what is the largest, most general lattice L that P generates? (We are not concerned about completeness here.)

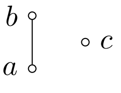
Let us look at some concrete examples, when P is a finite order of size ≤ 3. First of all, if P is a lattice itself, then $L = P$, so we may *assume that P is not a lattice.* Thus we may assume that P is not a linear order, so in particular P has size 2 or 3.

If P has two incomparable elements a, b, then applying $\curlyvee$ and $\curlywedge$ and by commutativity, associativity, and absorption the only elements we obtain are $a, b, a \curlyvee b, a \curlywedge b$, so L is isomorphic to $\mathbf{2} \times \mathbf{2}$ of Figure 7.

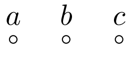
If the order has three elements a, b, c, we have three possible Hasse diagrams:



P_1



P_2



P_3

The lattice generated by P_1 is isomorphic to $\mathbf{2} \times \mathbf{2}$.

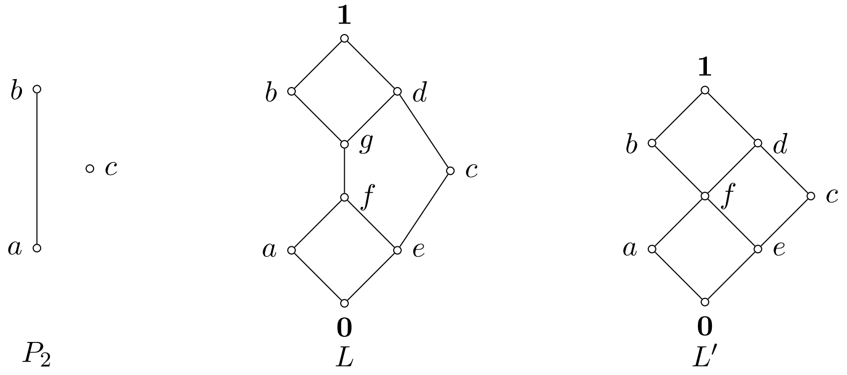


Figure 10. The lattice L, and the modular lattice L', generated by P_2

Next we turn our attention to P_2. First we look at the elements that can be constructed from a, b, c using a single application of either $\curlyvee$ or $\curlywedge$:

$$\begin{aligned} a &= a \curlywedge b & b &= a \curlyvee b \\ \mathbf{1} &= b \curlyvee c & \mathbf{0} &= a \curlywedge c \\ d &= a \curlyvee c & e &= b \curlywedge c. \end{aligned}$$

A further application of an operation gives

$$f = a \curlyvee (b \curlywedge c) \qquad g = b \curlywedge (a \curlyvee c).$$

These are the only two new elements, as $a \leq b$ and associativity imply that $\mathbf{1} = a \curlyvee b \curlyvee c$ and $\mathbf{0} = a \curlywedge b \curlywedge c$, while absorption yields $a \curlywedge (b \curlyvee c) = a$ and $b \curlyvee (a \curlywedge c) = b$. As a and $b \curlywedge c$ are below $a \curlyvee c$ it follows that $f = a \curlyvee (b \curlywedge c) \leq (a \curlyvee c)$, and as $a \leq b$ and $b \curlywedge c \leq b$ then $f \leq b$; so $f \leq b \curlywedge (a \curlyvee c) = g$. Therefore the set

$$L = \{\mathbf{0}, a, b, c, d, e, f, g, \mathbf{1}\}$$

is closed under $\curlyvee$ and $\curlywedge$ and hence it is a lattice whose Hasse diagram is in Figure 10. Observe that L is not modular as witnessed by the sub-lattice $\{d, e, f, g, c\}$—if the generated lattice is required to be modular, i.e. to satisfy (4.8), then $g = (f \curlyvee c) \curlywedge (f \curlyvee g) = f \curlyvee (c \curlywedge (f \curlyvee g)) = f$, so we obtain the lattice L' of Figure 10.

Finally, we turn our attention to the lattice generated by P_3: it can be shown that this is an infinite lattice. Thus the lattice generated by P_3 is the most complex lattice generated by an ordered set of size 3.

Definition 7.32. Let C be a non-empty set. The **free lattice over** C $\mathrm{Free}_{\mathbf{L}}(C)$ is the lattice generated by the order $(C, \leq)$ where $\leq$ is the identity relation, that is $c \leq c' \Leftrightarrow c = c'$. If the generated lattice is required to be modular or distributive we get $\mathrm{Free}_{\mathbf{M}}(C)$ and $\mathrm{Free}_{\mathbf{D}}(C)$.

If the sets C and D are in bijection then their free lattices are isomorphic, $\mathrm{Free}_{\mathbf{L}}(C) \cong \mathrm{Free}_{\mathbf{L}}(D)$, and similarly for the modular/distributive versions. In particular, if C is a finite non-empty set with n elements, these lattices will be denoted by $\mathrm{Free}_{\mathbf{L}}(n)$, $\mathrm{Free}_{\mathbf{M}}(n)$ and $\mathrm{Free}_{\mathbf{D}}(n)$. Therefore $\mathrm{Free}_{\mathbf{L}}(1) = \mathrm{Free}_{\mathbf{M}}(1) = \mathrm{Free}_{\mathbf{D}}(1)$ is the lattice with one element, and $\mathrm{Free}_{\mathbf{L}}(2) = \mathbf{2} \times \mathbf{2}$ which is distributive, so $\mathrm{Free}_{\mathbf{L}}(2) = \mathrm{Free}_{\mathbf{M}}(2) = \mathrm{Free}_{\mathbf{D}}(2)$. As we mentioned $\mathrm{Free}_{\mathbf{L}}(3)$ (and hence every $\mathrm{Free}_{\mathbf{L}}(m)$ for $m \geq 3$) is infinite. On other hand, $\mathrm{Free}_{\mathbf{M}}(3)$ has 28 elements, while $\mathrm{Free}_{\mathbf{M}}(4)$ (and therefore any $\mathrm{Free}_{\mathbf{M}}(n)$ for $n \geq 4$) is infinite (Exercise 7.81).

Every $\mathrm{Free}_{\mathbf{D}}(n)$ is finite, but in order to verify this fact we need a few preliminary results. A term is a conjunction of the variables $\{x_1, \dots, x_n\}$ if it is of the form

$$x_{i_1} \curlywedge \dots \curlywedge x_{i_k}$$

with $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$, while a term of the form

$$x_{j_1} \curlyvee \dots \curlyvee x_{j_h}$$

with $\{j_1, \dots, j_h\} \subseteq \{1, \dots, n\}$, is a disjunction of the variables $\{x_1, \dots, x_n\}$. When I is a finite set, by induction on $|I|$ one can show that in every distributive lattice the following holds:

$$x \curlywedge \bigvee_{i \in I} y_i = \bigvee_{i \in I} (x \curlywedge y_i) \quad \text{and} \quad x \curlyvee \bigwedge_{i \in I} y_i = \bigwedge_{i \in I} (x \curlyvee y_i), \tag{7.4}$$

An easy induction on the complexity of the term s yields the following result, which is the algebraic counterpart of the fact that every formula is tautologically equivalent to a formula in disjunctive normal form and to a formula in conjunctive normal form (see Section 3.C.1 and Exercise 3.45.)

Lemma 7.33. *For each term $s \in \mathrm{Term}_{LTC}(x_1, \dots, x_n)$ there are terms $u, v \in \mathrm{Term}_{LTC}(x_1, \dots, x_n)$ such that*

- *u is in **disjunctive form**, that is to say: a disjunction of conjunctions of variables among $\{x_1, \dots, x_n\}$,*
- *v is in **conjunctive form**, that is to say: a conjunction of disjunctions of variables among $\{x_1, \dots, x_n\}$,*
- *the formula $s = u \wedge s = v$ is logical consequence of the axioms of* distributive *lattices.*

By induction on the complexity of $t \in \mathrm{Term}(x_1, \dots, x_n)$ it follows from the axioms of distributive lattices that $x_1 \curlywedge \dots \curlywedge x_n \leq t \leq x_1 \curlyvee \dots \curlyvee x_n$. Moreover, since a term can be written in disjunctive form, that is a disjunction of conjunctions, the elements of $\mathrm{Free}_{\mathbf{D}}(n)$ are no more than the possible disjunctive forms on n many variables. Therefore $\mathrm{Free}_{\mathbf{D}}(n)$ is finite. For

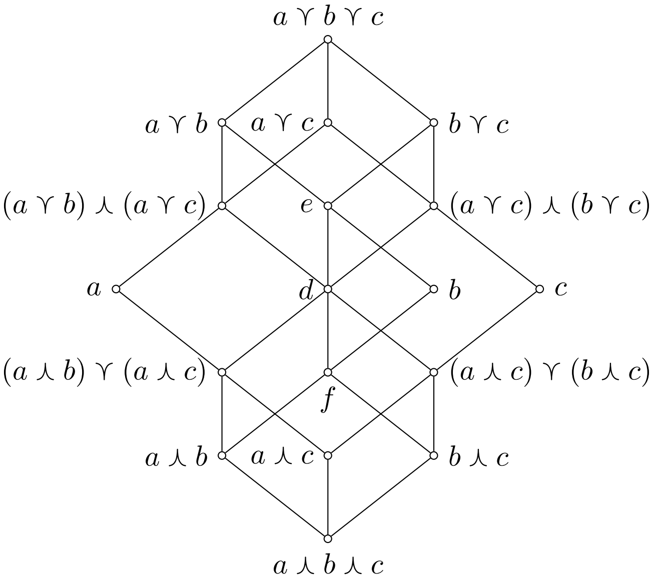

$a \curlyvee b \curlyvee c$
$a \curlyvee b$
$a \curlyvee c$
$b \curlyvee c$
$(a \curlyvee b) \curlywedge (a \curlyvee c)$
e
$(a \curlyvee c) \curlywedge (b \curlyvee c)$
a
d
b
c
$(a \curlywedge b) \curlyvee (a \curlywedge c)$
f
$(a \curlywedge c) \curlyvee (b \curlywedge c)$
$a \curlywedge b$
$a \curlywedge c$
$b \curlywedge c$
$a \curlywedge b \curlywedge c$

Figure 11. The lattice $\mathrm{Free}_{\mathbf{D}}(3)$ on the generators a, b and c, where $d = (a \curlyvee b) \curlywedge (a \curlyvee c) \curlywedge (b \curlyvee c) = (a \curlywedge b) \curlyvee (a \curlywedge c) \curlyvee (b \curlywedge c)$, $e = (a \curlyvee b) \curlywedge (b \curlyvee c)$, $f = (a \curlywedge b) \curlyvee (b \curlywedge c)$.

example, the elements of $\mathrm{Free}_{\mathbf{D}}(3)$ are disjunctions of k conjunctions on a, b, c, that is

$$
\begin{aligned}
&(k = 1) \quad a,\ b,\ c,\ a \curlywedge b,\ a \curlywedge c,\ b \curlywedge c,\ a \curlywedge b \curlywedge c,\\
&(k = 2) \quad a \curlyvee b,\ b \curlyvee c,\ b \curlyvee c,\ a \curlyvee (b \curlywedge c),\ b \curlyvee (a \curlywedge c),\ c \curlyvee (a \curlywedge b),\\
&\qquad\qquad (a \curlywedge b) \curlyvee (b \curlywedge c),\ (a \curlywedge b) \curlyvee (a \curlywedge c),\ (b \curlywedge c) \curlyvee (a \curlywedge c),\\
&(k = 3) \quad a \curlyvee b \curlyvee c,\ (a \curlywedge b) \curlyvee (b \curlywedge c) \curlyvee (a \curlywedge c).
\end{aligned}
$$

The Hasse diagram of $\mathrm{Free}_{\mathbf{D}}(3)$ is in Figure 11. The following question arises: are we sure that the elements described above are all distinct? Couldn't be the case that there is some further identification? Exercise 7.80 shows that this is not the case, hence $\mathrm{Free}_{\mathbf{D}}(3)$ has exactly 18 elements. As the free modular lattice has 28 elements this proves that $\mathrm{Free}_{\mathbf{D}}(3) \ncong \mathrm{Free}_{\mathbf{M}}(3)$.

7.E. Examples of lattices.

7.E.1. $\mathscr{P}(X)$ is a distributive lattice, and therefore any lattice of sets is distributive. In Section 32 we shall see that every distributive lattice is a sublattice of $\mathscr{P}(X)$, for some X, and in Exercise 7.96 we shall see the proof of this fact when the lattice is finite.

7.E.2. The set $\mathrm{Sgr}(G)$ of the subgroups of a group G ordered by inclusion is a lattice. The operations are $H \curlywedge K = H \cap K$ and $H \curlyvee K =$

$\bigcap \{J \in \mathrm{Sgr}(G) \mid H \cup K \subseteq J\} =$ the subgroup generated by $H \cup K$. It is not a sublattice of $\mathscr{P}(G)$.

The lattice $\mathrm{Sgr}(G)$ does not characterize the group G up to isomorphism, for example $\mathrm{Sgr}(\mathbb{Z}/4\mathbb{Z}) \cong \mathrm{Sgr}(\mathbb{Z}/9\mathbb{Z})$. The lattice $\mathrm{Sgr}(G)$ need not be distributive or modular—e.g. take the dihedral group D_4 of the symmetries of the square—but when G is abelian $\mathrm{Sgr}(G)$ is modular. More generally, the collection $\mathrm{NSgr}(G)$ of all normal subgroups of a group G is a sublattice of $\mathrm{Sgr}(G)$ and it is a modular lattice—this follows from the fact that for normal subgroups $H \curlyvee K = HK = \{hk \mid h \in H, k \in K\}$. Similarly, the family of all submodules of a left module M over a ring R is a modular lattice, since $(N_1 \cap N_2) + (N_1 \cap N_3) \subseteq N_1 \cap (N_2 + (N_1 \cap N_3))$. In general, the lattice of submodules is not distributive (Exercise 7.79).

7.E.3. The set $\mathrm{Cong}(M)$ of all congruences of a structure M ordered under inclusion is a lattice. If M is an R-module $\mathrm{Cong}(M)$ is modular, if M is a lattice $\mathrm{Cong}(M)$ is distributive [**Ber12**, p. 33].

7.E.4. By Example (b) the collection of all topologies on a set Y ordered under inclusion is a complete bounded lattice. The minimum is the trivial topology $\{\emptyset, X\}$, the maximum is the discrete topology $\mathscr{P}(X)$, and if $\mathcal{T}_i$ are topologies on X, then $\bigcurlywedge_{i\in I} \mathcal{T}_i = \bigcap_{i\in I} \mathcal{T}_i$ and $\bigcurlyvee_{i\in I} \mathcal{T}_i$ is the topology generated by $\bigcup_{i\in I} \mathcal{T}_i$, that is the topology on X that has as a basis $\{A_{i_1} \cap \dots \cap A_{i_n} \mid A_{i_j} \in \mathcal{T}_{i_j} \wedge i_1, \dots, i_n \in I\}$. The lattice of all topologies on a set is (almost) never modular [**Ste66**, Theorem 3.1].

7.E.5. If $H, K \in \mathrm{Sgr}(G)$ are finitely generated, then $H \curlyvee K$ is finitely generated, but $H \curlywedge K = H \cap K$ may fail to be finitely generated when G is not abelian.Therefore the family of all finitely generated subgroups of G is not a lattice, but an upper semi-lattice.

7.F. Boolean algebras.

7.F.1. *Complemented lattices.* A bounded lattice is **complemented** if it satisfies the statement

$$\forall x\, \exists y\, [x \curlywedge y = \mathbf{0} \wedge x \curlyvee y = \mathbf{1}]$$

The element y is a **complement** of x; if the complement of x is a unique, it will be denoted by x^*. If every element has a unique complement the lattice is **uniquely complemented**. In such a lattice $x^{**} = x$ for all x, and the following hold:

$$\forall x\, (x \curlyvee x^* = \mathbf{1}) \tag{7.5a}$$

$$\forall x\, (x \curlywedge x^* = \mathbf{0}) \tag{7.5b}$$

and

$$\forall x\,(x \curlyvee \mathbf{0} \eqcirc x) \tag{7.6a}$$

$$\forall x\,(x \curlywedge \mathbf{1} \eqcirc x) \tag{7.6b}$$

Thus Lemma 4.17 says that in a bounded distributive lattice, the complement of an element, if it exist, is unique.

Remark 7.34. The lattices $\mathcal{M}_3$ and $\mathcal{N}_5$ of Figure 7 are complemented, but not uniquely complement. Many of the early results in lattice theory led to a conjecture stating the converse of Lemma 4.17: every uniquely complemented lattice must be distributive. This conjecture turned out to be false as Dilworth proved in 1945 that every lattice can be embedded into a uniquely complemented one.

In Section 4.E we introduced $\mathcal{L}_{\text{Boole}}$ extending $\mathcal{L}_{\text{Ltc}}$ with a unary operation symbol * and two constant symbols $\mathbf{1}$ and $\mathbf{0}$, and defined a Boolean algebra to be a bounded, complemented, distributive lattice. It turns out that associativity and absorption for $\curlywedge$ and $\curlyvee$ follow from the other axioms, so let's re-define a **Boolean algebra** to be an $\mathcal{L}_{\text{Boole}}$-structure satisfying T_{Boole} which has as axioms:[3]

$$\forall x, y\,(x \curlyvee y \eqcirc y \curlyvee x) \tag{4.5a}$$

$$\forall x, y\,(x \curlywedge y \eqcirc y \curlywedge x) \tag{4.5b}$$

$$\forall x, y, z\,((x \curlyvee y) \curlywedge z \eqcirc (x \curlywedge z) \curlyvee (y \curlywedge z)) \tag{4.7a}$$

$$\forall x, y, z\,((x \curlywedge y) \curlyvee z \eqcirc (x \curlyvee z) \curlywedge (y \curlyvee z)) \tag{4.7b}$$

$$\forall x\,(x \curlyvee x^* \eqcirc \mathbf{1}) \tag{7.5a}$$

$$\forall x\,(x \curlywedge x^* \eqcirc \mathbf{0}) \tag{7.5b}$$

$$\forall x\,(x \curlyvee \mathbf{0} \eqcirc x) \tag{7.6a}$$

$$\forall x\,(x \curlywedge \mathbf{1} \eqcirc x). \tag{7.6b}$$

A Boolean algebra is **non-degenerate** if it satisfies $\mathbf{0} \neq \mathbf{1}$ or, equivalently, if the algebra has at least two elements.

What we said in Remark 4.13 can be repeated here for Boolean algebras. Most authors use $\vee$ and $\wedge$ for join and meet, but others use $+$ and $\cdot$. We will use the symbol $+$ for another important operation in Boolean algebras—see Section 7.G.

The dual of a term of $\mathcal{L}_{\text{Boole}}$ is the term obtained by exchanging $\curlywedge$ with $\curlyvee$ and $\mathbf{1}$ with $\mathbf{0}$; the dual of a formula φ is the formula φ^{Δ} obtained by replacing every term with its dual. The dual of a Boolean algebra $\mathcal{B} = (B, \curlywedge, \curlyvee, ^*, \mathbf{0}, \mathbf{1})$ is $\mathcal{B}^{\Delta} = (B, \sqcap, \sqcup, ^*, \bot, \top)$ where $\sqcap = \curlyvee$, $\sqcup = \curlywedge$, $\bot = \mathbf{1}$ and $\top = \mathbf{0}$. Since

[3] Theorem 7.35 will vindicate the adequacy of this definition.

axiom (na) is the dual of (nb) (for $n = 4.5$, 4.7, 7.5, 7.6), and since $\mathbf{0} \neq \mathbf{1}$ is self-dual, the dual of a Boolean algebra is a Boolean algebra. Moreover the map $\mathcal{B} \to \mathcal{B}^{\Delta}$, $x \mapsto x^*$, is an isomorphism.

Duality principle for boolean algebras. *If $\mathcal{B}$ is a Boolean algebra and σ is a sentence, then*

$$\mathcal{B} \models \sigma \quad \textit{if and only if} \quad \mathcal{B} \models \sigma^{\Delta}.$$

In particular: σ is logical consequence of the axioms for Boolean algebras if and only if σ^{Δ} is such.

Observe that in a Boolean algebra $\mathbf{1} = \mathbf{0} \curlyvee \mathbf{0}^* = \mathbf{0}^* \curlyvee \mathbf{0} = \mathbf{0}^*$, so by duality $\mathbf{0} = \mathbf{1}^*$.

Every complemented distributive lattice $(B, \leq)$ is a Boolean algebra $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}, \mathbf{1})$. Conversely:

Theorem 7.35. *Every Boolean algebra is a complemented distributive lattice.*

Proof. Given a Boolean algebra $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}, \mathbf{1})$ it is enough to show that $(B, \curlywedge, \curlyvee)$ is a lattice, since the distributivity laws (4.7) hold by assumption, $\mathbf{0}$ and $\mathbf{1}$ are the minimum and maximum by (7.6), and x^* is the complement of x by (7.5). Therefore we must check associativity (4.4) and absorption (4.6) for $\curlyvee$ and $\curlywedge$.

Applying the axioms of $T_{\textsc{Boole}}$ we obtain

$$x \curlywedge (x \curlyvee y) \eqcirc (x \curlyvee \mathbf{0}) \curlywedge (x \curlyvee y) \eqcirc x \curlyvee (\mathbf{0} \curlywedge y) \eqcirc x \curlyvee \mathbf{0} \eqcirc x$$

so by the Duality Principle $x \curlyvee (x \curlywedge y) \eqcirc x$ and hence the absorption laws (4.6) are valid.

From $y \eqcirc y \curlywedge \mathbf{1} \eqcirc y \curlywedge (x \curlyvee x^*) \eqcirc (y \curlywedge x) \curlyvee (y \curlywedge x^*)$ we obtain the following cancellation law: if $y \curlywedge x \eqcirc z \curlywedge x$ and $y \curlywedge x^* \eqcirc z \curlywedge x^*$, then $y \eqcirc z$.

We can now prove that

$$x \curlyvee (y \curlyvee z) \eqcirc (x \curlyvee y) \curlyvee z$$

follows from $T_{\textsc{Boole}}$, so that by duality the analogous property for $\curlywedge$ holds. By the cancellation law, it is enough to verify that $t \curlywedge x \eqcirc s \curlywedge x$ and $t \curlywedge x^* \eqcirc s \curlywedge x^*$, where t is $x \curlyvee (y \curlyvee z)$ and s is $(x \curlyvee y) \curlyvee z$.

$$(x \curlyvee (y \curlyvee z)) \curlywedge x \eqcirc x \qquad \text{by absorption}$$

and

$$\begin{aligned} ((x \curlyvee y) \curlyvee z) \curlywedge x &\eqcirc ((x \curlyvee y) \curlywedge x) \curlyvee (z \curlywedge x) && \text{by distributivity} \\ &\eqcirc x \curlyvee (z \curlywedge x) \eqcirc x && \text{by absorption} \end{aligned}$$

so $t \curlywedge x \eqcirc s \curlywedge x$. By distributivity, commutativity, and (7.6a)

$$\begin{aligned}(x \curlyvee (y \curlyvee z)) \curlywedge x^* &\eqcirc (x \curlywedge x^*) \curlyvee ((y \curlyvee z) \curlywedge x^*)\\ &\eqcirc \mathbf{0} \curlyvee ((y \curlyvee z) \curlywedge x^*)\\ &\eqcirc (y \curlyvee z) \curlywedge x^*\end{aligned}$$

and

$$\begin{aligned}((x \curlyvee y) \curlyvee z) \curlywedge x^* &\eqcirc ((x \curlyvee y) \curlywedge x^*) \curlyvee (z \curlywedge x^*)\\ &\eqcirc ((x \curlywedge x^*) \curlyvee (y \curlywedge x^*)) \curlyvee (z \curlywedge x^*)\\ &\eqcirc (\mathbf{0} \curlyvee (y \curlywedge x^*)) \curlyvee (z \curlywedge x^*)\\ &\eqcirc (y \curlywedge x^*) \curlyvee (x \curlywedge x^*)\\ &\eqcirc (y \curlyvee z) \curlywedge x^*,\end{aligned}$$

which is what we had to prove. □

The correspondence $(B, \curlyvee, \curlywedge, {}^*, \mathbf{0}, \mathbf{1}) \mapsto (B, \leq)$ transforming Boolean algebras into complemented distributive lattices is the inverse of the map $(B, \leq) \mapsto (B, \curlyvee, \curlywedge, {}^*, \mathbf{0}, \mathbf{1})$.

The axioms for Boolean algebras are universal sentences, hence by Proposition 4.8 every $\mathcal{L}_{\text{Boole}}$-substructure C of a Boolean algebra B is itself a Boolean algebra and we will say that C is a **subalgebra** of B. The **minimal algebra** is the unique (up to isomorphism) Boolean algebra with exactly two elements $\mathbf{2} = \{\mathbf{1}, \mathbf{0}\}$, and it is (isomorphic to) a subalgebra of any non-degenerate Boolean algebra.

By Example 4.19 any algebra of sets is a Boolean algebra. Let us see some more examples.

Examples 7.36. (a) If X is a topological space, a set U is **clopen** if it is both closed and open.

$$\mathbf{CLOP}(X) = \{U \subseteq X \mid U \text{ is clopen in } X\}$$

is a subalgebra of $\mathscr{P}(X)$, called the **clopen algebra**. If X is connected then $\mathbf{CLOP}(X)$ is the minimal algebra. In general $\mathbf{CLOP}(X)$ is not complete. Conversely, given a set $X \neq \emptyset$ every subalgebra $B \subseteq \mathscr{P}(X)$ generates a topology in which $B = \mathbf{CLOP}(X)$.

(b) Let $(L, \leq)$ be linearly ordered, and let $\mathcal{I}$ be the set of all intervals of the form $(a; b]$ with $a < b$ and of all half-lines of the form $\{x \in L \mid x \leq b\}$ and $\{x \in L \mid a < x\}$. The collection of all finite unions of sets in $\mathcal{I}$, is a subalgebra of $\mathscr{P}(L)$, called the **interval algebra** of $(L, \leq)$.

Recall that an atom of a Boolean algebra B is a minimal element of $B \setminus \{\mathbf{0}\}$ We will denote the set of atoms of B by $\operatorname{At}(B)$. An algebra is **atomic** if for all $b \in B \setminus \{\mathbf{0}\}$ there is an atom $a \leq b$. By Proposition 7.2 we have

Proposition 7.37. *Every finite Boolean algebra is atomic.*

The family $\mathscr{P}(X)$ is an atomic Boolean algebra, and the atoms are the singletons. In Section 25 we will prove that every Boolean algebra is isomorphic to a subalgebra of $\mathscr{P}(X)$ for some X, and in this Section will prove this when the algebra is finite (Corollary 7.48).

A Boolean algebra is **complete** if it is complete as a lattice. Every finite Boolean algebra is complete, but this is not true in general for infinite Boolean algebras. The next result generalizes the well-known set-theoretic identities $B \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} B \cap A_i$ and $B \cup \bigcap_{i \in I} A_i = \bigcap_{i \in I} B \cup A_i$.

Lemma 7.38. *Let B be a Boolean algebra and let $X \subseteq B$ be such that $\bigcurlyvee X$ exists. Then $\bigcurlyvee\{b \curlywedge x \mid x \in X\}$ exists for all $b \in B$, and*

$$b \curlywedge \bigcurlyvee X = \bigcurlyvee\{b \curlywedge x \mid x \in X\}.$$

Similarly, if $\bigcurlywedge X$ exists, then also $\bigcurlywedge\{b \curlyvee x \mid x \in X\}$ exists and it is equal to $b \curlyvee \bigcurlywedge X$.

Proof. $b \curlywedge x \leq b \curlywedge \bigcurlyvee X$ for each $x \in X$, so $b \curlywedge \bigcurlyvee X$ is an upper bound of $\{b \curlywedge x \mid x \in X\}$. If c is another upper bound of this set, then for each $x \in X$,

$$b \curlywedge x \leq c \Rightarrow x \leq b^* \curlyvee c$$

by Lemma 4.18 and therefore $\bigcurlyvee X \leq b^* \curlyvee c$, whence $b \curlywedge \bigcurlyvee X \leq c$. □

7.F.2. *Boolean terms.* Let t be a term of $\mathcal{L}_{\mathrm{Boole}}$ with variables $x_1, \dots, x_n$: replacing the occurrences of $\mathbf{0}$ and $\mathbf{1}$ with $x_1 \curlywedge x_1^*$ and $x_1 \curlyvee x_1^*$ respectively, and repeatedly applying De Morgan's laws, the term t is transformed into a term t' with the same variables $x_1, \dots, x_n$ in which the symbol for complements * is only applied to variables. In other words, $t' = s[x_1^*/y_1, \dots, x_n^*/y_n]$ where $s \in \mathrm{Term}_{\mathrm{LTC}}(x_1, \dots, x_n, y_1, \dots, y_n)$. By Lemma 7.33, s is equivalent to a term u in disjunctive form, and to a term v in conjunctive form. Thus:

Lemma 7.39. *For any term $t \in \mathrm{Term}_{Boole}(x_1, \dots, x_n)$ there are terms $u, v \in \mathrm{Term}_{LTC}(x_1, \dots, x_n, y_1, \dots, y_n)$ such that, letting*

$$u' = u[x_1^*/y_1, \dots, x_n^*/y_n], \quad v' = v[x_1^*/y_1, \dots, x_n^*/y_n]$$

then $u', v' \in \mathrm{Term}_{Boole}(x_1, \dots, x_n)$ and

- *u' is in* ***disjunctive form****, i.e. it is a disjunction of conjunctions of $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$,*
- *v' is in* ***conjunctive form****, i.e. it is a conjunction of disjunctions of $\{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$,*
- *the formula $t \doteq u' \wedge t \doteq v'$ follows from T_{Boole}.*

7.F.3. *Morphisms and products.* We said on page 70 that a morphism is a map between structures that preserves predicates, functions and constants. Thus a morphism of partial orders is simply an order preserving map, while a morphism of lattices is a monotone map preserving the inf and sup operations, that is it is a morphism of $\mathcal{L}_{\text{LTC}}$-structures. If two lattices are complemented and if f is a lattice morphism preserving the maximum and the minimum, that is to say: it is a morphism of the structures $f\colon (M, \curlywedge_M, \curlyvee_M, \mathbf{0}_M, \mathbf{1}_M) \to (L, \curlywedge_L, \curlyvee_L, \mathbf{0}_L, \mathbf{1}_L)$ then by Lemma 4.17 the morphism f preserves complements, that is

$$\forall x \in M\, (f(x^*) = f(x)^\star)$$

where * is the complement in L. A **Boolean algebra homomorphism** is a map between Boolean algebras that is a morphism of $\mathcal{L}_{\text{Boole}}$-structures. By the arguments above, it is a map preserving $\curlywedge$, $\curlyvee$, $\mathbf{0}$ and $\mathbf{1}$; equivalently, by De Morgan's laws it is enough that preserves $\curlywedge$ and * or that preserves $\curlyvee$ and *.

The axioms of T_{Boole} are positive formulæ, hence they are preserved under homomorphic images (Proposition 4.7) and products (Proposition 4.12).

7.G. Boolean rings. Addition in a Boolean algebra B is the binary operation defined by

$$a + b \overset{\text{def}}{=} (a \curlywedge b^*) \curlyvee (b \curlywedge a^*).$$

Addition is commutative and that if $f\colon B \to C$ is a homomorphism, then $f(a + b) = f(a) + f(b)$. Moreover, $(B, +, \curlywedge, \mathbf{0}_B, \mathbf{1}_B)$ is a commutative ring (Exercise 7.83). Therefore we can associate a commutative ring to each Boolean algebra,

$$(B, \curlyvee, \curlywedge, ^*, \mathbf{0}, \mathbf{1}) \mapsto (B, +, \cdot, \mathbf{0}, \mathbf{1}) \tag{7.7}$$

by taking $a + b$ as above, and letting

$$a \cdot b \overset{\text{def}}{=} a \curlywedge b.$$

This is an example of a **Boolean ring** that is a ring satisfying $\forall x (x^2 = x)$—if the multiplicative identity is not required we have a Boolean rng. Every Boolean rng is commutative and if it is a ring, it arises from some Boolean algebra (Exercise 7.90); every Boolean algebra homomorphism $f\colon B \to C$ is a ring homomorphism. Thus we have another axiomatization of the notion of Boolean algebra, as an $\mathcal{L}_{\text{Rings}}$-structure satisfying the axioms for Boolean rings.

The **kernel** of a Boolean algebras homomorphism $f\colon B \to C$ is

$$\ker(f) \overset{\text{def}}{=} \{b \in B \mid f(b) = \mathbf{0}_C\}.$$

Thus f is injective if and only if its kernel is $\{\mathbf{0}_B\}$.

Definition 7.40. An **ideal of a Boolean algebra** B is a non-empty subset I, closed under $\curlyvee$ and such that $\downarrow I = I$. An ideal I is **proper** if $I \neq B$; it is **trivial** if $I = \{\mathbf{0}_B\}$.

Definition 7.40 is justified by the fact that an ideal in this sense is an ideal in the sense of rings (Exercise 7.84). An ideal I of a Boolean algebra B is **principal** if it is of the form $\downarrow b = \{c \in B \mid c \leq b\}$ for some $x \in B$; the element b is called a **generator of** I and we will say that I is generated by b.

If I is a proper ideal of a ring R, then R/I is a ring and $0_{R/I} \neq 1_{R/I}$; if moreover R is Boolean, then R/I is also Boolean—this can either be verified directly or by observing that $\forall x(x^2 \eqcirc x)$ is a positive formula and then applying Proposition 4.6. In any ring, a proper ideal I is **prime** if $x \cdot y \in I \Rightarrow x \in I \vee y \in I$, or equivalently if R/I is an integral domain; it is **maximal** if there is no proper ideal containing I, or equivalently R/I is a field. In any ring a maximal ideal is prime, and the converse is true in any Boolean ring. In fact, a Boolean ring which is an integral domain must be the field $\mathbb{Z}/2\mathbb{Z}$, since otherwise any $a \neq \mathbf{0}, \mathbf{1}$ would yield $a \cdot a^* = a \curlywedge a^* = \mathbf{0}$. Therefore:

Proposition 7.41. *Let $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}_B, \mathbf{1}_B)$ be a non-degenerate Boolean algebra and let I be a proper ideal.*

(a) *Let $\sim_I$ be the equivalence relation on B defined by $x \sim_I y \Leftrightarrow x + y \in I$. The quotient set is a Boolean algebra $(B/I, \sqcap, \sqcup, {}', \mathbf{0}_{B/I}, \mathbf{1}_{B/I})$:*

$$[x] \sqcap [y] = [x \curlywedge y] \qquad [x] \sqcup [y] = [x \curlyvee y] \qquad [x]' = [x^*]$$
$$\mathbf{0}_{B/I} = [\mathbf{0}_B] \qquad \mathbf{1}_{B/I} = [\mathbf{1}_B].$$

The ordering on B/I is given by $[x] \sqsubseteq [y] \Leftrightarrow x \curlywedge y^* \in I$.

(b) *The following are equivalent:*
- *I is prime,*
- *I is maximal,*
- *$\forall x(x \notin I \Leftrightarrow x^* \in I)$,*
- *B/I is the minimal algebra $\mathbf{2}$.*

Remark 7.42. The equivalence "prime if and only if maximal" in (b) holds not only for Boolean algebras, but more generally for von Neumann regular rings (Section 9.D.1).

Observe that Proposition 7.41 yields a bijection

$$\{f\colon B \to \mathbf{2} \mid f \text{ a homomorphism}\} \to \{D \subseteq B \mid D \text{ is an ultrafilter}\}, \tag{7.8}$$

where $f \mapsto \{b \in B \mid f(b) = \mathbf{1}\}$.

Proposition 7.43. *For every finite Boolean algebra B there is a homomorphism $h\colon B \to \mathbf{2}$.*

Proof. Let $\mathcal{I} \subseteq \mathscr{P}(B)$ be the set of all proper ideals of B. Then $(\mathcal{I}, \subseteq)$ is a finite ordered set so by Proposition 7.2 it has a maximal element I. Then the canonical projection $B \to B/I$ is the required homomorphism. □

By dualizing the notion of ideal, the concept of filter is obtained.

Definition 7.44. A **filter of a Boolean algebra** B is a non-empty subset F such that

- if $x, y \in F$ then $x \curlywedge y \in F$ and
- if $x \in F$ and $x \leq y$ then $y \in F$.

A filter F is **proper** if $F \neq B$, it is **trivial** if $F = \{\mathbf{1}\}$, it is an **ultrafilter** if it is proper and maximal with respect to inclusion. Therefore a proper filter F is an ultrafilter if and only if $x \curlyvee y \in F \Rightarrow x \in F \vee y \in F$. if and only if $\forall x (x \notin F \Leftrightarrow x^* \in F)$.

7.H. Ideals and filters on a set. An **ideal/filter *on the set*** X is an ideal/filter *of the Boolean algebra* $\mathscr{P}(X)$. The addition operation in $\mathscr{P}(X)$ is the symmetric difference $Y + Z = Y \triangle Z$. Given a subalgebra $\mathcal{S} \subseteq \mathscr{P}(X)$, an ideal of $\mathcal{S}$ is a family $I \subseteq \mathcal{S}$ closed under finite unions and subsets; a filter of $\mathcal{S}$ is a family $F \subseteq \mathcal{S}$ closed under finite intersections and supersets. The ideal generated by $A \in \mathcal{S}$ is $\{B \in \mathcal{S} \mid B \subseteq A\}$. Dually, the filter generated by $A \in \mathcal{S}$ is $\{B \in \mathcal{S} \mid B \supseteq A\}$; when $A = \{a\}$, then F is an ultrafilter. A filter F on X is an ultrafilter if and only if $\forall Y \subseteq X (Y \in F \Leftrightarrow X \setminus Y \notin F)$ if and only if F and its dual ideal partition $\mathscr{P}(X)$. If I is an ideal of a subalgebra $\mathcal{S} \subseteq \mathscr{P}(X)$ the ordering on the quotient algebra $\mathcal{S}/I$ is

$$[Y] \leq [Z] \Leftrightarrow Y \setminus Z \in I.$$

Examples 7.45. (a) $\mathrm{Fin} = \{A \subseteq \mathbb{N} \mid A \text{ is finite}\}$ is a non-principal ideal on $\mathbb{N}$. The quotient algebra $\mathscr{P}(\mathbb{N})/\mathrm{Fin}$ is atomless: in fact if A is infinite (that is $[A] \neq \mathbf{0} = \mathrm{Fin}$) then A can be written as union of two infinite, disjoint sets B and C, that is $A = B \cup C$ and $B \cap C = \emptyset$, hence $\mathbf{0} < [B] < [A]$. The dual of the ideal of finite subsets of $\mathbb{N}$ is the **Fréchet filter** $\{X \subseteq \mathbb{N} \mid \mathbb{N} \setminus X \text{ is finite}\}$.

(b) If X is a topological space, $\mathcal{V}_x = \{Y \subseteq X \mid \exists U \text{ open} (x \in U \subseteq Y)\}$ the family of neighborhoods of a point $x \in X$ is a proper filter. When X is T_2, it is an ultrafilter if and only if it is principal if an only if x is an isolated point of X.

Proper ideals are usually associated to a notion of "smallness" for subsets of X—the union of two small sets is small, and the subsets of small sets are small. Dually a proper filter on X is a notion of "largeness" for subsets of X. Examples of proper ideals are:

- finite subsets of an infinite set,
- countable subsets of an uncountable set,
- inside $\mathscr{P}(\mathbb{R})$, the collection of null sets and the collection of meager.

In the last example and the next section we assume that the reader has a passing acquaintance with measure and category. (These notions that will be presented in Section 26.)

7.H.1. *Filters and quantifiers.* If $\mathcal{F}$ is a proper filter on X, then

$$\forall^{\mathcal{F}} x\, \varphi(x) \text{ means that } \{x \in X \mid \varphi(x)\} \in \mathcal{F},$$

i.e. that $\varphi(x)$ holds for all x except for a collection of points in the dual ideal $\check{\mathcal{F}}$. Similarly

$$\exists^{\mathcal{F}} x\, \varphi(x) \text{ means that } \{x \in X \mid \varphi(x)\} \notin \check{\mathcal{F}},$$

that is $\{x \in X \mid \neg\varphi(x)\} \notin \mathcal{F}$. Therefore

$$\forall^{\mathcal{F}} x\, \varphi(x) \Leftrightarrow \neg\exists^{\mathcal{F}} x\, \neg\varphi(x), \qquad \exists^{\mathcal{F}} x\, \varphi(x) \Leftrightarrow \neg\forall^{\mathcal{F}} x\, \neg\varphi(x).$$

For example:

- when $\mathcal{F} = \{X\}$ is the trivial filter, then $\check{\mathcal{F}} = \{\emptyset\}$, we obtain the usual quantifiers;
- when $\check{\mathcal{F}}$ is the ideal of null sets, we obtain the “measure-quantifiers” used in analysis, where $\forall^{\mu} x\, \varphi(x)$ means that $\{x \in X \mid \neg\varphi(x)\}$ is of measure-zero;
- when $\mathcal{F}$ is the filter of comeager sets, we obtain the “category-quantifiers”, where $\forall^{*} x\, \varphi(x)$ means that $\{x \in X \mid \varphi(x)\}$ is comeager.

Some of the above filters/ideals admit a higher-dimensional version; for example, we can speak of the ideal of null sets, meager sets, countable sets, ... of $\mathbb{R}^n$. The Fubini theorem says that

$$\begin{aligned} \forall^{\lambda} x \in \mathbb{R} \forall^{\lambda} y \in \mathbb{R}\, \varphi(x, y) &\Leftrightarrow \forall^{\lambda} y \in \mathbb{R} \forall^{\lambda} x \in \mathbb{R}\, \varphi(x, y) \\ &\Leftrightarrow \forall^{\lambda^2} (x, y) \in \mathbb{R}^2\, \varphi(x, y) \end{aligned}$$

where the last formula says that $\{(x, y) \in \mathbb{R}^2 \mid \neg\varphi(x, y)\}$ is null in $\mathbb{R}^2$. The Kuratowski-Ulam theorem says that

$$\begin{aligned} \forall^{*} x \in \mathbb{R} \forall^{*} y \in \mathbb{R}\, \varphi(x, y) &\Leftrightarrow \forall^{*} y \in \mathbb{R} \forall^{*} x \in \mathbb{R}\, \varphi(x, y) \\ &\Leftrightarrow \forall^{*} (x, y) \in \mathbb{R}^2\, \varphi(x, y) \end{aligned}$$

where the last formula says that $\{(x, y) \in \mathbb{R}^2 \mid \neg\varphi(x, y)\}$ is meager in $\mathbb{R}^2$. A filter $\mathcal{F}$ on a set X has the Fubini-Kuratowski-Ulam property if

$$\forall_{\mathcal{F}} x \forall_{\mathcal{F}} y\, (x, y) \in A \Leftrightarrow \forall_{\mathcal{F}} y\, \forall_{\mathcal{F}} x (x, y) \in A \tag{7.9}$$

where $A \subseteq X \times X$ belongs to a suitable collection of sets. The theorems of Fubini and Kuratowski-Ulam say that (7.9) holds when $X = \mathbb{R}$, A is Borel, and $\mathcal{F}$ is the filter of co-null sets or the filter of comeager sets. Not every $\mathcal{F}$ has the Fubini-Kuratowski-Ulam property (Exercise 7.104).

7.I. Representation theorem for atomic algebras.

Proposition 7.46. *If B is a Boolean algebra and $a \in B$, the following are equivalent:*

(a) *a is an atom;*

(b) *$a \neq \mathbf{0}$ and for all $b, c \in B$, $a \leq b \curlyvee c$ if and only if $a \leq b$ or $a \leq c$;*

(c) *for all $b \in B$, either $a \leq b$ or else $a \leq b^*$;*

(d) *the principal ideal generated by a^* is prime; equivalently, the principal filter generated by a is an ultrafilter.*

Proof. (a) ⇒ (b). If either $a \leq b$ or $a \leq c$ then $a \leq b \curlyvee c$. Conversely, if $a \nleq b$ and $a \nleq c$, then $a \curlywedge b^* \neq \mathbf{0}$ and $a \curlywedge c^* \neq \mathbf{0}$ by part (a) of Lemma 4.18. Since a is an atom, $a \curlywedge b^* = a$ and $a \curlywedge c^* = a$, that is $a \leq b^*$ and $a \leq c^*$, hence $a \leq b^* \curlywedge c^* = (b \curlyvee c)^*$. If $a \leq b \curlyvee c$ then $a \leq (b \curlyvee c)^* \curlywedge (b \curlyvee c) = \mathbf{0}$: a contradiction. Therefore $a \nleq b \curlyvee c$.

(b) ⇒ (c). Given $b \in B$, then $a \leq \mathbf{1} = b \curlyvee b^*$, hence either $a \leq b$ or $a \leq b^*$. But $a \leq b$ and $a \leq b^*$ cannot hold simultaneously, since this would imply that $a \leq \mathbf{0} = b \curlywedge b^*$.

(c) ⇒ (a). Note that (c) trivially implies that $a \neq \mathbf{0}$. If there is a $\mathbf{0} < b < a$, then $a \nleq b$ implies that $a \leq b^*$, hence $\mathbf{0} = a \curlywedge b^{**} = a \curlywedge b = b$, a contradiction.

(b) ⇔ (d) follows from the duality principle. □

Theorem 7.47. (a) *For every Boolean algebra B such that $\mathrm{At}(B) \neq \emptyset$, the function $\mathfrak{A} \colon B \to \mathscr{P}(\mathrm{At}(B))$*

$$\mathfrak{A}(b) = \{a \in \mathrm{At}(B) \mid a \leq b\}$$

is a homomorphism.

(b) *B is atomic if and only if $\mathfrak{A}$ is injective.*

(c) *If B is complete, or even: $\bigvee X$ exists for all $X \subseteq \mathrm{At}(B)$, then $\mathfrak{A}$ is surjective.*

Proof. (a) Let $a \in \mathrm{At}(B)$. Then $a \leq b \curlywedge c$ if and only if $a \leq b$ and $a \leq c$ and by Proposition 7.46, $a \leq b \curlyvee c$ if and only if $a \leq b$ or $a \leq c$. Thus $\mathfrak{A}(b \curlywedge c) = \mathfrak{A}(b) \cap \mathfrak{A}(c)$ and $\mathfrak{A}(b \curlyvee c) = \mathfrak{A}(b) \cup \mathfrak{A}(c)$, that is $\mathfrak{A}$ is a homomorphism.

(b) It is immediate to check that B is atomic if and only if $\ker(\mathfrak{A}) = \{\mathbf{0}\}$.

(c) Let $X \subseteq \mathrm{At}(B)$: we must show that $X = \mathfrak{A}(b)$ for some b. Let $b = \curlyvee X$. Clearly $X \subseteq f(b)$ and if, towards a contradiction, there is $a \in \mathfrak{A}(b) \setminus X$, by the definition of being an atom $\forall x \in X\, (a \curlywedge x = \mathbf{0})$, hence by Lemma 7.38

$$a = a \curlywedge b = a \curlywedge \bigcurlyvee X = \bigcurlyvee \{a \curlywedge x \mid x \in X\} = \mathbf{0},$$

a contradiction. Thus $\mathfrak{A}(b) = X$. □

Corollary 7.48. (a) *Every atomic Boolean algebra is isomorphic to an algebra of sets.*

(b) *Every atomic Boolean algebra which is complete (or even just: $\curlyvee X$ exists for all sets of atoms X) is isomorphic to the power-set algebra of some set.*

7.J. Completion of Boolean algebras*.

7.J.1. *The regular open algebra.* An open set U of a topological space $(X, \mathfrak{T})$ is **regular** if $U = \boldsymbol{r}(U)$, where $\boldsymbol{r}(Y) \overset{\text{def}}{=} \mathrm{Int}(\mathrm{Cl}(Y))$ for any Y. Let

$$\mathbf{RO}(X) = \{U \in \mathfrak{T} \mid U = \boldsymbol{r}(U)\}$$

be the family of all regular open sets of X. By Proposition 7.29 the map $\boldsymbol{r} \colon \mathfrak{T} \to \mathfrak{T}$ is a closure function, so for all open sets U, V

- $U \subseteq V \Rightarrow \boldsymbol{r}(U) \subseteq \boldsymbol{r}(V)$
- $U \subseteq \boldsymbol{r}(U)$
- $\boldsymbol{r}(\boldsymbol{r}(U)) = \boldsymbol{r}(U)$.

As $\mathfrak{T}$ is a complete lattice, $\operatorname{ran} \boldsymbol{r} = \mathbf{RO}(X)$ is a complete lattice with X and $\emptyset$ being the top and bottom elements, and the operations

$$U \curlywedge V = U \cap V \quad \text{and} \quad U \curlyvee V = \boldsymbol{r}(U \cup V).$$

If $U \in \mathfrak{T}$ then $U^* \overset{\text{def}}{=} \mathrm{Int}(X \setminus U)$ is regular by Example 7.22. Since $U \curlywedge U^* = \emptyset$ and $U \cup U^*$ is dense in X, then $U \curlyvee U^* = X$, so U^* is a complement of U. Therefore $\mathbf{RO}(X)$ is a complemented lattice.

Let $U \in \mathfrak{T}$ and $Y \subseteq X$.

Claim 7.48.1. $U \cap \mathrm{Cl}(Y) \subseteq \mathrm{Cl}(U \cap Y)$.

Proof. Let $x \in U \cap \mathrm{Cl}(Y)$ and W be open and such that $x \in W$. We must show that $W \cap (U \cap Y) \neq \emptyset$. As $U \cap W$ is open and x belongs to it, and $x \in \mathrm{Cl}\, Y$, then $(U \cap W) \cap Y \neq \emptyset$, which is what we had to prove. □

As the interior of an intersection is the intersection of the interiors,

$$U \cap \boldsymbol{r}(Y) = \mathrm{Int}(U \cap \mathrm{Cl}(Y)) \subseteq \boldsymbol{r}(U \cap Y).$$

Using this equation we can prove that the lattice $\mathbf{RO}(X)$ is distributive: by Remark 4.16 it is enough to check that $U \curlywedge (V \curlyvee W) \subseteq (U \curlywedge V) \curlyvee (U \curlywedge W)$ for all $U, V, W \in \mathbf{RO}(X)$:

$$\begin{aligned} U \curlywedge (V \curlyvee W) &= U \cap \boldsymbol{r}(V \cup W) \subseteq \boldsymbol{r}(U \cap (V \cup W)) \\ &= \boldsymbol{r}((U \cap V) \cup (U \cap W)) = (U \curlywedge V) \curlyvee (U \curlywedge W). \end{aligned}$$

It follows that $\mathbf{RO}(X)$ is a complete Boolean algebra, called the **regular open algebra** on X. In the next section we will prove that every complete Boolean algebra is isomorphic to an algebra of this form. Note that $\mathbf{CLOP}(X)$ is a subalgebra of $\mathbf{RO}(X)$, and a subalgebra of $\mathscr{P}(X)$, but, in general, $\mathbf{RO}(X)$ is not a subalgebra of $\mathscr{P}(X)$, since the operation $\curlyvee$ may not agree with the union.

7.J.2. *Boolean completion.* Let $(P, \leq)$ be an ordered set. Two elements $p, q \in P$ are **compatible**, $p \parallel q$, if $\exists r \in P\, (r \leq p, q)$; otherwise they are **incompatible** $p \perp q$. A set $D \subseteq P$ is **dense** if $\forall p \in P\, \exists q \in D\, (q \leq p)$; equivalently, if it is dense in P with the downward topology. A monotone map $f \colon P \to Q$ between ordered set is **dense** is $\operatorname{ran} f$ is dense in Q.

If P has minimum $\mathbf{0}$ (like in the case of Boolean algebras) the above definitions become trivial—any two elements are always compatible, and $D \subseteq P$ is dense if and only if $\mathbf{0} \in D$. For B a Boolean algebra and $X \subseteq B$, let $X^+ \stackrel{\text{def}}{=} X \setminus \{\mathbf{0}_B\}$.

Convention. When dealing with a Boolean algebra B, (in)compatibility and density are understood to refer to B^+, that is to say:

- Two elements $b, c \in B^+$ are **incompatible in** B if and only if $b \perp_{B^+} c$, that is $b \curlywedge c = \mathbf{0}$.
- $D \subseteq B$ is **dense in** B if and only if D^+ is dense in B^+, that is $\forall b \in B^+\, \exists d \in D^+ (d \leq b)$.
- A monotone $f \colon P \to B$ where $P$is an ordered set, is **dense** if $\operatorname{ran}(f)$ is dense in B.

If B is a Boolean algebra and $b, c \in B^+$ are such that $b \nleq c$, then $d \stackrel{\text{def}}{=} c \curlywedge b^* \neq \mathbf{0}_B$ and d, b are incompatible. This property is important enough to deserve a:

Definition 7.49. An ordered set P is **separative** if

$$\forall p, q \in P \left[p \nleq q \Rightarrow \exists r \leq p\ (r \perp q) \right].$$

Equivalently: if $\forall p, q \in P \left[{\downarrow} p \nsubseteq {\downarrow} q \Rightarrow \exists r \in {\downarrow} p\ ({\downarrow} r \cap {\downarrow} q = \emptyset) \right]$.

The next result is straightforward.

Proposition 7.50. *Suppose B is a Boolean algebra and that $D \subseteq B^+$ is dense. Then D is separative.*

Observe that for any ordered set P:

$$\begin{aligned}\boldsymbol{r}(\downarrow p) &= \{q \in P \mid \downarrow q \subseteq \mathrm{Cl}(\downarrow p)\}\\ &= \{q \in P \mid \forall r \leq q\,(\downarrow r \cap \downarrow p \neq \emptyset)\}\\ &= \{q \in P \mid \forall r \leq q\,(r \parallel p)\}.\end{aligned}$$

Proposition 7.51. *P is separative if and only if $\forall p \in P\ (\downarrow p \in \mathbf{RO}(P))$.*

Proof. Suppose P is separative. If $q \in \boldsymbol{r}(\downarrow p)$ then $\forall r \leq q\,(r \parallel p)$, and hence $q \in \downarrow p$ as P is separative. Conversely if $\downarrow p = \boldsymbol{r}(\downarrow p)$ for all $p \in P$, then $q \nleq p$ implies that $\exists r \leq q\,(r \perp p)$, thus P is separative. □

The next result is the converse of Proposition 7.50.

Theorem 7.52. *If P is separative then $: P \to \mathbf{RO}(P)^+$, $p \mapsto \downarrow p$ is a dense embedding.*

Proof. By Proposition 7.51 i is well-defined, and since the sets $\downarrow p$ form a basis for the downward topology, $\operatorname{ran} i$ is dense in P.

The map i is clearly monotone; to prove it is an embedding, let's assume that $i(p) \subseteq i(q)$ towards proving that $p \leq q$. Towards a contradiction, assume that $p \nleq q$. Choose $r \leq p$ such that $r \perp q$. Then $\downarrow r \cap \downarrow q = \emptyset$ and hence $i(r) \cap i(q) = \emptyset$. As $i(r) \leq i(p)$, this yields the desired contradiction. □

Lemma 7.53. *If B is a complete Boolean algebra and $D \subseteq B$ is dense, then $b = \curlyvee \{d \in D \mid d \leq b\}$ for all $b \in B$.*

Proof. Clearly $b \geq c \overset{\text{def}}{=} \sup_B \{x \in D \mid x \leq b\}$. If $b > c$ then pick a $x \in D$ such that $d \leq b \curlywedge c^* \neq \mathbf{0}$, hence $d \in \{x \in D \mid x \leq b\}$, and thus $d \leq c$: a contradiction. □

Lemma 7.54. *Let B, C_1, C_2 be Boolean algebras, and suppose C_1, C_2 are complete and $j_i \colon B \to C_i$ ($i = 1, 2$) are dense embeddings. Then there is a unique isomorphism $h \colon C_1 \to C_2$ such that $j_2 = h \circ j_1$.*

Proof. By Lemma 7.53 every $a \in C_1$ is of the form $a = \sup_{C_1} j_1[X_a]$, where $X_a = \{x \in B \mid j_1(x) \leq a\}$, and every $b \in C_2$ is of the form $b = \sup_{C_2} j_2[Y_b]$, where $Y_b = \{x \in B \mid j_2(x) \leq b\}$. Define $h \colon C_1 \to C_2$ by

$$h(a) = \sup_{C_2} j_2[X_a].$$

Then h is an order preserving bijection, and hence an isomorphism of Boolean algebras, and it is the unique function h' such that $j_2 = h' \circ j_1$. □

The **Boolean completion** of a separative order P is a complete Boolean algebra B together with a dense embedding $j\colon P \to B^+$; it exists by Theorem 7.55 and it is unique by Lemma 7.54. In particular, taking $P = B \setminus \{\mathbf{0}_B\}$:

Theorem 7.55. *Every Boolean algebra can be densely embedded in a complete Boolean algebra. Moreover this complete Boolean algebra is unique up to isomorphism.*

For B a Boolean algebra we have two types of completion: the Dedekind-McNeille completion $\mathbf{DM}(B)$ which is a complete lattice (Theorem 7.12), and the Boolean completion $\mathbf{RO}(B^+)$. It turns out that $\mathbf{DM}(B)$ is a Boolean algebra [**Bly05**, Theorem 6.13 p. 90] and since B densely embeds into it, then $\mathbf{DM}(B)$ is isomorphic to $\mathbf{RO}(B^+)$. In other words, the Dedekind-McNeille completion and the Boolean completion of a Boolean algebra are the same.

7.K. Free Boolean algebras and propositional calculus.

7.K.1. *Finitely generated Boolean algebras.* Given a Boolean algebra B and a subset C, the algebra generated by C is the smallest subalgebra B' of B containing C; we say that C is a set of generators for B'. By Proposition 4.2 $B' = \left\{ t^B(\vec{c}) \mid \vec{c} \in C \wedge t \in \mathrm{Term}_{\mathrm{BOOLE}} \right\}$ and by Lemma 7.39

$$\begin{aligned} B' &= \left((C \cup \{c^* \mid c \in C\} \cup \{\mathbf{0}, \mathbf{1}\})^{\curlywedge} \right)^{\curlyvee} \\ &= \left((C \cup \{c^* \mid c \in C\} \cup \{\mathbf{0}, \mathbf{1}\})^{\curlyvee} \right)^{\curlywedge} \end{aligned} \tag{7.10}$$

where for any $X \subseteq B$ we let

$$\begin{aligned} X^{\curlywedge} &= \{x_1 \curlywedge \ldots \curlywedge x_n \mid x_1, \ldots, x_n \in X \text{ and } n \geq 1\} \\ X^{\curlyvee} &= \{x_1 \curlyvee \ldots \curlyvee x_n \mid x_1, \ldots, x_n \in X \text{ and } n \geq 1\}. \end{aligned}$$

Remark 7.56. The reason for having $\mathbf{0}$ and $\mathbf{1}$ in (7.10) is to take care of $C = \emptyset$, in which case $B' = \{\mathbf{0}, \mathbf{1}\}$. If $C \neq \emptyset$, then $\mathbf{0} \in (C \cup \{c^* \mid c \in C\})^{\curlywedge}$ and $\mathbf{1} \in \left((C \cup \{c^* \mid c \in C\})^{\curlywedge} \right)^{\curlyvee}$, hence the algebra generated by C is

$$B' = \left((C \cup \{c^* \mid c \in C\})^{\curlywedge} \right)^{\curlyvee} = \left((C \cup \{c^* \mid c \in C\})^{\curlyvee} \right)^{\curlywedge}.$$

Corollary 7.57. *Let B be a Boolean algebra, $C \subseteq B$ a subalgebra, and $b \in B \setminus C$. The subalgebra of B generated by $C \cup \{b\}$ is*

$$\{(c_1 \curlywedge b) \curlyvee (c_2 \curlywedge b^*) \mid c_1, c_2 \in C\} = \{(c_1 \curlyvee b) \curlywedge (c_2 \curlyvee b^*) \mid c_1, c_2 \in C\}.$$

Corollary 7.58. *If B is a Boolean algebra and $C = \{c_1, \ldots, c_n\} \subseteq B$, then the subalgebra B' generated by C is finite, hence atomic, and the atoms are the minimal elements of $(C \cup \{c^* \mid c \in C\})^{\curlywedge} \setminus \{\mathbf{0}\}$.*

A Boolean algebra that admits a finite set of generators is said to be **finitely generated**, thus a finitely generated Boolean algebra is finite. By Corollary 7.58 a finitely generated algebra is finite.

7.K.2. *Propositional calculus.* Recall from Section 3.C.1 that given a nonempty set S of **propositional letters** one can construct the set $\mathrm{Prop}(S)$ of **propositions** over S by applying $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ to the elements in S. Let $\preceq$ be the binary relation on $\mathrm{Prop}(S)$ defined by

$$\mathrm{P} \preceq \mathrm{Q} \text{ if and only if } \vdash \mathrm{P} \Rightarrow \mathrm{Q}.$$

By Theorem 5.24 $\mathrm{P} \preceq \mathrm{Q}$ just in case $\mathrm{P} \Rightarrow \mathrm{Q}$ is a tautology. The relation $\preceq$ is a pre-order on $\mathrm{Prop}(S)$, and the induced equivalence relation is

$$\begin{aligned} \mathrm{P} \sim \mathrm{Q} \quad & \text{if and only if} \quad \vdash \mathrm{P} \Leftrightarrow \mathrm{Q} \\ & \text{if and only if} \quad \mathrm{P}, \mathrm{Q} \text{ are tautologically equivalent} \\ & \text{if and only if} \quad \forall v \colon S \to \{0,1\} \, (v(\mathrm{P}) = v(\mathrm{Q})) \end{aligned} \tag{7.11}$$

and hence we can define an order on the quotient $\mathrm{Prop}(S)/{\sim}$

$$[\mathrm{P}] \leq [\mathrm{Q}] \quad \text{if and only if} \quad \vdash \mathrm{P} \Rightarrow \mathrm{Q}.$$

Theorem 7.59. $(\mathrm{Prop}(S)/{\sim}, \leq)$ *is a complemented, distributive lattice with* **1** *the set of all tautologies,* **0** *the set of all propositional contradictions. Therefore it is a non-degenerate Boolean algebra with the operations*

$$[\mathrm{P}]^* = [\neg \mathrm{P}] \qquad [\mathrm{P}] \curlyvee [\mathrm{Q}] = [\mathrm{P} \vee \mathrm{Q}] \qquad [\mathrm{P}] \curlywedge [\mathrm{Q}] = [\mathrm{P} \wedge \mathrm{Q}].$$

Proof. Given $\mathrm{P}_0, \mathrm{P}_1 \in \mathrm{Prop}(S)$, we have that for $i = 0, 1$, $\vdash \mathrm{P}_0 \wedge \mathrm{P}_1 \Rightarrow \mathrm{P}_i$ and if $\vdash \mathrm{Q} \Rightarrow \mathrm{P}_i$ then $\vdash \mathrm{Q} \Rightarrow \mathrm{P}_0 \wedge \mathrm{P}_1$. Therefore

$$[\mathrm{P}_0 \wedge \mathrm{P}_1] = \inf([\mathrm{P}_0], [\mathrm{P}_1]) = [\mathrm{P}_0] \curlywedge [\mathrm{P}_1].$$

Similarly $[\mathrm{P}_0 \vee \mathrm{P}_1] = \sup([\mathrm{P}_0], [\mathrm{P}_1]) = [\mathrm{P}_0] \curlyvee [\mathrm{P}_1]$, so $(\mathrm{Prop}(S)/{\sim}, \leq)$ is a lattice. As $\vdash \mathrm{P} \Rightarrow \mathrm{Q}$ whenever Q is a tautology and P is arbitrary, then $\mathbf{1} = \{\mathrm{Q} \mid \mathrm{Q} \text{ is a tautology}\}$. Dually $\mathbf{0} = \{\mathrm{Q} \mid \mathrm{Q} \text{ is a propositional contradiction}\}$. As $\mathrm{P} \vee \neg \mathrm{P} \in \mathbf{1}$ and $\mathrm{P} \wedge \neg \mathrm{P} \in \mathbf{0}$ for all P, we have that $[\mathrm{P}]^* = [\neg \mathrm{P}]$ is the complement of $[\mathrm{P}]$. Finally distributivity follows from the fact that

$$\mathrm{P} \wedge (\mathrm{Q} \vee \mathrm{R}) \Leftrightarrow (\mathrm{P} \wedge \mathrm{Q}) \vee (\mathrm{P} \wedge \mathrm{R}) \qquad \mathrm{P} \vee (\mathrm{Q} \wedge \mathrm{R}) \Leftrightarrow (\mathrm{P} \vee \mathrm{Q}) \wedge (\mathrm{P} \vee \mathrm{R})$$

are tautologies, for any $\mathrm{P}, \mathrm{Q}, \mathrm{R} \in \mathrm{Prop}(S)$. □

By (7.11) any valuation $v \colon S \to \mathbf{2} = \{0, 1\}$ can be extended to a unique

$$\hat{v} \colon \mathrm{Prop}(S)/{\sim} \to \{0,1\}, \quad \hat{v}([\mathrm{P}]) = v(\mathrm{P}).$$

As $\hat{v}([\mathrm{P}]^*) = \hat{v}([\neg \mathrm{P}]) = v(\neg \mathrm{P}) = 1 - v(\mathrm{P})$ and $\hat{v}([\mathrm{P}] \curlyvee \hat{v}([\mathrm{Q}])) = \hat{v}([\mathrm{P} \vee \mathrm{Q}]) = \sup\{v(\mathrm{P}), v(\mathrm{Q})\}$, it follows that $\hat{v}$ is a homomorphism of Boolean algebras. Conversely, any homomorphism $f \colon \mathrm{Prop}(S)/{\sim} \to \mathbf{2}$ defines a valuation $v \colon S \to \{0,1\}$, $v(\mathrm{A}) = \hat{v}([\mathrm{A}])$, such that $\hat{v} = f$. As homomorphisms between B and $\mathbf{2}$ can be identified with ultrafilters (7.8) we obtain

Proposition 7.60. *There is a bijection between the set of all valuations* $\{0,1\}^S$ *and the set of ultrafilters on* $\mathrm{Prop}(S)/{\sim}$*.*

The algebra $\mathrm{Prop}(S)/{\sim}$ of all propositions over S obtained by identifying provably equivalent propositions, and it was the original motivation for the investigations of Boolean algebras. Recall (Definition 5.25) that $\Sigma \subseteq \mathrm{Prop}(S)$ is

- **consistent** if no contradiction can be derived from Σ—equivalently: not every proposition can be derived from it,
- **satisfiable** if it has a model, i.e. there is $v\colon S \to \{0,1\}$ such that $v(\mathrm{P}) = 1$ for all $\mathrm{P} \in \Sigma$.

Proposition 7.61. *For any* $\Sigma \subseteq \mathrm{Prop}(S)$ *the set* $F_\Sigma = \{[\mathrm{P}] \mid \Sigma \vdash \mathrm{P}\}$ *is a filter of* $\mathrm{Prop}(S)/{\sim}$*, and if* Σ *is consistent then* F_Σ *is proper.*

Conversely, if F *is a proper filter of* $\mathrm{Prop}(S)/{\sim}$*, then* $\Sigma = \{\mathrm{P} \mid [\mathrm{P}] \in F\}$ *is consistent, and* $F_\Sigma = F$*.*

Proof. If $[\mathrm{P}], [\mathrm{Q}] \in F_\Sigma$ then $\Sigma \vdash \mathrm{P}$ and $\Sigma \vdash \mathrm{Q}$, so $\Sigma \vdash \mathrm{P} \wedge \mathrm{Q}$, and hence $[\mathrm{P}] \curlywedge [\mathrm{Q}] = [\mathrm{P} \wedge \mathrm{Q}] \in F_\Sigma$. If $[\mathrm{P}] \in F$ and $[\mathrm{P}] \leq [\mathrm{Q}]$ then $\vdash \mathrm{P} \Rightarrow \mathrm{Q}$, so $\Sigma \vdash \mathrm{Q}$ by MP, and hence $[\mathrm{Q}] \in F_\Sigma$. Therefore F_Σ is a filter of $\mathrm{Prop}(S)/{\sim}$. If F_Σ is not proper, then every P is derivable from Σ, so Σ is inconsistent. Therefore if Σ is consistent, then F_Σ is proper.

Suppose now F is a filter, and let $\Sigma = \{\mathrm{P} \in \mathrm{Prop}(S) \mid [\mathrm{P}] \in F\}$. If $\mathrm{P}_1, \mathrm{P}_2 \in \Sigma$ then $[\mathrm{P}_1], [\mathrm{P}_2] \in F$ and hence $[\mathrm{P}_1] \curlywedge [\mathrm{P}_2] = [\mathrm{P}_1 \wedge \mathrm{P}_2] \in F$, so $\mathrm{P}_1 \wedge \mathrm{P}_2 \in \Sigma$. In other words: Σ is closed under taking conjunctions. If $\Sigma \vdash \mathrm{Q}$, then $\mathrm{P}_1, \dots, \mathrm{P}_n \vdash \mathrm{Q}$ for some $\mathrm{P}_1, \dots, \mathrm{P}_n \in \Sigma$, so $\mathrm{P}_1 \wedge \cdots \wedge \mathrm{P}_n \vdash \mathrm{Q}$, and hence $\vdash \mathrm{P}_1 \wedge \cdots \wedge \mathrm{P}_n \Rightarrow \mathrm{Q}$. As $\mathrm{P}_1 \wedge \cdots \wedge \mathrm{P}_n \in \Sigma$ and $[\mathrm{P}_1 \wedge \cdots \wedge \mathrm{P}_n] \leq [\mathrm{Q}]$, it follows that $[\mathrm{Q}] \in F$, and hence $\mathrm{Q} \in \Sigma$. In other words: Σ is closed under derivations, that is if $\Sigma \vdash \mathrm{Q}$ then $\mathrm{Q} \in \Sigma$. Therefore if F is a *proper* filter then Σ cannot derive every sentence, that is Σ is consistent. Moreover $[\mathrm{P}] \in F_\Sigma \Leftrightarrow \Sigma \vdash \mathrm{P} \Leftrightarrow [\mathrm{P}] \in F$, that is $F_\Sigma = F$. □

Recall that a first-order theory is complete if it is satisfiable and any sentence or its negation is logical consequence of it (Definition 3.31). The next result says that any satisfiable set of propositions can be extended to a complete one.

Proposition 7.62. *If* $\Sigma \subseteq \mathrm{Prop}(S)$ *is satisfiable then there is a satisfiable* $\Sigma' \subseteq \mathrm{Prop}(S)$ *such that* $\Sigma \subseteq \Sigma'$ *and either* $\mathrm{P} \in \Sigma$ *or else* $\neg\mathrm{P} \in \Sigma$*, for all* $\mathrm{P} \in \mathrm{Prop}(S)$*.*

Proof. Let $v\colon S \to \{0,1\} = \mathbf{2}$ be a model of Σ and let $\hat{v}\colon \mathrm{Prop}(S)/{\sim} \to \mathbf{2}$ be the induced homomorphism. Then $\Sigma' = \{\mathrm{P} \mid \hat{v}([\mathrm{P}]) = 1\}$ is as required. □

Arguing as in Lemma 3.8, if S is a non-empty set any $v\colon S \to B$, where B is a Boolean algebra, can be extended to a map, still denoted by v, from $\mathrm{Prop}(S)$ to B so that the following hold:

$$\begin{aligned}
v(\neg \mathrm{P}) &= v(\mathrm{P})^* \\
v(\mathrm{P} \wedge \mathrm{Q}) &= v(\mathrm{P}) \curlywedge v(\mathrm{Q}) \\
v(\mathrm{P} \vee \mathrm{Q}) &= v(\mathrm{P}) \curlyvee v(\mathrm{Q}) \\
v(\mathrm{P} \Rightarrow \mathrm{Q}) &= v(\mathrm{P})^* \curlyvee v(\mathrm{Q}) \\
v(\mathrm{P} \Leftrightarrow \mathrm{Q}) &= (v(\mathrm{P})^* \curlyvee v(\mathrm{Q})) \curlywedge (v(\mathrm{Q})^* \curlyvee v(\mathrm{P})) \\
v(\mathrm{P} \veebar \mathrm{Q}) &= (v(\mathrm{P}) \curlywedge v(\mathrm{Q})) \curlyvee (v(\mathrm{Q}) \curlyvee v(\mathrm{P}))^*.
\end{aligned} \tag{7.12}$$

Lemma 7.63. *Let* $v\colon S \to B$ *be as above, and let* $\mathrm{P}, \mathrm{Q} \in \mathrm{Prop}(S)$. *If* P *is a tautology, then* $v(\mathrm{P}) = \mathbf{1}_B$. *If* $\mathrm{P} \sim \mathrm{Q}$ *then* $v(\mathrm{P}) = v(\mathrm{Q})$.

Proof. If P is a tautology, then $\vdash \mathrm{P}$ where $\vdash$ is any of the equivalent notions of derivation. The most straightforward way to prove our result is using Shoenfield's system from Section 5.E: the only connectives are $\neg$ and $\vee$, all axioms are of the form $\neg \mathrm{P} \vee \mathrm{P}$, and there are four inference rules:

- from $\mathrm{P} \vee (\mathrm{Q} \vee \mathrm{R})$ derive $(\mathrm{P} \vee \mathrm{Q}) \vee \mathrm{R}$
- from $\mathrm{P} \vee \mathrm{P}$ derive P
- from P derive $\mathrm{Q} \vee \mathrm{P}$
- from $\mathrm{P} \vee \mathrm{Q}$ and $\neg \mathrm{P} \vee \mathrm{Q}$ derive $\mathrm{Q} \vee \mathrm{R}$.

It is immediate to check that any axiom gets value $\mathbf{1}_B$, and that each rule yields a proposition with value $\mathbf{1}_B$ whenever the assumptions have value $\mathbf{1}_B$. Therefore by induction on the length of the derivation we have that if $\vdash \mathrm{P}$, then $v(\mathrm{P}) = \mathbf{1}_B$.

If $\mathrm{P} \sim \mathrm{Q}$ then $\vdash \mathrm{P} \Leftrightarrow \mathrm{Q}$, so $\mathrm{P} \Leftrightarrow \mathrm{Q}$ is a tautology, and hence $(v(\mathrm{P})^* \curlyvee v(\mathrm{Q})) \curlywedge (v(\mathrm{Q})^* \curlyvee v(\mathrm{P})) = \mathbf{1}_B$ so that $v(\mathrm{P}) = v(\mathrm{Q})$. □

7.K.3. *Free Boolean algebras.* $\mathrm{Prop}(S)/{\sim}$ is the most general Boolean algebra that one can construct starting from S, so in analogy with Section 7.D.1 we call it the **free Boolean algebra generated by** S

$$\mathrm{Free}_{\mathrm{BOOLE}}(S) = \mathrm{Free}(S).$$

If S and S' are in bijection, then $\mathrm{Free}(S) \cong \mathrm{Free}(S')$, and we denote the free Boolean algebra with n generators by $\mathrm{Free}(n)$.

As every proposition is tautologically equivalent to one in conjunctive/disjunctive normal form, the set $\mathrm{Prop}^-(S)$ of all propositions constructed from S using only $\neg, \vee, \wedge$, intersects every equivalence class of $\mathrm{Prop}(S)/{\sim}$. By (7.10) the elements of $\mathrm{Free}(S)$ are $\sim$-equivalence classes of disjunctions

$$\mathrm{C}_1 \vee \ldots \vee \mathrm{C}_k$$

where each C_i is a conjunction of the form

$$\mathrm{A}_1^{\varepsilon_1} \wedge \cdots \wedge \mathrm{A}_m^{\varepsilon_m}$$

where $\varepsilon_j \in \{-1, 1\}$, $\mathrm{A}_i \in S$, and $\mathrm{A}^1 = \mathrm{A}$ and $\mathrm{A}^{-1} = \neg\mathrm{A}$.

If S is finite, say $S = \{\mathrm{A}_1, \ldots, \mathrm{A}_n\}$, then $\mathrm{Free}(S)$ is atomic, and the atoms are the equivalence classes of the propositions $\mathrm{A}_1^{\varepsilon_1} \wedge \cdots \wedge \mathrm{A}_n^{\varepsilon_n}$. If instead S is infinite, then $\mathrm{Free}(S)$ is atomless. To see this take a non-zero element $[\mathrm{P}]$ of $\mathrm{Free}(S)$, where $\mathrm{P} = \mathrm{C}_1 \vee \ldots \vee \mathrm{C}_k$ and each C_i is a conjunction of letters or negation of letters of S. As S is infinite, let A be a letter not occurring in P: then both $\mathrm{A} \wedge \mathrm{P}$ and $\neg\mathrm{A} \wedge \mathrm{P}$ are non-null, so $[\mathrm{A} \wedge \mathrm{P}], [\neg\mathrm{A} \wedge \mathrm{P}] < [\mathrm{P}]$.

We have thus proved:

Theorem 7.64. $\mathrm{Free}(n)$ *is atomic, has* 2^n *atoms, and hence has size* 2^{2^n}. *If* S *is infinite, then* $\mathrm{Free}(S)$ *is atomless.*

By Theorem 7.47 every finite Boolean algebra is isomorphic to an algebra of sets, and every Boolean algebra with n generators is isomorphic to the collection of sets generated $A_1, \ldots, A_n$ contained in some set U. In order to obtain $\mathrm{Free}(n)$ we should not assume any relation between $A_1, \ldots, A_n$. For example $\mathrm{Free}(2)$ can be seen as the collection of all 16 sets that can obtained from $A, B \subseteq U$,

$$\begin{aligned}\mathrm{Free}_{\mathrm{BOOLE}}(2) = \{&A \cap B, A \setminus B, B \setminus A, A^{\complement} \cap B^{\complement}, \emptyset, U, A, B, A^{\complement}, B^{\complement},\\ &A^{\complement} \cup B^{\complement}, A^{\complement} \cup B, A \cup B^{\complement}, A \cup B, A \triangle B, (A \cap B) \cup (A \cup B)^{\complement}\}.\end{aligned}$$

Not every finitely generated Boolean algebra is free, as there are Boolean algebras of size 2^n for any $n \geq 1$. But every Boolean algebra is the quotient of a free Boolean algebra.

Lemma 7.65. *If* B *is a Boolean algebra and* $S \subseteq B$ *is a set of generators, then there is a surjective homomorphism* $h\colon \mathrm{Free}(S) \to B$.

Proof. The inclusion map $S \to B$ is extended to a function $v\colon \mathrm{Prop}(S) \to B$ satisfying (7.12). By Lemma 7.63 v induces a homomorphism on the quotient

$$h\colon \mathrm{Prop}(S)/{\sim} = \mathrm{Free}(S) \to B,$$

as $h([\neg\mathrm{P}]) = h([\mathrm{P}])^*$ and $h([\mathrm{P} \vee \mathrm{Q}]) = h([\mathrm{P}]) \curlyvee h([\mathrm{Q}])$. □

Suppose $\Sigma \subseteq \mathrm{Prop}(S)$ is consistent, so that by Proposition 7.61 $F_\Sigma = \{[\mathrm{P}] \mid \Sigma \vdash \mathrm{P}\}$ is a filter of $\mathrm{Free}(S)$. Let

$$I_\Sigma = \{[\neg\mathrm{P}] \mid \Sigma \vdash \mathrm{P}\}$$

be the ideal dual of F_Σ. The quotient algebra $\mathrm{Free}(S)/I_\Sigma$ is the **Lindembaum algebra** of Σ.

Every Boolean algebra is isomorphic to a Lindembaum algebra.

Theorem 7.66. *Every Boolean algebra B is isomorphic to* $\mathrm{Free}(S)/I_\Sigma$ *where $S \subseteq B$ is any set of generators of B and $\Sigma \subseteq \mathrm{Prop}(S)$ is a suitable consistent set of propositions.*

Proof. By Lemma 7.65 $B \cong \mathrm{Free}(S)/I$ with $I = \ker h$. By Proposition 7.61 the filter F dual to I is of the form F_Σ for some consistent Σ, so the result follows. □

7.L. Axioms systems for lattices and Boolean algebras*. Lattices are be axiomatized in $\mathcal{L}_{\mathrm{LTC}}$ by associativity (4.4), commutativity (4.5), and absorption laws (4.6), for $\curlyvee$ and $\curlywedge$, so this yields a system T_{LTC} with six identities. These axioms are mutually independent [**PR08**, p. 8], so we cannot dispense of any of them. For distributive lattices we add the distributive laws (4.7), and by Remark 4.16 we only need to add just one of the two identities. But this does not mean that we end up with an independent set of axioms, as distributivity, absorption, and commutativity yield associativity [**PR08**, Theorem 3.2.1, p. 59]. Thus in defining distributive lattices (and Boolean algebras) we could have been more parsimonious by dropping associativity.

Lattices are axiomatized by identities, so one might ask what is the minimal number of identities needed to define the varieties of lattices, modular lattices, distributive lattices, ... McKenzie proved in 1970 that the variety of lattices is 1-based, i.e. it can be axiomatized by a single identity, and that any 1-based equational subvarieties of lattices, is either the collection of *all* lattices, or the collection of lattices with exactly one point (this one being axiomatized by $x = y$) [**PR08**, p. 28–29]. In particular, the notion of modular or distributive lattice cannot be axiomatized by a single identity. This should be contrasted with the situation for groups (see Remark 4.11).

The notion of Boolean algebra can be axiomatized in several ways: as a complemented distributive lattice, as a Boolean ring, or as a $\mathcal{L}_{\mathrm{BOOLE}}$-structure $(B, \curlywedge, \curlyvee, {}^*, \mathbf{0}, \mathbf{1})$ satisfying T_{BOOLE}. The axioms in T_{BOOLE} are not independent (Exercise 7.93). The constants $\mathbf{1}$ and $\mathbf{0}$ are definable from $\curlywedge$, $\curlyvee$ and *, and by De Morgan's laws the operations $\curlywedge$ and $\curlyvee$ are definable from each other using complementation. Therefore in order to axiomatize Boolean algebras it is enough to use * and just one among $\curlywedge$ and $\curlyvee$. In order to find a system based on, e.g., $\curlyvee$ and *, one could restate the axioms in T_{BOOLE} without mentioning $\curlywedge$, $\mathbf{0}$ and $\mathbf{1}$, but other, simpler axiomatizations can be given. In every Boolean algebra the following holds

$$\forall x, y\big[(x^* \curlyvee y^*)^* \curlyvee (x^* \curlyvee y)^* = x\big]. \tag{7.13}$$

Huntington proved the converse—see [**GH09**, pp. 478–481] for a proof.

Theorem 7.67. *Suppose B is a set with an associative and commutative binary operation $\curlyvee$, and a unary operation * satisfying* (7.13). *Then $b \mapsto b \curlyvee b^*$ is constantly equal to a certain value $\mathbf{1}$, and letting $\mathbf{0} = \mathbf{1}^*$ and $a \curlywedge b \overset{\text{def}}{=} (a^* \curlyvee b^*)^*$, we have that $(B, \curlyvee, \curlywedge, {}^*, \mathbf{0}, \mathbf{1})$ is a Boolean algebra.*

Thus (4.5a), (4.4a), and (7.13) form an axiom system for Boolean algebras, and moreover an independent one, meaning that neither of them can be derived from the other two [**GH09**, pp. 481]. An example of axiomatization of Boolean algebras by means of $\curlywedge$, * and $\mathbf{0}$ is presented in Exercise 7.92.

Shortly after Theorem 7.67 was proved, Robbins asked wether (7.13) could be replaced by $\forall x, y \big[((x \curlyvee y)^* \curlyvee (x^* \curlyvee y^*)^*)^* \eqcirc x\big]$. Observe that this new identity holds in every Boolean algebra, so the problem is whether any $(B, \curlyvee, {}^*)$ satisfying this equation (a Robbins algebra) must satisfy (7.13) (and hence be a Boolean algebra). The problem remained open for sixty years until McCune proved this conjecture in 1997 using Otter, a program for symbolic computation.

The variety of Boolean algebras is 1-based, i.e. it can be axiomatized by a single identity $t \eqcirc s$ (see Section 4.D). An example of such identity is

$$(((x \curlyvee y)^* \curlyvee z)^* \curlyvee (x \curlyvee (z^* \curlyvee (z \curlyvee u)^*)^*)^*)^* \eqcirc z.$$

If we want to be more parsimonious on the number of symbols of the language, we could replace $\curlywedge$, $\curlyvee$ and * by either one of the following binary operations: $x \,|\, y \overset{\text{def}}{=} (x \curlywedge y)^*$ and $x {\uparrow} y \overset{\text{def}}{=} (x \curlyvee y)^*$. Since $x \,|\, x = x {\uparrow} x = x^*$, the operations $\curlywedge$, $\curlyvee$ and * are definable in the structures $(B, |)$ and $(B, \uparrow)$, and hence Boolean algebras can be axiomatized in a language with just one binary operation symbol. In fact it is possible to give an axiomatization by means of a single identity of terms built from variables and $|$:

$$(x \mid ((y \mid x) \mid x)) \mid (y \mid (z \mid x)) \eqcirc y.$$

7.M. Relation algebras*. Relation algebras are structures providing an algebraic counterpart to the calculus of relations of Section 3.D.5.

The language $\mathcal{L}_{\mathrm{RlnAlg}}$ is a streamlined version of the language used in Section 3.D.5. It has two binary function symbols $\curlyvee, |$, two unary function symbols ${}^*, {}^{-1}$, and a constant symbol I. An $\mathcal{L}_{\mathrm{RlnAlg}}$-structure $(B, \curlyvee, |, {}^*, {}^{-1}, I)$

is a **relation algebra** if it satisfies the following identities:

$$x \curlyvee y = y \curlyvee x \tag{R1}$$

$$x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z \tag{R2}$$

$$(x^* \curlyvee y^*)^* \curlyvee (x^* \curlyvee y)^* = x \tag{R3}$$

$$x \mid (y \mid z) = (x \mid y) \mid z \tag{R4}$$

$$x \mid I = x \tag{R5}$$

$$(x^{-1})^{-1} = x \tag{R6}$$

$$(x \mid y)^{-1} = y^{-1} \mid x^{-1} \tag{R7}$$

$$(x \curlyvee y) \mid z = (x \mid z) \curlyvee (y \mid z) \tag{R8}$$

$$(x \curlyvee y)^{-1} = x^{-1} \curlyvee y^{-1} \tag{R9}$$

$$(x^{-1} \mid (x \mid y)^*) \curlyvee y^* = y^*. \tag{R10}$$

If B has at least two elements, by Theorem 7.67 R1, R2, and R3 imply that every relation algebra is a Boolean algebra $(B, \curlyvee, \curlywedge, {}^*, \mathbf{0}, \mathbf{1})$, with $a \curlywedge b = (a^* \curlyvee b^*)^*$, $\mathbf{0} = \mathbf{1}^*$ and $\mathbf{0} = I \curlyvee I^*$. So a relation algebra with at least two elements is a Boolean algebra with two additional operations $\mid$ and ${}^{-1}$, and a chosen element I.

Every $(\mathscr{P}(M \times M), \cup, |, {}^{\complement}, {}^{-1}, \mathrm{id})$ is a relation algebra (for R4–R9 see Table 2 on page 48, and for R10 see Proposition 3.15).

Exercises

Exercise 7.68. Let $f\colon (P, \leq_P) \to (Q, \leq_Q)$ be an isomorphism of orders. Show that:

(i) the map $\mathscr{P}(P) \to \mathscr{P}(Q)$, $X \mapsto f[X]$ sends initial/final segments to initial/final segments and therefore $(\mathrm{Down}(P), \subseteq) \cong (\mathrm{Down}(Q), \subseteq)$ and $(\mathrm{Up}(P), \subseteq) \cong (\mathrm{Up}(Q), \subseteq)$.

(ii) If $a \in P$ then $f \restriction \operatorname{pred} a\colon (\operatorname{pred} a, \leq_P) \to (\operatorname{pred} f(a), \leq_Q)$ is an isomorphism.

Exercise 7.69. (i) Show that the set of maximal elements and the set of minimal elements are definable in the language $\mathcal{L}_{\mathrm{ORDR}}$.

(ii) Give an example of an order with more than one maximal element, and one with a unique maximal element, which is not the maximum.

Exercise 7.70. Show that if $f\colon L \to L'$ is an embedding between complete lattices, then f preserves sups if and only if it preserves infs.

Exercise 7.71. Let $(P, \leq)$ be an ordered set and let $A \subseteq P$. Show that

(i) if $a = \curlyvee A$ then $\{a\}^{\blacktriangledown} = \bigcap_{x \in A} \{x\}^{\blacktriangledown}$ and if $a = \curlywedge A$ then $\{a\}^{\blacktriangle} = \bigcap_{x \in A} \{x\}^{\blacktriangle}$;

(ii) if $A_i \subseteq P$ for $i \in I$, then $(\bigcup_{i \in I} A_i)^{\blacktriangledown} = \bigcap_{i \in I} A_i^{\blacktriangledown}$ and $(\bigcup_{i \in I} A_i)^{\blacktriangle} = \bigcap_{i \in I} A_i^{\blacktriangle}$.

Exercise 7.72. Let P be an ordered set and let $i \colon P \to \mathbf{DM}(P)$ be its completion. Show that:

(i) P is the maximum of $\mathbf{DM}(P)$, and if $\mathbf{1}_P$ is the maximum of P, then $i(\mathbf{1}_P) = {\downarrow}\mathbf{1}_P = P$. If P has minimum $\mathbf{0}_P$ then $i(\mathbf{0}_P) = \{\mathbf{0}_P\}$ is the minimum of $\mathbf{DM}(P)$; the empty set $\emptyset$ belongs to $\mathbf{DM}(P)$ if and only if P has no minimum, and in that case $\emptyset$ is the minimum of $\mathbf{DM}(P)$.

(ii) P is a linear order if and only if $\mathbf{DM}(P)$ is a linear order.

(iii) If $p = \sup \operatorname{pred} p$ then $(\operatorname{pred} p)^{\blacktriangledown\blacktriangle} = ({\downarrow}p)^{\blacktriangledown\blacktriangle} = {\downarrow}p$.

Exercise 7.73. Let $(P, \leq)$ be an ordered set. Show that

$$\mathbf{DM}(P^{\vartriangle}) = \{A \subseteq P \mid A^{\blacktriangle\blacktriangledown} = A\} = \mathbf{DM}(P)^{\vartriangle}.$$

Exercise 7.74. Let $(P, \leq)$ be a preorder with the downward topology $\mathcal{T} = \operatorname{Down}(P)$. Show that:

(i) $\mathcal{T}$ is T_0 if and only if $\leq$ is antisymmetric;

(ii) $\mathcal{T}$ is T_2 if and only if it is T_1 if and only if $\leq$ is free on P, that is $\forall x, y \in P\, (x \leq y \Leftrightarrow x = y)$;

(iii) the closure of $X \subseteq P$ is ${\uparrow}X$.

Exercise 7.75. Show that if P, Q, R are ordered sets and $f \colon P \to Q$ and $g \colon Q \to R$ are residuated, then $g \circ f \colon P \to R$ is residuated and $(g \circ f)^* = f^* \circ g^*$.

Exercise 7.76. Suppose $\mathcal{C} \subseteq \mathscr{P}(A)$ is a family of sets closed under arbitrary intersections such that $A \in \mathcal{C}$. Show that there is a closure operator f on A such that $\mathcal{C} = \operatorname{ran} f$.

Exercise 7.77. Compute the Dedekind-McNeille completion of all ordered sets of size ≤ 5.

Exercise 7.78. Let $f \colon L \to L'$ with L and L' lattices. Show that:

(i) f is monotone if and only if $\forall a, b \in L\, (f(a \curlyvee b) \geq f(a) \curlyvee f(b))$ if and only if $\forall a, b \in L\, (f(a \curlywedge b) \leq f(a) \curlywedge f(b))$.

(ii) f is an isomorphism of ordered sets if and only if it is an isomorphism of lattices.

Exercise 7.79. Show that if V is a vector space of dimension n over a field $\Bbbk$, the set $L = \{W \subseteq V \mid W \text{ vector subspace of } V\}$, ordered under inclusion, is a complemented modular lattice, but it is not distributive when $n > 1$.

Exercise 7.80. Let T be a triangle in the plane with sides a, b and c. Show that the lattice of sets generated by a, b, c is isomorphic to $\mathrm{Free}_{\mathbf{D}}(3)$.

Exercise 7.81. In the lattice of linear subspaces of $\mathbb{R}^3$, consider the lines a, b, c and d generated by the vectors $(1, 0, 1)$, $(0, 1, 1)$, $(0, 0, 1)$ and $(1, 1, 1)$. Show that the sublattice generated by a, b, c, d is infinite. Conclude that $\mathrm{Free}_{\mathbf{M}}(4)$ is infinite.

Exercise 7.82. Fix a decreasing sequence of positive real numbers a_n such that $\lim_{n\to\infty} a_n = 0$ and $\sum_{n=0}^{\infty} a_n = +\infty$, and let $I = \{S \subseteq \mathbb{N} \mid \sum_{n\in S} a_n < \infty\}$. Show that:

(i) I is a non-principal ideal,

(ii) $\mathrm{Fin} \subseteq I$,

(iii) the projection of I on $\mathscr{P}(\mathbb{N})/\mathrm{Fin}$ is the ideal $\{[S] \mid \sum_{n\in S} a_n < \infty\}$,

(iv) the density-zero sets form a proper, non-principal ideal of $\mathscr{P}(\mathbb{N})$. (A subset X of $\mathbb{N}$ has density 0 if $\lim_{n\to\infty} \frac{|X\cap\{0,\dots,n\}|}{n} = 0$.)

Exercise 7.83. Show that the following hold in any Boolean algebra:

(i) $x = y \Leftrightarrow x + y = \mathbf{0}$;

(ii) $x + y = (x \curlyvee y) \curlywedge (x \curlywedge y)^*$;

(iii) $(x + y)^* = (x \curlywedge y) \curlyvee (x^* \curlywedge y^*)$;

(iv) $x \curlywedge y = \mathbf{0} \Rightarrow x + y = x \curlyvee y$;

(v) $x \curlyvee y = (x + y) + (x \curlywedge y)$;

(vi) $x + (y + z) = (x + y) + z$;

(vii) $x \curlywedge (y + z) = (x \curlywedge y) + (x \curlywedge z)$.

Exercise 7.84. Let B be a Boolean algebra. Show that I is an ideal in the sense of Definition 7.40 if and only if it is an ideal in the sense of rings.

Exercise 7.85. Show that Boolean algebras are finitely axiomatizable in the language $\mathcal{L}_{\mathrm{ORDR}}$.

Exercise 7.86. Let $\preccurlyeq$ be the divisibility relation[4] on the natural numbers, that is $m \preccurlyeq n \Leftrightarrow \exists k\,(km = n)$. Let $\mathrm{Div}(n) = \{m \in \mathbb{N} \mid m \preccurlyeq n\}$ be the set of the divisors of n.

Show that:

(i) $\mathrm{Div}(0) = \mathbb{N}$ and $(\mathrm{Div}(n), \preccurlyeq)$ is a distributive lattice with minimum 1 and maximum n.

[4] We use the symbol $\preccurlyeq$ rather than $|$, already used in Section 2.C to stress that we are working with a partial order.

(ii) $a \preccurlyeq b \Leftrightarrow \mathrm{Div}(a) \subseteq \mathrm{Div}(b)$, and in this case $\mathrm{Div}(a)$ is a sublattice of $\mathrm{Div}(b)$.

(iii) If $a = p_1^{k_1} \cdots p_n^{k_n}$ and $b = q_1^{k_1} \cdots q_m^{k_m}$ with distinct primes $p_1, \dots, p_n$ and $q_1, \dots, q_m$ with $1 \leq k_1 \leq \cdots \leq k_n$ and $1 \leq h_1 \leq \cdots \leq h_m$, then $\mathrm{Div}(a) \cong \mathrm{Div}(b)$ if and only if $n = m$ and $k_i = h_i$.

(iv) $\mathrm{Div}(n) \cong \mathrm{Sgr}(\mathbb{Z}/n\mathbb{Z})^{\Delta}$, where $\mathrm{Sgr}(\mathbb{Z}/n\mathbb{Z})$ is the lattice of subgroups of $\mathbb{Z}/n\mathbb{Z}$.

(v) If $n > 1$ is square-free, then $\mathrm{Div}(n)$ is a Boolean algebra.

Exercise 7.87. Show that:

(i) if L is a (distributive) lattice and $a \in L$, then $\downarrow a$ is a (distributive) lattice, and similarly for $\uparrow a$;

(ii) if B is a Boolean algebra and $a \neq \mathbf{0}$, then $\downarrow a$ is a Boolean algebra and it is isomorphic to $\uparrow a^*$. In particular, if $a \in B \setminus \{\mathbf{0}, \mathbf{1}\}$ then B is isomorphic to the product $(\downarrow a) \times (\downarrow a^*)$.

(iii) If $f \colon B \to C$ is a morphism of Boolean algebras, then $f \restriction \downarrow b \colon \downarrow b \to \downarrow f(b)$ is a morphism of Boolean algebras.

(iv) If $f \colon B \to C$ is a morphism of Boolean algebras such that $\ker(f)$ is principal, say $\ker(f) = \downarrow b$, then b^* is the largest $a \in B$ such that $f \restriction \downarrow a$ is injective.

Exercise 7.88. Show that $\mathscr{P}(A)$ and $\mathscr{P}(B)$ are isomorphic Boolean algebras if and only if A and B are in bijection.

Exercise 7.89. Let $B \subseteq \mathscr{P}(X)$ and $C \subseteq \mathscr{P}(Y)$ be algebras of sets, and suppose that $X \cap Y = \emptyset$. Show that $B \times C$ is isomorphic to $\{b \cup c \mid b \in B \wedge c \in C\} \subseteq \mathscr{P}(X \cup Y)$.

Exercise 7.90. If $(B, +, \cdot, 0, 1)$ is a Boolean ring, define $x \curlywedge y \overset{\text{def}}{=} x \cdot y$, $x \curlyvee y \overset{\text{def}}{=} x + y + x \cdot y$, and $x^* \overset{\text{def}}{=} 1 + x$. Show that:

(i) $\forall x \in B\, (x + x = 0)$;

(ii) B is a commutative ring;

(iii) $(B, \curlywedge, \curlyvee, {}^*, 0, 1)$ is a Boolean algebra.

Check that the correspondence $(B, +, \cdot, 0, 1) \mapsto (B, \curlyvee, \curlywedge, {}^*, 0, 1)$ between Boolean rings and Boolean algebras is the inverse of the correspondence (7.7).

Exercise 7.91. Let $(R, +, \cdot, 0, 1)$ be a (not necessarily commutative) ring with unit, and let $\bar{R} = \{x \in R \mid x^2 = x \text{ and } \forall y \in R\, (x \cdot y = y \cdot x)\}$. (An element in a ring such that $x^2 = x$ is called an idempotent.) Define

$$x \oplus y = x + y - 2x \cdot y.$$

Show that $(\bar{R}, \oplus, \cdot, 0, 1)$ is a Boolean ring.

Exercise 7.92. Let $(B, \curlywedge, {}^*, \mathbf{0})$ be a structure such that $\curlywedge$ is a binary operation that is commutative, associative and idempotent, while * is a unary operation such that

$$x \curlywedge y^* \eqcirc \mathbf{0} \Leftrightarrow x \curlywedge y \eqcirc x. \tag{7.14}$$

Suppose also that $\mathbf{0} \neq \mathbf{0}^*$. Define $\mathbf{1} \overset{\text{def}}{=} \mathbf{0}^*$, $x \leq y \Leftrightarrow x \curlywedge y \eqcirc x$ and $x \curlyvee y \overset{\text{def}}{=} (x^* \curlywedge y^*)^*$.

Show that:

(i) $x \curlywedge x^* \eqcirc \mathbf{0}$;

(ii) $\leq$ is an ordering on B, $x \curlywedge y \leq x$ and $x \curlywedge y \leq y$ for all x, y. Moreover $\mathbf{0}$ is least and $x \leq y \Leftrightarrow x \curlywedge y^* \eqcirc \mathbf{0}$ for all x, y;

(iii) $x^{**} \eqcirc x$, hence the function $x \mapsto x^*$ is a bijection of B. Moreover $\curlyvee$ is idempotent and $x \curlyvee x^* \eqcirc \mathbf{1}$;

(iv) $x \curlywedge y \eqcirc (x^* \curlyvee y^*)^*$ and $\curlyvee$ is associative, $x \curlyvee (y \curlyvee z) \eqcirc (x \curlyvee y) \curlyvee z$;

(v) $x \leq y \Leftrightarrow y^* \leq x^* \Leftrightarrow x \curlyvee y \eqcirc y$;

(vi) if $x \leq y$ then $x \curlywedge z \leq y \curlywedge z$ and $x \curlyvee z \leq y \curlyvee z$. In particular: if $x \leq y, z$ then $x \leq y \curlywedge z$ and if $x, y \leq z$ then $x \curlyvee y \leq z$;

(vii) $x \curlywedge (x^* \curlyvee y) \eqcirc x \curlywedge y$ and $x \curlyvee (x^* \curlywedge y) \eqcirc x \curlyvee y$;

(viii) the absorption laws (4.6) $(x \curlyvee y) \curlywedge y \eqcirc y$ and $(x \curlywedge y) \curlyvee y \eqcirc y$ hold;

(ix) the distributive laws (4.7)$(x \curlyvee y) \curlywedge z \eqcirc (x \curlywedge z) \curlyvee (y \curlywedge z)$ and $(x \curlywedge y) \curlyvee z \eqcirc (x \curlyvee z) \curlywedge (y \curlyvee z)$ hold.

Conclude that B is a Boolean algebra.

Exercise 7.93. (i) Show that the ring $\mathbb{Z}/2\mathbb{Z}$ with the operations

$$a \curlyvee b = a + b, \quad a \curlywedge b = a \cdot b, \quad a^* = a + 1$$

satisfies every axiom of T_{BOOLE} except (4.7b). Modify this example and find a model for T_{BOOLE} minus (4.7a), one for T_{BOOLE} minus (7.5a), and one for T_{BOOLE} minus (7.5b).

(ii) Show that (7.6b) and (7.6a) are logically equivalent modulo the other axioms of T_{BOOLE}.

Exercise 7.94. If L is a lattice, the set of $\curlyvee$-irreducible elements is $\mathfrak{J}(L) = \{x \in L \setminus \{\mathbf{0}\} \mid \forall y, z\, (x = y \curlyvee z \Rightarrow x = y \vee x = z)\}$. Show that

(i) if L is finite $a \nleq b$, then $\exists x \in \mathfrak{J}(L)\, (x \leq a \wedge x \nleq b)$;

(ii) if L is finite, then $a = \sup \{x \in \mathfrak{J}(L) \mid x \leq a\}$, for all $a \in L$;

(iii) if L is distributive, $x \in \mathfrak{J}(L)$ if and only if for all $a_1, \ldots, a_n \in L$, if $x \leq a_1 \curlyvee \ldots \curlyvee a_n$ then $x \leq a_i$ for some $1 \leq i \leq n$.

Exercise 7.95. Let $(P, \leq)$ is a finite order, and let $\mathrm{Down}(P)$ be the lattice of its initial segments (Example 7.10(a)). Show that $\downarrow x \in \mathfrak{J}(\mathrm{Down}(P))$ and that the function $P \to \mathfrak{J}(\mathrm{Down}(P))$, $x \mapsto \downarrow x$, is an order isomorphism.

Exercise 7.96. Show that in a finite distributive lattice the function $L \to \mathrm{Down}(\mathfrak{J}(L))$, $x \mapsto \{y \in \mathfrak{J}(L) \mid y \leq x\}$ is an isomorphism. In other words: finite distributive lattices are, up to isomorphism, lattices of sets.

Exercise 7.97. Suppose $\mathcal{A}$ is an atomic subalgebra of $\mathscr{P}(X)$ for some X. Show that if $\mathcal{A}$ is a finite, then $\mathrm{At}(\mathcal{A})$ is a partition of X, but this may fail if $\mathcal{A}$ is infinite.

Exercise 7.98. Show that

(i) a Boolean algebra is atomless if and only if it is dense as an ordered set,

(ii) if $(L, \leq)$ is a dense linear order, then the algebra of intervals is atomless.

Exercise 7.99. Show that two sets A and B are in bijection if and only if the Boolean algebras $\mathscr{P}(A)$ and $\mathscr{P}(B)$ are isomorphic. (Note that it is consistent with the axioms of set theory that there are infinite sets A and B that are not in bijection, yet $\mathscr{P}(A)$ and $\mathscr{P}(B)$ are in bijection.)

Exercise 7.100. Let $\subseteq^*$ be the preorder on $\mathscr{P}(\mathbb{N})$ given by $A \subseteq^* B$ if and only if $A \setminus B$ is finite, let $=^*$ be the induced equivalence relation, and let $\subset^*$ be its strict part. Show that

(i) If $A_0 \subset^* A_1 \subset^* A_2 \subset^* \ldots$ is an $\subset^*$-increasing chain, then there is $B \neq^* \mathbb{N}$ such that $\forall n \in \mathbb{N}(A_n \subset^* B)$.

(ii) If $A_n, B_n \subseteq \mathbb{N}$ are such that $n < m \Rightarrow A_n \subset^* A_m \subset^* B_m \subset^* B_n$, then there is $C \subseteq \mathbb{N}$ such that $\forall n \in \mathbb{N}\,(A_n \subseteq^* C \subseteq^* B_n)$.

Exercise 7.101. Let B be a Boolean algebra. Show that:

(i) If $X \subseteq B$ then
$$\bigcap\{F \mid F \supseteq X \text{ and } F \text{ is a filter}\} = \uparrow(X^{\curlywedge})$$
is the smallest filter containing X. It is called the **filter generated** by X.

(ii) For $X \subseteq B$, the filter generated by X is proper if and only if $\mathbf{0} \notin X^{\curlywedge}$.

(iii) If $f \colon B \to \{\mathbf{0}, \mathbf{1}\}$ is a surjective homomorphism of Boolean algebras, then $\ker(f)$ is a maximal ideal.

(iv) The filter generated by $\{a\}$ is an ultrafilter if and only if a is an atom.

Exercise 7.102. Let B be a Boolean algebra. For $D \subseteq B$ let $D^* = \{d^* \mid d \in D\}$. Show that
$$\forall b \in B \setminus \{\mathbf{0}\}\, \exists d \in D\, (\mathbf{0} < d \leq b) \Leftrightarrow \forall b \in B \setminus \{\mathbf{1}\}\, \exists d \in D^*\, (b \leq d < \mathbf{1}).$$

In other words $D \cap B^+$ is dense in B^+ with the downward topology if and only if $D^* \cap B^-$ is dense in $B^- \overset{\text{def}}{=} B \setminus \{\mathbf{1}\}$ with the upward topology.

Exercise 7.103. Suppose F is a filter on a set $X \neq \emptyset$. Show that:

(i) If F is an ultrafilter then: F is not principal if and only if $\{a\} \notin F$ for all $a \in X$, if and only if F extends $\{A \subseteq X \mid X \setminus A \text{ is finite}\}$, the filter of co-finite sets.

(ii) If $Y \in F$ then $F \restriction Y \overset{\text{def}}{=} F \cap \mathscr{P}(Y)$ is a filter on Y. Moreover, F is an ultrafilter on X if and only if $F \restriction Y$ is an ultrafilter on Y.

(iii) If $g \colon X \to Y$ then $g_*(F) \overset{\text{def}}{=} \{B \subseteq Y \mid g^{-1}[B] \in F\}$ is a filter on Y. Moreover, if F is an ultrafilter on X then $g_*(F)$ is an ultrafilter on Y.

(iv) If F is an ultrafilter on X and $\{X_0, \ldots, X_k\}$ is a partition of X, then there is a unique $i \leq k$ such that $X_i \in F$.

Exercise 7.104. Find a filter $\mathcal{F}$ on a set X that does not have the Fubini-Kuratowski-Ulam property.

Notes and remarks

[**DP02**] is an excellent introduction to lattices, for a complete treatise see [**Grä11**]. Part (a) of the Fixed Point Theorem 7.11 is usually attributed to Knaster and Tarski, while part (b) is from [**Tar55**]. In [**Dav55**] the converse is shown: if a monotone function in a lattice L has fixed points, then the lattice L is complete. Lattice were defined at the end of the nineteenth century by Dedekind while studying the ordering of ideals of a ring under inclusion; the notion of modular lattice stems from these studies (Example 7.E.2). The detailed analysis of $\mathrm{Free}_{\mathbf{M}}(3)$ is due to Dedekind, and dates to 1900. The size D_n of $\mathrm{Free}_{\mathbf{D}}(n)$ is called the Dedekind number of order n, and shows-up in many combinatorial questions. The values of D_n have been explicitly computed up to $n = 8$, and are:

$$1,\ 4,\ 18,\ 166,\ 7579,\ 7828352,\ 2414682040996,\ 56130437228687557907786.$$

Part (a) of Theorem 4.15 is due to Dedekind, while part (b) is due to Birkhoff.

Boolean algebras were introduced in 1847 by Boole, but the axiomatic treatment as algebraic structures satisfying certain properties is due to Huntington in 1904.

Exercise 7.92 is from [**Byr46**]—see also [**Men70**]. The binary operations $\mid$ and $\uparrow$ described in Section 7.L are the algebraic counterparts of the connectives of Sheffer and Peirce of Exercise 3.47. For an encyclopedic treatise on Boolean algebras see the three volume opus [**Kop89, MB89a, MB89b**]. In particular, Koppelberg's paper in the first volume is an excellent introduction to the subject.

The results presented in Section 7.L are taken from [**MVF$^+$02**], a paper we refer the reader to for proofs, historical background, and bibliographical references. The result in Exercise 7.96 is known as representation theorem for distributive lattices, and it is due to Birkhoff.

8. Computability

Certain tasks in mathematics can be performed in a mechanical way, following a prescribed protocol, while other tasks require new ideas. For example:

proving a new (non-trivial) result requires ingenuity, while *checking* that a certain argument is indeed a proof of the result in question is just a matter of patience and careful proofreading.[5] An effective procedure is a protocol that can be mechanically performed by some agent: the *input* can be finite objects (natural numbers, finite graphs, integers, ...) and by following such protocol (a finite set of instructions) a finite object will be produced as *output* in a finite number of steps. In other words: an effective procedure can be implemented as a computer program. For example, given a first-order language with finitely many non-logical symbols, there is an effective procedure to check whether a finite string of symbols is a term or a formula. Similarly, there is an effective procedure to check whether a $\mathcal{L}_{\text{RINGS}}$-sentence is an axiom of the theory ACF_0 of all algebraically closed fields of zero characteristic.

Since finite objects can be coded in arithmetic, we start with studying *effective* procedures on natural numbers. In twenties of the last century, several mathematically precise definitions of "effective function" were introduced, and all these definitions singled-out the same class of functions. In this section *operation* stands for *k-ary function on the natural numbers*, that is a map of the form $f\colon \mathbb{N}^k \to \mathbb{N}$, with the understanding that a 0-ary function is simply a natural number.

Many of the usual operations are effective, and a quick inspection is usually enough to convince oneself of this fact. This naïve approach can yield wrong results (see the Remarks 8.1 below) and shows its limits when we need to prove that a certain function is *not* computable. In this case the need for a rigorous definition becomes unavoidable. The definition of **computable function** is the formal counterpart of the informal notion of effective function. In the next sections we will look at two subclasses of the computable functions: the **elementary computable functions** and the **primitive recursive functions**.

Remarks 8.1. (a) Some functions are computable, even if at first sight one might think otherwise. For example, the constant functions are computable under any reasonable notion of computation, hence the unary function

$$f(n) = \begin{cases} 1 & \text{if P holds,} \\ 0 & \text{otherwise,} \end{cases}$$

is computable, where P is some open problem in mathematics, for example one of those number theory conjectures seen in Exercise 2.11 of Chapter I. In other words we know that the algorithm that computes f is one of two algorithms, but it is not known which of the two is

[5] We are under the rather optimistic assumption that the proof be clearly written and that all steps have been fully explicated.

the correct one. The situation is, to some extent, similar to that of Example 2.8 of Chapter I.

Another example is Ramsey's function $R\colon \mathbb{N} \to \mathbb{N}$ introduced on page 262, assigning to each n the least m such that for all 2-coloring of the complete graph K_m has a monochromatic subgraph isomorphic to K_n (Theorem 10.8). Although R is computable, the exact value of $R(n)$ for $n \geq 5$ is unknown.

(b) In order to show that $f\colon \mathbb{N}^2 \to \mathbb{N}$ is computable, it would seem enough to check that for each k the function $f_k\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto f(k,n)$, is computable and then argue as follows: given (k,n) fix an algorithm for f_k and use it to compute $f_k(n)$. However, this argument is not correct, since we must ensure the computability of the procedure assigning to each k the algorithm for f_k. For example, if $g\colon \mathbb{N} \to \mathbb{N}$ is not computable and $f(k,n) = g(k)$, then f_k is constant and hence computable, but the function f is not.

(c) In most cases, it is routine to check whether a certain set of integers is computable, but there are exceptions. Woods conjectured in [**Woo81**] that for all k and all a there is $i \leq k$ such that $a+i$ is coprime with a and with $a+k$, but soon after he found a counterexample: $k = 16$ and $a = 2184$. (In fact this is the least such counterexample.) We say that k is an **Erdős-Woods number** if it is a counterexample to Woods' conjecture, that is if there is a natural number a such that each of $a, a{+}1, \dots, a{+}k$ has a common factor with a or $a{+}k$. The set of all Erdős-Woods numbers is infinite [**Dow89**], and it is computable [**CHR03**], but proving this is far from trivial.

8.A. Elementary computable functions. Addition, multiplication, the distance between numbers $|x-y|$, and (the integer part of) division

$$\lfloor x/y \rfloor = \begin{cases} \text{the largest } k \text{ such that } y \cdot k \leq x & \text{if } y \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

are effective functions. Certain constructions yield new effective operations from old ones.

Definition 8.2. (i) Suppose that f be k-ary and that $g_0, \dots, g_{k-1}$ are n-ary. The **composition** of f with $g_0, \dots, g_{k-1}$ is the map $h\colon \mathbb{N}^n \to \mathbb{N}$

$$h(x_0, \dots, x_{n-1}) = f(g_0(x_0, \dots, x_{n-1}), \dots, g_{k-1}(x_0, \dots, x_{n-1})).$$

(ii) If f is $k+1$-ary, the **generalized sum of** f and the **generalized product on** f are the $k+1$-ary functions

$$\begin{aligned}\textstyle\sum f(x_0,\dots,x_{k-1},x_k) &= \sum_{y<x_k} f(x_0,\dots,x_{k-1},y),\\ \textstyle\prod f(x_0,\dots,x_{k-1},x_k) &= \prod_{y<x_k} f(x_0,\dots,x_{k-1},y),\end{aligned}$$

where $\sum f(x_0,\dots,x_{k-1},0)=0$ and $\prod f(x_0,\dots,x_{k-1},0)=1$.

The definition of composition might seem a bit too restrictive, as one might want g_is to be of different arity, or that the order of the variables in the g_is be different. The **projection functions** I^n_k, with $k<n$

$$I^n_k\colon \mathbb{N}^n \to \mathbb{N}, \quad (x_0,\dots,x_{n-1}) \mapsto x_k,$$

can be used to fix this problem. For example, the 3-ary function

$$h(x_0,x_1,x_2) = f(g_0(x_1,x_2), g_1(x_0), g_2(x_1,x_0,x_0))$$

is the composition of f with $\tilde{g}_0$, $\tilde{g}_1$ and $\tilde{g}_2$, where

$$\begin{aligned}\tilde{g}_0(\vec{x}) &= g_0(I^3_1(\vec{x}), I^3_2(\vec{x}))\\ \tilde{g}_1(\vec{x}) &= g_1(I^3_0(\vec{x}))\\ \tilde{g}_2(\vec{x}) &= g_2(I^3_1(\vec{x}), I^3_0(\vec{x}), I^3_0(\vec{x})).\end{aligned}$$

Here and below $\vec{x}$ is a typographical abbreviation of x_0, x_1, x_2, or more generally $x_0,\dots,x_{n-1}$ or even the n-tuple $(x_0,\dots,x_{n-1})$, if clear from the context.

Definition 8.3. The family $\mathcal{E}$ of **elementary computable functions** is the smallest class of functions containing addition, multiplication, the distance between numbers, the (integer part of) division, and the projections, and closed under composition and generalized sums and products.

Lemma 8.4. *The following functions are in $\mathcal{E}$:*

- $C_k\colon \mathbb{N}\to\mathbb{N}$, $n\mapsto k$;
- $\mathrm{sgn}\colon \mathbb{N}\to\mathbb{N}$ *mapping* 0 *to* 0, *and everything else to* 1; *the function* $\overline{\mathrm{sgn}}(n) = 1-\mathrm{sgn}(n)$;
- $S(n)=n+1$, *and* $x\mapsto x \dot{-} 1$, *where* $0\dot{-}1=0$ *and* $n\dot{-}1=n-1$ *if* $n>0$;
- *the exponential and the factorial.*

Proof. Note that

$$\begin{array}{lll} C_0(x) = |x - x| & \overline{\mathrm{sgn}}(x) = \prod_{y<x} C_0(y) & \mathrm{sgn} = \overline{\mathrm{sgn}} \circ \overline{\mathrm{sgn}} \\ C_1 = \overline{\mathrm{sgn}} \circ C_0 & C_{m+1} = C_m + C_1 & S(x) = x + C_1 \\ x^y = \prod_{z<y} x & x! = \prod_{z<x} S(z) & x \dot{-} 1 = |x - C_1(x)| \cdot \mathrm{sgn}(x). \end{array}$$ □

Following standard practice in mathematical logic $A(x_0, \dots, x_{n-1})$ stands for $(x_0, \dots, x_{n-1}) \in A$ and we say that $A \subseteq \mathbb{N}^k$ is a k-ary predicate. For example the binary predicates $x = y$, $x \leq y$, ... denote the sets $\{(x,y) \in \mathbb{N}^2 \mid x = y\}$, $\{(x,y) \in \mathbb{N}^2 \mid x \leq y\}$, ... We say that $A \subseteq \mathbb{N}^k$ is an **elementary computable set** or, equivalently, it is a k-ary **elementary computable predicate** if its characteristic function $\boldsymbol{\chi}_A^{\mathbb{N}^k} : \mathbb{N}^k \to \{0,1\}$ belongs to $\boldsymbol{\mathcal{E}}$. More generally: if $\mathcal{F}$ is a family of functions, we will say that A is in $\mathcal{F}$ or, equivalently, that it is an $\mathcal{F}$-predicate if $\boldsymbol{\chi}_A \in \mathcal{F}$.

Lemma 8.5. *Suppose $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ is closed under composition, generalized sums and products. If a k-ary function f is in $\mathcal{F}$ then* $\mathrm{Gr}(f)$ *of is a $k+1$-ary $\mathcal{F}$-predicate.*

Proof. $\boldsymbol{\chi}_{\mathrm{Gr}(f)}(n_1, \dots, n_k, m) = \overline{\mathrm{sgn}}(|f(n_1, \dots, n_k) - m|)$. □

The converse of Lemma 8.5 is not true, as there are non-elementary functions whose graph is elementary (Proposition 8.33).

Examples 8.6. Let $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ be closed under compositions, generalized sums and products.

(A) If $A(x_1, \dots, x_m)$ is an $\mathcal{F}$-predicate and $f_1, \dots, f_m \in \mathcal{F}$ are k-ary, then $A(f_1(x_1, \dots, x_k), \dots, f_m(x_1, \dots, x_k))$ is a k-ary $\mathcal{F}$-predicate, since its characteristic function is $\boldsymbol{\chi}_A(f_1(x_1, \dots, x_k), \dots, f_m(x_1, \dots, x_k))$.

(B) If $A, B \subseteq \mathbb{N}^n$ are $\mathcal{F}$-predicates, then $\neg A \overset{\text{def}}{=} A^{\complement} = \mathbb{N}^n \setminus A$ and $A \wedge B \overset{\text{def}}{=} A \cap B$ are $\mathcal{F}$-predicates, since $\boldsymbol{\chi}_{\neg A} = \overline{\mathrm{sgn}} \circ \boldsymbol{\chi}_A$ and $\boldsymbol{\chi}_{A \cap B} = \boldsymbol{\chi}_A \cdot \boldsymbol{\chi}_B$. Thus also $A \vee B \overset{\text{def}}{=} A \cup B$, $A \setminus B$, and $A \triangle B$ are $\mathcal{F}$-predicates. The predicates $A \Rightarrow B$ and $A \Leftrightarrow B$ are simply the sets $\neg A \cup B$ and $(\neg A \cup B) \cap (\neg B \cup A)$ respectively, and hence these are also $\mathcal{F}$-predicates. Thus the family of subsets of $\mathbb{N}^k$ whose characteristic functions belong to $\mathcal{F}$ is a Boolean algebra.

(C) $x < y$ is in $\mathcal{F}$, as its characteristic function is $\overline{\mathrm{sgn}}\lfloor S(x)/S(y) \rfloor$. Thus by (A) and (B) are $\mathcal{F}$-predicates:
- $x \leq y$, since it is equivalent to $\neg(y < x)$,
- $x = y$, since it is equivalent to $x \leq y \wedge y \leq x$,
- $x \neq y$.

(D) If $\{A_1, \ldots, A_k\}$ is a partition of $\mathbb{N}^n$ and the A_is are in $\mathcal{F}$, and if $g_1, \ldots, g_k \in \mathcal{F}$ are n-ary functions, then the function $f \colon \mathbb{N}^n \to \mathbb{N}$ defined by

$$f(\vec{x}) = \begin{cases} g_1(\vec{x}) & \text{if } \vec{x} \in A_1, \\ g_2(\vec{x}) & \text{if } \vec{x} \in A_2, \\ \vdots & \\ g_k(\vec{x}) & \text{if } \vec{x} \in A_k, \end{cases}$$

is in $\mathcal{F}$, since $f(\vec{x}) = g_1(\vec{x}) \cdot \boldsymbol{\chi}_{A_1}(\vec{x}) + \cdots + g_k(\vec{x}) \cdot \boldsymbol{\chi}_{A_k}(\vec{x})$.

(E) If $A \subseteq \mathbb{N}^{n+1}$ is in $\mathcal{F}$ then so is

$$\forall z < y\, A(\vec{x}, z) \stackrel{\text{def}}{=} \{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \forall z\, (z < y \Rightarrow A(\vec{x}, z))\}$$

as its characteristic function is $\prod_{k<y} \boldsymbol{\chi}_A(\vec{x}, k)$. Thus also

$$\begin{aligned} \exists z < y\, A(\vec{x}, z) &\stackrel{\text{def}}{=} \{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \exists z\, (z < y \wedge A(\vec{x}, z))\} \\ &= \neg\{(\vec{x}, y) \in \mathbb{N}^{n+1} \mid \forall z\, (z < y \Rightarrow \neg A(\vec{x}, z))\} \end{aligned}$$

is in $\mathcal{F}$. Similarly $\forall z \leq y\, A(\vec{x}, z)$ and $\exists z \leq y\, A(\vec{x}, z)$ are in $\mathcal{F}$. The predicates

$$\forall z < y\, A(\vec{x}, z), \quad \exists z < y\, A(\vec{x}, z), \quad \forall z \leq y\, A(\vec{x}, z), \quad \exists z \leq y\, A(\vec{x}, z)$$

are obtained from A by **bounded quantification**.

(F) If $A \subseteq \mathbb{N}^{n+1}$ is in $\mathcal{F}$, then the $n+1$-ary function

$$\boldsymbol{\mu} z \leq y\, A(\vec{x}, z) = \begin{cases} \min\{z \leq y \mid A(\vec{x}, z)\} & \text{if this set is non-empty,} \\ y & \text{otherwise,} \end{cases}$$

is in $\mathcal{F}$. In fact $h \in \mathcal{F}$ where

$$h(\vec{x}, w) = \overline{\text{sgn}}(\textstyle\sum_{z<S(w)} \boldsymbol{\chi}_A(\vec{x}, z)) = \begin{cases} 0 & \text{if } \exists z \leq w\, A(\vec{x}, z), \\ 1 & \text{otherwise,} \end{cases}$$

and hence $\boldsymbol{\mu} z \leq y\, A(\vec{x}, z) = \sum_{w<y} h(\vec{x}, w)$ is in $\mathcal{F}$. The predicate

$$\boldsymbol{\mu} z \leq y\, A(\vec{x}, z)$$

is obtained by **bounded minimization**. If $g(\vec{y})$ is in $\mathcal{F}$, then the function $(\vec{x}, \vec{y}) \mapsto \boldsymbol{\mu} z \leq g(\vec{y})\, A(\vec{x}, z)$ is in $\mathcal{F}$.

(G) If $g \in \mathcal{F}$ is $n+1$-ary, then for all $k \in \mathbb{N}$ the $n+1$-ary function

$$f(\vec{x}, y) = \begin{cases} \min\{z \leq y \mid g(\vec{x}, z) = k\} & \text{if this set is non-empty,} \\ y & \text{otherwise,} \end{cases}$$

is in $\mathcal{F}$. In fact $f(\vec{x}, y) = \boldsymbol{\mu} z \leq y\, A(\vec{x}, z)$, where $A \subseteq \mathbb{N}^{n+1}$ is obtained from the graph of g, i.e. the set $\{(\vec{x}, y, w) \in \mathbb{N}^{n+2} \mid g(\vec{x}, y) = w\}$, by

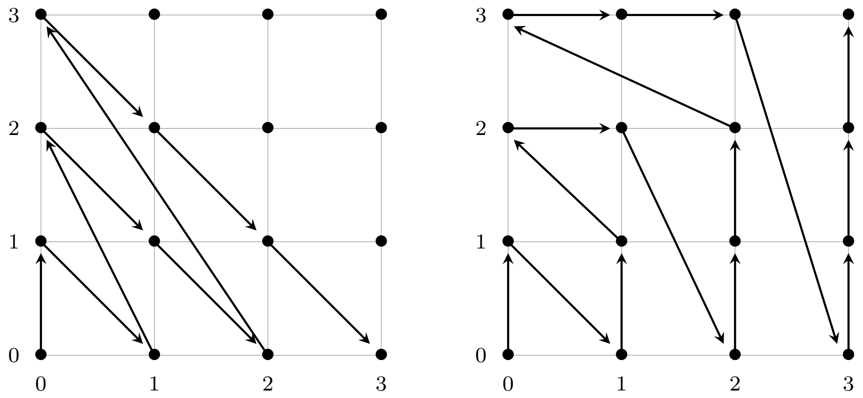


Figure 12. Triangular and square enumerations of $\mathbb{N} \times \mathbb{N}$

setting w equal to k, that is to say: putting in place of w the function $C_k(I^n_0(\vec{x}))$. The result follows from Lemma 8.5, and Example (F) above.

The following is a partial converse to Lemma 8.5.

Proposition 8.7. *Let $\mathcal{F} \supseteq \boldsymbol{\mathcal{E}}$ be a family of functions closed under composition, and generalized sums and products. Let f, g be k-ary functions such that:* $\mathrm{Gr}(f)$ *is an $\mathcal{F}$-predicate, $g \in \mathcal{F}$, and $\forall \vec{x} \in \mathbb{N}^k\, f(\vec{x}) \leq g(\vec{x})$. Then $f \in \mathcal{F}$.*

Proof. $f(\vec{x}) = \boldsymbol{\mu} y \leq g(\vec{x})\, [(\vec{x}, y) \in \mathrm{Gr}(f)]$. □

8.A.1. *Coding of sequences.* The set $\mathbb{N} \times \mathbb{N}$ is in bijection with $\mathbb{N}$, that is there is a bijection $f \colon \mathbb{N}^2 \to \mathbb{N}$ and two functions $g_0, g_1 \colon \mathbb{N} \to \mathbb{N}$ such that $f(g_0(n), g_1(n)) = n$, for all $n \in \mathbb{N}$. In fact the functions f, g_0, g_1 can be taken to be in $\boldsymbol{\mathcal{E}}$:

Examples 8.8. (A) As every nonzero natural number is of the form $2^n(2m+1)$, let $f(n, m) = 2^n(2m+1) \mathbin{\dot{-}} 1$, $g_0(n) = \lfloor \log_2(n+1) \rfloor$ and $g_1(n) = \lfloor \lfloor n + 1/2^{g_0(n)} \rfloor / 2 \rfloor \mathbin{\dot{-}} 1$.

(B) The **square enumeration** is obtained by listing the elements of $\mathbb{N}^2$ following the ordering[6]

$$(x, y) <_{\mathrm{G}} (x', y') \Leftrightarrow \big(\max(x, y) < \max(x', y') \vee \\ [\max(x, y) = \max(x', y') \wedge (x < x' \vee [x = x' \wedge y < y'])]\big).$$

(C) The **diagonal** or **triangular enumeration** is obtained by listing the elements of $\mathbb{N}^2$ according to the ordering

$$(x, y) \lhd (x', y') \Leftrightarrow x + y < x' + y' \vee [x + y = x' + y' \wedge x < x'].$$

[6] $<_{\mathrm{G}}$ is the Gödel ordering and will be used in Section 18.C.

Exercise 8.54 show that the paring functions of Examples (A), (B) and (C) are in $\boldsymbol{\mathcal{E}}$. Although all three enumerations are important, the diagonal one is the most useful. The resulting bijection is denoted by $\boldsymbol{J}\colon \mathbb{N}^2 \to \mathbb{N}$, and has a particularly simple analytical expression:

$$\boldsymbol{J}(x,y) = \frac{1}{2}(x+y)(x+y+1)+x \tag{8.1}$$

Write

$$(\cdot)_0, (\cdot)_1 \colon \mathbb{N} \to \mathbb{N} \tag{8.2}$$

for the inverse maps, defined by $\boldsymbol{J}((n)_0, (n)_1) = n$.

It is possible to code in an elementary way the set $\mathbb{N}^{<\mathbb{N}}$ of all finite sequences of natural numbers. Our goal is to find

- an elementary computable $\mathrm{Seq} \subseteq \mathbb{N}$ coding all finite sequences of natural numbers,
- an elementary computable $\ell\colon \mathbb{N} \to \mathbb{N}$ such that $\ell(m)$ is the length of the sequence coded by $m \in \mathrm{Seq}$,
- an elementary computable method for decoding $\mathrm{Seq} \times \mathbb{N} \to \mathbb{N}$, $(m,i) \mapsto (\!(m)\!)_i$, such that $(\!(m)\!)_i$ is the i-th element of the sequence coded by m, if $i < \ell(m)$.

Recalling the notation from Section 3.E, we assume that 0 codes $\langle\rangle$ the empty sequence. The number in Seq coding the sequence $\langle n_0, \dots, n_k\rangle$ is denoted by

$$\langle\!\langle n_0, \dots, n_k \rangle\!\rangle.$$

We present two methods to achieve this. The first method (Section 8.A.2) uses exponentiation and prime numbers to code sequences; the second method (Section 8.A.3) is based on elementary facts about addition and multiplication, and for this reason it is the preferred method.

8.A.2. *Coding by exponentiation and primes.* Let $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ be the function that enumerates the primes, that is $\mathbf{p}(0) = 2$, $\mathbf{p}(1) = 3$, $\mathbf{p}(2) = 5$, ... Given $n_0, \dots, n_k \in \mathbb{N}$ the number

$$m = \mathbf{p}(0)^{n_0+1}\mathbf{p}(1)^{n_1+1}\cdots\mathbf{p}(k)^{n_k+1}$$

codes the sequence $\langle n_0, \dots, n_k\rangle$. Then

$$\{n \in \mathbb{N} \mid \forall p, q \text{ primes} \,(p \mid n \land q < p \Rightarrow q \mid n)\}$$

codes $\mathbb{N}^{<\mathbb{N}}$. The functions $\mathbf{e}\colon \mathbb{N}^2 \to \mathbb{N}$ and $\mathbf{l}\colon \mathbb{N} \to \mathbb{N}$ defined by

- $\mathbf{e}(0,i) = \mathbf{e}(1,i) = 0$ and if k is the largest integer such that $\mathbf{p}(i)^{k+1} \mid n$, then $\mathbf{e}(n,i) = k$;
- $\mathbf{l}(0) = \mathbf{l}(1) = 0$ and $\mathbf{l}(n) =$ the least i such that $[\mathbf{p}(i) \nmid n]$.

yield the decoding machinery, and the length, that is $\mathbf{e}(n,i) = ((n))_i$ and $\mathbf{l}(n) = \ell(n)$.

8.A.3. *Coding by Gödel's $\boldsymbol{\beta}$ function.* Let us start with some elementary facts from number theory.

The function

$$\text{Rem}\colon \mathbb{N}^2 \to \mathbb{N} \tag{8.3}$$

defined by $\text{Rem}(n,m) =$ the remainder of the division of n by $m > 0$, and $\text{Rem}(n,0) = 0$ is elementarily computable.

Fix pairwise co-prime $1 < c_0, \dots, c_{n-1} \in \mathbb{N}$ and let $N = \prod_{i<n} c_i$. Then $\forall k\ [N \mid k \Leftrightarrow \forall i < n\,(c_i \mid k)]$ hence the map

$$\mathbb{Z}/N \to \mathbb{Z}/c_0 \times \cdots \mathbb{Z}/c_{n-1}, \quad \{0, \dots, N-1\} \ni x \mapsto (x/c_0, \dots, x/c_{n-1})$$

is an isomorphism, where x/c_i is the equivalence class of x in $\mathbb{Z}/c_i$. Therefore, for any choice of (not necessarily distinct) $a_0, \dots, a_{n-1} \in \mathbb{N}$ there is a unique $x < N$ such that $x/c_i = a_i/c_i$ for all $i < n$. We have thus proved:

Theorem 8.9 (Chinese remainder Theorem)**.** *If $1 < c_0, \dots, c_{n-1} \in \mathbb{N}$ are pairwise co-prime, then for each $a_0, \dots, a_{n-1} \in \mathbb{N}$ there is a unique $0 \leq x < \prod_{i<n} c_i$ such that $x \equiv a_i \mod c_i$ for $i < n$.*

The coding strategy will be the following: given $a_0, \dots, a_{n-1}$, choose $1 < c_0, \dots, c_{n-1}$ pairwise co-prime and such that $a_i < c_i$. By Theorem 8.9 an x can be found so that $a_i = \text{Rem}(x, c_i)$, hence the integer x encodes the string $\langle a_0, \dots, a_{n-1} \rangle$. Now for the details.

Lemma 8.10. *Let y be a positive integer such that $i \mid y$ for all $1 \leq i < n$ and let*

$$c_i = 1 + (i+1) \cdot y.$$

Then $c_0, \dots, c_{n-1}$ are pairwise co-prime.

Moreover, if $y \geq \max\{a_0, \dots, a_{n-1}\}$, where $\langle a_0, \dots, a_{n-1} \rangle \in \mathbb{N}^{<\mathbb{N}}$, then $a_i < c_i$ for all $i < n$.

Proof. Towards a contradiction suppose that p is prime such that $p \mid c_i$ and $p \mid c_j$, with $i < j < n$. Then $p \mid (c_j - c_i) = (j - i) \cdot y$ and hence $p \mid (j - i)$ or $p \mid y$. Since $j - i < n$, and by hypothesis $(j - i) \mid y$, it follows that $p \mid y$ and hence c_i is congruent modulo p to 1: a contradiction. □

Definition 8.11. $\boldsymbol{\beta}\colon \mathbb{N}^2 \to \mathbb{N}$ is the map

$$\boldsymbol{\beta}(m,i) = \text{Rem}((m)_0, 1 + (i+1) \cdot (m)_1).$$

The following is consequence of Lemma 8.10:

Lemma 8.12 (Gödel)**.** *For every $n > 0$ and every $\langle a_0, \dots, a_{n-1} \rangle \in \mathbb{N}^{<\mathbb{N}}$ there is m such that $\boldsymbol{\beta}(m,i) = a_i$, for $i < n$.*

Proof. Let $y > a_0, \dots, a_{n-1}$ be such that $i \mid y$ for all $i < n$. By Lemma 8.10 the numbers $c_i \overset{\text{def}}{=} 1 + (i+1) \cdot y$ are pairwise coprime. By the Chinese remainder theorem there is $x < \prod_{i<n} c_i$ such that $x \equiv a_i \mod c_i$ for $i < n$. Let $m = \boldsymbol{J}(x, y)$. Then

$$\boldsymbol{\beta}(m, i) = \mathrm{Rem}(x, 1 + (i+1) \cdot y) = \mathrm{Rem}(x, c_i) = a_i. \qquad \square$$

Given $a_0, \dots, a_{n-1}$ set

$$\text{(8.4)} \quad \langle\!\langle a_0, \dots, a_{n-1} \rangle\!\rangle = \text{the least } m \text{ such that}$$
$$\boldsymbol{\beta}(m, 0) = n \land \forall i < n\, (\boldsymbol{\beta}(m, i+1) = a_i).$$

It is clear that $\boldsymbol{\beta}$ is in $\boldsymbol{\mathcal{E}}$, and so are the functions

$$\ell(x) = \boldsymbol{\beta}(x, 0), \qquad (\!(x)\!)_i = \boldsymbol{\beta}(x, i+1),$$

and the predicate

$$\mathrm{Seq} = \{n \mid \neg\exists m < n\, [\ell(m) = \ell(n) \land \forall i < \ell(n)\, (\boldsymbol{\beta}(n, i) = \boldsymbol{\beta}(m, i))]\}\,.$$

The function $\mathrm{IS}\colon \mathbb{N}^2 \to \mathbb{N}$

$$\mathrm{IS}(x, i) = \boldsymbol{\mu} y \le x\, \big(\ell(y) = i \;\land\; \forall j < i\big((\!(x)\!)_j = (\!(y)\!)_j\big)\big)$$

is elementary computable. If $x = \langle\!\langle a_0, \dots, a_{k-1} \rangle\!\rangle$ and $i \le k$, then $\mathrm{IS}(x, i) = \langle\!\langle a_0, \dots, a_{i-1} \rangle\!\rangle$; for this reason IS is called the *initial-segment function*. The *concatenation function* $\mathrm{Conc}\colon \mathbb{N}^2 \to \mathbb{N}$ is defined as

$$\mathrm{Conc}(x, y) = \begin{cases} \langle\!\langle a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1} \rangle\!\rangle & \text{if } x = \langle\!\langle a_0, \dots, a_{n-1} \rangle\!\rangle \\ & \text{and } y = \langle\!\langle b_0, \dots, b_{m-1} \rangle\!\rangle, \\ 0 & \text{if } x \notin \mathrm{Seq} \lor y \notin \mathrm{Seq}. \end{cases}$$

Proposition 8.13. (a) *There is an elementary computable function* $B\colon \mathbb{N}^2 \to \mathbb{N}$ *such that for all* $a_0, \dots, a_{n-1} \in \mathbb{N}$

$$\langle\!\langle a_0, \dots, a_{n-1} \rangle\!\rangle \le B(\max\{a_0, \dots, a_{n-1}\}, n).$$

(b) *For every* $n \ge 1$ *the function* $\mathbb{N}^n \to \mathbb{N}$, $\langle a_0, \dots, a_{n-1} \rangle \mapsto \langle\!\langle a_0, \dots, a_{n-1} \rangle\!\rangle$, *is elementary computable.*

(c) $\mathrm{Conc}, \mathrm{IS} \in \boldsymbol{\mathcal{E}}$.

Proof. (a) The function $w(k, n) = \max\{k, n\} \cdot n!$ is in $\boldsymbol{\mathcal{E}}$, and so is

$$B(k, n) = \boldsymbol{J}\big(\prod_{i \le n} c(i, k, n), w(k, n)\big),$$

where $c(i, k, n) = 1 + (i+1) \cdot w(k, n)$. Given $a_0, \dots, a_{n-1} \in \mathbb{N}$, by Theorem 8.9 and Lemma 8.10 there is $x < \prod_{i \le n} c(i, k, n)$ such that $n \equiv x \mod c(0, k, n)$ and $a_i \equiv x \mod c(i+1, k, n)$. Since $\boldsymbol{J}$ is increasing in both variables,

$$\exists z \le B(k, n)\, \big[\ell(z) = n \land \forall i < n\, ((\!(z)\!)_{i+1} = a_i)\big].$$

(b) Letting $k = \max\{a_0, \ldots, a_{n-1}, n\}$, then

$$\langle\!\langle a_0, \ldots, a_{n-1} \rangle\!\rangle = \boldsymbol{\mu} z \leq B(k, n) \left[\ell(z) = n \wedge \bigwedge_{i<n} (\!(z)\!)_{i+1} = a_i\right],$$

and hence $(a_0, \ldots, a_{n-1}) \mapsto \langle\!\langle a_0, \ldots, a_{n-1} \rangle\!\rangle$ is in $\boldsymbol{\mathcal{E}}$.

(c) It is enough to find $g \colon \mathbb{N}^2 \to \mathbb{N}$ in $\boldsymbol{\mathcal{E}}$ such that for all $x, y \in \mathrm{Seq}$

$$\begin{aligned}\mathrm{Conc}(x, y) = \boldsymbol{\mu} z \leq g(x, y) \big[&\ell(z) = \ell(x) + \ell(y) \\ &\wedge \forall i < \ell(x) \left((\!(z)\!)_i = (\!(x)\!)_i\right) \wedge \forall j < \ell(y) \left((\!(z)\!)_{\ell(x)+j} = (\!(y)\!)_j\right)\big].\end{aligned}$$

Since $\boldsymbol{\beta}(x, i) \leq x$ for all i, the map

$$\begin{aligned}h(x) &= \max\{(\!(x)\!)_0, \ldots, (\!(x)\!)_{\ell(x)-1}\} \\ &= \boldsymbol{\mu} n \leq x \left[\forall i < \ell(x) \left(\boldsymbol{\beta}(x, i+1) \leq n\right)\right]\end{aligned}$$

is in $\boldsymbol{\mathcal{E}}$, and so are the functions

$$\begin{aligned}&w(x, y) = \max\{h(x), h(y), \ell(x), \ell(y)\} \cdot (\ell(x) + \ell(y))! \\ &c_i(x, y) = 1 + (i+1) w(x, y).\end{aligned}$$

Arguing as in part (a) one can define

$$g(x, y) = \boldsymbol{J}\left(\textstyle\prod_{i \leq \ell(x)+\ell(y)} c_i(x, y), w(x, y)\right). \qquad \square$$

8.B. Primitive recursive functions.

Definition 8.14. If f is k-ary and g is $k+2$-ary, we shall say that the $k+1$-ary function

$$h(\vec{x}, n) = \begin{cases} f(\vec{x}) & \text{if } n = 0, \\ g(\vec{x}, n-1, h(\vec{x}, n-1)) & \text{if } n > 0, \end{cases}$$

is obtained by **primitive recursion from f and g**. The variables $\vec{x}$ are called **parameters of the recursion**; when these are not present, that is if g is 2-ary and $a \in \mathbb{N}$, then $h \colon \mathbb{N} \to \mathbb{N}$ defined by

$$h(n) = \begin{cases} a & \text{if } n = 0, \\ g(n-1, h(n-1)) & \text{if } n > 0, \end{cases}$$

is obtained by **primitive recursion without parameters from a and g**.

The primitive recursion schemata (with or without parameters) can be merged into a single scheme if constants are taken to be 0-ary functions. If in the recursion scheme g does not depend on the $k+1$-st variable, that is g is $k+1$-ary and

$$h(\vec{x}, n) = g(\vec{x}, h(\vec{x}, n-1)), \quad (n > 0)$$

then h is obtained by **iteration** via g starting from f or from a.

If h is obtained from effective functions f and g by primitive recursion as in Definition 8.14, then h is effective as well—in order to compute $h(\vec{x}, n)$ we compute in order

$$\begin{aligned}
h(\vec{x}, 0) &= f(\vec{x}) \\
h(\vec{x}, 1) &= g(\vec{x}, 0, h(\vec{x}, 0)) = g(\vec{x}, 0, f(\vec{x})) \\
h(\vec{x}, 2) &= g(\vec{x}, 1, h(\vec{x}, 1)) = g(\vec{x}, 1, g(\vec{x}, 0, f(\vec{x}))) \\
&\vdots \\
h(\vec{x}, n) &= g(\vec{x}, n-1, h(\vec{x}, n-1)).
\end{aligned}$$

Definition 8.14 is different from ordinary definitions, in that the object to be defined f appears on the left and on the right of the defining equation. In Section 12.B these definitions will be shown to be perfectly legal (Theorem 12.3).

Definition 8.15. The family $\mathcal{P}$ of **primitive recursive functions** is the smallest class of functions containing $\{c_0, S\} \cup \{I^n_k \mid k < n\}$ and closed under composition and primitive recursion.

We say that $A \subseteq \mathbb{N}^k$ is a **primitive recursive set** or, equivalently, it is a k-ary **primitive recursive predicate** if its characteristic function is a primitive recursive function.

Theorem 8.16. *The class $\mathcal{P}$ is closed under generalized sums and products and contains $\mathcal{E}$.*

$\mathcal{P}$ is the smallest class containing $\mathcal{E}$ and closed under composition and primitive recursion.

For a proof of Theorem 8.16 see Exercise 8.55. The family $\mathcal{P}$ is larger than $\mathcal{E}$ (Exercise 8.64), nevertheless $\mathcal{E}$ is closed under **bounded primitive recursion** (Exercise 8.59).

Theorem 8.17. *Suppose $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ is obtained by primitive recursion from $g\colon \mathbb{N}^{n+2} \to \mathbb{N}$ and $f\colon \mathbb{N}^n \to \mathbb{N}$. (If $n = 0$, that is if the recursion is without parameters, then f is a natural number.) If $f, g, k \in \mathcal{E}$ and*

$$\forall \vec{x} \in \mathbb{N}^{n+1}\, [h(\vec{x}) \leq k(\vec{x})],$$

then $h \in \mathcal{E}$.

Recall the coding apparatus for finite sequences introduced in the preceding Section. Given $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$, let $f^{\mathrm{m}}\colon \mathbb{N}^{k+1} \to \mathbb{N}$ be the function defined by primitive recursion:

$$f^{\mathrm{m}}(\vec{x}, y) = \begin{cases} \langle\!\langle f(\vec{x}, 0) \rangle\!\rangle & \text{if } y = 0, \\ \mathrm{Conc}(f^{\mathrm{m}}(\vec{x}, y-1), \langle\!\langle f(\vec{x}, y) \rangle\!\rangle) & \text{otherwise.} \end{cases}$$

In other words:

$$f^{\mathrm{m}}(\vec{x}, y) = \langle\!\langle f(\vec{x}, 0), \dots, f(\vec{x}, y) \rangle\!\rangle$$

remembers all values $f(\vec{x}, y')$ with $y' \leq y$, and because of this it is called the **memory-function of f**. The following result is straightforward.

Lemma 8.18. *Suppose $\mathcal{F}$ is a family of functions containing the coding apparatus, and closed under composition and primitive recursion. Then $f \in \mathcal{F} \Leftrightarrow f^{\mathrm{m}} \in \mathcal{F}$.*

In Definition 8.14, in order to compute the value $h(\vec{x}, n)$ it is enough to know the value immediately before $h(\vec{x}, n-1)$, but there are situations where $h(\vec{x}, n)$ depends also on $h(\vec{x}, i)$, for $i < n$.

Definition 8.19. If f is k-ary and g is $k+2$-ary, we will say that the $k+1$-ary function

$$h(\vec{x}, n) = \begin{cases} f(\vec{x}) & \text{if } n = 0, \\ g(\vec{x}, n-1, h^{\mathrm{m}}(\vec{x}, n-1)) & \text{if } n > 0, \end{cases}$$

is obtained by **generalized primitive recursion from f and g**.

Proposition 8.20. *Let $\mathcal{F} \supseteq \mathcal{P}$ be closed under composition and primitive recursion. If h is obtained by generalized primitive recursion from $f, g \in \mathcal{F}$ then $h \in \mathcal{F}$.*

Proof. Let $H \colon \mathbb{N}^{k+1} \to \mathbb{N}$ be the function defined by primitive recursion

$$H(\vec{x}, n) = \begin{cases} F(\vec{x}) & \text{if } n = 0, \\ G(\vec{x}, n-1, H(\vec{x}, n-1)) & \text{if } n > 0, \end{cases}$$

where

$$\begin{aligned} &F \colon \mathbb{N}^k \to \mathbb{N} & F(\vec{x}) &= \langle\!\langle f(\vec{x}) \rangle\!\rangle, \\ &G \colon \mathbb{N}^{k+2} \to \mathbb{N} & G(\vec{x}, m, y) &= \mathrm{Conc}(y, \langle\!\langle g(\vec{x}, m, y) \rangle\!\rangle). \end{aligned}$$

As $z \mapsto \langle\!\langle z \rangle\!\rangle$ is primitive recursive, then $F \in \mathcal{F}$, and since $\mathcal{F}$ is closed under primitive recursion, it follows that G and H belong to $\mathcal{F}$. As

$$H(\vec{x}, n) = \langle\!\langle h(\vec{x}, 0), h(\vec{x}, 1), \dots, h(\vec{x}, n) \rangle\!\rangle = h^{\mathrm{m}}(\vec{x}, n)$$

it follows that $h(\vec{x}, n) = (\!(H(\vec{x}, n))\!)_n$, and hence $h \in \mathcal{F}$. □

8.C. Computable functions. We have seen that many effective operations are in $\mathcal{P}$, but there are examples of effective functions that are not primitive recursive. Our goal is to give a rigorous definition of the largest class of effective functions, called the **computable functions**. To achieve this we must first take a closer look at the informal notion of algorithm. First of all notice that algorithms may yield *partial* functions. For example, suppose $P \subseteq \mathbb{N}^2$ is **decidable**, that is there is an effective procedure to determine whether

$P(n,m)$ holds or not—equivalently its characteristic function $\boldsymbol{\chi}_P \colon \mathbb{N}^2 \to \{0,1\}$ is effective. Let $Q = \operatorname{dom} P$, that is $n \in Q \Leftrightarrow \exists m\, P(n,m)$. Sets of this form are said to be **semi-decidable**. Every decidable $Q \subseteq \mathbb{N}$ is semi-decidable, just take $P = Q \times \mathbb{N}$; a less trivial example of semi-decidable predicate is the Collatz set C of Example 7.17. The algorithm

> given n, search for an m such that $P(n,m)$, and in case
> you find it, output 1 as result

defines an effective partial constant function from $\mathbb{N}$ to $\mathbb{N}$, $f \colon Q \to \mathbb{N}$, $f(n) = 1$. If $n \in Q$ then after finitely many steps we conclude that $f(n) = 1$, but if $n \notin Q$ the algorithm goes into an infinite loop and the process never halts. Similarly the function

$$g(n) = \boldsymbol{\mu} m\, P(n,m) \overset{\text{def}}{=} \min\{m \in \mathbb{N} \mid (n,m) \in P\}$$

is effective, but g need not be total, as there could be n such that $\neg P(n,m)$ for all m. If $\forall n\, \exists m\, P(n,m)$ then g is total, but there are situations when the outcome is not so definite. Suppose that the sentence $\forall n\, \exists m\, P(n,m)$ formalizes some open problem in number theory, for example asserting that a certain set A of prime numbers is infinite: $\forall n\, \exists m\, (n < m \wedge A(m))$. Examples of such A are the set of all Wieferich's primes or its complement (Example 2.3), the set $\{p \mid p \text{ and } p+2 \text{ are prime}\}$, the set of all Mersenne primes $\{p \mid p \text{ is prime and } \exists n\, (2^n - 1 = p)\}$, ... Then g is an effective function whose domain is an initial segment I of $\mathbb{N}$, but we cannot prove to that $I = \mathbb{N}$.[7]

An even more puzzling phenomenon occurs when proving $\forall n \exists m P(n,m)$ requires a suitably strong theory. Peano Arithmetic (PA for short) is the first order theory in which a decent theory of the natural numbers can be developed. Its language $\mathcal{L}_{\mathsf{PA}}$ has a unary function symbol for the successor, two binary function symbols for addition and multiplication, and a binary relation symbol for the order; it will be presented in great detail in Section 12.D. In Section 35 examples will be given of $\mathcal{L}_{\mathsf{PA}}$-formulæ $\varphi(x,y)$ such that: the set P defined by φ is in $\boldsymbol{\mathcal{E}}$ and hence it is decidable via some elementary function, $\mathsf{T} \vdash \forall x\, \exists y\, \varphi$, yet $\mathsf{PA} \nvdash \forall x\, \exists y\, \varphi$, where T is any suitably strong extension of PA. We all agree that g is effective, but from the point of view of PA the function g cannot be shown to be total, while this can be established in T. For this reason such g is said to be **provably-total-in-T**. A concrete example is the function g of Example 1.1 in Section 1, i.e. the Goodstein sequence: it is clearly computable, but to argue that it is total one need to resort to theories that are stronger than PA. This phenomenon is quite general, meaning for any sufficiently strong theory theory S (for example PA), there is a stronger T and a suitable φ for which the argument above applies.

[7] Naturally this uncertain situation could be resolved in the future by a major breakthrough in number theory.

By a **partial** k-ary function we mean a function with values in $\mathbb{N}$ and domain a subset of $\mathbb{N}^k$; if the domain is indeed $\mathbb{N}^k$ we say that the function is **total**. It is convenient to adopt the following

Notation. If f is a partial k-ary function

$$f(\vec{x})\downarrow \text{ stands for } \vec{x} \in \operatorname{dom} f \qquad f(\vec{x})\uparrow \text{ stands for } \vec{x} \notin \operatorname{dom} f.$$

The composition of f partial k-ary with $g_1, \ldots, g_k$ partial n-ary is the partial n-ary function $h\colon D \to \mathbb{N}$, where $h(\vec{x}) = f(g_1(\vec{x}), \ldots, g_k(\vec{x}))$ and

$$\begin{aligned} D &= \{\vec{x} \in \mathbb{N}^n \mid \vec{x} \in \operatorname{dom} g_1 \cap \cdots \cap \operatorname{dom} g_k \wedge (g_1(\vec{x}), \ldots, g_k(\vec{x})) \in \operatorname{dom} f\} \\ &= \{\vec{x} \in \mathbb{N}^n \mid g_1(\vec{x})\downarrow \wedge \cdots \wedge g_k(\vec{x})\downarrow \wedge f(g_1(\vec{x}), \ldots, g_k(\vec{x}))\downarrow\}. \end{aligned}$$

If f is a partial $k+1$-ary function, then $\boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ is the partial k-ary function g defined as follows:

$$g(\vec{x}) = \begin{cases} \min\{y \mid f(\vec{x}, y) = 0 \wedge \forall z \leq y\, f(\vec{x}, z)\downarrow\} & \text{if this set is non-empty,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Let us pause for some examples.

- If f is total, then $\boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ is the least y such that $f(\vec{x}, y) = 0$, if such y exists, and undefined otherwise.
- Suppose $(n, m) \in \operatorname{dom} f$ if and only if m is even, and in this case $f(n, m) = 0$. Then $\boldsymbol{\mu} y\, [f(x, y) = 0]$ is total and equal to c_0.
- Suppose $(n, m) \in \operatorname{dom} f$ if and only if m is odd, and in this case $f(n, m) = 0$. Then $\boldsymbol{\mu} y\, [f(x, y) = 0]$ is the empty function.
- If $f(n, m) = |n - m|$ then $\boldsymbol{\mu} y\, [f(x, y) = 0]$ is total, and it is the identity function.

Definition 8.21. The collection $\mathfrak{C}$ of **computable functions** is the smallest family $\mathcal{F}$ of partial functions on $\mathbb{N}$ containing $\{+, \cdot, \boldsymbol{\chi}_{\leq}\} \cup \{I^n_k \mid k < n\}$, and closed under composition and the $\boldsymbol{\mu}$-operator, that is: if $f \in \mathcal{F}$ is $k+1$-ary then the partial k-ary function $\boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ is in $\mathcal{F}$.

The collection of *total* computable functions is $\mathfrak{C}^{\text{tot}}$.

Theorem 8.22. *The class $\mathfrak{C}^{\text{tot}}$ is closed under primitive recursion and contains $\mathfrak{P}$.*

$\mathfrak{C}$ is the smallest class containing $\mathfrak{P}$ and closed under composition and the $\boldsymbol{\mu}$-operator.

For a proof of Theorem 8.22 see Exercise 8.69. There are total computable functions that are not primitive recursive (Section 8.D), so

$$\mathfrak{E} \subset \mathfrak{P} \subset \mathfrak{C}^{\text{tot}} \subset \mathfrak{C}.$$

The projections, addition, multiplication, and the characteristic function of the ordering are total functions The composition of total functions yields a total function, so the culprit for obtaining partial functions is the $\boldsymbol{\mu}$-operator. Applying $\boldsymbol{\mu}$ to well-behaved functions guarantees total functions. It is easy to check that $\mathfrak{C}^{\mathrm{tot}}$ is the smallest class $\mathcal{F}$ of total functions containing $\{+, \cdot, \boldsymbol{\chi}_{\leq}\} \cup \{I^n_k \mid k < n\}$, closed under composition, and such that if $f \in \mathcal{F}$ is $k+1$-ary and $\forall \vec{x}\, \exists y\, [f(\vec{x}, y) = 0]$, then $\vec{x} \mapsto \boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ is in $\mathcal{F}$.

By Kleene's Theorem 8.40 the $\boldsymbol{\mu}$-operator can be applied exactly once to a total function in order to obtain any function in $\mathfrak{C}$: for any ariety $n > 0$ there is an elementary computable $k_n \colon \mathbb{N}^{n+2} \to \mathbb{N}$ such that for each n-ary $f \in \mathfrak{C}$ there is an $e \in \mathbb{N}$ such that

$$f(x_1, \dots, x_n) = (\boldsymbol{\mu} y\, (k_n(e, x_1, \dots, x_n, y) = 0)_0$$

where $z \mapsto (z)_0$ is defined on page 204.

The definitions of $\mathfrak{E}$, $\mathfrak{P}$, $\mathfrak{C}$ all share the same structure: start from a family $\mathcal{F}_0$ of basic functions, and construct $\mathcal{F}_{n+1}$ by closing $\mathcal{F}_n$ under composition and an appropriate construction principle, so that the resulting family is $\mathcal{F} = \bigcup_{n \in \mathbb{N}} \mathcal{F}_n$. Therefore

- if $\mathcal{F} = \mathfrak{E}$, then $\mathcal{F} = \{+, \cdot, d, q\} \cup \{I^n_k \mid k < n\}$, where $d(x, y) = |x - y|$ and $q(x, y) = \lfloor x/y \rfloor$, and the construction principle is taking generalized sums and products;
- if $\mathcal{F} = \mathfrak{P}$, then $\mathcal{F}_0 = \{c_0, S\} \cup \{I^n_k \mid k < n\}$ and the construction principle is primitive recursion;
- if $\mathcal{F} = \mathfrak{C}$, then $\mathcal{F}_0 = \{+, \cdot, \boldsymbol{\chi}_{\leq}\} \cup \{I^n_k \mid k < n\}$ and the construction principle is the $\boldsymbol{\mu}$-operator.

Thus $\mathfrak{E}$, $\mathfrak{P}$, and $\mathfrak{C}$ are examples of induction systems in the sense of Definition 7.14 in Section 7.A.1. In particular, if we need to prove that every function in $\mathcal{F}$ has property P we can proceed by induction: we prove that every function in $\mathcal{F}_0$ has property P, and that if every function in $\bigcup_{k<n} \mathcal{F}_k$ has property P, then every function in $\mathcal{F}_n$ has property P.

A set $A \subseteq \mathbb{N}^k$ is a **computable** if its characteristic function is computable. If A is a $k+1$-ary computable predicate then $\overline{\mathrm{sgn}} \circ \boldsymbol{\chi}_A$ is a computable, total, $k+1$-ary function, and hence the function

$$\mathbb{N}^k \to \mathbb{N} \qquad \vec{x} \mapsto \boldsymbol{\mu} y\, A(\vec{x}, y)$$

assigning to each $\vec{x}$ the least y (if it exists) such that $A(\vec{x}, y)$ is computable.

Remark 8.23. Up until the eighties of the last century people used the adjective *recursive* as synonymous of computable, and computability theory was called *recursion theory.* Nowadays *recursive* is used mainly when referring to a computing procedure that feeds on some previously computed values.

Every function in $\mathfrak{C}$ is effective. Conversely,

Church's thesis. *Every effective operation is in* $\mathfrak{C}$.

Every computable set is decidable, and by Church's thesis every decidable set is computable. Church's thesis is neither a theorem nor a conjecture, but rather an empirical observation: it asserts that the *rigorous* definition of recursive function captures the *vague* notion of intuitively computable function. We cannot exclude that Church's thesis might be refuted, one day: it would be enough to exhibit a function which is effectively computable in the naïve sense, and yet it can be shown not to be computable in the sense of Definition 8.21. There are, nevertheless, good reasons to believe Church's thesis since:

(A) all known examples of effective operations are in fact computable functions;

(B) several distinct formalizations of the concept of effective operation have been proposed—the definition above of computable function given above is one of these; among the other ones are the *Turing machines* and *Post systems*. These formalizations, although ostensibly different, *define the same class of functions* $\mathfrak{C}$.

Because of this, Church's thesis is accepted (as an empirical fact) in mathematics, and it is often used in proofs to argue that a given function is computable. This is quite similar to what happens in calculus, where a from some point on it is argued in an informal way that a given function is continuous, instead of computing the δ from the ε. Actually, this amounts to ask the reader to fill-in the gaps that the author of the text is too lazy to write. This chore can be left to the reader only when the reader is familiar enough with the basics of the subject, and for this reason our treatment, at the beginning, will be quite detailed.

Remarks 8.24. (a) Knowing that a function is in $\mathfrak{C}$ does not mean that we know its algorithm. For example the function f defined by $f(n) = 0$ if a certain open problem in number theory (like the ones named in Exercise 2.11) is true, and $f(n) = 1$ otherwise; then f is computable, since it is constant, but we do not know which program computes the function.

(b) The notion of computable function describes a rather idealized concept of "computation", unfettered by the inherent limitations of physical devices. In other words, even if we know the algorithm witnessing that f is computable, it is not clear that the function is *feasable*, meaning that we can actually compute $f(n)$ for all n. For example the computation of $n!$ is *not feasible* even for small values of n even if the function

$n \mapsto n!$ is primitive recursive. For this reason, in the second half of the last century, a theory of feasible computations, known as **complexity theory**, emerged.

(c) There are countably many functions in $\mathfrak{C}$, and hence there are countably many computable sets. Therefore computable sets and functions are a small minority in the family of all sets and operations on the natural numbers (see Section 13).

Suppose that in the definition of $\boldsymbol{\mu}$-operator the condition $\forall z \leq y\, f(\vec{x}, z)\downarrow$ is removed, so that the definition of $g = \boldsymbol{\mu} y\, [f(\vec{x}, y) = 0]$ becomes

$$g(\vec{x}) = \begin{cases} \min\{y \mid f(\vec{x}, y) = 0\} & \text{if this set is non-empty,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

With this relaxed definition of $\boldsymbol{\mu}$-operator we could generate non-computable functions. Imagine that $f(x, y)$ is a partial computable function and that `A` is an algorithm (i.e. a computer program) that calculates f: given an input (n, m)

- if $(n, m) \in \operatorname{dom} f$ then after enough time has elapsed the algorithm `A` applied to (n, m) stops and outputs $f(n, m)$,
- if $(n, m) \notin \operatorname{dom} f$ then `A` will go-on forever without any output.

Let us see how to compute $g(x) = \boldsymbol{\mu} y\, (f(x, y) = 0)$. The naïve idea would be to calculate in order: $f(n, 0)$, $f(n, 1)$, $\ldots$ until we reach an integer m such that $f(n, m) = 0$, and set $m = g(x)$. Unfortunately $f(n, k)$ might be undefined for some $k < m$, and hence the procedure described above would run into a grinding halt before reaching the input (n, m). A better strategy would be applying the algorithm `A` simultaneously to

$$(n, 0), (n, 1), (n, 2), \ldots .$$

Since our computer is multitasking we can spend some time on input $(n, 0)$, then some time on inputs $(n, 0), (n, 1)$, then some time on inputs $(n, 0), (n, 1), (n, 2)$, and so on. If at time t the algorithm `A` stops on input (n, m) yielding output 0, we cannot argue that $f(n) = m$ since at some later time $t' > t$ we might verify that the algorithm `A` stops on input (n, m') yielding output 0 with $m' < m$. But waiting forever might not be wise since f might not be defined on (n, m'). From the arguments above, it should be clear that culprit for the subtle nature of the computable functions is the minimization operator.

The elements of $\mathfrak{C}$ are *partial functions*, so by a k-ary computable function we always mean a function with domain *contained* in $\mathbb{N}^k$ and taking values in $\mathbb{N}$. When we mean a computable $f \colon \mathbb{N}^k \to \mathbb{N}$, i.e. an element of $\mathfrak{C}^{\text{tot}}$, we speak of a *total* computable k-ary function.

Examples 8.25. (a) The empty function is in $\mathfrak{C}$—consider, for example $f(x) = \boldsymbol{\mu} y\, [S(y) = 0]$.

(b) For any computable $D \subseteq \mathbb{N}^k$ there is a k-ary computable f such that $\operatorname{dom} f = D$; for example

$$f(\vec{x}) = \begin{cases} 1 & \text{if } x \in D, \\ \boldsymbol{\mu} y\, [S(y) = 0] & \text{otherwise.} \end{cases}$$

The functions in Example 8.25 are partial, but can be easily extended to a total computable functions. In fact any computable function f whose domain is a computable set D can be extended to a total computable $\tilde{f}$—just map the complement of D to some fixed value. On the other hand, there are computable partial functions that cannot be extended to a total computable function (Theorem 8.43), i.e. there are $f \in \mathfrak{C}$ such that there is no $g \in \mathfrak{C}^{\text{tot}}$ such that $g \restriction \operatorname{dom} f = f$. This means that $\operatorname{dom} f$ is not computable, and sets of this form are called semi-computable (see Section 8.E).

8.C.1. *Some properties of computable functions.*

Lemma 8.26. *A total k-ary function f is computable if and only if its graph* $\operatorname{Gr}(f)$ *is a $k+1$-ary computable predicate.*

Proof. One direction follows from Lemma 8.5. Conversely, if $\boldsymbol{\chi}_{\operatorname{Gr}(f)}$ is computable, then also f is computable: given $\vec{x}$ one looks for the first (and unique) y such that $(\vec{x}, y) \in \operatorname{Gr}(f)$, and such y is $f(\vec{x})$. Formally:

$$f(\vec{x}) = \boldsymbol{\mu} y\, [1 \dot{-} \boldsymbol{\chi}_{\operatorname{Gr}(f)}(\vec{x}, y) = 0]. \qquad \square$$

Proposition 8.27. *For every unary, total computable f there is a partial unary computable g which is the right-inverse of f, that is* $\operatorname{dom} g = \operatorname{ran} f$ *and* $\forall y \in \operatorname{dom} g\ (f(g(y)) = y)$.

Proof. The function $(y, x) \mapsto |f(x) - y|$ is computable, and

$$g(y) = \boldsymbol{\mu} x\, [|f(x) - y| = 0]$$

is the required function. □

Proposition 8.27 can be extended to partial functions as well—see Corollary 8.47.

Corollary 8.28. *The inverse of a computable bijection is computable. In particular, the set of all computable bijections of* $\mathbb{N}$ *is a group.*

The **enumerating function** of an infinite set $A \subseteq \mathbb{N}$ is a function $f \colon \mathbb{N} \to \mathbb{N}$ mapping n to the n-th element of A.

Proposition 8.29. *Suppose that $A \subseteq \mathbb{N}$ is infinite, and that f is the enumerating function. Then A is computable if and only if f is computable.*

Proof. Suppose that A is computable: f is computable since

$$f(n) = \begin{cases} \min(A) & \text{if } n = 0 \\ g(f(n-1)) & \text{if } n > 0 \end{cases}$$

where $g(k) = \boldsymbol{\mu} m\,[A(m) \wedge m > k]$.

The other direction follows from $A(x) \Leftrightarrow \exists y \leq x\,[|f(y) - x| = 0]$. □

Proposition 8.29 does not generalize to other classes of functions: if $\mathcal{F}$ is $\boldsymbol{\mathcal{E}}$ or $\boldsymbol{\mathcal{P}}$, there are sets in $\mathcal{F}$ whose enumerating function is in $\boldsymbol{\mathcal{C}} \setminus \mathcal{F}$—Proposition 8.33(a). The next result will be useful in the next section.

Lemma 8.30. *Let A and B be infinite sets that partition $\mathbb{N}$ and let f_A and f_B be their enumerating functions. Let $\mathcal{F}$ be $\boldsymbol{\mathcal{E}}$ or $\boldsymbol{\mathcal{P}}$ If $\mathrm{Gr}(f_A) \in \mathcal{F}$, then $\mathrm{Gr}(f_B)$, A and B are in $\mathcal{F}$.*

Proof. $(x, y) \in \mathrm{Gr}(f_B)$ if and only if

$$\begin{aligned} x = y < f_A(0) \vee \big(\exists u, v < y\,[(u, v) \in \mathrm{Gr}(f_A) \\ \wedge \neg\exists z, w < y\,(u < z \wedge (z, w) \in \mathrm{Gr}(f_A)) \wedge y = x + u]\big) \end{aligned}$$

hence $\mathrm{Gr}(f_B) \in \mathcal{F}$. Moreover $A = \{y \mid \exists x \leq y\,[(x, y) \in \mathrm{Gr}(f_A)]\} \in \mathcal{F}$ hence $B = \mathbb{N} \setminus A \in \mathcal{F}$. □

Using the bijection $\boldsymbol{J} \colon \mathbb{N}^2 \to \mathbb{N}$ of (8.1) one can define the bijections

$$\boldsymbol{J}^n \colon \mathbb{N}^n \to \mathbb{N}, \qquad \boldsymbol{J}^n(x_0, \ldots, x_{n-1}) = \boldsymbol{J}(x_0, \boldsymbol{J}^{n-1}(x_1, \ldots, x_{n-1})) \tag{8.5}$$

where $\boldsymbol{J}^1 = \mathrm{id}_{\mathbb{N}}$ and $\boldsymbol{J}^2 = \boldsymbol{J}$. The inverse functions

$$(\cdot)^n_k \colon \mathbb{N} \to \mathbb{N} \qquad (k < n)$$

are defined by

$$\boldsymbol{J}^n((x)^n_0, \ldots, (x)^n_{n-1}) = x. \tag{8.6}$$

The bijections $\boldsymbol{J}^n$ and their inverses are elementary computable (Exercise 8.61). A function

$$f \colon \mathbb{N}^n \to \mathbb{N}^m, \qquad f(\vec{x}) = (f_0(\vec{x}), \ldots, f_{m-1}(\vec{x}))$$

is elementary computable (primitive recursive) if the $f_i \colon \mathbb{N}^n \to \mathbb{N}$ $(i < m)$ are elementary computable (primitive recursive) computable. The notion of computable function and computable set can be extended to other domains, such as $\mathbb{N}^{<\mathbb{N}}$: a function $F \colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ is elementary computable (primitive recursive) if and only if there is an elementary computable (primitive recursive) $f \colon \mathbb{N} \to \mathbb{N}$ such that

$$F(x_0, \ldots, x_n) = (y_0, \ldots, y_m) \Leftrightarrow f(\langle\!\langle x_0, \ldots, x_n \rangle\!\rangle) = \langle\!\langle y_0, \ldots, y_m \rangle\!\rangle,$$

and a set $A \subseteq \mathbb{N}^{<\mathbb{N}}$ is elementary computable (primitive recursive) if and only if the set

$$\{\langle\!\langle x_0, \dots, x_n \rangle\!\rangle \mid (x_0, \dots, x_n) \in A\}$$

is elementary computable (primitive recursive).

8.D. Computable, but not primitive recursive functions. Ackermann's function Ack: $\mathbb{N}^2 \to \mathbb{N}$ is a concrete example of a computable function that it is not primitive recursive. It is defined as

$$\mathrm{Ack}(m,n) = \begin{cases} n+1 & \text{if } m = 0, \\ \mathrm{Ack}(m-1,1) & \text{if } m > 0 \text{ and } n = 0, \\ \mathrm{Ack}(m-1, \mathrm{Ack}(m, n-1)) & \text{if } m > 0 \text{ and } n > 0. \end{cases}$$

For ease of notation let $\mathrm{Ack}_m \colon \mathbb{N} \to \mathbb{N}$, $n \mapsto \mathrm{Ack}(m,n)$. Then $\mathrm{Ack}_0 \in \boldsymbol{\mathcal{E}}$ and an easy induction proves that

$$m > 0 \Rightarrow \mathrm{Ack}_m(n) = \mathrm{Ack}_{m-1}^{(n+1)}(1) \tag{8.7a}$$

$$\forall m\, (\mathrm{Ack}_m \text{ is increasing})\,. \tag{8.7b}$$

Therefore the computation of the values of the function Ack_m boils-down to computing values of the functions $\mathrm{Ack}_{m-1}, \mathrm{Ack}_{m-2}, \dots, \mathrm{Ack}_0$. By Church's thesis, Ackermann's function is computable. To prove this rigorously argue as follows.

By equations (8.7), in order to compute $\mathrm{Ack}(m,n)$ it is enough to know Ackermann's function restricted to some finite $D \subseteq \mathbb{N} \times \mathbb{N}$. Let $\mathcal{F}$ be the collection of all pairs (f, D) such that:

(A) $D \subseteq \mathbb{N} \times \mathbb{N}$ is finite and $f \colon D \to \mathbb{N}$,

(B) $\forall m, n \left[(m, n+1) \in D \Rightarrow (m,n) \in D\right]$,

(C) $\forall n \left[(0,n) \in D \Rightarrow f(0,n) = n+1\right]$,

(D) $\forall m \left[(m+1, 0) \in D \Rightarrow f(m+1,0) = f(m,1)\right]$,

(E) $\forall m, n \left[(m+1, n+1) \in D \Rightarrow (m+1, n) \in D \wedge (m, f(m+1,n)) \in D \wedge f(m+1,n+1) = f(m, f(m+1,n))\right]$.

For every (m,n) we have that $(\mathrm{Ack} \restriction D, D) \in \mathcal{F}$, where $D = \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid i \leq m \wedge j \leq k_{m-1}\}$ and

$$\begin{cases} k_0 = n, \\ k_{i+1} = \mathrm{Ack}_{m-i}^{(k_i+1)}(1) \quad \text{for } 0 < i \leq m. \end{cases}$$

Thus

$$\mathrm{Ack}(m,n) = k \Leftrightarrow \exists (f,D) \in \mathcal{F} \left[(m,n) \in D \wedge f(m,n) = k\right].$$

Every $(f, D) \in \mathcal{F}$ is in essence a finite sequence of natural numbers, hence it can be coded as an element of Seq and let $S \subseteq \mathrm{Seq}$ be the set of numbers that code an element of $\mathcal{F}$. Thus an element of S is a finte sequence of natural numbers, each coding a triple $\boldsymbol{J}(\boldsymbol{J}(n, m), f(n, m))$. Equations (A)–(E) can be translated into conditions on the naturals showing that S is elementary computable. For example, condition (A) can be rendered as

$$\forall i, i' < \ell(s)\, \forall m, n, k, k' < s\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(n, m), k) \\ \wedge\ (\!(s)\!)_{i'} = \boldsymbol{J}(\boldsymbol{J}(n, m), k') \Rightarrow k = k']$$

while (B) and (C) become, respectively

$$\forall i, i' < \ell(s)\, \forall m, n, k, k' < s\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(n, m), k) \\ \wedge\ (\!(s)\!)_{i'} = \boldsymbol{J}(\boldsymbol{J}(n, m), k') \Rightarrow k = k']$$

and

$$\forall m, n < s\, \big[\exists i < \ell(s)\, \exists k < s\, \boldsymbol{J}(\boldsymbol{J}(m, n+1), k) = (\!(s)\!)_i \\ \Rightarrow \exists i' < \ell(s)\, \exists k < s\, \boldsymbol{J}(\boldsymbol{J}(m, n), k') = (\!(s)\!)_{i'}\big].$$

Therefore

$$\mathrm{Ack}(m, n) = k \Leftrightarrow \exists s \in S\, \exists i < \ell(s)\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(m, n), k)]$$

and hence $\mathrm{Ack}(m, n) = (\boldsymbol{\mu} y\, A(m, n, y))_1$, where

$$A(m, n, \boldsymbol{J}(s, k)) \Leftrightarrow s \in S \wedge \exists i < \ell(s)\, [(\!(s)\!)_i = \boldsymbol{J}(\boldsymbol{J}(m, n), k)]. \tag{8.8}$$

Since $A \subseteq \mathbb{N}^3$ is elementary computable, it follows that Ack is computable.

Theorem 8.31. *If $f \colon \mathbb{N}^n \to \mathbb{N}$ is primitive recursive, then there is a c such that*

$$\forall x_1, \dots, x_n\ (f(x_1, \dots, x_n) < \mathrm{Ack}(c, x_1 + \cdots + x_n))\,.$$

For a proof see Exercise 8.68.

Corollary 8.32. *Ackermann's function is not primitive recursive.*

Proof. If, towards a contradiction, Ack were primitive recursive, then also $f(n) = \sum_{i=0}^{n} \mathrm{Ack}(i, n)$ would be primitive recursive, hence $\forall n\, (f(n) < \mathrm{Ack}(c, n))$ for suitable c. In particular, if $n \geq c$ then

$$\mathrm{Ack}(c, n) \leq \sum_{i=0}^{n} \mathrm{Ack}(i, n) = f(n) < \mathrm{Ack}(c, n)$$

a contradiction! □

By Corollary 8.28, the inverse of a recursive bijection is recursive.

Proposition 8.33. (a) *There is an infinite elementary recursive subset of $\mathbb{N}$ whose enumerating map is computable but not in $\boldsymbol{\mathcal{P}}$.*

(b) *There is a computable function not in $\boldsymbol{\mathcal{P}}$ whose graph is in $\boldsymbol{\mathcal{E}}$.*

(c) *There is an elementary computable bijection of $\mathbb{N}$ whose inverse is computable but not in $\boldsymbol{\mathcal{P}}$.*

Proof. Let A be the elementary predicate in (8.8). The function

$$f_0 \colon \mathbb{N} \to \mathbb{N}, \qquad x \mapsto \boldsymbol{\mu} y\, A(x, x, y)$$

is increasing and dominates every primitive recursive unary function, since $n \mapsto \operatorname{Ack}(n, n)$ has this property and $(k)_1 \leq k$ for all k. In particular f_0 is total, computable nut not in $\boldsymbol{\mathcal{P}}$, and $\operatorname{ran}(f_0)$ and $\mathbb{N} \setminus \operatorname{ran}(f_0)$ are infinite. Let f_1 be the enumerating function of $\mathbb{N} \setminus \operatorname{ran}(f_0)$. Since

$$\operatorname{Gr}(f_0) = \bigl\{(x, y) \mid A(x, x, y) \wedge \forall y' < y\, [\neg A(x, x, y')]\bigr\}$$

is in $\boldsymbol{\mathcal{E}}$, then $\operatorname{Gr}(f_1)$ and $\operatorname{ran}(f_0)$ are in $\boldsymbol{\mathcal{E}}$ as well by Lemma 8.30. This proves (a) and (b).

Let $g \colon \mathbb{N} \to \mathbb{N}$ be the bijection given by copying f_0 on the even numbers and f_1 on the odd numbers:

$$g(x) = \begin{cases} f_0(n) & \text{if } x = 2n, \\ f_1(n) & \text{if } x = 2n + 1. \end{cases}$$

Then g is a bijection, its graph

$$\{(2x, y) \mid (x, y) \in \operatorname{Gr}(f_0)\} \cup \{(2x + 1, y) \mid (x, y) \in \operatorname{Gr}(f_1)\}$$

is elementary, and $g^{-1}(y) \leq 2y + 1$, thus $g^{-1} \in \boldsymbol{\mathcal{E}}$ by Proposition 8.7. Since $f_0(n) = g(2n)$ it follows that g is computable but not in $\boldsymbol{\mathcal{P}}$. □

8.E. Computable and semi-computable sets. Example 8.6(A) can be generalized to the case of computable functions. In other words, if $A(x_1, \ldots, x_k)$ is a computable predicate and $f_1, \ldots, f_k$ are n-ary computable *total* functions, then

$$A(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$$

is computable. We abbreviate this by saying that computable predicates are closed under computable substitutions.

A similar argument holds for Examples 8.6(B)–(F). In particular, the family of computable subsets of $\mathbb{N}^k$ is a Boolean algebra, and if $A(\vec{x}, y)$ is $k + 1$-ary computable, then the $k + 1$-ary predicates obtained from A by bounded quantifications

$$\forall z \leq y\, A(\vec{x}, y) \qquad\qquad \exists z \leq y\, A(\vec{x}, y)$$

are computable.

Definition 8.34. A predicate $A \subseteq \mathbb{N}^k$ is **semi-computable** if there is a computable $\tilde{A} \subseteq \mathbb{N}^{k+1}$ which projects onto A, that is

$$A(\vec{x}) \Leftrightarrow \exists y\, \tilde{A}(\vec{x}, y).$$

Every computable predicate is semi-computable, but not conversely (Theorem 8.48). If $\Phi \colon \mathbb{N}^n \to \mathbb{N}^k$ is a computable bijection and $n, k \geq 1$, then

$$A \subseteq \mathbb{N}^n \text{ is (semi-)computable} \Leftrightarrow \Phi[A] \subseteq \mathbb{N}^k \text{ is (semi-)computable.}$$

Proposition 8.35. *A semi-computable predicate is the domain of some computable function.*

Proof. Suppose $A(\vec{x}) \Leftrightarrow \exists y\, B(\vec{x}, y)$ with B computable. The function $f(\vec{x}) = \boldsymbol{\mu} y\, B(\vec{x}, y)$ is computable, and $\operatorname{dom} f = A$. □

Proposition 8.36. *Let f be a partial k-ary function. If* $\operatorname{Gr}(f)$ *is semi-computable, then f is computable.*

Proof. Let $A \subseteq \mathbb{N}^{k+2}$ be computable and such that $(\vec{x}, y) \in \operatorname{Gr}(f) \Leftrightarrow \exists z\, A(\vec{x}, y, z)$. Then $f(\vec{x}) = (\boldsymbol{\mu} w\, A(\vec{x}, (w)_0, (w)_1))_0$ is computable. □

Proposition 8.37. *The family of semi-computable sets is closed under*

(a) *substitution under computable total functions: if A is k-ary and semi-computable and $f_1, \dots, f_k$ are n-ary computable total functions, then $A(f_1(\vec{x}), \dots, f_k(\vec{x}))$ is n-ary semi-computable;*

(b) *projections: if $A \subseteq \mathbb{N}^k$ is semi-computable and $k > 1$, then the $k-1$-ary predicate $\exists x_k\, A$ defined by*

$$(x_1, \dots, x_{k-1}) \in \exists x_k\, A \Leftrightarrow \exists x_k\, (x_1, \dots, x_{k-1}, x_k) \in A$$

is semi-computable;

(c) *intersections and unions;*

(d) *bounded quantifications.*

Proof. Suppose $A(\vec{x})$, $B(\vec{x})$ are k-ary semi-computable, and A' and B' are computable $k+1$-ary predicates such that $A(\vec{x})$ if and only if $\exists y\, A'(\vec{x}, y)$ and $B(\vec{x})$ if and only if $\exists y\, B'(\vec{x}, y)$.

(a) If $f_1, \dots, f_k$ are n-ary computable total functions, then the n-ary predicate $A(f_1(\vec{x}), \dots, f_k(\vec{x}))$ is semi-computable, since $A(f_1(\vec{x}), \dots, f_k(\vec{x}))$ if and only if $\exists y\, A'(f_1(\vec{x}), \dots, f_k(\vec{x}), y)$, and $A'(f_1(\vec{x}), \dots, f_k(\vec{x}), y)$ is computable.

(b) We have that

$$\begin{aligned}(x_1, \dots, x_{k-1}) \in \exists x_k\, A &\Leftrightarrow \exists x_k\, \exists y\, A'(x_1, \dots, x_{k-1}, x_k, y)\\ &\Leftrightarrow \exists z\, [\exists x_k \leq z\, \exists y \leq z\, A'(x_1, \dots, x_{k-1}, x_k, y)]\end{aligned}$$

so we are done since the predicate in square brackets is computable, as it is obtained from a computable predicate using bounded quantifications.

(c) $(x_1, \dots, x_k) \in A \cup B$ just in case $\exists y\, (A'(\vec{x}, y) \vee B'(\vec{x}, y))$ so $A \cup B$ is semi-computable. Moreover

$$(x_1, \dots, x_k) \in A \cap B \Leftrightarrow \exists z\, \exists y \leq z\, \exists y' \leq z\, (A'(\vec{x}, y) \wedge B'(\vec{x}, y')).$$

(d) For the bounded existential quantifier

$$(x_1, \dots, x_{k-1}, z) \in \exists x_k \leq z\, A \Leftrightarrow \exists x_k\, [A(x_1, \dots, x_{k-1}, x_k) \wedge (x_k \leq z)],$$

so we apply part (b).

For the bounded universal quantifier

$$\begin{aligned}(x_1, \dots, x_{k-1}, z) \in \forall x_k \leq z\, A &\Leftrightarrow \forall x_k \leq z\, \exists y\, A'(x_1, \dots, x_{k-1}, x_k, y)\\ &\Leftrightarrow \exists w\, [\forall x_k \leq z\, \exists y \leq w\, A'(x_1, \dots, x_{k-1}, x_k, y)]\end{aligned}$$

so we are done since the predicate in square brackets is computable, as it is obtained from a computable predicate using bounded quantifications. □

The semi-computable sets form a bounded distributive lattice, but not a Boolean algebra, as the complement of a semi-computable set need not be semi-computable. If this is the case, then the set in question is computable, and this is the content of the following result of Post.

Theorem 8.38. *A predicate A is computable if and only if A and $\neg A$ are semi-computable.*

Proof. If $A \subseteq \mathbb{N}^k$ is computable then so is $\neg A = A^{\complement} = \mathbb{N}^k \setminus A$, and hence A and $\neg A$ are semi-computable. Conversely, suppose $B_0, B_1 \subseteq \mathbb{N}^{k+1}$ are computable and such that

$$A(\vec{x}) \Leftrightarrow \exists y\, B_1(\vec{x}, y) \qquad\qquad \neg A(\vec{x}) \Leftrightarrow \exists y\, B_0(\vec{x}, y).$$

Then $f\colon \mathbb{N}^k \to \mathbb{N}$, $f(\vec{x}) = \boldsymbol{\mu} y\, [B_0(\vec{x}, y) \vee B_1(\vec{x}, y))]$ is computable, and since there is no y such that $B_0(\vec{x}, y) \wedge B_1(\vec{x}, y)$, it follows that $A(\vec{x}) \Leftrightarrow B_1(\vec{x}, f(\vec{x}))$. Thus A is computable, as it is obtained from B_1 via a computable substitution. □

Proposition 8.39. *Let $A \subseteq \mathbb{N}$.*

(a) *A is semi-computable if and only if $A = \operatorname{ran} f$ for some computable, partial unary f.*

(b) *$A \neq \emptyset$ is semi-computable if and only if $A = \operatorname{ran} f$ for some computable $f\colon \mathbb{N} \to \mathbb{N}$.*

(c) *A is semi-computable and infinite if and only if $A = \operatorname{ran} f$ for some injective, computable $f\colon \mathbb{N} \to \mathbb{N}$.*

(d) *A is computable and infinite if and only if $A = \operatorname{ran} f$ for some increasing, computable $f\colon \mathbb{N} \to \mathbb{N}$.*

Proof. If $A = \operatorname{ran} f$, then A is the projection of $\operatorname{Gr}(f)$ which is computable, that is

$$A(y) \Leftrightarrow \exists x\, [(x, y) \in \operatorname{Gr}(f)].$$

This proves the $\Leftarrow$ direction of parts (a) and (b).

If $A = \emptyset$ then $A = \operatorname{ran} f$ with f the empty function of Example 8.25(a), so part (a) is proved.

If $A \neq \emptyset$, suppose $A(x) \Leftrightarrow \exists y\, [(x, y) \in B]$ for some computable $B \subseteq \mathbb{N}^2$, and let a be an element of A. The function $f\colon \mathbb{N} \to \mathbb{N}$

$$f(n) = \begin{cases} (n)_0 & \text{if } B((n)_0, (n)_1), \\ a & \text{otherwise,} \end{cases}$$

is computable, and $A = \operatorname{ran} f$.

(c) By part (a) A is the range of some computable $g\colon \mathbb{N} \to \mathbb{N}$. Define $f\colon \mathbb{N} \to \mathbb{N}$ as follows: $f(0) = g(0)$, and let $f(n+1) = g(k)$ where k is least such that $g(k) \notin \{f(0), \dots, f(n)\}$. Then $\operatorname{ran} f = \operatorname{ran} g = A$, and by Church's thesis f is computable.

(d) The map $f\colon \mathbb{N} \to \mathbb{N}$

$$\begin{cases} f(0) = \min A \\ f(n+1) = \boldsymbol{\mu} y\, [A(y) \wedge f(n) < y] \end{cases}$$

is increasing, computable, and $\operatorname{ran} f = A$.

Conversely, suppose $A = \operatorname{ran} f$ with f increasing. Then $A(x) \Leftrightarrow \exists x \leq y\, (f(x) = y)$ and hence A is computable. □

The next result, known as **Kleene's normal form theorem**, proves that any partial n-ary computable function f can be obtained by applying the $\boldsymbol{\mu}$-operator to an elementary computable function k_n, and composing with another elementary computable function U, using an integer e. In loose terms, in order to compute $f(\vec{x})$ it is enough to search for the least computation y witnessing that the computer k_n with input $\vec{x}$ and program e stops, and then extract the value $f(\vec{x})$ from y by means of U.

Theorem 8.40 (Kleene). *For each arity $n > 0$ there are elementary computable functions $\mathrm{k}_n\colon \mathbb{N}^{n+2} \to \mathbb{N}$ and $\mathrm{U}\colon \mathbb{N} \to \mathbb{N}$ such that every partial computable n-ary function f is of the form*

$$f(\vec{x}) = \mathrm{U}(\boldsymbol{\mu} y\, [\mathrm{k}_n(\vec{x}, y, e) = 0])$$

for some $e \in \mathbb{N}$. In fact U can be taken to be the map $x \mapsto (x)_0$, the first inverse of the bijection $\boldsymbol{J}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Kleene's theorem is proved in Section 8.F.3, but for the time being let us observe some corollaries. The condition $\mathrm{k}_n(\vec{x}, y, e) = 0$ can be replaced by an elementary predicate $\mathrm{K}_n(\vec{x}, y, e)$, so that $f(\vec{x}) = \mathrm{U}(\boldsymbol{\mu} y \, \mathrm{K}_n(\vec{x}, y, e))$, and we write φ_e^n for the e-th n-ary computable function $\vec{x} \mapsto \mathrm{U}(\boldsymbol{\mu} y \, \mathrm{K}_n(\vec{x}, y, e))$. Thus

$$\{\varphi_e^n \mid e \in \mathbb{N}\}$$

is the set of all n-ary computable functions. When $n = 1$ we write φ_e instead of φ_e^1.

The $n + 1$-ary map $(\vec{x}, e) \mapsto \mathrm{U}(\boldsymbol{\mu} y \, \mathrm{K}_n(\vec{x}, y, e))$ is computable, so:

Theorem 8.41. *For each $n \geq 1$ there is an $(n + 1)$-ary computable function F such that $F(\vec{x}, e) = \varphi_e^n(\vec{x})$, for all $\vec{x} \in \mathbb{N}^n$ and all $e \in \mathbb{N}$.*

In other words the n-ary *partial* computable functions can be computably enumerated by an $n + 1$-ary *partial* computable function. On the other hand there is no $n + 1$-ary *total* computable function that enumerates all n-ary total computable functions. We prove this for $n = 1$, leaving the obvious generalization to the reader.

Proposition 8.42. *Let $\mathcal{F}$ be $\boldsymbol{\mathcal{E}}$, or $\boldsymbol{\mathcal{P}}$, or $\boldsymbol{\mathfrak{C}}^{\mathrm{tot}}$. There is no $F \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ in $\mathcal{F}$ such that*

$$\{F_e \mid e \in \mathbb{N}\} = \mathcal{F} \cap \mathbb{N}^{\mathbb{N}},$$

where $F_e \colon \mathbb{N} \to \mathbb{N}$, $x \mapsto F(e, x)$.

Proof. Otherwise $f(x) = F(x, x) + 1$ would be in $\mathcal{F}$, and hence $f = F_e$ for some $e \in \mathbb{N}$. But then $f(e) = F(e, e) + 1 = f(e) + 1$, a contradiction. □

The argument above does not apply to the partial binary computable function F from Theorem 8.41 that enumerates every partial unary computable function, as the function $f(x) = F(x, x) + 1$ in the proof above is φ_e for some $e \notin \operatorname{dom} f$. On the other hand there is no total computable $G \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ extending F, as letting $g(x) = G(x, x) + 1$ and arguing as above we reach a contradiction. Therefore we have proved:

Theorem 8.43. *There is a partial binary computable function that cannot be extended to a total computable function.*

Proposition 8.44. *Let f be a partial k-ary function.*

(a) *f is computable if and only if $\mathrm{Gr}(f)$ is semi-computable.*

(b) *If f is computable, then $\operatorname{dom} f$ is semi-computable.*

(c) *If f is computable and $\operatorname{dom} f$ is computable, then $\mathrm{Gr}(f)$ is computable.*

Proof. (a) The reverse direction is Proposition 8.36. For the forward direction suppose f is computable. By Kleene's theorem there is $e \in \mathbb{N}$ such that $f(\vec{x}) = \mathrm{U}(\boldsymbol{\mu} y\, \mathrm{K}_n(\vec{x}, y, e))$. Then

$$(\vec{x}, y) \in \mathrm{Gr}(f) \Leftrightarrow \exists z \left[y = \mathrm{U}(z) \wedge \mathrm{K}_n(\vec{x}, z, e) \wedge \forall z' < z\, (\neg \mathrm{K}_n(\vec{x}, z', e)) \right].$$

The set in the square brackets is computable, and hence $\mathrm{Gr}(f)$ is semi-computable.

(b) $\vec{x} \in \operatorname{dom} f \Leftrightarrow \exists y\, [(\vec{x}, y) \in \mathrm{Gr}(f)]$, so we are done by part (a) and Proposition 8.37.

(c) If f is computable then $\mathrm{Gr}(f)$ is semi-computable by part (a), so it is enough to show that $\mathrm{Gr}(f)^{\complement}$ is semi-computable, and then apply Post's theorem. Since

$$(\vec{x}, y) \notin \mathrm{Gr}(f) \Leftrightarrow [\vec{x} \notin \operatorname{dom} f \vee \exists z\, (z \neq y \wedge (\vec{x}, z) \in \mathrm{Gr}(f))],$$

and $\operatorname{dom} f$ is computable, then $\mathrm{Gr}(f)^{\complement}$ is semi-computable. □

Corollary 8.45. *Let $D \subseteq \mathbb{N}^k$ be computable and let $f\colon D \to \mathbb{N}$. The following are equivalent:*

(a) *f is computable,*

(b) *$\mathrm{Gr}(f)$ is computable,*

(c) *$\mathrm{Gr}(f)$ is semi-computable.*

Theorem 8.46. *For every semi-computable $A \subseteq \mathbb{N}^2$ there is a unary computable g such that $\operatorname{dom} g = \operatorname{dom} A$ and $\forall x \in \operatorname{dom} A\, [(x, g(x)) \in A]$.*

Proof. If $B \subseteq \mathbb{N}^3$ is computable and such that $A(x, y) \Leftrightarrow \exists z\, B(x, y, z)$, then

$$g(x) = (\boldsymbol{\mu} w\, [B(x, (w)_0, (w)_1)])_0$$

is the required function. □

Corollary 8.47. *Every unary computable function has a computable right-inverse, that is: if f is unary computable there is g unary computable such that $\operatorname{dom} g = \operatorname{ran} f$ and $\forall y \in \operatorname{dom} g\, [f(g(y)) = y]$.*

Proof. Apply Theorem 8.46 to $A = \{(x, y) \in \mathbb{N}^2 \mid (y, x) \in \mathrm{Gr}(f)\}$. □

Recall that φ_e is the e-th computable unary function $x \mapsto \mathrm{U}(\boldsymbol{\mu} y\, \mathrm{K}_1(x, y, e))$. The **halting set**

$$H = \{e \in \mathbb{N} \mid \exists y\, (k_1(e, y, e) = 0)\} = \{e \in \mathbb{N} \mid \varphi_e(e)\downarrow\}$$

is the set of all programs that terminate when applied to themselves.

Theorem 8.48. *The set H is semi-computable, but not computable.*

Proof. The set H is semi-computable as it is the projection an elementary computable predicate. Towards a contradiction, suppose H is computable. We argue as in Proposition 8.42. The binary predicate $H(x) \Rightarrow \mathrm{K}_1(x, y, x)$ is computable and $f(x) = \mathrm{U}(\boldsymbol{\mu} y\, H(x) \Rightarrow \mathrm{K}_1(x, y, x)) + 1$ is a total computable unary function such that

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{if } x \in H \\ 1 & \text{otherwise.} \end{cases}$$

Let $e \in \mathbb{N}$ such that $\varphi_e = f$. As f is total, $e \in H$, so

$$\varphi_e(e) = f(e) = \varphi_e(e) + 1$$

a contradiction! □

A **Diophantine set** is of the form

$$\mathbb{N} \cap \{f(n_1, \dots, n_k) \mid n_1, \dots, n_k \in \mathbb{Z}\},$$

where $f \in \mathbb{Z}[x_1, \dots, x_n]$. Diophantine sets are semi-computable, and a deep theorem by Davis, Matiyasevich, Putnam and Robinson the converse holds.

Theorem 8.49. *Every semi-computable subset of* $\mathbb{N}$ *is Diophantine.*

8.F. Programs. To prove that $f\colon \mathbb{N}^k \to \mathbb{N}$ is in $\mathcal{F}$ where $\mathcal{F}$ is $\mathfrak{E}$, $\mathfrak{P}$, or $\mathfrak{C}$, one needs to show that f can be obtained from basic functions by means of specific constructions such as composition, generalized sums and products, primitive recursion, or minimization.

8.F.1. *Programs for elementary functions.* The first-order language $\mathcal{L}_{\mathcal{E}}$ for the elementary functions has constant symbols

$$\texttt{Add}, \quad \texttt{Mult}, \quad \texttt{Div}, \quad \texttt{Quot}, \quad \texttt{Proj}^n_k \quad (0 \leq k < n)$$

and $k+1$-ary function symbols

$$\texttt{Com}_k$$

and unary function symbols

$$\texttt{Sum} \quad \text{and} \quad \texttt{Prod}.$$

We will now show that each elementary function can be computed by closed terms of $\mathcal{L}_{\mathcal{E}}$, and for this reason these are called **programs** for elementary functions. The programs `Add`, `Mult`, `Div`, and `Quot` compute the binary functions $x+y$, $x \cdot y$, $|x-y|$, and $\lfloor x/y \rfloor$, respectively, and the program $\texttt{Proj}^n_k$ computes the projection function I^n_k. If `P` is a program that computes a k-ary function f and $\texttt{Q}_0, \dots \texttt{Q}_{k-1}$ are programs that compute the n-ary functions $g_0, \dots, g_{k-1}$ then

- $\texttt{Com}_k(\texttt{P}, \texttt{Q}_0, \dots, \texttt{Q}_{k-1})$ computes $f(g_0(\vec{x}), \dots, g_{k-1}(\vec{x}))$;
- `Sum(P)` and `Prod(P)` compute $\sum f$ and $\prod f$.

Thus every elementary function is computed by a program, but not every program computes an elementary function, since $\mathtt{Com}_k(\mathtt{P}, \mathtt{Q}_0, \dots, \mathtt{Q}_{k-1})$ is a meaningful just in case the arity of the described functions match accordingly. When this happens, we say it is a well-formed program, and write Elm for the collection of the well-formed programs. A program which is not well-formed is said to be ill-formed.[8] Let $\mathrm{ClTerm}_{\mathcal{E}}$ be the set of all closed terms of $\mathcal{L}_{\mathcal{E}}$, and let $\mathrm{ar}\colon \mathrm{ClTerm}_{\mathcal{E}} \to \mathbb{N}$ be the function defined by induction on the complexity of terms as follows:

$$\mathrm{ar}(\mathtt{Add}) = \mathrm{ar}(\mathtt{Mult}) = \mathrm{ar}(\mathtt{Div}) = \mathrm{ar}(\mathtt{Quot}) = 2$$

$$\mathrm{ar}(\mathtt{Sum}(\mathtt{P})) = \mathrm{ar}(\mathtt{Prod}(\mathtt{P})) = \mathrm{ar}(\mathtt{P})$$

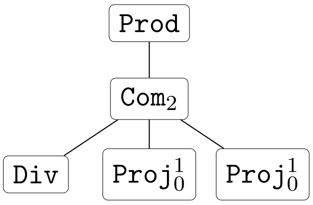
$$\mathrm{ar}\left(\mathtt{Com}_k(\mathtt{P}, \mathtt{Q}_0, \dots, \mathtt{Q}_{k-1})\right) = \begin{cases} n & \text{if } \mathrm{ar}(\mathtt{P}) = k \text{ and } \mathrm{ar}(\mathtt{Q}_i) = n \text{ for all } i < k, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\textsc{Elm} = \{\mathtt{P} \in \mathrm{ClTerm}_{\mathcal{E}} \mid \mathrm{ar}(\mathtt{P}) \neq 0\}$, and when $\mathtt{P} \in \textsc{Elm}$ and $f\colon \mathbb{N}^k \to \mathbb{N}$ is the function defined by P, then $k = \mathrm{ar}(\mathtt{P})$.

If $\mathtt{P}$ computes $f\colon \mathbb{N}^k \to \mathbb{N}$, and $\mathtt{Q}$ and $\mathtt{R}$ compute $x \mapsto x+1$ and $x \mapsto x \dot{-} 1$, respectively, then also $\mathtt{Com}_1(\mathtt{R}, \mathtt{Com}_1(\mathtt{Q}, \mathtt{P}))$ computes f. By iterating the silly procedure of adding and subtracting 1 at the end of a computation, we can construct infinitely many programs that compute the same functions, that is

$$\forall f \in \mathcal{E}\, [\{\mathtt{P} \in \textsc{Elm} \mid \mathtt{P} \text{ computes } f\} \text{ is infinite}]. \tag{8.9}$$

As noted in Section 3.A, any term of a first-order language is best described in terms of its syntactic tree. For example, the well-formed program $\mathtt{Prod}(\mathtt{Com}_2(\mathtt{Div}, \mathtt{Proj}^1_0, \mathtt{Proj}^1_0))$ that computes $\overline{\mathrm{sgn}}(x)$ can be written as



8.F.2. *Programs for primitive recursive functions.* The language $\mathcal{L}_{\mathcal{P}}$ for the primitive recursive functions has constant symbols $\mathtt{Zero}$, $\mathtt{Succ}$ and $\mathtt{Proj}^n_k$ for $0 \leq k < n$, a binary function symbol $\mathtt{Rec}$, and the $k+1$-ary function symbols $\mathtt{Com}_k$ as before. A program for a primitive recursive function is a closed term of $\mathcal{L}_{\mathcal{P}}$, and let $\mathrm{ClTerm}_{\mathcal{P}}$ be the set of all these programs. Every function in $\mathcal{P}$ is computed by some program:

- $\mathtt{Zero}$ and $\mathtt{Succ}$ compute the functions $n \mapsto c_0(n) = 0$ and $n \mapsto n+1$ respectively,

[8] In computer science we would say that the compiler returns a `syntax-error` message when dealing with an ill-formed program.

- $\texttt{Proj}^n_k$ and $\texttt{Com}_k$ act as before,
- if $\texttt{P}$ computes the k-ary function f and $\texttt{Q}$ computes the $k+2$-ary function g, then $\texttt{Rec}(\texttt{P},\texttt{Q})$ is the program computing the $k+1$-ary function $h(\vec{x},0) = f(\vec{x})$ and $h(\vec{x},y+1) = g(\vec{x},y,h(\vec{x},y))$.

Every primitive recursive function is computed by a program in $\mathrm{ClTerm}_{\mathfrak{P}}$ and, just as in the case of the elementary function, not every program computes a function. The set of all well-formed programs for primitive recursive functions is denoted by PREC, and in analogy with (8.9) we have that

$$\forall f \in \mathfrak{P}\,[\{\texttt{P} \in \mathrm{P}\textsc{Rec} \mid \texttt{P} \text{ computes } f\} \text{ is infinite}].$$

8.F.3. *Programs for computable functions.* The language $\mathcal{L}_{\mathfrak{C}}$ for computable functions has constant symbols $\texttt{Add}$, $\texttt{Mult}$, $\texttt{Less}$ and $\texttt{Proj}^n_k$ for $0 \leq k < n$, a unary function symbol $\texttt{Min}$, and the $k+1$-ary function symbols $\texttt{Com}_k$ as before. The set of all closed terms is denoted by $\mathrm{ClTerm}_{\mathfrak{C}}$, and its elements will be called programs for computable functions. Here $\texttt{Less}$ is the program that computes the binary function $\boldsymbol{\chi}_{\leq}(x,y)$, and if $\texttt{P}$ is a program that computes a $k+1$-ary function $f(\vec{x},y)$ such that $\forall\vec{x}\,\exists y\,[f(\vec{x},y)=0]$, then $\texttt{Min}(\texttt{P})$ is the program that computes the k-ary function $\vec{x} \mapsto \boldsymbol{\mu} y\,[f(\vec{x},y)=0]$.

Every computable function is computed by some program—in fact by an argument as in (8.9) it is computed by infinitely many programs. Just like what happened with $\mathfrak{E}$ and $\mathfrak{P}$, not every element of $\mathrm{ClTerm}_{\mathfrak{C}}$ computes a function of $\mathfrak{C}$, and we will write REC for the set of well-formed programs that do calculate computable functions, namely such that if we define an appropriate arity function $\mathrm{ar}\colon \mathrm{ClTerm}_{\mathfrak{C}} \to \mathbb{N}$ then $\texttt{P} \in \textsc{Rec}$ if and only if

(A) $\mathrm{ar}(\texttt{P}) \neq 0$, and

(B) if $\texttt{P}$ is $\texttt{Min}(\texttt{Q})$ and $\texttt{Q}$ computes some $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$, then for any $\vec{x}$ there is a y such that $f(\vec{x},y)=0$.

Note that checking (A) is a straightforward task, but guaranteeing (B) is much harder.

We can now sketch a the proof of Kleene's normal form Theorem 8.40. Given a program $\texttt{P}$ for a computable $f\colon \mathbb{N}^k \to \mathbb{N}$, the **complete computation** of $\texttt{P}$ on input $\vec{x} = (x_0,\dots,x_{k-1})$ is the sequence recording all calculations that lead to $f(\vec{x})$. The formal definition is a bit involved, since we need to code everything (programs, sequences of computations, ...) as natural numbers. Granted all this, one defines elementary predicates $\mathrm{K}_k \subseteq \mathbb{N}^{k+2}$ for $k>0$ such that $\mathrm{K}_k(e,\vec{x},y)$ holds if and only if

- e is a program for computable functions satisfying (A),
- $y = \boldsymbol{J}(n,s)$ where $s \in \mathrm{Seq}$ codes the computations that witness that n is the desired result.

The definition of K_k is by induction on the complexity of the closed term e. Given a computable function $f\colon \mathbb{N}^k \to \mathbb{N}$ pick a program $\mathtt{P}$ that computes it. Then for any $x_0, \dots, x_{k-1}$ there is a finite sequence of calculations that yield $f(\vec{x})$, and let s be the number coding such sequence; then $\mathrm{K}_k(\mathtt{P}, \vec{x}, \boldsymbol{J}(f(\vec{x}), s))$ holds and therefore $f(\vec{x}) = (\boldsymbol{\mu} y\, \mathrm{K}_k(\mathtt{P}, \vec{x}, y))_0$.

8.G. Computability on other domains. Given a bijection $u\colon \mathbb{N} \to X$ one can transfer the computability notions from $\mathbb{N}$ to X. For example, letting $u\colon \mathbb{N} \to \mathbb{Z}$, $u(2n) = n$ and $u(2n+1) = -n-1$, then addition and multiplication in $\mathbb{Z}$ are computable. This idea can be generalized to infinite countable first-order structures for **computable languages**, that is a language with countably many symbols R_n, f_m, c_i where each of n, m, i ranges over an initial segment of the natural numbers, and the maps $n \mapsto k$ and $m \mapsto k$ assigning to each R_n and f_m its arity are computable. An infinite countable $\mathcal{L}$-structure $\mathcal{M} = \langle M, R^{\mathcal{M}}, \dots, f^{\mathcal{M}}, \dots, c^{\mathcal{M}}, \dots \rangle$ is **computable** if it admits a **computable presentation**, that is a bijection $u\colon \mathbb{N} \to M$ such that for each n-ary function symbol f, the map

$$\mathbb{N}^n \to \mathbb{N}, \quad (k_1, \dots, k_n) \mapsto u^{-1}\bigl(f^{\mathcal{M}}(u(k_1), \dots, u(k_n))\bigr)$$

is computable, and for each n-ary predicate symbol R, the set

$$\{(k_1, \dots, k_n) \in \mathbb{N}^n \mid (u(k_1), \dots, u(k_n)) \in R^{\mathcal{M}}\}$$

is computable. The choice of the bijection u is important for checking the computability of the predicates and operations. It is easy to check that $(\mathbb{Z}, +, \cdot, <)$ is a computable ordered ring, but checking the analogous fact for other countable structures such as $(\mathbb{Q}, +, \cdot, <)$ can be very cumbersome.

8.H. Other definitions of computable functions*.

8.H.1. *Machines.*

Later

8.H.2. *Alternative presentation of computable functions.* An $f\colon \mathbb{N}^k \to \mathbb{N}$ is computable if and only if $f \circ \Phi^k\colon \mathbb{N} \to \mathbb{N}$ is computable, where $\Phi^k\colon \mathbb{N}^k \to \mathbb{N}$ is a computable bijection. (This is part (iv) of Exercise 8.61 when $\Phi^k = \boldsymbol{J}^k$ is obtained by composing $\boldsymbol{J}$ using the projection functions.) Therefore the family of all computable operations can be recovered from the set of computable unary functions, using any computable coding of sequences. This suggests the following question: is there a definition of the set of all unary computable functions that avoids n-ary operations with $n > 1$? The **quadratic-excess function** $\mathrm{Exc}\colon \mathbb{N} \to \mathbb{N}$ is defined by $\mathrm{Exc}(n) = n - (\lfloor \sqrt{n} \rfloor)^2$; it is elementary. The **inversion** of $f\colon \mathbb{N} \to \mathbb{N}$ is the partial function defined by $f^{-1}(m) = \boldsymbol{\mu} n\, [f(n) = m]$. A family $\mathcal{F}$ of partial unary functions is **closed under inversion** if $f^{-1} \in \mathcal{F}$ for every total $f \in \mathcal{F}$.

Theorem 8.50. *The family of computable functions is the smallest family of operations containing I^n_k, $+$, S,* Exc *and closed under composition and inversion.*

The family of computable unary functions is the smallest family of unary functions containing S and Exc*, and closed under composition, addition, and inversion.*

A similar result holds for primitive recursive functions.

Theorem 8.51. *$\mathcal{P}$ is the smallest family of operations containing I^n_k, $+$, S,* Exc*, and closed under composition and iterations without parameters.*

$\mathcal{P} \cap \mathbb{N}^{\mathbb{N}}$ is the smallest family of functions containing S, Exc*, and closed under addition, composition, and iterations without parameters.*

Exercises

Exercise 8.52. Let $\mathcal{F}$ be a family of operations, closed under composition.

(i) If $\mathcal{F}$ contains the projections, $\sigma\colon \{0, \dots, n-1\} \to \{0, \dots, m-1\}$ and $f \in \mathcal{F}$ is n-ary, then $g \in \mathcal{F}$ where

$$g(x_0, \dots, x_{m-1}) = f(x_{\sigma(0)}, \dots, x_{\sigma(n-1)}).$$

(ii) If $\mathcal{F}$ is closed under generalized sums and products, and if $f, g \in \mathcal{F}$ are $k+1$-ary, then the following are in $\mathcal{F}$:

$$(x_0, \dots, x_k) \mapsto \sum_{y < g(x_0, \dots, x_k)} f(x_0, \dots, x_{k-1}, y)$$

$$(x_0, \dots, x_k) \mapsto \prod_{y < g(x_0, \dots, x_k)} f(x_0, \dots, x_{k-1}, y).$$

Exercise 8.53. The following functions are in $\mathcal{E}$:

- the truncated difference

$$x \mathbin{\dot{-}} y = \begin{cases} x - y & \text{if } x \geq y, \\ 0 & \text{otherwise;} \end{cases}$$

- the function Rem of (8.3);
- the maximum and minimum functions $\max_k, \min_k\colon \mathbb{N}^k \to \mathbb{N}$

$$\max_k(x_0, \dots, x_{k-1}) = \max\{x_0, \dots, x_{k-1}\}$$
$$\min_k(x_0, \dots, x_{k-1}) = \min\{x_0, \dots, x_{k-1}\};$$

- the function $f\colon \mathbb{N}^2 \to \mathbb{N}$, $f(k, n) = 0$ if $k < 2$ or $n = 0$, and $f(k, n) = \lfloor \log_k n \rfloor$ otherwise.

Exercise 8.54. Show that the coding of pairs of natural numbers in Examples 8.8 (A), (B) and (C) are in $\mathcal{E}$.

Exercise 8.55. Let $\mathcal{F}$ be the smallest family of functions closed under compositions and primitive recursion and containing C_0, S and the projections I^n_k. Show that the following functions and predicates are in $\mathcal{F}$:

- the operations $x + y$, $x \cdot y$, x^y, $x \dot{-} 1$;
- $\overline{\mathrm{sgn}}(x)$, $\mathrm{sgn}(x)$, $x \dot{-} y$, $|x - y|$;
- $x < y$, $x \leq y$, $x = y$, $\lfloor x/y \rfloor$;
- if $f \in \mathcal{F}$ is $k + 1$-ary, then $\sum f, \prod f \in \mathcal{F}$.

Conclude that $\mathcal{P} = \mathcal{F}$.

Exercise 8.56. Let $\mathcal{F} \supseteq \mathcal{E}$ be a family of operations closed under composition, and generalized sum and product. Show that if the function g and the predicate A are in $\mathcal{F}$, then the following functions are in $\mathcal{F}$:

$$f_1(\vec{x}, y) = \begin{cases} \min\{z \leq y \mid A(\vec{x}, z)\} & \text{if this set is non-empty,} \\ 0 & \text{otherwise;} \end{cases}$$

$$f_2(\vec{x}, y) = \begin{cases} \max\{z \leq y \mid A(\vec{x}, z)\} & \text{if this set is non-empty,} \\ y & \text{otherwise;} \end{cases}$$

$$f_3(\vec{x}, y) = \begin{cases} \max\{z \leq y \mid A(\vec{x}, z)\} & \text{if this set is non-empty,} \\ 0 & \text{otherwise;} \end{cases}$$

$$f_4(\vec{x}, y) = \min\{g(\vec{x}, z) \mid z \leq y\};$$

$$f_5(\vec{x}, y) = \max\{g(\vec{x}, z) \mid z \leq y\}.$$

Exercise 8.57. Show that the following predicates and functions are in $\mathcal{E}$:

(i) the divisibility relation $x \mid y$, the set Pr of prime numbers, and the predicate $P(k, x)$: “x is the k-th prime”;

(ii) the function $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ enumerating Pr [Hint: $\mathbf{p}(k) \leq 2^{2^k}$];

(iii) the coding via exponential seen in Section 8.A.2, that is the functions $\mathbf{e}\colon \mathbb{N}^2 \to \mathbb{N}$ and $\mathbf{l}\colon \mathbb{N} \to \mathbb{N}$ defined on page 278 and the set $\mathrm{Seq}^* = \{\mathbf{p}(0)^{n_0+1} \cdots \mathbf{p}(k)^{n_k+1} \mid n_0, \ldots, n_k \in \mathbb{N}\}$;

(iv) the functions lcm and gcd;

(v) the function sending n to the number of primes $\leq n$;

(vi) Euler’s φ function, where $\varphi(n)$ is the number of $k < n$ that are coprime with n, with $\varphi(0) = 0$ by convention;

(vii) the functions ω and Ω defined by $\omega(0) = \omega(1) = \Omega(0) = \Omega(1) = 0$, and if $m = p_1^{k_1} \cdots p_n^{k_n}$ with $p_1 < \cdots < p_n$ primes, then $\omega(m) = n$ and $\Omega(m) = k_1 + \cdots + k_n$;

(viii) the function $\sigma_k\colon \mathbb{N} \to \mathbb{N}$ sending 0 to 0 and $n > 0$ to $\sum_{d|n} d^k$ the sum of divisors of n raised to the power k. In particular, $\sigma_0(n)$ counts the number of divisors of n and $\sigma_1(n)$ is the sum of the divisors of n. Thus the set of **perfect numbers**, that is the numbers n that are equal to the sum of their divisors $d < n$, i.e. such that $\sigma_1(n) = 2n$, is elementary recursive;

(ix) the function $f\colon \mathbb{N}^2 \to \mathbb{N}$ defined by

$$f(n,m) = \begin{cases} \dbinom{n}{m} & \text{if } m \leq n, \\ 0 & \text{otherwise;} \end{cases}$$

(x) the function $L_b\colon \mathbb{N} \to \{0, \ldots, b-1\}$, with $b > 1$, assigning to n its last digit in the expansion in base b;

(xi) the function $f\colon \mathbb{N} \to \mathbb{N}$

$$f(n) = \begin{cases} 0 & \text{if } n = 0 \text{ or } n \notin \mathrm{Seq} \\ 2^{m_0} + \cdots + 2^{m_k} & \text{if } n = \langle\!\langle m_0, \ldots, m_k \rangle\!\rangle. \end{cases}$$

Exercise 8.58. Show that:

(i) $\sigma\colon \mathbb{N} \to \mathbb{N}$ is in $\boldsymbol{\mathcal{E}}$ where

$$\sigma(s) = \begin{cases} 2^{m_0} + \cdots + 2^{m_k} & \text{if } s = \langle\!\langle m_0, \ldots, m_k \rangle\!\rangle \\ 0 & \text{if } s \notin \mathrm{Seq}; \end{cases}$$

(ii) for each $n \geq 1$ there exist unique $k \geq 0$ and $m_0 > \cdots > m_k$ such that $n = 2^{m_0} + \cdots + 2^{m_k}$;

(iii) the binary predicate

$$\{(m,n) \mid 1 \leq n = \sum_{i \leq k} 2^{m_i} \wedge m_0 > \cdots > m_k \wedge \exists i \leq k\, (m = m_i)\}$$

is in $\boldsymbol{\mathcal{E}}$.

Exercise 8.59. (i) Given $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ let $f^*\colon \mathbb{N}^{k+1} \to \mathbb{N}$ be defined by

$$f^*(\vec{x}, y) = 2^{f(\vec{x},0)+1} \cdot 3^{f(\vec{x},1)+1} \cdots \mathbf{p}(y)^{f(\vec{x},y)+1}$$

where $\mathbf{p}(i)$ is the i-th prime number (Exercise 8.57). In other words: f^* is the analogue of the memory-function f^{m} for the coding-scheme of Section 8.A.2. Show that $f \in \boldsymbol{\mathcal{E}} \Leftrightarrow f^* \in \boldsymbol{\mathcal{E}}$.

(ii) Let $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ be obtained by primitive recursion from $g\colon \mathbb{N}^{n+2} \to \mathbb{N}$ and $f\colon \mathbb{N}^n \to \mathbb{N}$. (If $n = 0$, that is if the recursion is without parameters, then f is a natural number.) Moreover suppose that $\forall \vec{x} \in \mathbb{N}^{n+1}\, [h(\vec{x}) \leq k(\vec{x})]$. Show that if $f, g, k \in \boldsymbol{\mathcal{E}}$ then $h \in \boldsymbol{\mathcal{E}}$.

(iii) Show that $f \in \boldsymbol{\mathcal{E}} \Leftrightarrow f^{\mathrm{m}} \in \boldsymbol{\mathcal{E}}$.

(iv) Repeat part (ii) when h is obtained from g and f using generalized primitive recursion (Definition 8.19).

(v) Prove that $\boldsymbol{\mathcal{E}}$ is the smallest family of operations on $\mathbb{N}$ containing C_0, S, I^n_k and closed under composition and bounded primitive recursion.

Exercise 8.60. Assume either $\mathcal{F} = \boldsymbol{\mathcal{E}}$ or $\mathcal{F} = \boldsymbol{\mathcal{P}}$. Show that:

(i) if $f\colon \mathbb{N} \to \mathbb{N}$ is increasing and belongs to $\mathcal{F}$, then $\operatorname{ran}(f)$ is in $\mathcal{F}$;

(ii) if f is the enumerating function of $A \subseteq \mathbb{N}$ which is in $\mathcal{F}$, and if there exists $h\colon \mathbb{N} \to \mathbb{N}$ in $\mathcal{F}$ such that $\forall n\,(f(n) \leq h(n))$ then $f \in \mathcal{F}$;

(iii) the enumerating function of Seq is elementary recursive.

Exercise 8.61. Let $\mathcal{F}$ be one of the classes $\boldsymbol{\mathcal{E}}$, $\boldsymbol{\mathcal{P}}$, $\boldsymbol{\mathcal{C}}^{\mathrm{tot}}$. Check that

(i) the functions $\boldsymbol{J}^m$ and $(\cdot)^m_i$ $(i < m)$ are in $\mathcal{F}$;

(ii) the $f_i\colon \mathbb{N}^n \to \mathbb{N}$ $(1 \leq i \leq m)$ are in $\mathcal{F}$ if and only if $\tilde{f}\colon \mathbb{N}^n \to \mathbb{N}$, $\tilde{f}(\vec{x}) = \boldsymbol{J}^m(f_0(\vec{x}), \dots, f_{m-1}(\vec{x}))$ is in $\mathcal{F}$.

(iii) $A \subseteq \mathbb{N}^m$ is in $\mathcal{F}$ if and only if $\{n \in \mathbb{N} \mid ((n)^m_0, \dots, (n)^m_{m-1}) \in A\}$ is in $\mathcal{F}$.

(iv) $f\colon \mathbb{N}^n \to \mathbb{N}$ is in $\mathcal{F}$ if and only if $\check{f}\colon \mathbb{N} \to \mathbb{N}$, $\check{f}(x) = f((x)^n_0, \dots, (x)^n_{n-1})$ is in $\mathcal{F}$.

Exercise 8.62. Write conditions (D) and (E) on page 217 as statements on natural numbers and check that S is elementary recursive.

Exercise 8.63. Show that **Fibonacci's sequence** defined as $F(0) = F(1) = 1$ and $F(n) = F(n-1) + F(n-2)$ when $n \geq 2$, is elementary recursive.

Exercise 8.64. Let $E\colon \mathbb{N}^2 \to \mathbb{N}$ be the primitive recursive function defined as

$$\begin{cases} E(x,0) = x \\ E(x,y+1) = x^{E(x,y)}. \end{cases}$$

Show that:

(i) $x \leq E(x,y)$;

(ii) $E(x,y) < E(x,y+1)$, if $x > 1$;

(iii) $E(x,y) < E(x+1,y)$, if $x > 1$;

(iv) $E(x,y) + E(x,z) < E(x,\max(y,z)+1)$, if $x > 1$;

(v) $E(x,y) \cdot E(x,z) < E(x,\max(y,z)+1)$, if $x > 1$;

(vi) $E(x,y)^{E(x,z)} < E(x,\max(y+1,z+2))$, if $x > 1$;

(vii) $E(E(x,y),z) \leq E(x,y+2z)$, if $x > 1$;

(viii) if $f \in \boldsymbol{\mathcal{E}}$ is k-ary, then there is $c \in \mathbb{N}$ such that

$$\max(\vec{x}) > 1 \Rightarrow f(\vec{x}) < E(\max(\vec{x}), c);$$

(ix) $E \notin \boldsymbol{\mathcal{E}}$.

Exercise 8.65. Show that if $f\colon \mathbb{N} \to \mathbb{N}$ is in $\boldsymbol{\mathcal{P}}$, then the function $(x, n) \mapsto f^{(n)}(x)$ coding the sequence of the iterates $f^{(n)}$ is in $\boldsymbol{\mathcal{P}}$.

Is the analogous statement for $\boldsymbol{\mathcal{E}}$ true?

Exercise 8.66. Let $\mathcal{F}$ be $\boldsymbol{\mathcal{P}}$ or $\boldsymbol{\mathcal{C}}^{\mathrm{tot}}$. Let h_0, h_1 be defined via the simultaneous recursion

$$\begin{cases} h_0(\vec{x}, 0) = f_0(\vec{x}) \\ h_0(\vec{x}, y+1) = g_0(\vec{x}, y, h_0(\vec{x}, y), h_1(\vec{x}, y)) \end{cases}$$
$$\begin{cases} h_1(\vec{x}, 0) = f_1(\vec{x}) \\ h_1(\vec{x}, y+1) = g_1(\vec{x}, y, h_0(\vec{x}, y), h_1(\vec{x}, y)). \end{cases}$$

Show that if $f_0, f_1, g_0, g_1 \in \mathcal{F}$, then $h_0, h_1 \in \mathcal{F}$.

Exercise 8.67. Verify that for all $m \in \mathbb{N}$ the function

$$\mathrm{Ack}_m\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \mathrm{Ack}(m, n)$$

is primitive recursive, where Ack is Ackermann's function.

Exercise 8.68. Prove Theorem 8.31 by verifying the following fact:

(i) $y < \mathrm{Ack}(x, y)$;

(ii) $\mathrm{Ack}(x, y) < \mathrm{Ack}(x, y+1)$;

(iii) $\mathrm{Ack}(x, y+1) \leq \mathrm{Ack}(x+1, y)$;

(iv) $\mathrm{Ack}(x, y) \leq \mathrm{Ack}(x+1, y)$;

(v) $\mathrm{Ack}(1, y) = y + 2$;

(vi) $\mathrm{Ack}(2, y) = 2y + 3$;

(vii) for all $c_1, \ldots, c_n$ there is d such that $\forall x \left(\sum_{1 \leq i \leq n} \mathrm{Ack}(c_i, x) \leq \mathrm{Ack}(d, x)\right)$;

(viii) for all n-ary $f \in \boldsymbol{\mathcal{P}}$ there is c such that $\forall x_1, \ldots, x_n\, (f(x_1, \ldots, x_n) < \mathrm{Ack}(c, x_1 + \cdots + x_n))$.

Exercise 8.69. Show that:

(i) $\overline{\mathrm{sgn}}(n) = \boldsymbol{\chi}_{\leq}(n + n, n)$, and $\mathrm{sgn} = \overline{\mathrm{sgn}} \circ \overline{\mathrm{sgn}}$ are computable.

(ii) The computable predicates are closed under Boolean operations (negation, conjunctions, disjunctions). Thus the binary predicates $=$, $\neq$, and $\leq$ are computable.

(iii) The maps $C_k\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto k$, are computable.

(iv) If P is computable, then so is $\exists z < y\, P(\vec{x}, z)$.

(v) $\boldsymbol{J}, (\cdot)_0, (\cdot)_1, \boldsymbol{\beta}$ are computable.

(vi) $f \in \boldsymbol{\mathcal{C}}^{\mathrm{tot}} \Leftrightarrow f^{\mathrm{m}} \in \boldsymbol{\mathcal{C}}^{\mathrm{tot}}$ where f^{m} is as the memory-function of f.

Let h be obtained from $f, g \in \mathfrak{C}^{\mathrm{tot}}$ by primitive recursion as in Definition 8.14, and let

$$G(\vec{x}, n, m) = \begin{cases} f(\vec{x}, n) & \text{if } m = 0, \\ g(\vec{x}, n, m) & \text{otherwise.} \end{cases}$$

Then $G \in \mathfrak{C}^{\mathrm{tot}}$ and $h(\vec{x}, n) = G(\vec{x}, n, h^{\mathrm{m}}(\vec{x}, n))$. Since

$$\begin{aligned} h^{\mathrm{m}}(\vec{x}, n) = \boldsymbol{\mu} y \, \big[&\mathrm{Seq}(y) \wedge \boldsymbol{\beta}(y, 0) = n \\ &\wedge \forall i < n \, \exists z \leq y \, (\forall j < i \, ((\!(y)\!)_j = (\!(z)\!)_i) \wedge (\!(y)\!)_i = G(z, i, n)) \big] \end{aligned}$$

is in $\mathfrak{C}^{\mathrm{tot}}$, it follows that $h \in \mathfrak{C}^{\mathrm{tot}}$. Conclude that $\mathfrak{P} \subseteq \mathfrak{C}^{\mathrm{tot}}$.

Exercise 8.70. If $\mathcal{F}$ is closed under primitive recursion, composition, and contains I^2_1, then $\mathcal{F}$ is closed under iterations. In particular, $\mathfrak{P}$ is closed under iterations.

Exercise 8.71. Show that every infinite semi-computable subset of $\mathbb{N}$ contains an infinite computable set.

Exercise 8.72. Prove part (c) of Proposition 8.39 without appealing to Church's Thesis.

Exercise 8.73. Let $\mathrm{Tot} = \{e \in \mathbb{N} \mid \varphi_e \colon \mathbb{N} \to \mathbb{N}\}$ be the set of all codes for total unary computable functions. Show that Tot is not semi-computable.

Notes and remarks

Our treatment of computability theory follows fairly closely [**Mon76**, Chapter 1]. The class $\mathfrak{E}$ of elementary recursive functions, introduced by Kalmàr in 1943, are the computable functions relevant to computer science. It is possible to avoid generalized sums and products in the definition of elementary function; in fact $\mathfrak{E}$ is the smallest class of functions closed under composition and containing the projections and a fixed set of functions, such as $\{S, x \dot{-} y, \lfloor x/y \rfloor, x^y\}$, or $\{x + y, x \dot{-} y, \lfloor x/y \rfloor, 2^y\}$, or $\{x + y, x^2, x \mod y, 2^y\}$ [**Maz02**]. The classes $\mathfrak{P}$ and of all computable functions were introduced earlier as an attempt to capture the notion of effective function by several mathematicians, including Gödel, Turing, and Post. Around 1920, Ackermann and Sudan, at the time Hilbert's students, came up with the first examples of computable, but not primitive recursive. The function Ack is a variant, due to Péter and R. Robinson of the original functions devised by Ackermann and Sudan. Theorems 8.50 and 8.51 are due to J. Robinson and R. Robinson, respectively, and can be found in [**Mon76**, Chapter 3].

The map $\boldsymbol{J}$ was defined by Cantor. It is a quadratic polynomial, and if a quadratic polynomial $f \in \mathbb{R}[x, y]$ yields a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, then either $f(x, y) = \boldsymbol{J}(x, y)$ or else $f(x, y) = \boldsymbol{J}(y, x)$ [**Smo91**].

Chapter III

Definability in algebra and number theory

9. Definability in algebra

9.A. Groups.

9.A.1. *Subgroups.* The language $\mathcal{L}_{\text{subGrp}}$ is $\mathcal{L}_{\text{Grps}}$ with an additional unary predicate symbol S. The $\mathcal{L}_{\text{subGrp}}$-structures are of the form $(G, \cdot, {}^{-1}, 1, H)$: if these satisfy the axioms for groups and the sentence

$$S(1) \land \forall x, y \left(S(x) \land S(y) \Rightarrow S(x \cdot y^{-1}) \right)$$

then we are considering groups together with a preferred subgroup. If we want to say that such subgroup is normal and non-trivial we use the sentence

$$\forall x, y \left(S(x) \Rightarrow S(y \cdot x \cdot y^{-1}) \right) \land \exists x \, (x \neq 1 \land S(x)) \land \exists x \neg S(x).$$

A group G is **simple** if it has no proper normal subgroups, that is if

$$\forall S \, (S \text{ normal subgroup} \land \exists x \, (S(x) \land x \neq 1) \Rightarrow \forall x \; S(x)) \, .$$

This is a formula in second-order logic (see Observation 3.25) since the universal quantifier ranges on subsets hence it is confined in the realm of pseudo-formulæ. In fact there is no system of first-order axioms whose models are the simple groups.

Theorem 9.1. *The class of all simple groups is not axiomatizable in any first-order language $\mathcal{L}$ extending $\mathcal{L}_{Grps}$.*

Proof. Towards a contradiction, suppose Σ is a set of $\mathcal{L}$-sentences such that $\text{Mod}(\Sigma)$ is the collection of all simple groups. Adding the commutativity property we obtain an axiom system Σ' such that $\text{Mod}(\Sigma')$ is the class of all abelian simple groups, that is to say those groups that are either trivial (i.e. consisting of one element) or else isomorphic to $\mathbb{Z}/p\mathbb{Z}$, with p prime. But this contradicts Theorem 4.48. □

9.A.2. *Ordered groups.* An ordering $\leq$ on a group G is compatible if one or both of the following holds in $(G, \cdot, \leq)$:

$$\forall x, y, z \, (x \leq y \Rightarrow z \cdot x \leq z \cdot y) \tag{9.1a}$$

$$\forall x, y, z \, (x \leq y \Rightarrow x \cdot z \leq y \cdot z). \tag{9.1b}$$

First of all observe that $\leq$ could be replaced by $<$ above, and that if G is abelian, then (9.1a) and (9.1b) are equivalent. If $(G, \cdot, \leq)$ satisfies (9.1a) then $\leq$ is a **left-order** on G, if it satisfies (9.1b) it is a **right-order**, and if it satisfies both (9.1a) and (9.1b) it is a **bi-order**. The notions of left/right order are dual to each other, in the sense that if $\leq$ is a left/right order on G then $\leq^\star$ is a right/left order on G, where

$$g \leq^\star h \Leftrightarrow h^{-1} \leq g^{-1}. \tag{9.2}$$

If $\leq$ is linear we speak of **linearly left-ordered** and **linearly right-ordered** groups. The **cone of positive elements** of G is

$$P_G = \{g \in G \mid 1 \leq g\}.$$

As customary in group theory, if $X, Y \subseteq G$ we set $X^{-1} = \{g^{-1} \mid g \in X\}$, $XY = \{gh \mid g \in X, h \in Y\}$, and $gX = \{g\}X = \{gh \mid h \in X\}$.

Lemma 9.2. *Let $\leq$ be a compatible order on G.*

(a) *If $\leq$ is a left-order then $g \leq h \Leftrightarrow g^{-1}h \in P_G$, if $\leq$ is a right-order then $g \leq h \Leftrightarrow hg^{-1} \in P_G$, and if $\leq$ is a bi-order then $g \leq h \Leftrightarrow h^{-1} \leq g^{-1}$.*

(b) *If $1_G < g$, then $o(g) = \infty$, and hence g cannot be maximal. If $g < 1_G$, then $o(g) = \infty$, and hence g cannot be minimal.*

(c) *$P_G \cap P_G^{-1} = \{1_G\}$ and $P_G^2 = P_G$.*

Proof. (a) is immediate.

If $1_G < g$ then $g < g^2$ (so that g cannot be maximal) and by transitivity and induction we have $1_G < g^n$ for all $n > 0$. The case when $g < 1_G$ is analogous, so (b) is proved.

We now prove (c). For the sake of definiteness let's assume that $\leq$ is a left-order on G, the case of right-orders being similar. If $g \in P_G \cap P_G^{-1}$, then $g = h^{-1}$ for some $h \in P_G$, so that $1_G = h^{-1}h \geq h^{-1}1_G = h^{-1} = g$, and hence $g = 1_G$. If $g, h \in P_G$, then $1_G \leq h$ so $g \leq gh$ and since $1_G \leq g$ we have $1_G \leq gh$. Therefore $P_G^2 \subseteq P_G$. The other inclusion follows from $1_G \in P_G$. □

If $\leq$ is the identity relation, that is $g \leq h \Leftrightarrow g = h$, then $(G, \cdot, \leq)$ is bi-ordered. In other words any group can be seen as an ordered group, but if we require more of the ordering the subject becomes less trivial. For example, by Lemma 9.2(b) if $(G, \leq)$ is upward (or downward) directed with more than one element, then G has a torsionless element, so G it must be infinite.

Lemma 9.3. *Let $\leq$ be a compatible order on G.*

(a) *If $\leq$ is a bi-order, then $gP_G g^{-1} = P_G$ for all $g \in G$.*

(b) *If $\leq$ is total, then $P_G \cup P_G^{-1} = G$.*

Proof. (a) If $\leq$ is a bi-order and $1_G \leq h$, then $g = g1_G \leq gh$ and $1_G = gg^{-1} \leq ghg^{-1}$. This implies that $gP_G g^{-1} \subseteq P_G$ for all $g \in G$. The other inclusion is similar.

(b) is immediate. □

Conversely:

Proposition 9.4. *Suppose G is a group and $P \subseteq G$ is such that $P \cap P^{-1} = \{1_G\}$ and $P^2 \subseteq P$.*

- *If $\forall g \in G \left(gPg^{-1} = P\right)$ then P is the positive cone of a bi-order on G.*
- *If $P \cup P^{-1} = G$ then P is the positive cone of a linear order on G, which can be taken to be either a left-order or a right-order.*

Proof. Define $\leq$ on G by $g \leq h \Leftrightarrow g^{-1}h \in P$. Clearly $\leq$ is reflexive and for transitivity argue as follows: if $g \leq h$ and $h \leq g$ then $g^{-1}h = (h^{-1}g)^{-1} \in P \cap P^{-1} = \{1_G\}$, so $g = h$.

Suppose $gPg^{-1} = P$ for all $g \in G$. If $g \leq h$ and $k_1, k_2 \in G$ are arbitrary, then $(k_1gk_2)^{-1}(k_1hk_2) = k_2^{-1}g^{-1}hk_2 \in k_2^{-1}Pk_2 = P$, so $k_1gk_2 \leq k_1hk_2$. This proves that $\leq$ is a bi-order on G.

Suppose now that $P \cup P^{-1} = G$. Then $g^{-1}h \in P$ or $h^{-1}g = (g^{-1}h)^{-1} \in P$, so either $g \leq h$ or $h \leq g$, for all $g, h \in G$. If $g \leq h$ and $k \in G$ then $(kg)^{-1}(kh) = g^{-1}h \in P$, so $kg \leq kh$. Thus $\leq$ is a linear left-order on G. In order to construct a linear right-order on G we repeat the argument above using the ordering $g \leq h \Leftrightarrow hg^{-1} \in P$. □

Therefore the class of ordered groups can be axiomatized in a language with a symbol for the binary operation, and a unary predicate symbol.

If $(G, \cdot_G, \leq_G)$ and $(H, \cdot_H, \leq_H)$ are linearly left/right-ordered groups, the product structure is not a linearly left/right-ordered group, unless one of the two factors is trivial. On the other hand, $(G \times H, \cdot_{G\times H}, \leq_{\text{lex}})$ is linearly left/right-ordered, where $\leq_{\text{lex}}$ is the lexicographic order on $G \times H$ (Definition 4.9). This suggests the following:

Definition 9.5. A group $(G, \cdot)$ is **left-orderable** if $(G, \cdot, \leq)$ is linearly left-ordered, for some $\leq$.

The notion of being **right-orderable** and **bi-orderable** are as expected, but observe that by (9.2) a group is left-orderable if and only if it is right-orderable. If an abelian group is left/right-orderable, then it is bi-orderable.

Examples 9.6. (a) The group $(\mathbb{R}, +)$ is bi-orderable, via the usual ordering on the reals. The group $(\mathbb{R}^2, +)$ is also bi-orderable, as witnessed by the lexicographic order or by the order given by any cone

$$P_\theta = \{(a, b) \in \mathbb{R}^2 \mid a = b = 0 \lor (a > 0 \land b < a\theta) \lor (a < 0 \land b \leq a\theta)\}$$

with $\theta \in \mathbb{R} \setminus \{1\}$.

(b) The group $(\mathbb{R} \setminus \{0\}, \cdot)$ is not orderable, since there is an element of order 2, against Lemma 9.2(b).

(c) The free group on 2 generators $\boldsymbol{F}(2)$ (see Section 18.D.2) is bi-orderable, so not all bi-orderable groups are abelian.

(d) An abelian group is orderable if and only if it is torsion-free (Exercise 32.13).

Thus the collection of all torsion-free abelian groups is an example of a class which is not finitely axiomatizable in a language $\mathcal{L}$, and that becomes finitely axiomatizable in some $\mathcal{L}' \supseteq \mathcal{L}$.

Definition 9.7. Let $\mathcal{L} \subseteq \mathcal{L}'$ be first-order languages. The **reduction** of an $\mathcal{L}'$-structure $\mathcal{M}'$ is the $\mathcal{L}$-structure $\mathcal{M}$ obtained by forgetting the interpretations of all symbols of $\mathcal{L}'$ that do not belong to $\mathcal{L}$. Conversely, an **expansion** of an $\mathcal{L}$-structure $\mathcal{M}$ is any $\mathcal{L}'$-structure $\mathcal{M}'$ whose reduction is $\mathcal{M}$.

The reduction of a rng $(R, +, -, 0, \cdot)$ is the abelian group $(R, +, -, 0)$; conversely any abelian group $(G, +, -, 0)$ can be expanded (possibly in more than one way) to a rng $(G, +, -, 0, \cdot)$, for example by setting $a \cdot b = 0$ for all $a, b \in G$. Recall Definition 4.51 of (basic) elementary class.

Definition 9.8. A class $\mathscr{C}$ of $\mathcal{L}$-structures is **pseudo-elementary** (**basic pseudo-elementary**) if it is the collection of reductions of structures in some elementary (respectively: basic elementary) class $\mathscr{C}'$ in a language $\mathcal{L}' \supseteq \mathcal{L}$.

The essence of Example 9.6(d) is that the class of all torsion-free abelian groups is elementary, but not basic elementary in $\mathcal{L}_{\text{AbGr}}$, but it is basic pseudo-elementary.

Definition 9.9. A linearly ordered group G is **Archimedean** if for all $1_G < g < h$ there is $n \in \mathbb{N}$ such that $h \leq g^n$.

The additive group structure of an Archimedean field (see Section 4.L) is an Archimedean group, and $\mathbb{R}$ and its subgroups are examples of Archimedean groups. In fact by a theorem of Hölder, every Archimedean group is isomorphic to a subgroup of $(\mathbb{R}, +)$ [**Bly05**, Theorem 10.16 p. 188]. In particular, any Archimedean group being abelian it is usually denoted using the additive notation $(G, +, \leq)$, and the equations (9.1) become

$$\forall x, y, z\, (x \leq y \Rightarrow x + z \leq y + z).$$

The class $\mathscr{C}$ of all Archimedean ordered groups is not pseudo-elementary. In fact if $\mathscr{C}$ were the collection of all reductions of an axiomatizable class $\mathscr{C}'$ in a language $\mathcal{L}'$, then all $\mathscr{C}'$ and hence $\mathscr{C}$ must have structures of arbitrarily large cardinality (Theorem 31.29), against Hölder's theorem.

Examples of non Archimedean linearly ordered groups are $\mathbb{Z} \times \mathbb{Z}$ with the lexicographic order, and $\boldsymbol{F}(2)$ (Example 9.6(c)).

In a linearly (left-)ordered group G the ordering $\leq$ is highly homogeneous: if $a < b$ and $c < d$ and $a^{-1} \cdot b = c^{-1} \cdot d$ then there is an increasing bijection $f\colon G \to G$ such that $f(a) = c$, $f(b) = d$, and mapping $(a; b)$ onto $(c; d)$—just take $f(x) = c \cdot a^{-1} \cdot x$. In particular we have two mutually exclusive possibilities:

- the ordering is **discrete** that is $\forall x\, \exists y\ (x < y \wedge \neg \exists z\, (x < z \wedge z < y))$ that is $\exists y (1_G < y \wedge \neg \exists z\, (1_G < z \wedge z < y))$;
- the ordering is **dense**, that is $\forall x, y\, (x < y \Rightarrow \exists z\, (x < z \wedge z < y))$ that is $\forall y (1_G < y \Rightarrow \exists z\, (1_G < z \wedge z < y))$.

The ordering of $G = (\mathbb{Z}, +)$ is discrete, as there is no element between 0 (that is 1_G) and the element 1, while the ordering of $G = (\mathbb{Q}, +)$ is dense. In a divisible ordered abelian group the order is dense, but the converse does not hold (Exercise 9.19).

Adding to the theory of ordered abelian groups the axioms δ_n for divisibility (see page 97), the theory of **divisible ordered abelian groups** is obtained. It is a non-finitely axiomatizable theory (Exercise 9.24(i)) and in Chapter VII (Exercise 31.56(iv)) we will see that it is a complete theory. Therefore every divisible ordered abelian groups is elementarily equivalent to $(\mathbb{Q}, +, <)$ or, equivalently to $(\mathbb{R}, +, <)$.

9.A.3. *$\mathbb{Z}$-groups.* When dealing with ordered abelian groups it is customary to adopt the additive notation, so if $(G, +_G, -_G, 0_G, \leq_G)$ is discrete, then there is an element denoted by 1_G such that $0_G <_G 1_G$ and there is no element between 0_G and 1_G.[1] Thus it is convenient to work with the language $\mathcal{L}$ with an additional symbol 1 so that a discretely ordered abelian group is an $\mathcal{L}$-structure $(G, +_G, -_G, 0_G, 1_G, \leq_G)$ satisfying the relevant axioms.

The group $\mathbb{Z} \times \mathbb{Z}$ with the lexicographic order $\leq_{\text{lex}}$ is a discretely ordered abelian group with $1_{\mathbb{Z}\times\mathbb{Z}} = (0, 1)$. Moreover the element $(1, 0)$ is neither even

[1] In this case 1_G does not denote the identity of the group, which is 0_G, but the element that is immediately above 0_G.

nor odd, that is

$$\tag{9.3} \begin{aligned} \neg\exists(n,m) \in \mathbb{Z}\times\mathbb{Z}\,\big[&(n,m)+(n,m)=(1,0) \\ &\vee\ (n,m)+(n,m)=(1,0)+1_{\mathbb{Z}\times\mathbb{Z}}\big]. \end{aligned}$$

For a fixed $n \geq 2$, every integer is congruent modulo n to some $1 \leq m \leq n$, that is $\mathbb{Z}$ satisfies the sentences

$$\tag{π_n} \forall x\,\exists y\,\Big(\bigvee_{1\leq m\leq n} x + m1 = ny\Big).$$

By (9.3) $\mathbb{Z}\times\mathbb{Z}$ does not satisfy π_2, hence the theory of discretely ordered abelian groups is not complete.

A discretely ordered abelian group satisfying the axioms π_n for $n \geq 2$, is a **$\mathbb{Z}$-group**. The theory of $\mathbb{Z}$-groups is not finitely axiomatizable (Exercise 9.24(ii)) and in Chapter VII (Exercise 31.56(v)) we will prove that it is complete. Thus every $\mathbb{Z}$-group is elementarily equivalent to $(\mathbb{Z}, +, -, 0, 1, <)$.

If G is an ordered abelian group, then $G \times \mathbb{Z}$ is a divisible, discretely ordered abelian group with the lexicographic order. If moreover G is divisible, then $G \times \mathbb{Z}$ is a $\mathbb{Z}$-group.

If G is a discretely ordered abelian group, then $Z = \{k1_G \mid k \in \mathbb{Z}\}$ is a subgroup of G isomorphic to $\mathbb{Z}$ and G/Z is abelian. Moreover, if $a+Z \neq b+Z$, then either $a + Z < b + Z$, that is $\forall g \in a + Z\,\forall h \in b + Z\ (g < h)$ or else $b + Z < a + Z$, that is $\forall g \in a + Z\,\forall h \in b + Z\ (h < g)$. Therefore G/Z is an ordered abelian group. Moreover, if G is a $\mathbb{Z}$-group, then G/Z is divisible.

9.B. Rings. Recall that $\mathcal{L}_{\text{Rings}}$ consists of two binary function symbols $+$ and $\cdot$, a unary function symbol $-$, together with two constant symbols 0 and 1. An $\mathcal{L}$-structure $(R, +, -, \cdot, 0, 1)$ satisfying (3.11) and (3.12) on page 53 is a ring. Every integer $n \in \mathbb{Z}$ can be identified with a closed term: assign to $n > 0$ the term $n1$ using the notation for terms nt introduced on page 25, then extend this identification to $\mathbb{Z}$. The closed terms $2 + 2$, $2 \cdot 2$ and 4 are distinct: in an arbitrary $\mathcal{L}$-structure they may denote different elements, but in a ring they denote the same object. Similarly, to each polynomial $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$ we assign the term

$$a_0 + (a_1 \cdot x) + (a_2 \cdot x^2) + \cdots + (a_n \cdot x^n).$$

This example is quite general, since every term of our language can be seen as a polynomial in several variables with integer coefficients.

Given a ring R, every element of the prime subring is definable by means of the formula $x = n$, for some $n \in \mathbb{Z}$. If R has finite characteristic m, the prime subring $\mathbb{Z}/m\mathbb{Z}$ is definable in R via the formula $x = 0 \vee x = 1 \vee \cdots \vee x = m-1$. If R has finite characteristic 0, the definability of the prime subring $\mathbb{Z}$ depends on R. In Section 11 we will see that $\mathbb{Z}$ is definable in $\mathbb{Q}$, but it is not definable in $\mathbb{R}$ or in $\mathbb{C}$. On the other hand $\mathbb{Z}$ is always definable in $\Bbbk[X]$ for any field $\Bbbk$ of zero characteristic (Exercise 9.22).

9.B.1. *Ideals.* If we need to formalize in the language of rings facts involving ideals, we face obstacles similar to the ones encountered when looking at subgroups in the language of groups. Also in this case we add a new unary predicate symbol I to $\mathcal{L}_{\mathrm{RINGS}}$, and add as axiom

(9.4) $\exists x I(x) \land \neg I(1) \land \forall x, y, z\, (I(x) \land I(y) \Rightarrow I(x - y) \land I(x \cdot z) \land I(z \cdot x))$

saying that the truth set of $I(x)$ is a proper (two-sided) ideal. The notion of prime and maximal ideal are rendered by $\forall x, y\, (I(x \cdot y) \Rightarrow I(x) \lor I(y))$ and $\forall x\, (\neg I(x) \Rightarrow \exists y\, I(x \cdot y - 1))$, respectively.

Definition 9.10. A semi-rng is an algebraic structure $(R, +, \cdot, 0)$ such that $(R, +, 0)$ is a commutative monoid, $(R, \cdot)$ is a semigroup, the operation $\cdot$ is distributive with respect to $+$, and $0 \cdot x = x \cdot 0 = 0$ for all $x \in R$. If there is an element $1 \in R$ that is neutral with respect to $\cdot$ it is called a semi-ring, and if the operation $\cdot$ is commutative it is called a commutative semi-rng. The language for semi-rngs is obtained by removing the symbol $-$ from the language $\mathcal{L}_{\mathrm{RNGS}}$.

Every rng is a semi-rng. Examples of semi-rngs that are not rngs, are

- $\mathbb{N}$ with the usual operations,
- $\mathbb{R} \cup \{+\infty\}$ with the operation of addition $x \oplus y \overset{\mathrm{def}}{=} \min(x, y)$ and multiplication $x \otimes y \overset{\mathrm{def}}{=} x + y$, with the convention that $x + y = +\infty$ whenever at least one among x and y are $+\infty$,[2]
- the set of all ideals in a r(i)ng,
- the set $R[X]$ of all polynomials with coefficients in a semi-r(i)ng R,
- a family of sets containing the empty set and closed under finite unions and intersections, or more generally, a distributive lattice with minimum (see Section 7.D).

9.B.2. *Ordered fields.* As mentioned on page 55 an ordered field is an $\mathcal{L}_{\mathrm{ORINGS}}$-structure satisfying T_{OFLDS}, that is the axioms for fields and the compatibility of the ordering with the operations. Equivalently (Exercise 9.29) it is a structure for the language extending $\mathcal{L}_{\mathrm{RINGS}}$ via a unary predicate P, satisfying

$$\forall x\, (P(x) \veebar P(-x) \veebar x = 0)$$
$$\forall x, y\, (P(x) \land P(y) \Rightarrow P(x + y) \land P(x \cdot y))$$

In other words: an ordered field is a field F with a distinguished subset P, called the cone of positive elements, which is closed under addition and

[2] This semi-ring is of central importance in an area of mathematics known as *tropical geometry*, hence $\mathbb{R} \cup \{+\infty\}$ is known as the *tropical semi-ring.*

multiplication, and so that F is partitioned into three disjoint subsets P, $-P$ and $\{0\}$.

Definition 9.11. An ordered field is **real closed** if every positive element is a square and every polynomial of odd degree has a root.

Examples of Archimedean real closed fields are $\mathbb{R}$ and $\overline{\mathbb{Q}} \cap \mathbb{R}$, the field of algebraic real numbers. Real closed fields are axiomatizable by adding to $T_{\mathrm{OF}_{\mathrm{LDS}}}$ the existence of the square root of positive elements

$$\forall x \left(x \geq 0 \Rightarrow \exists y \, (y^2 \mathrel{\dot{=}} x) \right)$$

together with the infinite sentences asserting that all polynomials of odd degree have a root:

$$(\rho_n) \qquad \begin{aligned} &\forall a_0, \ldots, a_{2n+1} \bigl(a_{2n+1} \neq 0 \Rightarrow \\ &\quad \exists x \left(a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{2n+1} \cdot x^{2n+1} \mathrel{\dot{=}} 0 \right) \bigr). \end{aligned}$$

In Chapter **??** we shall prove that the theory of real closed fields is complete, hence every real closed field is elementarily equivalent to the real field $\mathbb{R}$. We will show that no finite sub-list of the ρ_ns is enough for the definition of a real closed field, hence by Theorem 4.49 the first-order theory of real closed fields is not finitely axiomatizable.

9.B.3. *Vector spaces.* The first-order language considered up to now had finitely many non-logical symbols, but it is easy encounter languages that do not fit in this picture. For example we can consider a vector space over a field $\Bbbk$ as a structure $(V, +, \{f_x \mid x \in \Bbbk\}, \mathbf{0})$ where $+\colon V \times V \to V$ is the sum of vectors, $\mathbf{0} \in V$ is the zero vector and $f_x\colon V \to V$, $f_x(\mathbf{v}) = x\mathbf{v}$ is the scalar multiplication. The language $\mathcal{L}_\Bbbk$ has as many unary operations as the elements of $\Bbbk$. More generally a left R-module (with R a ring) can be seen as a structure $(M, +, \{f_x \mid x \in R\}, \mathbf{0})$, where $f_x\colon M \to M$, $f_x(m) = xm$, is the multiplication by $x \in R$. (If $\Bbbk$ and R are finite, then so are $\mathcal{L}_\Bbbk$ and $\mathcal{L}_R$.)

Similarly one can axiomatize the notion of G-set, that is a non-empty set X together with an action of the group G on X, that is a map $G \times X \to X$, $(g, x) \mapsto g.x$, such that $1_G.x = x$ and $g.(h.x) = (gh).x$ for all $g, h \in G$ and $x \in X$. The ensuing structure will be of the form $(X, \{f_g \mid g \in G\})$ where $f_g(x) = g.x$.

Remark 9.12. Having seen these examples, the reader might ask what is the point in focusing on first-order languages, since many concepts in various areas of mathematics seem to require quantification over the natural numbers or over arbitrary subsets of the structure. The reason is simple: first-order logic allows us to prove results on models (for example: the Compactness Theorem 4.46) that would not be provable in a more general context.

9.C. Many-sorted structures and languages. The first-order structures seen so far (groups, rings, ...) have the peculiarity that all of their elements are of the same kind. There are nevertheless cases in mathematics where items of different kind conjure to build a new object.

9.C.1. *Vector spaces as two-sorted structures.* The definition of vector space over a field $\Bbbk$ (or more generally: the definition of R-module) uses two types of objects, vectors and scalars. In Section 9.B.3, the field of scalars is hidden by the unary functions f_x, with $x \in \Bbbk$, but what if we want to give a first-order axiomatization of the notion of vector space, irrespective of the field $\Bbbk$? A solution is to consider structures M where the universe is of the form $W \uplus \Bbbk$, with two unary predicates V and $S(x)$ to formalize "x is a vector" and "x is a scalar", so that the structure satisfies the sentence

$$\forall x \ (V(x) \Leftrightarrow \neg S(x)) \, .$$

That is to say: every element is either a vector or a scalar, but not both. The symbols $\oplus$ and $\otimes$ are used for sum of vectors and scalar multiplication, and $\boxplus$ and $\boxtimes$ for the operations on the field $\Bbbk$. The problem is that $\oplus, \otimes, \boxplus, \boxtimes$ are partial functions, defined only on certain pairs of elements, hence these should be construed as ternary predicates. In other words, among the axioms we must add statements of the form

$$\forall x, y \ (V(x) \land V(y) \Rightarrow \exists ! z \, (\oplus(x, y, z)))$$

and similarly for $\otimes$, $\boxplus$ and $\boxtimes$. For example, commutativity of addition of vectors is stated as

$$\forall x, y, z \ (V(x) \land V(y) \land V(z) \land \oplus(x, y, z) \Rightarrow \oplus(y, x, z))$$

and distributivity of scalar multiplication with respect to addition of vectors can be stated as

$$\forall x, y, z, x', y', z', w \, \big[V(x) \land V(y) \land V(z) \land V(x') \land V(y') \land V(z') \land \\ S(w) \land \otimes(w, x, x') \land \otimes(w, y, y') \land \otimes(w, z, z') \land \oplus(x, y, z) \Rightarrow \oplus(x', y', z') \big] .$$

We leave to the reader to check that notion of vector space over an arbitrary field is finitely axiomatizable using the symbols $V, S, \oplus, \otimes, \boxplus$ and $\boxtimes$.

The formalization just presented is rather baroque, since we must specify if a variable ranges over vectors of scalars. Mathematical practice suggests to introduce two types of variables: those for vectors, denoted with boldface letters $\mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots$, and those for scalars, denoted with Greek letters $\alpha, \beta, \gamma, \ldots$. From scalar variables it is possible to construct scalar terms using $\boxplus$ and $\boxtimes$; a vector term is defined as follows: every vector variable is a vector term, the symbol $+$ applied to vector terms yields a vector term, and the symbol $\cdot$ applied to a scalar and a vector term yields a vector term. Therefore distributivity of scalar multiplication with respect to addition becomes

$$\forall \mathbf{u}, \mathbf{v}, \alpha \left[\alpha \cdot (\mathbf{u} + \mathbf{v}) = \alpha \cdot \mathbf{u} + \alpha \cdot \mathbf{v}\right].$$

9.C.2. *A family of sets as a two sorted structure.* Another example of two sorted structure is given by any family $\mathcal{S} \subseteq \mathscr{P}(A)$. In order to see $\mathcal{S}$ as a first-order structure, fix two unary predicates, U for the elements of A and S for the sets in $\mathcal{S}$, plus a binary predicate E to tell when an element belongs to a set. Thus $\mathcal{S}$ can be seen as a structure $\mathcal{M} = (M, U^{\mathcal{M}}, S^{\mathcal{M}}, E^{\mathcal{M}})$ where $M = A \uplus \mathcal{S}$, $U^{\mathcal{M}} = A$, $S^{\mathcal{M}} = \mathcal{S}$, and $E^{\mathcal{M}} = \{(x, X) \in A \times \mathcal{S} \mid x \in X\}$. The structure $\mathcal{M}$ satisfies

$$\begin{gathered} \forall x (U(x) \Leftrightarrow \neg S(x)) \\ \forall x, y\, (S(x) \wedge S(y) \wedge \forall z\, [U(z) \Rightarrow (E(z, x) \Leftrightarrow E(z, y))] \Rightarrow x = y), \end{gathered} \tag{9.5}$$

that is: any object is either a point or else a set, and two sets are the same if they have the same elements.

If we want to describe $\mathcal{M}$ as a two-sorted structure it is convenient, as in the case of vector spaces, to distinguish variables for elements of A (denoted with lower case letters $x, y, z, \ldots$) from variables for subsets of A (denoted with capital letters $X, Y, Z, \ldots$). Then (9.5) becomes

$$\begin{gathered} \forall X\, \forall x\ (X \neq x) \\ \forall X, Y\ [\forall z\ (E(z, X) \Leftrightarrow E(z, Y)) \Rightarrow X = Y]\,, \end{gathered}$$

If we require that $\emptyset \in \mathcal{S}$, that $\mathcal{S}$ be closed under complements and under intersections, then $\mathcal{M}$ must satisfy

$$\begin{gathered} \exists X\ (\neg \exists x\, E(x, X))\,, \\ \forall X\, \exists Y\, \forall z\ (E(z, X) \Leftrightarrow \neg E(z, Y))\,, \\ \forall X, Y\, \exists Z\, \forall w\ [E(w, Z) \Leftrightarrow (E(w, X) \wedge E(w, Y))]\,. \end{gathered}$$

Conversely, a two-sorted structure $\mathcal{M}$ satisfying the statements above, is of the form $\mathcal{S} \subseteq \mathscr{P}(A)$ where $\emptyset \in \mathcal{S}$ is a closed under complements and intersections (and hence closed under unions and $A \in \mathcal{S}$). Families $\mathcal{S}$ as above are Boolean algebras, and were introduced in Section 7.

9.C.3. *Directed multigraphs.* A **multigraph** is a set V together with a set E of edges between them. The difference between this notion and that of a graph in Section 3.D.2 is that there might be several edges between the same vertexes, and that a vertex may be linked to itself. A **directed multigraph** is a multigraph in which the edges have an orientation. It can be seen as a two-sorted structure (V, E, s, t) with $s, t \colon E \to V$ assigning to each edge e a vertex $s(e)$ called source, and a vertex $t(e)$ called target. If one wants to recast this as a familiar one-sorted structure, we introduce a language with two unary predicates $V(x), E(x)$ and two binary predicates $s(x,y)$ and $t(x,y)$ and require that the structure $\mathcal{M} = (M, V^{\mathcal{M}}, E^{\mathcal{M}}, s^{\mathcal{M}}, t^{\mathcal{M}})$ satisfies:

$$\forall x(V(x) \Leftrightarrow \neg E(x))$$
$$\forall x,y\,(s(x,y) \Rightarrow E(x) \wedge V(y)) \wedge \forall x\,(E(x) \Rightarrow \exists! y\, s(x,y))$$
$$\forall x,y\,(t(x,y) \Rightarrow E(x) \wedge V(y)) \wedge \forall x\,(E(x) \Rightarrow \exists! y\, t(x,y)).$$

9.D. Further examples*.

9.D.1. *Notions involving ideals.* Notions involving quantifications over ideals cannot, in general, be formalized in first-order logic. The **radical** of an ideal $\mathfrak{a}$ of a commutative ring R is the ideal

$$\sqrt{\mathfrak{a}} = \{x \in R \mid \exists n \in \mathbb{N}\,(x^n \in \mathfrak{a})\}\,.$$

When $\mathfrak{a} = \{0_R\}$ is the null ideal, we have the **nil-radical** $\mathrm{Nil}(R)$ of R. Even if $\mathfrak{a}$ is definable, it may happen that $\sqrt{\mathfrak{a}}$ is not definable; in particular the nil-radical is not, in general, a definable subset of R. An equivalent[3] formulation is given by [**AM69**, Prop. 1.8, Chapter 1]

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ prime ideal and } \mathfrak{p} \supseteq \mathfrak{a}\}\,,$$

but in this case this definition uses a quantification over subset. On the other hand, the **Jacobson radical**

$$\mathrm{Jac}(R) = \bigcap \{\mathfrak{m} \mid \mathfrak{m} \text{ maximal ideal}\}$$

is definable, since it is the truth set of the formula $\forall y \exists z\,((1 - x \cdot y) \cdot z = 1)$ [**AM69**, Prop. 1.9, Chapter 1].

A commutative ring with $0_R \neq 1_R$ is said to be **Noetherian** if every increasing sequence of proper ideals

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

is such that $J_n = J_{n+1}$ for all sufficiently large n. Equivalently: a ring is Noetherian if every proper ideal is finitely generated. Noetherian rings are not first-order axiomatizable, but the collection of rings that are *not* Noetherian is axiomatizable, provide that we add a unitary predicate I. In fact it is enough to require T_{CRings} together with the sentence (9.4) that says that the truth set of I is an ideal, and the sentences

$$\forall x_1, \dots, x_n \left(\bigwedge\nolimits_{1 \leq i \leq n} I(x_i) \Rightarrow \exists y\,(I(y) \wedge \forall z_1, \dots, z_n\,(\textstyle\sum_{i=1}^n z_i \cdot x_i \neq y))\right)$$

for all $n \geq 1$.

A commutative ring such that $0_R \neq 1_R$ and with exactly one maximal ideal is called a **local ring**. This notion would not seem be formalizable in the extended language of Section 9.B.1, because of the quantification on

[3] The equivalence of the two definitions depends on the axiom of choice.

subsets. But a commutative ring R such that $0_R \neq 1_R$ is local if and only if either x or $1 + x$ is invertible for all $x \in R$ [**AM69**, Prop. 1.6, Chapter 1], so being a local ring is indeed formalizable in $\mathcal{L}_{\text{Rings}}$.

A ring R is **von Neumann regular** if every finitely generated left ideal is generated by an idempotent—see [**Kap95, Goo91**]. Examples of von Neumann regular rings are: any skew-field, the ring of endomorphism of a vector space over a skew-field, and Boolean rings (p. 176). The definition above is not first-order, but a different equivalent definition entails finite axiomatizability: R is a von Neumann regular ring if and only if $\forall x \in R\, \exists y \in R\, (x = xyx)$.

9.D.2. *Rings of holomorphic functions.* A function $f \colon U \to \mathbb{C}$, with U a nonempty open subset of $\mathbb{C}$, is **holomorphic** if it is differentiable in all points of its domain, i.e. $\lim_{w \to z} \frac{f(w)-f(z)}{w-z}$ exists for all $z \in U$. An entire function is a holomorphic function on $\mathbb{C}$. The set $\mathcal{H}(U)$ of holomorphic functions on U is a commutative ring with the operations of pointwise addition and product. By identifying each complex number with the constant function on U defined by it, we have that $\mathbb{C} \subseteq \mathcal{H}(U)$. The study of $\mathcal{H}(U)$ is very important for classifying the open set U up to conformal equivalence—two open sets U, U' are conformally equivalent if there is a holomorphic bijection $\phi \colon U \to U'$. If $\phi \colon U \to U'$ is a holomorphic bijection, then $\Phi \colon \mathcal{H}(U) \to \mathcal{H}(U')$, $f \mapsto f \circ \phi^{-1}$, is a ring isomorphism such that $\Phi(\mathrm{i}) = \mathrm{i}$. Conversely, if $\Phi \colon \mathcal{H}(U) \to \mathcal{H}(U')$ is a ring isomorphism such that $\Phi(\mathrm{i}) = \mathrm{i}$, then U and U' are conformally equivalent [**LR84**, p. 130]. Therefore the ring structure $\mathcal{H}(U)$ encodes all the information on the complex structure of U.

As we observed $\mathbb{C}$ is contained in the ring $\mathcal{H}(U)$—in fact it is a definable subset [**Huu94**]. The proof is non-trivial, but in the case $U = \mathbb{C}$ is easier, as it follows from an application of Picard's Little Theorem [**Con78**, p. 297]: *An entire non-constant function can avoid at most one values, that is if f is entire and $\mathbb{C} \setminus \operatorname{ran}(f)$ has at least two points, then f is constant.* Thus $\mathbb{C}$ is defined in $\mathcal{H}(\mathbb{C})$ by the formula $\varphi_{\mathbb{C}}(x)$

$$x \mathrel{\dot{=}} 0 \lor x \mathrel{\dot{=}} 1 \lor (x \mid 1 \land (x - 1) \mid 1)\,.$$

The constants 0, 1 and the divisibility predicate $\mid$ are definable in the ring $\mathcal{H}(\mathbb{C})$, and will be used freely.

Although $\mathbb{N}$ is not definable in the complex field $\mathbb{C}$, it is definable in the ring $\mathcal{H}(\mathbb{C})$. Let us show that the formula $\varphi_{\mathbb{N}}(x)$

$$x \in \mathbb{C} \land \forall f, g\, [f \mid g \land \forall y \in \mathbb{C}\ (f + y \mid g \Rightarrow f + y + 1 \mid g) \Rightarrow f + x \mid g],$$

where $z \in \mathbb{C}$ stands for $\varphi_{\mathbb{C}}(z)$, defines $\mathbb{N}$ in $\mathcal{H}(\mathbb{C})$.

Let $n \in \mathbb{N}$ and let f, g be entire functions such that $f \mid g$, and such that $f + y \mid g \Rightarrow f + y + 1 \mid g$ for all $y \in \mathbb{C}$. Then $f, f + 1, \ldots, f + n$ divide g, hence n satisfies $\varphi_{\mathbb{N}}(x)$.

To prove the converse we need to recall the following easy fact on holomorphic functions:

(9.6) if $g \in \mathcal{H}(\mathbb{C})$ and $g(z_0) = 0$ for some $z_0 \in \mathbb{C}$, then $z - z_0$ divides g.

Let $h \in \mathcal{H}(\mathbb{C})$ be an element satisfying $\varphi_{\mathbb{N}}(x)$. Then $h \in \mathbb{C}$. Let $f(z) = z$ and g be a function that annihilates on the set $\{-k \mid k \in \mathbb{N}\}$, for example $g(z) = 1/\Gamma(z)$ where $\Gamma(z) = \int_0^\infty t^{z-1}\mathrm{e}^{-t}\,\mathrm{d}t$. Let $y \in \mathbb{C}$: by (9.6) $f + y \mid g$ if and only if $y \in \mathbb{N}$, hence $f + y \mid g \Rightarrow f + y + 1 \mid g$, and therefore $f + h \mid g$. But from what we just said this implies $h \in \mathbb{N}$.

9.E. The term algebra. In this Section $\mathcal{L}$ will be a *first-order language without relational symbols.*

For M an $\mathcal{L}$-structure, let

$$\mathrm{Cong}(M) = \{E \mid E \text{ is a congruence on } M\}$$

where the notion of congruence was defined in (4.1). The identity id_M and the trivial relation $M \times M$ are congruences. If $\mathcal{E}$ is a family of equivalence relations (or congruences) on M, then $\bigcap \mathcal{E}$ is an equivalence relation (or congruence) on M. If R is a binary relation on M, then

$$\bigcap\{E \in \mathrm{Cong}(M) \mid R \subseteq E\}$$

is the **congruence generated** by R. For notational ease we will often use the same symbol for a relation and the congruence it generates.

If $\mathcal{E}$ is a family of equivalence relations on M then $\bigcup \mathcal{E}$ is not necessarily an equivalence relation, since transitivity might fail, even when $\mathcal{E}$ has size two. Thus given a family $\mathcal{E} \subseteq \mathrm{Cong}(M)$, the congruence generated by $\bigcup \mathcal{E}$ is the relation $\sim \overset{\text{def}}{=} \bigcap\{R \supseteq \bigcup \mathcal{E} \mid R \in \mathrm{Cong}(M)\}$. Equivalently (Exercise 9.34)

$$a \sim b \Leftrightarrow \exists x_0, \dots, x_n \in M\, \exists E_0, \dots, E_n \in \mathcal{E}$$
$$x_0 = a \wedge x_n = b \wedge \forall i < n\ (x_i\ E_i\ x_{i+1})$$

The set $\mathrm{Term} = \mathrm{Term}_{\mathcal{L}}$ of all terms of $\mathcal{L}$ can be seen as an $\mathcal{L}$-structure if the interpretation of the function and constant symbols are the symbols themselves: if f is an n-ary function symbol, then

$$f^{\mathrm{Term}} \colon \mathrm{Term}^n \to \mathrm{Term}, \quad f^{\mathrm{Term}}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$$

and $c^{\mathrm{Term}} = c$ for all constant symbols c. A similar result holds if the set Term is replaced by $\mathrm{Term}(x_0, \dots, x_{n-1})$ the set of all terms whose variables are among $x_0, \dots, x_{n-1}$, or by the set of all closed terms $\mathrm{ClTerm}_{\mathcal{L}} = \mathrm{ClTerm}$.

Let T be an equational $\mathcal{L}$-theory and let Σ be a set of identities whose universal closure are the axioms of T. Each identity of Σ is of the form

$$(\alpha) \qquad t(x_0, \dots, x_{n-1}) = s(x_0, \dots, x_{n-1})$$

with $t, s \in \mathrm{Term}$, and each one of these identities yields a congruence $\sim_\alpha$ on Term defined as the intersection of all congruences $\approx$ on Term satisfying

$$\begin{aligned}&\forall u_0, \dots, u_{n-1}, v_0, \dots, v_{n-1} \in \mathrm{Term}\bigl(u_0 \approx v_0 \land \cdots \land u_{n-1} \approx v_{n-1} \\ &\qquad\qquad \Rightarrow t[u_0/x_0, \dots, u_{n-1}/x_{n-1}] \approx s[v_0/x_0, \dots, v_{n-1}/x_{n-1}]\bigr).\end{aligned}$$

The congruence generated $\bigcup_\alpha \sim_\alpha$ is called the congruence generated by Σ and it is denoted by $\sim_\Sigma$.

If $\sim$ is a congruence on Term then $\mathrm{Term}(x_1, \dots, x_n)/{\sim}$ is isomorphic to $\mathrm{Term}/{\approx}$ where $\approx$ is the congruence generated by the relation $\sim \cup \{x_n \approx x_m \mid n < m\}$. Let $\mathcal{L}_\infty$ be the language obtained by adding new constant symbols $\{d_n \mid n \in \mathbb{N}\}$ to $\mathcal{L}$. The map

$$\mathrm{Term}_{\mathcal{L}} \to \mathrm{ClTerm}_{\mathcal{L}_\infty}, \qquad t \mapsto t[d_0/x_0, d_1/x_1, \dots]$$

is a bijection, and if $\sim$ is a congruence on $\mathrm{Term}_{\mathcal{L}}$ then

$$t \sim s \Leftrightarrow t[d_0/x_0, d_1/x_1, \dots] \sim s[d_0/x_0, d_1/x_1, \dots].$$

Thus $\mathrm{Term}_{\mathcal{L}}/{\sim}$ and $\mathrm{ClTerm}_{\mathcal{L}_\infty}/{\sim}$ are isomorphic $\mathcal{L}$-structures, and so are $\mathrm{Term}_{\mathcal{L}}(x_0, \dots, x_{n-1})$ and $\mathrm{ClTerm}_{\mathcal{L}_n}$, where $\mathcal{L}_n$ is the language obtained by adding $d_0, \dots, d_{n-1}$ to $\mathcal{L}$. Let K be a non-empty set—by replacing K with another set in bijection with it if needed, we may consider it to be a set of constant symbols disjoint from the constant symbols of $\mathcal{L}$. Then T is a theory in the language $\mathcal{L} \cup K$ as well, and the structure

$$\mathrm{Free}_T(K) = \mathrm{ClTerm}_{L \cup K}/{\sim_\Sigma}$$

is the **term model** for T over $\mathcal{L} \cup K$, or **free model** of T on K-generators. The use of the word "model" is justified by the next theorem. An equational theory is **non-trivial** if it not all of its models are singletons, that is if it has a model with at least two elements—see Example 9.15 below for a trivial equational theory.

Theorem 9.13. *If $\mathcal{L}$, T and K are as above, then* $\mathrm{Free}_T(K) \vDash T$*. If moreover T is non-trivial, then*

- *$K \subseteq \mathrm{Free}_T(K)$ is a set of generators for $\mathrm{Free}_T(K)$,*
- *if $M \vDash T$ and $F\colon K \to M$ is any function, then there is a unique morphism $\hat{F}\colon \mathrm{Free}_T(K) \to M$ extending F,*
- *if K and K' are in bijection, then $\mathrm{Free}_T(K) \cong \mathrm{Free}_T(K')$.*

See [**Ber12**, Section 4.3] for a proof.

9.E.1. *Examples.* Consider the language for semigroups $\mathcal{L}_{\mathrm{SG{\scriptsize RPS}}}$ with just one binary operation $*$.

Example 9.14. Let $\sim$ be the congruence generated by the associative law, that is

$$(t * s) * u \sim t * (s * u),$$

for all terms t, s, u. The quotient algebra $\mathrm{Term}/{\sim}$ is a semigroup and its elements can be identified with expressions of the form

$$x_1^{n_1} * x_2^{n_2} * \cdots * x_k^{n_k},$$

where the variables $x_1, \dots, x_k$ are not necessarily distinct, and $n_1, \dots, n_k > 0$—if besides associativity we also require commutativity, that is $t * s \sim s * t$ for all pairs of terms t and s, then the variables can be taken to be distinct.

If $K = \{a\}$, then the elements of $\mathrm{Free}_T(K)$ are of the form a^n with $n \geq 1$, and $(\mathrm{Free}_T(K), *) \cong (\mathbb{N} \setminus \{0\}, +)$. If $K = \{a, b\}$, then the elements of $\mathrm{Free}_T(K)$ are of the form $a^{n_1} b^{m_1} a^{n_2} b^{m_2} \dots a^{n_k} b^{m_k}$ with $k \geq 1$, $m_1, n_2, \dots, n_k > 0$, $n_1, m_k \geq 0$ and $n_1 + m_1 > 0$ if $k = 1$.

Example 9.15. If $\sim$ is the congruence generated by the identity $(x*y)*z \mathrel{\dot=} y$, the quotient algebra $\mathrm{Term}/{\sim}$ has only one element, that is to say $s \sim t$ for all $s, t \in \mathrm{Term}$. This follows from the fact that $\forall x, y, z\,((x * y) * z \mathrel{\dot=} y) \Rightarrow \forall x, y\,(x \mathrel{\dot=} y)$ is valid, by Example 5.3.

Example 9.16. Consider the language $\mathcal{L}_{\mathrm{G{\scriptsize RPS}}}$ but with the binary operation denoted by $*$. Consider the congruence $\sim$ generated by the associative law for $*$, by $1 * t \sim t$, and by $t^{-1} * t \sim 1$. The quotient structure $\mathrm{Term}/{\sim}$ is a group (Exercise 4.84) whose elements are equivalence classes of terms built from the constant 1 and from variables, that, as stated on page 23, are an infinite list of objects $v_0, v_1, \dots$. It is the most general group that can be built from the variables v_n; such a group is called the **free group of rank** ω and will be discussed in Section 18.D.2. If we restrict ourselves to $\mathrm{Term}(v_1, \dots, v_n)/{\sim}$ or equivalently $\mathrm{ClTerm}(c_1, \dots, c_n)/{\sim}$ with $c_1, \dots, c_n$ new constants, the most general group on n generators is obtained, the **free group of rank** n.

The elements of $\mathrm{Term}(x)/{\sim}$ can be identified with expressions of the form x^n with $n \in \mathbb{Z}$, hence the free group on one generator is isomorphic to $(\mathbb{Z}, +)$. The elements of $\mathrm{Term}(x, y)/{\sim}$ can be identified with expressions of the form

$$x^{n_1} * y^{m_1} * x^{n_2} * y^{m_2} * \cdots * x^{n_k} * y^{m_k}$$

where $k \geq 1$, $m_1, n_2, \dots, n_k \in \mathbb{Z} \setminus \{0\}$ and $n_1, m_k \in \mathbb{Z}$, with the agreement that if $k = 1$ and $n_1 = m_k = 0$, the resulting expression is the equivalence class of the term 1. If $\equiv$ is a congruence extending $\sim$, the structure $\mathrm{Term}(x, y)/{\equiv}$ is a group generated by two elements $[x]$ and $[y]$ which will be the homomorphic image of $\mathrm{Term}(x, y)/{\sim}$, and every group generated by two elements can be obtained as a quotient of the free group of rank 2. For example:

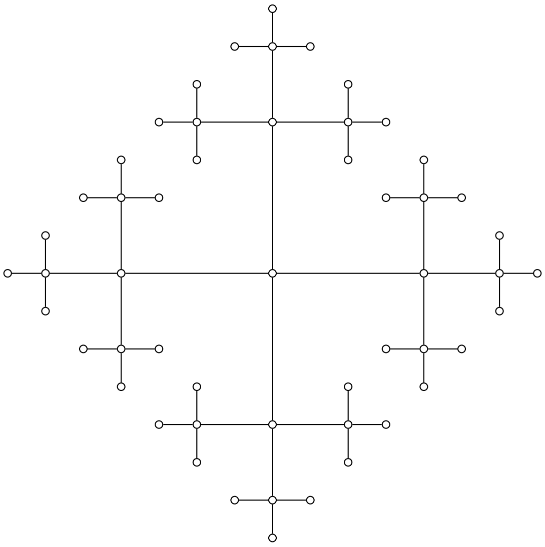
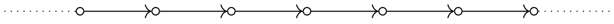


Figure 13. The Cayley graph of the free group on two generators

- if $\equiv$ enforces commutativity, then the expressions can be simplified to $x^n * y^m$ with $n, m \in \mathbb{Z}$, hence $\mathrm{Term}/{\equiv}$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$,
- if $\equiv$ enforces commutativity and $x^n \equiv 1$ and $y^m \equiv 1$, then $\mathrm{Term}/{\equiv}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$,
- if $\equiv$ enforces $x^4 \equiv 1$ and $(x * y)^2 \equiv 1$, then $\mathrm{Term}/{\equiv}$ is isomorphic to the dihedral group D_4 of all isometries of the square—for example x represents a rotation of $\pi/2$ and y is the reflection along the diagonal.

A group $G = \mathrm{ClTerm}(c_1, \dots, c_n)/{\equiv}$ defined by some congruence extending $\sim$ is described by its **Cayley graph**: it is a directed graph with G as a set of vertexes, and such that for distinct $g, h \in G$ there is an edge from g to h just in case $g * c_i = h$ for some $1 \leq i \leq n$. Thus the Cayley graph of $\mathbb{Z}$ looks like



while the Cayley graph of the free group on two generators $\mathrm{ClTerm}(a, b)/{\sim}$ is described in Figure 13. In algebra the free group $\boldsymbol{F}(C)$ on a non-empty set C of generators is usually defined to be the set of all irreducible words on C. A word on C is a finite sequences of the form $c_1^{\varepsilon_1} \cdot c_2^{\varepsilon_2} \cdots c_n^{\varepsilon_n}$ with $c_i \in C$ and $\varepsilon_i \in \{-1, 1\}$, with the understanding that c^1 is identified with c. A word w is reducible if $c_i = c_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$ for some $i + 1 < n$; a pair of consecutive elements of w as above is said to be offending. A word that is not reducible is **irreducible**. By repeatedly removing all offending pairs, any word can be thinned-down to a unique reduced word. The inverse of the word $w = c_1^{\varepsilon_1} \cdot c_2^{\varepsilon_2} \cdots c_n^{\varepsilon_n}$ is $w^{-1} \overset{\text{def}}{=} c_n^{-\varepsilon_n} \cdots c_2^{-\varepsilon_2} \cdot c_1^{-\varepsilon_1}$. If $w, z \in \boldsymbol{F}(C)$

set $w \cdot z$ to be the sequence w followed by z, and the reduced. It can be shown [**Hun80**, p. 65] that the operation is associative, that w^{-1} is indeed the inverse of w, and that the empty word is the identity element.

Example 9.17. If $\mathcal{L}$ is the language of unitary semi-rings, that is the language containing $+, \cdot, 0$ and 1, let $\sim$ be the congruence generated by the associative and commutative property for $+$ and $\cdot$, by $0 + t \sim t$, $1 \cdot t \sim t$, and $0 \cdot t \sim 0$. Then $\mathrm{Term}(x_1, \dots, x_n)/{\sim}$ is the free semigroup on n generators and it is isomorphic to $\mathbb{N}[X_1, \dots, X_n]$, the semi-ring of polynomials in n variables and coefficients in $\mathbb{N}$.

Exercises

Exercise 9.18. Show that there are uncountably distinct linear orders $\leq$ that make $(\mathbb{Z} \times \mathbb{Z}, +, \leq)$ a bi-ordered group.

Exercise 9.19. Let $\{\xi_n \mid n \in \mathbb{N}\} \subseteq (0;1)$ be $\mathbb{Q}$-linearly independent, and let $G = \bigcup_n \mathbb{Z}[\xi_0, \dots, \xi_n]$ where $\mathbb{Z}[\xi_0, \dots, \xi_n] = \{\sum_{i=0}^{n} k_i \xi_i \mid k_i \in \mathbb{Z}\}$. Show that G is a densely ordered abelian group which is not 2-divisible.

Exercise 9.20. Complete the verification that the notion of vector space over an arbitrary field is finitely axiomatizable in the language $V, S, \oplus, \otimes, \boxplus$ and $\boxtimes$.

Exercise 9.21. Let R be a ring. Show that:

(i) R is not definable in the group $(R[X], +)$;

(ii) the unknown X is not definable in the ring $(R[X], +, \cdot)$.

Exercise 9.22. Let R be an integral domain of characteristic zero. Show that:

(i) $\mathbb{Z}$ is definable without parameters in $(R[X], +, \cdot, R)$, that is in the structure obtained expanding the ring of polynomials with a unary predicate for the elements of R. Thus $\mathbb{Z}$ is definable in $R[X]$ if R is definable in $R[X]$.

(ii) if R is a field, then $\mathbb{Z}$ is definable without parameters in $(R[X], +, \cdot)$.

Exercise 9.23. Show that the congruences in groups and rings can be identified with normal subgroups and ideals, respectively.

Exercise 9.24. Show that the following first-order theories are not finitely axiomatizable:

(i) the theory of ordered divisible abelian groups,

(ii) the theory of $\mathbb{Z}$-groups.

Exercise 9.25. Let G be a group and let H be a subgroup. Suppose that some left coset aH is definable without parameters in G. Show that H is definable without parameters in G

Exercise 9.26. Let $\mathcal{L}_{\text{SUBGRP}}$ be the language defined in Section 9.A.1. Find a sentence σ of $\mathcal{L}_{\text{SUBGRP}}$ such that

$$(G, \cdot, {}^{-1}, 1_G, H) \vDash \sigma \quad \text{if and only if} \quad G/H \text{ is an abelian group.}$$

Exercise 9.27. Find sentences σ_n in the language for additive groups such that $G \vDash \sigma_n$ if and only if $G/2G$ has size n. Conclude that $\mathbb{Z}^n$ and $\mathbb{Z}^m$ are elementarily equivalent if and only if $n = m$.

Exercise 9.28. Show that in a local ring the maximal ideal is definable without parameters.

Exercise 9.29. Let $\Bbbk$ be a field. Show that

(i) if $<$ turns $\Bbbk$ into an ordered field, then $P = \{x \in \Bbbk \mid 0 < x\}$ is the cone of positive elements; conversely given a P as above, the relation $x < y \Leftrightarrow y - x \in P$ turns $\Bbbk$ into an ordered field.

(ii) The following properties are true in an ordered field
- $\forall x \neq 0 \ (x^2 \in P)$;
- $1 \in P$ and the characteristic of the field is 0;
- $x \in P \Rightarrow x^{-1} \in P$;
- $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$.

Exercise 9.30. Work with $\mathcal{L}_{\text{ABGR}}$ and suppose $\sim$ is a congruence on Term enforcing and abelian group structure. Show that $\mathrm{Term}/{\sim}$ is isomorphic to $(\mathbb{Z}[X], +)$.

Exercise 9.31. Show that

(i) if $\sim$ is a congruence on some $\mathcal{L}$-structure M, then $M \to M/{\sim}$, $a \mapsto [a]_\sim$, is a surjective homomorphism;

(ii) if $F \colon M \twoheadrightarrow N$ is a surjective homomorphism, then the equivalence relation $a \sim b \Leftrightarrow F(a) = F(b)$ is a congruence on M.

Exercise 9.32. (i) Verify in detail that the structures described in Section 9.B.3, that is: modules over a ring R and vector spaces over a field $\Bbbk$, are axiomatizable in the first-order languages $\mathcal{L}_R$ and $\mathcal{L}_\Bbbk$.

(ii) Show that the theory of vector spaces over $\Bbbk$ is finitely axiomatizable if and only if $\Bbbk$ is finite. Is the analogous statement true for R-modules?

Exercise 9.33. Let $\Bbbk$ be a finite field and let $\mathcal{L}_\Bbbk$ be the language of Section 9.B.3. Show that:

(i) "the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent" is a first-order formula in $\mathcal{L}_\Bbbk$;

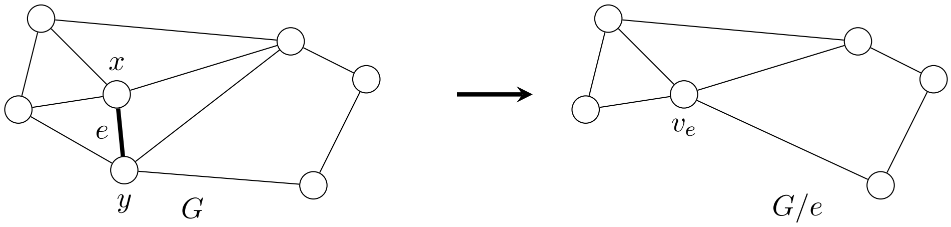


Figure 14. Contraction by the edge $e = \{x, y\}$

(ii) the theory T_n of $\Bbbk$-vector spaces of fixed dimension n is finitely axiomatizable, and that the theory T_∞ of infinite dimensional $\Bbbk$-vector spaces is axiomatizable, but not finitely axiomatizable;

(iii) the theories T_n and T_∞ are complete.

Exercise 9.34. Show that the congruence generated by $\bigcup \mathcal{E}$ is $\bigcup_{n\in\mathbb{N}} R_n$, where

$$R_n = \bigl\{(x, y) \in M^2 \mid \exists x_1, \dots, x_n \in M \, \exists E_0, \dots, E_n \in \mathcal{E} \\ \forall i \leq n \; (x_i \; E_i \; x_{i+1} \wedge x_0 = x \wedge x_{n+1} = y)\bigr\} .$$

Notes and remarks

Exercise 9.22 is from [**Rob51**], where it is also shown that $\mathbb{Z}$ is definable in $\mathbb{Z}[X]$. In 1936, motivated by problems in lattice theory von Neumann introduced the notion of regular ring (Section 9.D.1). Since the term *regular ring* is also used in algebra to denote a totally unrelated concept, it is customary nowadays to include the *von Neumann* in their definition.

10. Definability in graphs

Recall form Section 3.D.2 that a graph is a structure (V, E) with E an irreflexive symmetric relation. Given $G = (V, E)$ and an edge $e = \{x, y\} \in E$, the **contraction** of G by e is $G/e = (V/{\sim}, E')$ where $\sim$ is the equivalence relation on V that identifies the vertices x and y, and E' is the relation induced on the quotient (see Figure 14). We say that H is a **minor** of G, in symbols $H \leq G$, if H can be obtained from $H' \subseteq G$ via a finite sequence of contractions, that is to say: there are $H_0, H_1, \dots, H_n$ such that $H = H_0$, $H_n = H'$ and H_i is H_{i+1}/e_{i+1} where e_{i+1} is an edge of H_{i+1}.

10.A. Axioms for graphs. The axioms for graphs are formulated in the language $\mathcal{L}_{\text{Grph}}$ containing a binary relation symbol E and assert that this relation is irreflexive and symmetric, that is

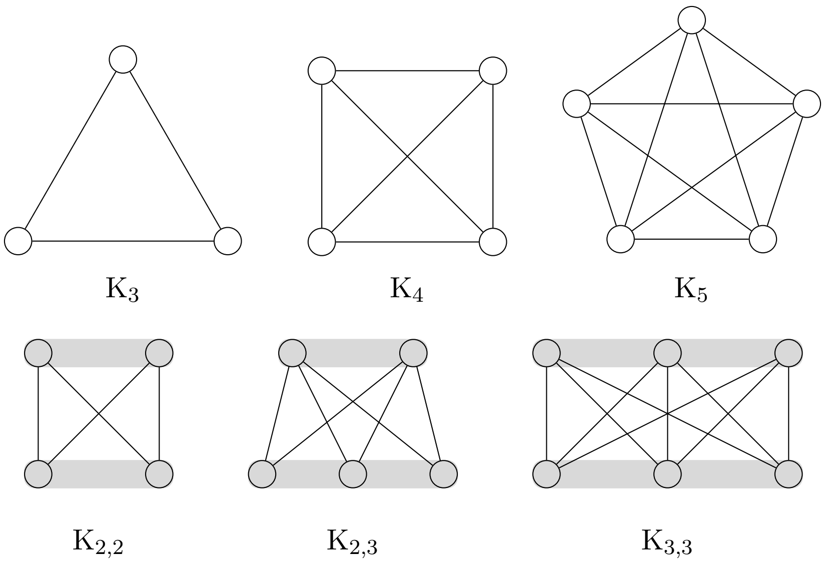
$$T_{\text{Grph}} \quad \begin{cases} \forall x \neg E(x,x) \\ \forall x,y\,(E(x,y) \Rightarrow E(y,x))\,. \end{cases}$$

We say that $G' = (V', E')$ is a subgraph of a graph $G = (V, E)$, is symbols $G' \subseteq G$, if $V' \subseteq V$ and $E' \subseteq E \cap V' \times V'$.

Remark 10.1. The notion of subgraph does not coincide with that of a substructure since it is not required that $E' = E \cap (V' \times V')$. Whenever $V' \subseteq V$ and $E' = E \cap (V' \times V')$ we say that (V', E') is the **subgraph induced by** (V, E) on V'.

A graph is **complete** if any two distinct vertexes are connected by an edge, that is if E is total; in this case we will say that it is the complete graph on V. Two complete graphs with the same number of vertices are isomorphic, and K_n denotes the complete graph on n vertices (Figure 15). If the induced subgraph on $X \subseteq V$ is complete, we still say that X is a **clique**. At the other extreme of the spectrum, a set X of vertexes is **independent** if any two vertexes of X are never connected by an edge, that is if E restricted to X is free. A graph is independent if its set of vertexes is independent, that is if it has no edges.

The statement of Exercise 2.13 can be restated as a statement on graphs: in every graph with six vertices there are three vertices that are mutually



K_3 K_4 K_5

$\mathrm{K}_{2,2}$ $\mathrm{K}_{2,3}$ $\mathrm{K}_{3,3}$

Figure 15. Complete and bipartite graphs

connected or mutually disconnected. This is a particular case of the following result:

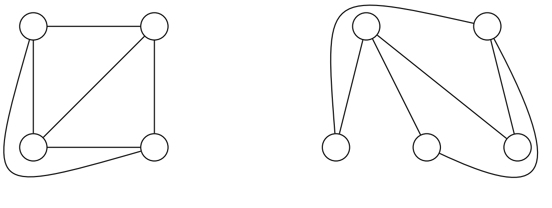
Theorem 10.2. *$\forall n \exists m \geq n$ such that every graph with m vertices contains the complete graph K_n, or it has n mutually disconnected vertices.*

A graph is **bipartite** if the set of vertices V can be partitioned into two disjoint non-empty sets A_0 and A_1 such that there are no edges between vertices of the same partition. The bipartite graph in which A_0 has size n and A_1 has size m, and every vertex in A_i is linked to every vertex in A_{1-i} is denoted by $\mathrm{K}_{n,m}$ (Figure 15). In order to give a first-order formulation of the notion of bipartite graph a two-sorted language is employed, that is two unary predicate symbols A_0 and A_1 are introduced with the axioms:

$$\exists x \, A_0(x) \;\land\; \exists x \, A_1(x)$$
$$\forall x \, (A_0(x) \Leftrightarrow \neg A_1(x))$$
$$\forall x, y \left[\big(A_0(x) \land A_0(y)\big) \lor \big(A_1(x) \land A_1(y)\big) \Rightarrow \neg E(x,y) \right].$$

If in the definition of bipartite graph we require that the set of vertices be partitioned into k pieces, rather than two pieces, the notion of k-partite graph is obtained. As we shall see in Section 10.C also k-partite graphs can be finitely axiomatized.

A graph is **planar** if it can be drawn on the plane so that distinct edges do not intersect. The graphs K_4 and $\mathrm{K}_{2,3}$ are planar,



while it can be shown that neither K_5 nor $\mathrm{K}_{3,3}$ are planar—these are the minimal counterexample to planarity, since a graph G is planar if and only if either K_5 or $\mathrm{K}_{3,3}$ are minors of G.

10.B. Acyclic and connected graphs. Recall that a graph is **acyclic** if it does not contain cycles, that is if $\forall n \geq 3 \, \chi_n$ holds, where χ_n is the formula

$$(\chi_n) \quad \neg \exists x_1, \ldots, x_n \left(\textstyle\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \land E(x_1, x_n) \land \bigwedge_{1 \leq i < n} E(x_i, x_{i+1}) \right).$$

Unfortunately $\forall n \geq 3 \, \chi_n$ is just a pseudo-formula—in order to give a first-order axiomatization of the class of acyclic graphs one needs to add to the axioms for graphs all the sentences χ_n.

Recall that a graph is **connected** if every pair of vertices is connected by a path; equivalently (V, E) is connected if the graph given by the transitive closure of E is the complete graph on V. A **connected component** of a graph is an induced subgraph which is connected and maximal with respect to inclusion among connected induced subgraphs. Every graph (V, E) is the disjoint union of its connected components, that is there is a partition $\bigcup_{i \in I} V_i = V$ of the set of vertices such that the induced subgraph on each V_i is a connected component. Connectedness is usually stated as

$$\forall x, y \, \exists k \geq 1 \, \exists z_0, \ldots, z_k \left(x = z_0 \wedge y = z_k \wedge \bigwedge_{i<k} E(z_i, z_{i+1}) \right),$$

but this is a pseudo-formula since

- the quantifier in "$\exists k \geq 1$" ranges over non-zero natural numbers, and not on the vertices, and
- the quantification $\exists z_1, \ldots, z_k$ and the conjunction $\bigwedge_{i<k} E(z_i, z_{i+1})$ are not fixed once and for all, but depend on k.

The **distance of two vertices** v, w in a graph (V, E) is $d(v, w)$, the length $d(v, w)$ of the shortest path between them, if they belong to the same connected component, or $d(v, w) = \infty$ otherwise. The **diameter** of a graph(V, E) is the smallest $N \leq \infty$ such that $d(v, w) \leq N$ for any $v, w \in V$. Observe that $d(v, w) = 0 \Leftrightarrow v = w$, that $\{(v, w) \in V^2 \mid d(v, w) \leq k\}$ is definable in (V, E), and that (V, E) is connected if and only if $d(v, w) < \infty$ for any $v, w \in V$.

Proposition 10.3. *Suppose (V, E) is a graph of infinite diameter. Then there is a disconnected graph that is elementarily equivalent to (V, E).*

Proof. It is enough to show that $\mathrm{Th}(V, E) \cup \{n < d(c_0, c_1) \mid n \in \mathbb{N}\}$ is finitely satisfiable, where c_0, c_1 are two new symbols for constants. By assumption $\forall n \in \mathbb{N} \, \exists v, w \in V \, (n < d(v, w) \leq \infty)$, so for any n we can assign c_0, c_1 to suitable vertexes whose distance is greater than n, so that $\mathrm{Th}(V, E) \cup \{n < d(c_0, c_1)\}$ is satisfied. By compactness there is $\mathcal{M} = (V', E', c_0^{\mathcal{M}}, c_1^{\mathcal{M}})$ that models $\mathrm{Th}(V, E) \cup \{n < d(c_0, c_1) \mid n \in \mathbb{N}\}$. Therefore (V', E') is a graph elementarily equivalent to (V, E) with two vertexes in distinct connected components. □

The graph $(\mathbb{N}, E)$ where $n \, E \, m \Leftrightarrow |n - m| = 1$ is connected and satisfies the hypotheses of Proposition 10.3, therefore we have:

Corollary 10.4. *The class of connected graphs is not axiomatizable.*

10.C. Colorability. Given a graph $G = (V, E)$, a **k-coloring of the vertices of** G is a map $F \colon V \to \{0, \ldots, k-1\}$ such that $F \colon G \to \mathrm{K}_k$. The numbers $0, \ldots, k-1$ are called **colors** of F. Equivalently: it is a morphism of structures $F \colon G \to \mathrm{K}_k$. A graph is **$k$-colorable** if it admits a k-coloring of vertices. The notion that a graph is k-colorable is first-order—it is enough to introduce new unary predicates $A_0, \dots, A_{k-1}$ with the axioms

$$\forall x\, (A_0(x) \vee \cdots \vee A_{k-1}(x))$$
$$\neg \exists x \bigvee_{i<j<k} (A_i(x) \wedge A_j(x))$$
$$\forall x, y \big(E(x, y) \Rightarrow \neg \bigvee_{i<k} A_i(x) \wedge A_i(y)\big).$$

In fact to say that a graph is k-colorable is just another way to say that the graph is k-partite. In particular: a graph is bipartite if and only if it is 2-colorable. If G is a finite graph with vertices $\{v_0, \dots, v_{n-1}\}$, then the map $v_i \mapsto i$ witnesses n-colorability. The least k such that a finite graph is k-colorable is the **chromatic number** of G and is denoted with $\boldsymbol{\chi}(G)$. Thus $\boldsymbol{\chi}(\mathrm{K}_n) = n$, while a graph without edges is 1-colorable.

An **ordered graph** is a graph (V, E) with an order on V such that $v \mathrel{E} w$ iff v is an immediate predecessor of w or, conversely, w is an immediate predecessor of v; a graph is **orderable** if there is an order that makes it an ordered graph.

Theorem 10.5. *Let $G = (V, E)$ be a finite graph.*

(a) *G is 2-colorable iff it does not contain cycles of odd length.*

(b) *G is orderable iff it is acyclic.*

Proof. (a) If $x_1, \dots, x_n$ is a cycle and F is a 2-coloring, then

$$\forall i \leq n\ (F(x_1) \neq F(x_i) \Leftrightarrow i \text{ even})$$

and since $F(x_1) \neq F(x_n)$, then G does not contain odd cycles. For the converse direction, let $\bigcup_{i \in I} V_i = V$ be the partition of the set of vertices of G in connected components. Since V is finite, also I is finite, hence we can choose $v_i \in V_i$ and define $F \colon V \to \{0, 1\}$ by

$$F(v) = 1 \Leftrightarrow \text{ there is a } k\text{-path from some } v_i \text{ to } v, \text{ with } k \text{ even.}$$

The assumption guarantees that F is indeed a 2-coloring.

(b) If G is orderable, then it contains no cycles by the transtive property. For the other direction, argue as in part (a): if $\{V_i \mid i \in I\}$ are the connected components choose $v_i \in V_i$ and define the ordering on each V_i as follows: v_i is the minimum in V_i, the vertexes linked to v_i cover it, and so on. □

Remark 10.6. The proof of the ($\Rightarrow$) direction in (a) and (b) does not require that the graph be finite. For the ($\Leftarrow$) direction, if G is infinite, it may happen that I, the set of indexes of the pieces of the partition in its connected components, be infinite, and in order to select the vertices $v_i \in V_i$ one must appeal to a set-theoretic principle known as the Axiom of Choice.

The following result, known as the Four Color Theorem, is one of the central results in the subject.

Theorem 10.7. *Every finite planar graph is* 4*-colorable.*

Theorem 10.7 is generally stated as follows: any map in a plane can be colored using four colors in such a way that regions sharing a common boundary do not share the same color. (In order to verify this equivalence it is enough to associate a vertex v to every region in the map, and instate an edge $\{v, w\}$ just in case v and w represent contiguous regions.)

The dual notion of "coloring of vertices" is that of "coloring of edges": given a graph $G = (V, E)$, a function $F\colon E \to \{0, \dots, k-1\}$ is a **k-coloring of edges** of G and the numbers $0, \dots, k-1$ are called colors. A subset $H \subseteq V$ is **monochromatic** for some k-coloring F if the edges of the induced subgraph by H have all the same color, that is if there is $i < k$ such that $F(\{x, y\}) = i$ for distinct $x, y \in H$. Since any graph with m vertices is a subgraph of K_m, Theorem 10.2 boils-down to the case $k = 2$ of the following result, known as Ramsey's Theorem.

Theorem 10.8. $\forall n, k\, \exists m \geq n$ *such that for every k-coloring of* K_m *there is a monochromatic induced subgraph isomorphic to* K_n.

10.D. Infinite graphs. Let us see two examples of graphs whose set of vertexes is (an infinite subset of) $\mathbb{N}$.

The **countable complete graph** is $\mathrm{K}_\omega = (\mathbb{N}, E)$ where $E = \{\{n, m\} \mid n \neq m\}$, that is: every pair of distinct vertexes is joined by an edge. Every countable graph can be identified with a subgraph of K_ω. Ramsey's Theorem 10.8 holds for K_ω as well: for all $k > 0$ and every k-coloring of the edges of K_ω, there is an infinite $H \subseteq \mathbb{N}$ such that the induced subgraph on H (which is isomorphic to K_ω) is monochromatic. We will prove this result in Section 29.

The **countable random graph** R_ω is the graph $(\mathbb{N} \setminus \{0, 1\}, E)$ defined by:

$$n \mathrel{E} m \Leftrightarrow n \neq m \wedge (p_n \mid m \vee p_m \mid n)$$

where $(p_n)_{n \geq 2}$ is the increasing enumeration of all prime numbers, that is $p_2 = 2, p_3 = 3, p_4 = 5, \dots$. (The reason for starting from 2 is that 1 divides every number and 0 is divisible by any number, so 0 and 1 would be E-related to anything, and this is a property that we wish to avoid.)

Definition 10.9. A graph $G = (V, E)$ satisfies **property Rnd** if for any two non-empty disjoint, finite subsets of vertexes A, B there is a vertex x that has an edge with each vertex of A and no edge with any vertex in B, that is

$$\forall y \in A\ (x \mathrel{E} y) \wedge \neg \exists z \in B\ (x \mathrel{E} z)\,.$$

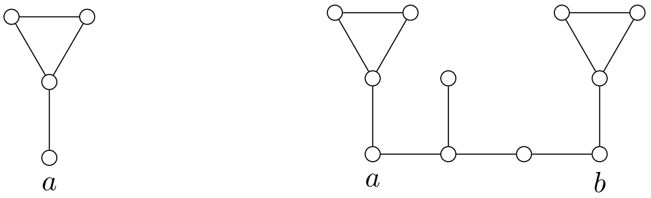


Figure 16. The graph H_a, and an R-link between H_a and H_b

Proposition 10.10. R_ω *has property* Rnd.

Proof. Take $x = (\prod_{n \in A} p_n)^k$ with k sufficiently large so that $p_x \nmid m$ for all $m \in B$. □

Property Rnd can be recast using infinitely many statements

$$(\mathrm{Rnd}_n) \quad \forall y_1, \dots, y_n, z_1, \dots, z_n \Big[\bigwedge_{1 \le i,j \le n} y_i \neq z_j \\ \Rightarrow \exists x \, \big(\bigwedge_{1 \le i \le n} E(x, y_i) \wedge \neg E(x, z_i) \big) \Big],$$

thus an axiom system for R_ω in the language $\mathcal{L}_{\mathrm{Grph}}$ is T_{RndGrph} whose axioms are T_{Grph}, the sentence $\boldsymbol{\varepsilon}_{\geq 3}$ "there are at least three distinct vertexes", and the sentences Rnd_n. Theorem 13.43 in Section 13.I shows that any countable graph satisfying T_{RndGrph} is isomorphic to R_ω, and for this reason any such graph is called a random graph (Exercise 24.43). By Theorem 4.37 the theory T_{RndGrph} is complete.

10.E. Interpretability in graphs*. Graphs can interpret just about any structure you can think of. Here we will show how to interpret any structure of the form $\mathcal{M} = (M, R)$ with $R \subseteq M \times M$, in a suitable graph $G_{\mathcal{M}}$ defined as follows. For each $a \in M$ consider the graph H_a, and for each $a, b \in M$ such that $a \; R \; b$ link H_a and H_b as in Figure 16. (The asymmetry of the path from a to b codes that a is in relation with b.) The graph $G_{\mathcal{M}}$ is then obtained by taking all the H_as together with the R-links between H_a and H_b, whenever $a \; R \; b$.

Let us check that $\mathcal{M}$ is indeed interpretable in $G_{\mathcal{M}}$. The universe of the structure $\mathcal{M}$, that is the set M, is identified with the set of all vertices as defined by the formula

$$\psi_U(x) \Leftrightarrow \exists z_1, z_2, z_3 \, \psi_H(x, z_1, z_2, z_3)$$

where $\psi_H(x, z_1, z_2, z_3)$ says that z_1, z_2, z_3 are the vertexes of H_a, that is

$$\begin{aligned}(x\ E\ z_1 \wedge z_1\ E\ z_2 \wedge z_2\ E\ z_3 \wedge z_3\ E\ z_1 \wedge x \neq z_2 \wedge x \neq z_3)&\\ \wedge \forall w\ (w\ E\ z_1 \Rightarrow w = x \vee w = z_2 \vee w = z_3)&\\ \wedge \forall w\ (w\ E\ z_2 \Rightarrow w = z_1 \vee w = z_3)&\\ \wedge \forall w\ (w\ E\ z_3 \Rightarrow w = z_1 \vee w = z_2)&\,.\end{aligned}$$

The relation R is identified with the set of all ordered pairs of vertices defined by the formula

$$\psi_R(x, y) \Leftrightarrow \psi_U(x) \wedge \psi_U(y) \wedge \exists u_1, u_2, u_3\, \psi_L(x, u_1, u_2, u_3, y),$$

where $\psi_L(x, u_1, u_2, u_3, y)$ says that there is a link between x and y, that is

$$\begin{aligned}\big[x\ E\ u_1 \wedge u_1\ E\ u_2 \wedge u_1\ E\ u_3 \wedge u_3\ E\ y \wedge x \neq u_2 \wedge x \neq u_3 \wedge y \neq u_1&\\ \wedge \forall w\ (w\ E\ u_1 \Rightarrow w = x \vee w = u_2 \vee w = u_3)&\\ \wedge \forall w\ (w\ E\ u_3 \Rightarrow w = u_1 \vee w = y)&\\ \wedge \forall w\ (w\ E\ u_2 \Rightarrow w = u_1)\big]&\end{aligned}$$

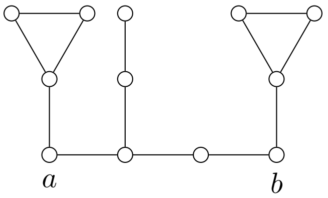
A vertex of $G_{\mathcal{M}}$ either belongs to some H_a, hence it satisfies $\varphi_H(x)$

$$\exists a, z_1, z_2, z_3\ [\psi_H(a, z_1, z_2, z_3) \wedge (x = a \vee x = z_1 \vee x = z_2 \vee x = z_3)]$$

or else it belongs to some link hence it satisfies $\varphi_L(x)$

$$\exists a, u_1, u_2, u_3, b\ [\psi_L(a, u_1, u_2, u_3, b) \wedge (x = u_1 \vee x = u_2 \vee x = u_3)]\,.$$

Therefore the collection of all graphs of the form $G_{\mathcal{M}}$, that is: the collection of all graphs that code a structure in the language with one binary relation, is axiomatized by $\forall x\,(\varphi_H(x) \veebar \varphi_L(x))$, where $\veebar$ is the exclusive disjunction. The constructions above apply to languages with more than one binary relations. For example if we have two relations R and S then define the H_as and the R-links as before, while the S-links from H_a to H_b are coded as:



Exercises

Exercise 10.11. (i) For each graph (V, E) let $C_v = \{w \in V \mid w \mathrel{E} v\}$ be the set of vertexes connected to $v \in V$. Thus v has valence n iff C_v has size n. Consider the following classes of $\mathcal{L}_{\mathrm{GRPH}}$-structures:

- $\mathscr{C}_n$ the collection of all graphs such that each vertex has valency n, i.e. each C_v has size n,
- $\mathscr{C}_{<\omega}$ the collection of all **locally finite graphs**, i.e. such that each C_v is finite,
- $\mathscr{C}_\infty$ the collection of all graphs such that each C_v is infinite.

For each of the classes $\mathscr{C}_n$, $\bigcup_n \mathscr{C}_n$, $\mathscr{C}_{<\omega}$, and $\mathscr{C}_\infty$ determine whether it is an axiomatizable class, and in the affirmative case whether it is finitely axiomatizable.

(ii) Consider the following classes of $\mathcal{L}_{\mathrm{GRPH}}$-structures:

- $\mathscr{C}_n$ the collection of all graphs that contain a cycle of length n (with $n \geq 3$),
- $\mathscr{C}_{<\omega} = \bigcup_{n \geq 3} \mathscr{C}_n$ the collection of all graphs that contain a cycle,
- $\mathscr{C}_\infty$ the collection of all graphs that don't contain a cycle.

For each of the classes $\mathscr{C}_n$, $\mathscr{C}_{<\omega}$, and $\mathscr{C}_\infty$ determine whether it is an axiomatizable class, and in the affirmative case whether it is finitely axiomatizable.

Exercise 10.12. Show that the following classes of graphs are axiomatizable, but not finitely axiomatizable, in the language $\mathcal{L}_{\mathrm{GRPH}}$:

(i) all bipartite graphs;

(ii) all graphs (V, E) such that $\{w \in V \mid v \mathrel{E} w\}$ and $\{w \in V \mid \neg(v \mathrel{E} w)\}$ are infinite, for every $v \in V$.

Exercise 10.13. Recall that T_{RNDGRPH} extends T_{GRPH} with the axioms RND_n for $n \geq 1$ and $\boldsymbol{\varepsilon}_{\geq 3}$. Show that:

(i) K_2 satisfies all axioms of T_{RNDGRPH} except $\boldsymbol{\varepsilon}_{\geq 3}$, while $\mathrm{K}_i \not\models \mathrm{RND}_2$ if $i \geq 3$;

(ii) every graph satisfying T_{RNDGRPH} is infinite;

(iii) if $(V, E) \models T_{\mathrm{RNDGRPH}}$, then for every v there are infinitely many vertexes that are liked to v, and infinitely many vertexes that are not linked to v;

(iv) if $(V, E) \models T_{\mathrm{RNDGRPH}}$ and $\emptyset \neq A, B \subseteq V$ are finite and disjoint, then the set $\{v \in V \mid \forall a \in A\, (a \mathrel{E} v) \wedge \forall b \in B\, \neg(b \mathrel{E} v)\}$ is infinite;

(v) if $(V, E) \models T_{\mathrm{RNDGRPH}}$ and $V' \subseteq V$ and $V \setminus V'$ is finite, then the induced subgraph on V' satisfies T_{RNDGRPH};

(vi) the disjoint union of two graphs that satisfy $T_{\textsc{RndGrph}}$ does not satisfy $T_{\textsc{RndGrph}}$.

Exercise 10.14. The **tensor product** $G \times H$ of two graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$ is the graph whose vertex set is $V_G \times V_H$ and with edges

$$(v_1, w_1)\ E_{G\times H}\ (v_2, w_2) \Leftrightarrow (v_1\ E_G\ v_2 \wedge w_1\ E_H\ w_2)\,.$$

In other words, $G \times H$ is the product of structures (V_G, E_G) and (V_H, E_H). Show that $\boldsymbol{\chi}(G \times H) \leq \min(\boldsymbol{\chi}(G), \boldsymbol{\chi}(H))$, where $\boldsymbol{\chi}$ is the chromatic number.

Notes and remarks

Graph theory is an important area of combinatorics; the interested reader should consult [**Die05**] for a thorough treatment. The theorem on planarity of graphs that do not contain as minor K_5 nor $\mathrm{K}_{3,3}$ was proved by Kuratowski and Wagner in the 30s of the twentieth century. The Four Color Theorem 10.7 was proved in 1976 by Appel and Haken [**AH76**]. The countable random graph was invented in 1959 by Erdős and Rényi, and independently by Gilbert. Theorem 10.8, proved in 1930 by Ramsey, is the cornerstone of a vast area of combinatorics known as Ramsey theory. The least m satisfying the statement of the theorem, that is such that every k-coloring of K_m has an induced monochromatic subgraph isomorphic to K_n, is denoted by $R(n, k)$, or simply $R(n)$ when $k = 2$. It can be shown that $R(2) = 3$, $R(3) = 6$ and $R(4) = 18$. For larger ns only upper and lower estimates of $R(n)$ are known—for example $43 \leq R(5) \leq 49$ and $102 \leq R(6) \leq 165$. This situation is akin to Example 2.8—if $\mathrm{A}(n)$ is the statement that given n randomly chosen persons there are at least 5 that are mutually acquainted or there are at least 5 that don't know each other, then $\mathrm{A}(43) \vee \mathrm{A}(44) \vee \cdots \vee \mathrm{A}(49)$, hence in particular we know that $\exists n \mathrm{A}(n)$, but we do not know which of the disjuncts are true. Determining the exact value of $R(n)$ is extremely difficult, and many experts in combinatorics believe that the exact value of $R(6)$ will not be determined any time soon. We will prove Ramsey's Theorem in Section 15. The statement that the inequality in Exercise 10.14 can be strengthened to equality is an open problem in graph theory, known as Hedetniemi's conjecture.

Section 10.E is from [**Mar02**].

11. Definability in the integers, in the real and complex numbers

11.A. Natural numbers.

11.A.1. *The successor operator.* Consider the structure $(\mathbb{N}, S)$ where $S(n) = n + 1$ is the successor of n. The relevant language has a unary function symbol $\mathtt{S}$. The element 0 is definable in $(\mathbb{N}, S)$ since it is the only witness to

$$(\varphi_0(x)) \qquad \forall y\, (\mathtt{S}(y) \neq x)\,.$$

Moreover the function S is injective, and no matter how many times it is applied, it will never take us back to the starting point. In other words, the structure $(\mathbb{N}, S)$ satisfies the set of axioms

$$T_{(\mathbb{N},S)} \quad \begin{cases} \exists! x\, \forall y\, (\mathtt{S}(y) \neq x) \\ \forall x, y\, (x \neq y \Rightarrow \mathtt{S}(x) \neq \mathtt{S}(y)) \\ \sigma_n & (n \geq 1) \end{cases}$$

where σ_n is $\forall x (\mathtt{S}^{(n)}(x) \neq x)$. Note that σ_m follows from $\sigma_{m \cdot k}$, hence $T_{(\mathbb{N},S)}$ is not an independent set of axioms. The set of the σ_ns cannot be cut-down to a finite list, since the structure $\mathbb{N} \uplus (\mathbb{Z}/n\mathbb{Z})$ with the successor operation $x \mapsto x+1$ satisfies the first two axioms of $T_{(\mathbb{N},S)}$ and σ_i for $1 \leq i < n$, but does not satisfy σ_n. Thus by Theorem 4.49 we have that

Proposition 11.1. *$T_{(\mathbb{N},S)}$ is not finitely axiomatizable.*

The natural number $k > 0$ is the unique element of $(\mathbb{N}, S)$ satisfying

$$(\varphi_k(x)) \qquad \exists y \big(\varphi_0(y) \wedge \mathtt{S}^{(k)}(y) = x\big),$$

where φ_0 is the formula defining 0. Thus every finite set $\{k_1, \ldots, k_n\} \subseteq \mathbb{N}$ is definable via the formula

$$\varphi_{k_1}(x) \vee \varphi_{k_2}(x) \vee \cdots \vee \varphi_{k_n}(x).$$

Thus every co-finite set of natural numbers (that is of the form $\mathbb{N} \setminus F$ with F finite) is definable. As we shall see in Section 11.A.2, these are the only subsets of $\mathbb{N}$ that are definable in $(\mathbb{N}, S)$.

Let (M, S_M) be a model of $T_{(\mathbb{N},S)}$ and let 0_M be the element of M defined by $\varphi_0(x)$ above. The theory $T_{(\mathbb{N},S)}$ implies that the elements 0_M, $S_M(0_M)$, $S_M(S_M(0_M)), \ldots$ are all distinct, hence the map $F \colon \mathbb{N} \to M$,

$$\begin{cases} F(0) = 0_M \\ F(n+1) = S_M(F(n)) \end{cases}$$

is a monomorphism $(\mathbb{N}, S) \to (M, S_M)$. In fact F is onto if and only if $(\mathbb{N}, S)$ and (M, S_M) are isomorphic. A model (M, S_M) which is not isomorphic to $(\mathbb{N}, S)$ is called a **non-standard model**.

Suppose (M, S_M) is non-standard. The equivalence relation $\sim$ on $M \setminus \operatorname{ran}(F)$ defined by

$$x \sim y \Leftrightarrow \exists n \in \mathbb{N} \big[x = \underbrace{S_M \circ \cdots \circ S_M}_{n \text{ times}}(y) \vee y = \underbrace{S_M \circ \cdots \circ S_M}_{n \text{ times}}(x)\big] \tag{11.1}$$

partitions $M \setminus \operatorname{ran}(F)$ in equivalence classes, and since 0_M is the only element not in $\operatorname{ran}(S_M)$, each equivalence class is isomorphic to $\mathbb{Z}$. Therefore we have proved:

Proposition 11.2. *The non-standard models (M, S_M) of $T_{(\mathbb{N},S)}$ are, up to isomorphism, of the form $M = \mathbb{N} \uplus (I \times \mathbb{Z})$ with $I \neq \emptyset$ an arbitrary set and $S_M \colon M \to M$ is defined as*

$$S_M(x) = \begin{cases} k+1 & \text{if } x = k \in \mathbb{N}, \\ (i, k+1) & \text{if } x = (i,k) \in I \times \mathbb{Z}. \end{cases}$$

Thus $T_{(\mathbb{N},S)}$ does not characterize $(\mathbb{N}, S)$ up to isomorphism.

Remarks 11.3. (a) The map F above is defined by recursion, and a rigorous proof of its existence will be given in Theorem 12.2 in Section 12.

(b) The expression (11.1) does not give that $\sim$ is definable in M, since $S_M^{(n)}(x) \overset{\text{def}}{=} S_M \circ \cdots \circ S_M(x)$ is a term only when n is a fixed natural number.

Proposition 11.4. *The theory $T_{(\mathbb{N},S)}$ is complete.*

Sketch of the proof. We will nee some facts that will be proved in Section 20. Suppose M and N are uncountable models of $T_{(\mathbb{N},S)}$. Then they must be non-standard and therefore of the form $M = \mathbb{N} \uplus (I \times \mathbb{Z})$ and $N = \mathbb{N} \uplus (J \times \mathbb{Z})$. If M and N have the same cardinality, then I and J must be in bijection, and hence M and N are isomorphic. Therefore $T_{(\mathbb{N},S)}$ is complete by Theorem 4.37. □

11.A.2. *Elimination of quantifiers.* In order to study the collection of definable subsets of $(\mathbb{N}, S)$ it is convenient to extend the language with a constant $\overline{0}$ for zero. The language so obtained is denoted by $\mathcal{L}_{\mathsf{D}}$.[4] Since 0 is definable in $(\mathbb{N}, S)$, it follows that $X \subseteq \mathbb{N}^k$ is definable in $(\mathbb{N}, S)$ if and only if it is definable in $(\mathbb{N}, S, 0)$.

Definition 11.5. Let $\mathcal{L}$ be a language extending $\mathcal{L}_{\mathsf{D}}$. For each $n \in \mathbb{N}$ let $\overline{n}$ be the closed $\mathcal{L}$-term defined as follows. If $n = 0$, then $\overline{n}$ is the constant symbol $\overline{0}$. If $n = m+1$, then $\overline{n}$ is the term $\mathtt{S}(\overline{m})$. The terms $\overline{n}$ so defined are called **numerals**.

The terms of the extended language are those of the original language, that is of the form $\mathtt{S}^{(n)}(x)$, plus the numerals. A formula $\varphi(x_1, \ldots, x_n)$ of the extended language can be translated into $\exists y\, (\varphi_0(y) \land \varphi'(x_1, \ldots, x_n, y))$ a formula of the original language with $\varphi'(x_1, \ldots, x_n, y)$ obtained by replacing the terms of the form $\overline{k}$ with $\mathtt{S}^{(k)}(y)$. It follows that $\varphi(x_1, \ldots, x_n)$ and $\exists y\, (\varphi_0(y) \land \varphi'(x_1, \ldots, x_n, y))$ are equivalent modulo $T_{(\mathbb{N},S)}$. The expanded structure $(\mathbb{N}, S, 0)$ has the same definable subsets of $(\mathbb{N}, S)$.

[4] The subscript D is for Dedekind.

From now on, the language used will be $\mathcal{L}_{\mathsf{D}}$, and the theory of the original language $T_{(\mathbb{N},S)}$ containing only the symbol $\mathtt{S}$, is replaced by its analogue

$$T_{(\mathbb{N},S,0)}\begin{cases}\forall x\left(\mathtt{S}(x)\neq\overline{0}\right)\\ \forall x\left(x\neq\overline{0}\Rightarrow\exists y(\mathtt{S}(y)=x)\right)\\ \forall x,y\,(x\neq y\Rightarrow\mathtt{S}(x)\neq\mathtt{S}(y))\\ \forall x(\mathtt{S}^{(n)}(x)\neq x) & (\sigma_n, n\geq 1).\end{cases}$$

Definition 11.6. Let T be a theory in a language with constants. We say that T **admits elimination of quantifiers** if a quantifier-free formula φ' can be assigned to any formula φ so that φ and φ' have the same free variables, and are logically equivalent modulo T. If the assignment $\varphi \rightsquigarrow \varphi'$ can be performed in a mechanical way, then T **admits effective elimination of quantifiers**.

Definition 11.7. A theory T for which there is an algorithm to check whether or not a sentence σ is logical consequence of T, is said to be **decidable**.

The notions of *mechanical procedure* and of *decidable theory* implicitly entail that the theory be **effectively axiomatized**, that is to say: there are effective methods to check whether a given string of symbols is a formula, and to check whether a given sentence is an axiom of the theory.

Proposition 11.8. *Let T be an effectively axiomatized theory.*

Suppose T admits elimination of quantifiers, and that T is complete for atomic sentences, that is to say: either $T\models\sigma$ or else $T\models\neg\sigma$, for all atomic sentences σ. Then T is complete.

Suppose T admits the effective elimination of quantifiers, and T is decidable for all atomic sentences, that is to say: for all atomic sentences σ it is possible to determine in a mechanical way whether $T\models\sigma$ or $T\models\neg\sigma$. Then T is decidable.

Proof. Given a sentence σ, let θ be a quantifier-free sentence which is logically equivalent to σ modulo T. Since θ is Boolean combination of atomic sentences, the result follows. □

Remarks 11.9. (a) The requirement in Proposition 11.8 that either $T\models\sigma$ or else $T\models\neg\sigma$ for all atomic sentences σ, cannot be removed (Exercise 11.50).

(b) In Chapter VII we will show that a complete theory in a language with finitely many non-logical symbols is decidable.

The following criterion is useful for verifying that a theory admits elimination of quantifiers.

Lemma 11.10. *The following are equivalent:*

(a) *T admits elimination of quantifiers,*

(b) *given a formula $\exists x\psi$ with ψ quantifier-free, there is a quantifier-free formula θ with the same free variables as $\exists x\psi$, and so that $\exists x\psi$ and θ are logically equivalent modulo T,*

(c) *as* (b)*, but with ψ of the form $\alpha_1 \wedge \cdots \wedge \alpha_n$ and α_i atomic or negation of an atomic formula.*

If the assignment $\exists x\psi \rightsquigarrow \theta$ in (b) *and* (c) *is effective, then condition* (a) *can be strengthened to*

(a′) *T admits the effective elimination of quantifiers.*

Proof. Clearly (a) ⇒ (b) ⇒ (c).

(c) ⇒ (b): If ψ is quantifier-free, then we may assume it is in disjunctive normal form (Section 3.C.1), that is of the form $\varphi_1 \vee \cdots \vee \varphi_k$ with each φ_i a conjunction of formulæ that are atomic or negated atomic. So $\exists x\psi$ is logically equivalent to $(\exists x\varphi_1) \vee \cdots \vee (\exists x\varphi_k)$, and hence by (c) it is logically equivalent modulo T to some quantifier-free formula θ with the same free variables as $\exists x\psi$.

(b) ⇒ (a): It is enough to show that for any φ in prenex form there is a quantifier-free φ' which is logically equivalent to φ modulo T, and with the same free variables. The proof is by induction on the complexity of φ.

If φ is quantifier-free, then there is nothing to prove. If φ is $\exists x\psi$, then by inductive assumption there is a quantifier-free ψ' with the same free variables as ψ, and logically equivalent to ψ modulo T. Thus φ is logically equivalent to $\exists x\psi'$ modulo T, and by hypothesis there is a quantifier-free θ with the same free variables as $\exists x\psi$ and logically equivalent to $\exists x\psi$ modulo T. Therefore θ is the required formula. If φ is $\forall x\psi$, then it is logically equivalent to $\neg\exists x\neg\psi$, hence by the preceding case there is a quantifier-free formula θ, with the same free variables as in $\exists x\neg\psi$, and which is logically equivalent to $\exists x\neg\psi$ modulo T. Then $\neg\theta$ is the required formula. □

Theorem 11.11. *$T_{(\mathbb{N},S,0)}$ admits elimination of quantifiers.*

The proof of this result is elementary, but lengthy, so it is postponed to Section 11.A.3.

Remark 11.12. Theorem 11.11 does not hold if we were to use the language containing only the symbol S. For example the formula $\varphi_0(x)$ defining 0 is not logically equivalent to a quantifier-free formula.

Every sentence σ in the language containing S and $\overline{0}$ is logically equivalent modulo $T_{(\mathbb{N},S,0)}$ to a quantifier-free sentence σ', that is to say: a Boolean combination of formulæ of the form $\mathtt{S}^{(n)}(\bar{0}) \doteq \mathtt{S}^{(m)}(\bar{0})$, and for such sentence it is straightforward to check whether it or its negation follows logically from $T_{(\mathbb{N},S,0)}$. Therefore we obtain another proof of Proposition 11.4 that $T_{(\mathbb{N},S,0)}$ and $T_{(\mathbb{N},S)}$ are complete theories.

The proof of Theorem 11.11 yields:

Corollary 11.13. *$T_{(\mathbb{N},S,0)}$ and $T_{(\mathbb{N},S)}$ are decidable theories.*

The subsets of $\mathbb{N}$ that are definable in $(\mathbb{N}, S, 0)$ are exactly the finite and cofinite sets. In order to describe the definable sets of dimension two, the following family comes handy: let $\mathcal{D}$ be the smallest family of subsets of $\mathbb{N}^2$ containing

- every point in $\mathbb{N}^2$,
- the diagonal lines $\{(n,m) \in \mathbb{N}^2 \mid m = n + k\}$, for some $k \in \mathbb{Z}$, and
- the horizontal and vertical lines $\{(n,k) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$ and $\{(k,n) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$, for $k \in \mathbb{N}$,

and closed under finite unions and intersections, and complements. Then $\mathcal{D}$ is the family of subsets of $\mathbb{N}^2$ that are definable in $(\mathbb{N}, S)$, and the sets in $\mathcal{D}$ are of the form $P \triangle (\bigcup L)$ or $\mathbb{N}^2 \setminus (P \triangle (\bigcup L))$ where P is a finite (possibly empty) set of points and L is a finite (possibly empty) set of lines, and $\{(n,m) \mid n < m\} \notin \mathcal{D}$ (Exercise 11.60). In particular:

Corollary 11.14. *The order relation is not definable in* $(\mathbb{N}, S)$.

Recall that the covering relation (see page 46) is definable from the ordering (Exercise 4.65). As the successor function defines the covering relation, this proves that, in general, it is not possible to define the ordering relation from the covering relation.

Remark 11.15. Quantifier elimination for a theory T yields important information on the definable subsets of *any* model of T. For example, Theorem 11.11 shows that, given a non-standard model $M = \mathbb{N} \uplus (I \times \mathbb{Z})$ of $T_{(\mathbb{N},S,0)}$, the definable subsets of dimension 1 with parameters $p_1, \ldots, p_n \in M$ are the finite sets of the form $F \subseteq \mathbb{N} \cup \{p_1, \ldots, p_n\}$ and their complements. In particular, no element of $M \setminus \mathbb{N}$ is definable without parameters, and $\mathbb{N}$ is not definable, even allowing parameters.

In Chapter VII we will prove (Section 32.D.1) the following useful criterion for proving elimination of quantifiers.

Proposition 11.16. *Let T be a first-order theory in a language $\mathcal{L}$ with constants. Suppose that for any pair M, N of models of T and for any isomorphism $F \colon M' \to N'$, where M' is a substructure of M and N' is a* *substructure of N,*

$$M \vDash \exists y \varphi[a_1, \dots, a_n] \Leftrightarrow N \vDash \exists y \varphi[F(a_1), \dots, F(a_n)],$$

where $\varphi(y, x_1, \dots, x_n)$ is a conjunction of atomic formulæ or negated atomic formulæ, and $a_1, \dots, a_n \in M'$. Then T admits elimination of quantifiers.

Remark 11.17. There are theories T without constants that nevertheless admit elimination of quantifiers for formulæ that are not sentences, that is to each non-closed formula φ we can associate an open formula φ' with the same free variables, so that φ and φ' are logically equivalent modulo T. In this case we say that T admits elimination of quantifiers for non-closed formulæ and Proposition 11.16 above holds also in this case.

Besides $T_{(\mathbb{N},S,0)}$, there are several theories admit elimination of quantifiers:

- the theory of natural numbers with the order (Exercise 11.49) or with addition (p. 273),
- the theory of dense linear orders without end points (Exercise 11.71),
- the theory of algebraically closed fields of fixed characteristic (Theorem 11.44),
- the theory of real closed fields (Section 11.D.1).

11.A.3. *Proof of Theorem 11.11*.* In this section "equivalent" means "logically equivalent modulo $T_{(\mathbb{N},S,0)}$". An atomic formula of the language with $\mathtt{S}$ and $\overline{0}$ is an equation of the following type:

type 1: $\mathtt{S}^{(n)}(x) = \mathtt{S}^{(m)}(y)$, with x and y distinct variables,

type 2: $\mathtt{S}^{(n)}(x) = \overline{m}$,

type 3: $\mathtt{S}^{(n)}(x) = \mathtt{S}^{(m)}(x)$,

type 4: $\overline{n} = \overline{m}$.

Proposition 11.18. *Given a quantifier-free sentence, either it or its negation follows from $T_{(\mathbb{N},S,0)}$. In fact there is an algorithm that, given a quantifier-free sentence σ, determines whether $T_{(\mathbb{N},S,0)} \models \sigma$ or else $T_{(\mathbb{N},S,0)} \models \neg\sigma$.*

Proof. If σ is atomic, then, as it is a sentence, it is of type 4, hence it is logically equivalent modulo $T_{(\mathbb{N},S,0)}$ to $\overline{k} = \overline{0}$, for some $k \geq 0$. If $k = 0$ then $T_{(\mathbb{N},S,0)} \models \sigma$, and if $k > 0$ then $T_{(\mathbb{N},S,0)} \models \neg\sigma$ by axiom σ_k. A similar argument applies to negations of atomic sentences. Since a quantifier-free sentence can be taken to be in disjunctive normal form, the argument above can be modified into an effective method to check whether $T_{(\mathbb{N},S,0)} \models \sigma$ or else $T_{(\mathbb{N},S,0)} \models \neg\sigma$. □

Thus Corollary 11.13 follows at once.

The axiom $\forall x, y\, (x \neq y \Rightarrow \mathtt{S}(x) \neq \mathtt{S}(y))$ implies that

If θ is...	then $\exists x\theta$ is equivalent to...
$x = \overline{m}$	$\overline{0} = \overline{0}$
$x \neq \overline{m}$	$\overline{0} = \overline{0}$
$x = x$	$\overline{0} = \overline{0}$
$x \neq x$	$\overline{0} \neq \overline{0}$
$\mathtt{S}^{(m)}(x) = y$	$y \neq \overline{0} \wedge \cdots \wedge y \neq \overline{m-1}$
$x = \mathtt{S}^{(m)}(y)$	$y = y$
$x \neq \mathtt{S}^{(m)}(y)$	$y = y$
$\mathtt{S}^{(m)}(x) \neq y$	$y = y$

Table 1.

- equalities of type 1 are equivalent either to '$\mathtt{S}^{(k)}(x) = y$' or to '$x = y$' or else to '$x = \mathtt{S}^{(k)}(y)$', with $k > 0$, depending whether n is larger, equal, or smaller than m;
- equalities of type 2 are equivalent either to '$x = \overline{0}$' (if $n = m$) or to '$\mathtt{S}^{(k)}(x) = \overline{0}$' (if $k = n - m > 0$) or else to '$x = \overline{k}$' (if $k = m - n > 0$);
- equalities of type 3 are equivalent to '$\mathtt{S}^{(k)}(x) = x$' with $k = |n - m|$;
- finally those of type 4 are equivalent to '$\overline{k} = \overline{0}$' with $k = |n - m|$.

The axioms $\forall x \left(\mathtt{S}(x) \neq \overline{0}\right)$ and σ_k imply that if φ is atomic or the negation of an atomic formula, then it is equivalent to a formula φ' with the same free variables, taken from the following list:

$$\boxed{\begin{array}{ll} x = \mathtt{S}^{(m)}(y) & x \neq \mathtt{S}^{(m)}(y) \\ x = \overline{m} & x \neq \overline{m} \\ x = x & x \neq x \\ \overline{0} = \overline{0} & \overline{0} \neq \overline{0} \end{array}} \tag{11.2}$$

where $m \geq 0$. Call formulæ in the first column *equalities*, those in the second column *inequalities*.

Lemma 11.19. *If* θ *is a conjunction of formulæ that are atomic or negations of atomic formulæ* $\psi_1 \wedge \cdots \wedge \psi_n$*, then* $\exists x\theta$ *is equivalent to a quantifier-free* θ' *with the same free variables as* $\exists x\theta$*.*

Proof. Suppose $n = 1$, that is to say θ is either an atomic formula or the negation of an atomic formula. We may assume that θ is a formula in the list (11.2). If the variable x does not occur in θ, then $\exists x\theta$ is logically equivalent to θ which is quantifier-free, hence we may assume that x occurs in θ. The result follows from Table 1. Checking these equivalences is straightforward. For example, for all y there are infinitely many x such that $\mathtt{S}^{(m)}(x) \neq y$—more precisely: given an $M \vDash T_{(\mathbb{N},S,0)}$ and an element $b \in M$, the set

$$\mathbf{T}^M_{\mathtt{S}^{(m)}(x) \neq y} \cap M \times \{b\} \tag{11.3}$$

is cofinite, hence non-empty: since b is arbitrary, it follows that $\mathbf{T}^M_{\exists x (\mathtt{S}^{(m)}(x) \neq y)} = M$.

Suppose now $n > 1$ and let $y_1, \dots, y_k$ be the variables different from x occurring in θ. If the variable x does not occur in some of the ψ_i, e.g. $i = 1$, then $\exists x \theta$ is logically equivalent to $\psi_1 \wedge \exists x\, (\psi_2 \wedge \dots \wedge \psi_n)$, and by inductive hypothesis $\exists x\, (\psi_2 \wedge \dots \wedge \psi_n)$ is equivalent to a quantifier-free formula, whence the result. If some of the ψ_is were

$$x = x \qquad \text{or} \qquad \mathtt{S}^{(k)}(x) \neq \overline{0} \quad (k > 0) \tag{11.4}$$

then θ would be equivalent to the formula obtained by removing ψ_i from the conjunction, and the inductive hypothesis applies. Similarly, if some of the ψ_is were

$$x \neq x \qquad \text{or} \qquad \mathtt{S}^{(k)}(x) = \overline{0} \quad (k > 0) \tag{11.5}$$

then $\exists x \theta$ would be equivalent to $\overline{0} \neq \overline{0} \wedge \bigwedge_{1 \leq i \leq k} (y_i = y_i)$. Therefore we may assume that

- the variable x occurs in every ψ_i,
- no ψ_i is of the form either (11.4) or (11.5),
- every ψ_i is of the form

$$\begin{array}{cc} \mathtt{S}^{(m_i)}(x) = y & \mathtt{S}^{(m_i)}(x) \neq y \\ x = \mathtt{S}^{(m_i)}(y) & x \neq \mathtt{S}^{(m_i)}(y) \\ x = \overline{m_i} & x \neq \overline{m_i} \end{array}$$

where $m_i \geq 0$ and y is one of the $y_1, \dots, y_k$.

Case 1: Every ψ_i is an inequality. We distinguish two cases.

- $\exists x \theta$ is a sentence. Then the ψ_is are of the form $x \neq \overline{m_i}$, hence the sentence $\exists x \theta$ is true in every model of $T_{(\mathbb{N},S,0)}$: just take x to be the element $S^{(m)}(0)$ with m sufficiently large. In other words: $\exists x \theta$ is logically equivalent modulo $T_{(\mathbb{N},S,0)}$ to $\overline{0} = \overline{0}$.
- $\exists x \theta$ is not a sentence. Then the ψ_is are of the form $\mathtt{S}^{(m_i)}(x) \neq y_j$ or of the form $\mathtt{S}^{(m_i)}(y_j) \neq x$ with $j = 1, \dots, k$, and maybe some of the ψ_is are of the form $x \neq \overline{m}$. Arguing as in the case of formula (11.3), for all $M \vDash T_{(\mathbb{N},S,0)}$ and every $b_1, \dots, b_k \in M$ the set

$$\mathbf{T}^M_{\theta(x, y_1, \dots, y_k)} \cap M \times \{(b_1, \dots, b_k)\}$$

is cofinite, since it is a finite intersection of cofinite sets. It follows that $\mathbf{T}^M_{\exists x \theta} = M^k$, that is to say: $\exists x \theta$ is equivalent to $\bigwedge_{1 \leq i \leq k} (y_i = y_i)$.

The result holds in Case 1, hence we can suppose that at least one of the ψ_is is an equality.

Case 2: At least one ψ_i of the form $x = t$ where t is $\overline{m}$ or $\mathtt{S}^{(m)}(y_h)$, with $1 \leq h \leq k$. Then $\exists x\theta$ is equivalent to the formula θ'

$$\bigwedge_{\substack{1\leq j\leq n\\ j\neq i}} \psi_j \llparenthesis t/x \rrparenthesis$$

obtained by removing ψ_i from the conjunction θ, and replacing the term t instead of x in the other ψ_js. The result holds in Case 2, thus we may assume:

Case 3: At least one ψ_i of the form $\mathtt{S}^{(m_i)}(x) = y_h$, with $1 \leq h \leq k$. Let i be the least such index, and let $j_1, \dots, j_p$ be the other indexes j such that ψ_j is of the form $\mathtt{S}^{(m_j)}(x) = t_j$, which is equivalent to $\mathtt{S}^{m_j}(y_h) = \mathtt{S}^{m_i}(t_j)$. Then $\exists x\theta$ is equivalent to the formula θ' obtained by removing the formula ψ_i from the conjunction θ, and replacing $\psi_{j_1}, \dots, \psi_{j_p}$ with the formulæ $\mathtt{S}^{(m_{j_1})}(y_h) = \mathtt{S}^{(m_i)}(t_{j_1}), \dots, \mathtt{S}^{(m_{j_p})}(y_h) = \mathtt{S}^{(m_i)}(t_{j_p})$.

Since in both Cases 2 and 3 the formula θ' is quantifier-free and has he same free variables as $\exists x\theta$, the result is proved. □

This completes the proof of Theorem 11.11.

11.A.4. *The ordering.* Consider the structure $(\mathbb{N}, <)$. The successor function is definable via the formula

$$(\sigma(x,y)) \qquad\qquad x < y \land \neg\exists z\,(x < z \land z < y)\,,$$

hence the definable sets in $(\mathbb{N}, <)$ are exactly those of $(\mathbb{N}, <, S, 0)$. The theory $T_{(\mathbb{N},<,S,0)}$ is obtained by adding to $T_{(\mathbb{N},S,0)}$ the sentences asserting that $<$ is a strict linear order

$$(11.6a) \qquad\qquad \neg\exists x\,(x < x)$$

$$(11.6b) \qquad\qquad \forall x, y, z\,(x < y \land y < z \Rightarrow x < z)$$

$$(11.6c) \qquad\qquad \forall x, y\,(x < y \veebar x = y \veebar y < x)\,,$$

where $\veebar$ is the exclusive disjunction (see pag. 9), together with the sentence asserting that $\mathtt{S}(x)$ is the immediate successor of x

$$(11.6d) \qquad\qquad \forall x, y\,(x < \mathtt{S}(x) \land \neg\,(x < y \land y < \mathtt{S}(x)))\,.$$

The sentences $\forall x(\mathtt{S}^{(n)}(x) \neq x)$ follows from transitivity of the order relation, hence $T_{(\mathbb{N},<,S,0)}$ is finitely axiomatizable. The theory $T_{(\mathbb{N},<,S,0)}$ admits elimination of quantifiers (Exercise 11.49): it follows that $T_{(\mathbb{N},<)}$ and $T_{(\mathbb{N},<,S,0)}$ are complete and decidable theories. Also in this case, the only subsets of $\mathbb{N}$

that are definable in $(\mathbb{N}, <, S, 0)$ or, equivalently, in $(\mathbb{N}, <)$, are the finite and cofinite sets. The relation $x < y$ can be written as $\exists k\bigl(y \mathrel{=\!=} \mathtt{S}(\mathtt{S}^{(k)}(x))\bigr)$ or as

$$y \mathrel{=\!=} \mathtt{S}(x) \vee y \mathrel{=\!=} \mathtt{S}(\mathtt{S}(x)) \vee y \mathrel{=\!=} \mathtt{S}(\mathtt{S}(\mathtt{S}(x))) \vee \dots,$$

but these are pseudo-formulæ so we cannot infer that the ordering is definable in $(\mathbb{N}, S)$. In fact this is not the case by Exercise 11.60.

A straightforward adaptation of the proof of Proposition 11.2 yields:

Proposition 11.20. *The non-standard models (M, S_M) of $T_{(\mathbb{N},<)}$ are, up to isomorphism, of the form $M = \mathbb{N} \uplus (I \times \mathbb{Z})$ with $(I, \prec)$ an arbitrary non-empty linearly ordered set, and $<_M$ is the standard order on $\mathbb{N}$, every $n \in \mathbb{N}$ comes before every $(i, a) \in I \times \mathbb{Z}$, and*

$$(i, a) <_M (j, b) \Leftrightarrow i \prec j \vee [i = j \wedge a < b].$$

Since any set I can be linearly ordered,[5] every model of $T_{(\mathbb{N},S)}$ can be turned into a model of $T_{(\mathbb{N},<)}$.

Arguing as in Proposition 11.4 one can prove that

Proposition 11.21. *The theory $T_{(\mathbb{N},<)}$ is complete.*

11.A.5. *Addition.* Consider the structure $(\mathbb{N}, +)$. The ordering $x < y$ is defined by the formula

$$x \neq y \wedge \exists z\,(x + z \mathrel{=\!=} y)\,,$$

hence the definable sets in the structures $(\mathbb{N}, +, <, S, 0)$ and $(\mathbb{N}, +)$ are the same. For all $n \geq 2$, the relation $\equiv_n$ of congruence modulo n is definable in $(\mathbb{N}, +)$ via the formula

$$(\chi_n(x, y)) \qquad \exists z\,\bigl(x + \underbrace{z + \dots + z}_{n} \mathrel{=\!=} y \;\vee\; y + \underbrace{z + \dots + z}_{n} \mathrel{=\!=} x\bigr),$$

hence $(\mathbb{N}, +, <, S, 0, \equiv_2, \equiv_3, \dots)$ and $(\mathbb{N}, +)$ have the same definable sets.

Definition 11.22. Presburger arithmetic is the theory $T_{(\mathbb{N},+,<,S,0)}$ in the language with symbols $+, <, \mathtt{S}, \overline{0}$ and with the axioms:

- the axioms for linear orders (the statements (11.6) on page 271),
- the axioms for abelian monoids (the statements (3.11a), (3.11b), (3.11c) on page 53),
- $\forall x, y, z\,(x + z \mathrel{=\!=} y + z \Rightarrow x \mathrel{=\!=} y)$ (cancellation law),
- $\forall x, y\,\bigl(x + y \mathrel{=\!=} \overline{0} \Rightarrow x \mathrel{=\!=} \overline{0} \wedge y \mathrel{=\!=} \overline{0}\bigr)$ (positivity law),
- $\forall x, y\,(x < y \Leftrightarrow x \neq y \wedge \exists z\,(x + z \mathrel{=\!=} y))$ (compatibility law),

[5] At least if we assume some form of the axiom of choice—see Section 28.C.

- the infinite list of statements

$$(\pi'_n) \qquad \forall x \exists! y \left(\chi_n(x,y) \wedge y < \overline{n}\right)$$

for every $n \geq 2$.

Note that the axiom π'_n can be re-written as

$$\forall x \exists! y \, \exists! z \left(x = nz + y \wedge y < \overline{n}\right),$$

that is the axiom π_n for $\mathbb{Z}$-groups (see page 240) recast for the structure $(\mathbb{N}, +, <, S, 0, \equiv_2, \equiv_3, \dots)$.

The theory $T_{(\mathbb{N},+,S,0)}$ does not admit elimination of quantifiers, since the formula $\chi_n(x,y)$ is not equivalent to any open formula with free variables x and y. In some sense, these are the only obstructions to elimination of quantifiers. Let $T_{(\mathbb{N},+,\equiv)}$ be the theory (still dubbed Presburger arithmetic) in the language expanded with infinitely many new binary relation symbols $\equiv_n$ ($n \geq 2$), with the axioms of $T_{(\mathbb{N},+)}$ together with the axioms

$$\forall x, y \; (x \equiv_n y \Leftrightarrow \chi_n(x,y))$$

for all $n \geq 2$. Then $T_{(\mathbb{N},+,\equiv)}$ admits elimination of quantifiers and every atomic sentence is decidable [**End01**, pag. 197–201]. Therefore $T_{(\mathbb{N},+,\equiv)}$ and $T_{(\mathbb{N},+)}$ are complete decidable theories.

Every finite or cofinite subset of $\mathbb{N}$ is definable in $(\mathbb{N}, +)$, since every definable set in $(\mathbb{N}, <)$ is also definable in $(\mathbb{N}, +)$. Besides the finite and cofinite sets it is also possible to define any periodic set, that is every arithmetic progression. In fact $\{a \cdot n + b \mid n \in \mathbb{N}\}$ is defined by

$$x \equiv_a \overline{b}.$$

Since the family of definable subsets is closed under symmetric difference, every eventually periodic subset of $\mathbb{N}$ is definable in $(\mathbb{N}, +)$. By elimination of quantifiers it can be shown that the rank 1 definable sets of $(\mathbb{N}, +)$ are exactly the subsets of $\mathbb{N}$ that are eventually periodic, and their complements. Addition is neither definable in $(\mathbb{N}, <)$ nor in $(\mathbb{N}, S)$: otherwise the set of even numbers would be definable in these structures against the fact that the subsets of $\mathbb{N}$ that are definable in $(\mathbb{N}, <)$ or in $(\mathbb{N}, S)$ are the finite and the cofinite ones.

Let's now take a look at the non-standard models of $T_{(\mathbb{N},+)}$. By the positivity and compatibility laws, 0 is the minimum of $(M, <)$, and by the cancellation law the element z whose existence is asserted in the axiom of compatibility of sum and order is unique.

Proposition 11.23. *$M \vDash T_{(\mathbb{N},+,\equiv)}$ if and only if it is (isomorphic to)*

$$G^+ = \{g \in G \mid 0_G = g \vee 0_G <_G g\},$$

where G is a $\mathbb{Z}$-group.

Proof. Say $(M, +, <, S, 0, \equiv_2, \equiv_3, \dots)$ is a model of Presburger arithmetic, and suppose $F\colon M \setminus \{0\} \to M'$ is a bijection where M' is a set disjoint from M. Then F can be used to define $+$ and $<$ on M' by letting

$$\forall x, y \in M \setminus \{0\} \; [F(x) + F(y) = F(x + y) \;\wedge\; (F(x) < F(y) \Leftrightarrow y < x)] .$$

The order $<$ can be extended to a total order on $G \overset{\text{def}}{=} M \cup M'$ by declaring the elements in M' to appear before the elements in M. In order to define $+$ on G it is enough to define $x + y$ when $x \in M'$ and $y \in M$ or when $x \in M$ and $y \in M'$. By requiring that $x + y = y + x$ we may assume that $x \in M'$ and $y \in M$. If $F^{-1}(x) = y$, then set $x + y = 0$, so we may assume that either $F^{-1}(x) < y$ or else $y < F^{-1}(x)$. If the former holds then $F^{-1}(x) + z = y$ for some unique $z \in M \setminus \{0\}$, and set $x + y = z$; if the latter holds then $y + z = F^{-1}(x)$ for some unique $z > 0$, and set $x + y = F(z)$. It is easy to check that $(G, +, <)$ is a $\mathbb{Z}$-group.

The other direction, that G^+ is a model of Presburger arithmetic for any $\mathbb{Z}$-group G, is left to the reader. □

If G is a $\mathbb{Z}$-group and $Z = \{k1_G \mid k \in \mathbb{Z}\}$, the quotient $(G/Z, <)$ is a dense linear order without endpoints, hence the order in a non-standard model of Presburger arithmetic is of the form $\mathbb{N} \uplus L \times \mathbb{Z}$, with L a dense linear order without endpoints. A concrete example of a non-standard model of Presburger arithmetic is $\mathbb{N} \uplus \mathbb{Q} \times \mathbb{Z}$ with addition operation defined by $n + (q, z) = (q, z + n)$ and $(q_1, z_1) + (q_2, z_2) = (q_1 + q_2, z_1 + z_2)$ (Exercise 11.47).

11.A.6. *Multiplication, divisibility, and coprimality.* Consider the structures $(\mathbb{N}, \perp)$, $(\mathbb{N}, |)$ and $(\mathbb{N}, \cdot)$, where $\perp$ is the co-primality predicate, that is

$$x \perp y \Leftrightarrow \forall z\, (z \mid x \wedge z \mid y \Rightarrow z \mathrel{=\!\!\!=} 1)$$

and $|$ is the divisibility predicate. The relation $|$ is definable in $(\mathbb{N}, \cdot)$, while the definability of $\perp$ in $(\mathbb{N}, |)$ follows from the definability of 1 in the structure $(\mathbb{N}, |)$ (Exercise 4.77). The converse is not true, i.e. $|$ is not definable in $(\mathbb{N}, \perp)$ (Exercise 11.46) and $\cdot$ is not definable in $(\mathbb{N}, |)$ (Exercise 12.30).

It is possible to find a complete set of axioms for the structure $(\mathbb{N}, \cdot)$, known as **Skolem arithmetic**, admitting elimination of quantifiers [**Smo91**, page 333].

By Exercise 4.77 the set of primes is definable in $(\mathbb{N}, |)$ and hence also in $(\mathbb{N}, \cdot)$. The set of primes is not eventually periodic, so it is not definable in $(\mathbb{N}, +)$.

Corollary 11.24. *The divisibility relation, and multiplication are not definable in* $(\mathbb{N}, +)$.

Using the identity

$$z \mathrel{=\!\!\!=} \overline{0} \vee (x + y) \mathrel{=\!\!\!=} z \Leftrightarrow (xz + 1)(yz + 1) \mathrel{=\!\!\!=} z^2(xy + 1) + 1 \tag{11.7}$$

one can show that addition is quantifier-free definable both in $(\mathbb{N}, S, \cdot)$ and in $(\mathbb{Z}, S, \cdot)$. The next result shows that the successor function cannot be removed.

Proposition 11.25. *The set* $\{(n, m, k) \in \mathbb{N}^3 \mid n + m = k\}$ *is not definable in the structure* $(\mathbb{N}, \cdot)$.

Proof. Let F be a permutation on the set of primes. Every natural number bigger than 1 can be written in a unique way as $p_1^{n_1} \cdots p_k^{n_k}$ with $p_1 < \cdots < p_k$ primes, so F extends to a permutation of $\mathbb{N}$ by letting $F(0) = 0$, $F(1) = 1$ and $F(p_1^{n_1} \cdots p_k^{n_k}) = F(p_1)^{n_1} \cdots F(p_k)^{n_k}$. It is immediate to check that $F \colon (\mathbb{N}, \cdot) \to (\mathbb{N}, \cdot)$ is an automorphism, but $F(n + m) \neq F(n) + F(m)$ if F is not the identity. □

By what we saw the structures $(\mathbb{N}, S)$ and $(\mathbb{N}, |)$ are the least expressive among those considered so far, but if we merge them in a single structure $(\mathbb{N}, S, |)$ addition and multiplication, and hence the ordering, can be defined (Exercise 11.70). To recap:

Proposition 11.26. (a) *S is not definable in $(\mathbb{N}, |)$ and $|$ is not definable in $(\mathbb{N}, S)$.*

(b) *$+$ and $\cdot$ are definable in any of $(\mathbb{N}, <, |)$, $(\mathbb{N}, +, |)$, $(\mathbb{N}, <, \cdot)$.*

11.B. Arithmetic. In this section we shall prove that, contrarily to what we have seen before, the structure $(\mathbb{N}, +, \cdot)$ can turn recursive definitions into standard ones. In particular, the exponential map, defined recursively by

$$x^0 = 1 \qquad\qquad x^{y+1} = x^y \cdot x$$

is definable. In fact every computable set and function is definable in arithmetic. This means that the family of definable subsets of $(\mathbb{N}, +, \cdot)$ is very rich. On the other hand, this plethora of definable subsets forbids the possibility of finding an axiom system for the theory of $(\mathbb{N}, +, \cdot)$ that admits elimination of quantifiers. As we shall see in Chapter VIII, the theory of $(\mathbb{N}, +, \cdot)$ is neither effectively axiomatizable, nor decidable. In Section 12 **Peano arithmetic**, a theory with a reasonable set of axiom and strong enough to prove many of the elementary facts on natural numbers, will be presented.

In Section 8.A.1 the diagonal enumeration of $\mathbb{N} \times \mathbb{N}$ is defined and the resulting bijection $\boldsymbol{J} \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\boldsymbol{J}(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x$$

is definable in $(\mathbb{N}, +, \cdot)$ by the formula

$$(\psi_{\boldsymbol{J}}(x, y, z)) \qquad \exists w (w + w \doteq (x + y) \cdot (x + y + 1) \land w + x \doteq z).$$

The two inverse maps $n \mapsto (\cdot)_0$ and $n \mapsto (\cdot)_1$ so that $\boldsymbol{J}((\cdot)_0, (\cdot)_1) = n$ are defined by

$(\psi_0(z, x))$ $\qquad\qquad\qquad\qquad \exists y\, \psi_{\boldsymbol{J}}(x, y, z)$

$(\psi_1(z, y))$ $\qquad\qquad\qquad\qquad \exists x\, \psi_{\boldsymbol{J}}(x, y, z).$

The bijection $\boldsymbol{J}$ induces a bijection

$$\mathscr{P}(\mathbb{N} \times \mathbb{N}) \to \mathscr{P}(\mathbb{N}), \quad X \mapsto \boldsymbol{J}[X] = \{\boldsymbol{J}(n, m) \mid (n, m) \in X\}$$

mapping definable sets to definable sets: if $X \subseteq \mathbb{N} \times \mathbb{N}$ is defined by $\varphi(x, y)$ then $\boldsymbol{J}[X] \subseteq \mathbb{N}$ is defined by

$$\exists x, y\, (\psi_{\boldsymbol{J}}(x, y, z) \wedge \varphi(x, y));$$

conversely, if $Y \subseteq \mathbb{N}$ is defined by $\varphi(z)$ then $\boldsymbol{J}^{-1}[Y] = \{(n, m) \mid \boldsymbol{J}(n, m) \in Y\}$ is defined by

$$\exists z\, (\psi_{\boldsymbol{J}}(x, y, z) \wedge \varphi(z)).$$

By Remark 4.42 the family of all definable sets of dimension 1 can always be identified with a subfamily of the collection of definable sets of dimension 2, but here we have a complete identification.

Composing $\boldsymbol{J}$ with itself we get a definable bijection

$$\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (n, m, k) \mapsto \boldsymbol{J}(n, \boldsymbol{J}(m, k)),$$

and by iterating this construction we get a definable bijection $\mathbb{N}^k \to \mathbb{N}$, for $k \geq 1$, that carries definable sets to definable sets.

Using Gödel's $\boldsymbol{\beta}$ function we constructed a coding machinery, that is

- a computable set $\mathrm{Seq} \subseteq \mathbb{N}$ coding all finite sequences of natural numbers,
- a computable function $\ell \colon \mathbb{N} \to \mathbb{N}$ such that $\ell(m)$ is the length of the sequence coded by $m \in \mathrm{Seq}$,
- for all $k \in \mathbb{N}$ a computable map $\mathbb{N}^{k+1} \to \mathbb{N}$, $\langle n_0, \ldots, n_k \rangle \mapsto \langle\!\langle n_0, \ldots, n_k \rangle\!\rangle$,
- a computable decoding map $\mathrm{Seq} \times \mathbb{N} \to \mathbb{N}$, $(m, i) \mapsto (\!(m)\!)_i$, so that $(\!(m)\!)_i$ is the i-th element of the sequence coded by m, if $i < \ell(m)$.

The function Rem is definable in $(\mathbb{N}, +, \cdot)$, since

$$\mathrm{Rem}(n, m) = r \Leftrightarrow r < m \wedge \exists q (n = q \cdot m + r).$$

and therefore

$$\boldsymbol{\beta}(m, i) = \mathrm{Rem}((m)_0, 1 + (i + 1) \cdot (m)_1).$$

is also definable in $(\mathbb{N}, +, \cdot)$. Therefore we have shown the existence of a coding apparatus that is *definable* in $(\mathbb{N}, +, \cdot)$.

We now show that the existence of any definable coding apparatus, i.e. the existence of definable Seq, ℓ, $\langle n_0, \ldots, n_k \rangle \mapsto \langle\!\langle n_0, \ldots, n_k \rangle\!\rangle$ and $(m, i) \mapsto (\!(m)\!)_i$ as above, guarantees the existence of many sets and functions in $(\mathbb{N}, +, \cdot)$.

Example 11.27. The factorial is defined by the formula with free variables x and y asserting *"there is a finite sequence $\langle s_0, \dots, s_x \rangle$ of length $x+1$ such that $s_0 = 1$ and $s_x = y$ and $s_{i+1} = s_i \cdot (i+1)$"*, in symbols

$$\begin{aligned}\exists s[\varphi_{\mathrm{Seq}}(s) \wedge \ell(s) \circeq x+1 \wedge (\!(s)\!)_0 \circeq 1 \wedge (\!(s)\!)_x \circeq y \\ \wedge \forall i \leq x\,(i+1 \leq x \Rightarrow (\!(s)\!)_{i+1} \circeq (\!(s)\!)_i \cdot (i+1))],\end{aligned}$$

where φ_{Seq} is a formula defining Seq.

Example 11.28. The exponential function $(n, m) \mapsto n^m$ is defined by the formula with free variables x, y, z asserting *"there is a finite sequence $\langle s_0, \dots, s_y \rangle$ such that $s_0 = 1$ and $s_y = z$ and $s_{i+1} = s_i \cdot x$"*, in symbols

$$\begin{aligned}\exists s[\varphi_{\mathrm{Seq}}(s) \wedge \ell(s) \circeq y+1 \wedge (\!(s)\!)_0 \circeq 1 \wedge (\!(s)\!)_y \circeq z \\ \wedge \forall i \leq y\,(i+1 \leq y \Rightarrow (\!(s)\!)_{i+1} \circeq (\!(s)\!)_i \cdot x)].\end{aligned}$$

Remarks 11.29. (a) The two examples show that if $f \colon \mathbb{N} \to \mathbb{N}$ is defined recursively by $f(0) = k$ and $f(n+1) = g(n, f(n))$, then f is definable in $(\mathbb{N}, +, \cdot)$ whenever g is definable. In particular, if $g \colon \mathbb{N} \to \mathbb{N}$ is definable, then the sequence of the iterates $f(n) = g^{(n)}(0)$ is definable, hence

$$\{g^{(n)}(0) \mid n \in \mathbb{N}\} = \{x \in \mathbb{N} \mid \exists y(f(y) = x)\}$$

is definable in arithmetic.

(b) Since the exponential function is definable in $(\mathbb{N}, +, \cdot)$ (Example 11.28) some of the examples of formalization seen in Sections 2.B, 2.C and 3.B can be carried out in the language of arithmetic: for example Fermat's Last Theorem (Exercise 2.11(vii)) and the *abc*-conjecture (Example 3.4) are formalizable in the language containing the symbols $+$ and $\cdot$. Even the **Riemann Hypothesis**, the statement that the non-trivial zeros of the ζ-function lie on the line $\Re(s) = \frac{1}{2}$, turns out to be formalizable in this language (see page 479).

(c) The fact that recursive definitions can be turned into standard definitions is perhaps the most important consequence of the existence of a definable coding machinery. Not every structure is endowed with such coding device—quite the contrary, this is the exception rather than the rule. Thus the ability of defining recursively defined objects is a rare feature among structures. For example, the function $g \colon \mathbb{R} \to \mathbb{R}$, $g(x) = x + 1$, is definable in $(\mathbb{R}, +, \cdot)$, but $\mathbb{N} = \left\{g^{(n)}(0) \mid n \in \mathbb{N}\right\}$ is not definable in this structure (Corollary 11.42).

Our official coding of sequences is obtained by using Gödels' $\boldsymbol{\beta}$ function, but one might wonder if the same can be achieved using simpler methods. For example, we could try to code the sequence $\langle n_0, \dots, n_k \rangle$ by

$$m = \boldsymbol{J}(k+1, \boldsymbol{J}(n_0, \boldsymbol{J}(n_1, \dots \boldsymbol{J}(n_{k-1}, n_k) \cdots))),$$

so that $\ell(m)$ would be $(m)_0 = k+1$ and then recover the sequence from m by $((m)_1)_0 = n_0$, $(((m)_1)_1)_0 = n_1$, $\dots (\cdots((m)_1)_1 \cdots)_1 = n_k$. Then Seq would be the set $\{n \in \mathbb{N} \mid (n)_0 \neq 0\} \cup \{0\}$, where 0 is for coding $\langle\rangle$. The decoding function would be $(m,i) \mapsto (f(m,i))_0$ where f is *inductively defined* by $f(m,0) = (m)_1$ and $f(m,i+1) = (f(m,i))_1$, if $i+1 < \ell(m)$. The problem is that inductively defined functions are definable in $\langle \mathbb{N}, +, \cdot \rangle$ once we have the coding apparatus, which is exactly what we were trying to achieve. So this approach does not work.

Another way of tackling the problem is coding using primes and exponentials as in Section 8.A.2. Recall that $\mathbf{p}\colon \mathbb{N} \to \mathbb{N}$ enumerates the primes, and that the sequence $\langle n_0, \dots, n_k \rangle$ can be coded by the number

$$m = \mathbf{p}(0)^{n_0+1}\mathbf{p}(1)^{n_1+1} \cdots \mathbf{p}(k)^{n_k+1}.$$

Then Seq would be the set of all $n \neq 1$ such that if a prime p divides n, then every prime $p' < p$ divides n. The functions $\mathbf{e}\colon \mathbb{N}^2 \to \mathbb{N}$ and $\mathbf{l}\colon \mathbb{N} \to \mathbb{N}$ defined by

- $\mathbf{e}(0,i) = \mathbf{e}(1,i) = 0$ and if k is the largest integer such that $\mathbf{p}(i)^{k+1} \mid n$, then $\mathbf{e}(n,i) = k$;
- $\mathbf{l}(0) = \mathbf{l}(1) = 0$ and $\mathbf{l}(n) =$ the least i such that $[\mathbf{p}(i) \nmid n]$.

yield the decoding machinery, and the length, that is $\mathbf{e}(n,i) = (n)_i$ and $\mathbf{l}(n) = \ell(n)$. The problem with this coding is that it uses the exponential function in an essential way, and in order to show that exponentiation is definable in $(\mathbb{N}, +, \cdot)$ we need a definable coding apparatus. So this approach does not work either.

11.B.1. *The arithmetical hierarchy.* We introduce a hierarchy of formulæ giving a useful stratification of definable subsets of $(\mathbb{N}, +, \cdot)$. It is convenient to expand the language by allowing a unary function symbol S for the successor operation, a binary relation symbol $<$ for the order, and a constant symbol $\overline{0}$ for zero. The resulting language is used in Section 12.D to formalize Peano arithmetic, and for this reason is denoted by $\mathcal{L}_{\mathsf{PA}}$.

Definition 11.30. If φ is an $\mathcal{L}_{\mathsf{PA}}$-formula, then $\exists x < y\, \varphi$ and $\forall x < y\, \varphi$ are abbreviations for $\exists x\, (x < y \wedge \varphi)$ and $\forall x\, (x < y \Rightarrow \varphi)$. Similarly $\exists x \leq y\, \varphi$ and $\forall x \leq y\, \varphi$ are shorthand for $\exists x\, ((x < y \vee x \doteq y) \wedge \varphi)$ and $\forall x\, ((x < y \vee x \doteq y) \Rightarrow \varphi)$. These formulæ are obtained from φ by **bounded quantifications**.

A formula is

- Δ_0 if it is obtained from atomic formulæ using connectives and bounded quantifications;
- Σ_n with $n \geq 1$ if it is of the form $\exists x_n \forall x_{n-1} \dots \mathsf{Q} x_1 \varphi$ with φ a Δ_0 formula, and Q is $\exists$ or $\forall$ depending if n is odd or even;

- Π_n with $n \geq 1$ if it is of the form $\forall x_n \exists x_{n-1} \ldots \mathsf{Q} x_1 \varphi$ with φ a Δ_0 formula, and Q is $\exists$ or $\forall$ depending if n is even or odd.

A set $A \subseteq \mathbb{N}^k$ is Δ_0 or Σ_n or Π_n if it can be defined in $(\mathbb{N}, +, \cdot, S, <, 0)$ by means of a Δ_0 or Σ_n or Π_n formula.

Moreover A is Δ_n if it is Σ_n and Π_n.

Lemma 11.31. (a) *The Δ_0 subsets of $\mathbb{N}^k$ are closed under complements, intersections, unions, and bounded quantifications.*

(b) *A subset of $\mathbb{N}^k$ is Σ_n if and only if its complement is Π_n.*

(c) *Let A be a subset of $\mathbb{N}^{k+1}$. If A is Σ_1 then $\exists x_k\, A \overset{\text{def}}{=} \{\vec{a} \in \mathbb{N}^k \mid \exists b\, A(\vec{a}, b)\}$ is Σ_1; if A is Π_1 then $\forall x_k\, A \overset{\text{def}}{=} \{\vec{a} \in \mathbb{N}^k \mid \forall b\, A(\vec{a}, b)\}$ is Π_1.*

(d) *Σ_1 subsets of $\mathbb{N}^k$ are closed under intersections and unions. Similarly, Π_1 subsets of $\mathbb{N}^k$ are closed under intersections and unions.*

(e) *Σ_1 subsets of $\mathbb{N}^k$ are closed under bounded quantifications. Similarly, Π_1 subsets of $\mathbb{N}^k$ are closed under bounded quantifications.*

Proof. (a) and (b) are immediate.

(c) Suppose A is Σ_1, that is $A(\vec{x}) \Leftrightarrow \exists x_{k+1}\, \varphi$ with $\varphi(x_0, \ldots, x_{k+1})$ a Δ_0 formula. Then

$$\begin{aligned}(x_0, \ldots, x_{k-1}) \in \exists x_k\, A &\Leftrightarrow \exists x_k\, \exists x_{k+1}\, \varphi \\ &\Leftrightarrow \exists y\, \exists x_k < y\, \exists x_{k+1} < y\, \varphi\end{aligned}$$

and the result follows from the fact that $\exists x_k < y\, \exists x_{k+1} < y\, \varphi$ is Δ_0.

The case for $\forall x_k\, A \overset{\text{def}}{=} \{\vec{a} \in \mathbb{N}^k \mid \forall b\, A(\vec{a}, b)\}$ when A is Π follows from part (b).

(d) Suppose $A, B \subseteq \mathbb{N}^k$ are defined by $\exists x_k\, \varphi$ and $\exists x_k\, \psi$ with φ, ψ formulæ in Δ_0. Then $(x_0, \ldots, x_{k-1}) \in A \cup B \Leftrightarrow \exists x_k\, (\varphi \vee \psi)$ and

$$\begin{aligned}(x_0, \ldots, x_{k-1}) \in A \cap B &\Leftrightarrow \exists x_k\, \varphi \wedge \exists x_k\, \psi \\ &\Leftrightarrow \exists y\, \exists x_k < y\, \exists x'_k < y\, (\varphi(\vec{x}, x_k) \wedge \psi(\vec{x}, x'_k)).\end{aligned}$$

Therefore Σ_1 subsets of $\mathbb{N}^k$ are closed under unions and intersections, so the same holds for Π_1 using part (b).

(e) Suppose $A \subseteq \mathbb{N}^k$ is Σ_1 and let φ be Δ_0 so that $\exists x_k\, \varphi$ defines A. The set $\exists y < x_i\, A$ is defined by $\exists y\, \exists x_k\, (y < x_i \wedge \varphi)$, so it is Σ_1 by part (c) and the fact that $y < x_i \wedge \varphi$ is Δ_0. The set $\forall y < x_i\, A$ is defined by $\exists z\, \forall y < x_i\, \exists x_k < z\, \varphi$, so it is Σ_1. Therefore the collection of all Σ_1 subsets of $\mathbb{N}^k$ is closed under bounded quantifications. The result for Π_1 subsets follows from part (b). □

Recall from page 92 that a (possibly partial) k-ary function is definable in a structure if its graph is a definable subset of dimension $k + 1$.

Theorem 11.32. *The graph of a computable function is* Σ_1.

Proof. The set of all computable functions is $\bigcup_{n\in\mathbb{N}}\mathcal{F}_n$, where

$$\begin{aligned}\mathcal{F}_0 &= \{+,\cdot,\boldsymbol{\chi}_{\leq}\}\cup\{I^m_k \mid k,m\in\mathbb{N}\wedge k<m\}\\ \mathcal{F}_{n+1} &= \mathcal{F}_n\cup\{f\mid f \text{ is the composition of functions in } \mathcal{F}_n\}\cup\\ &\quad\cup\{\boldsymbol{\mu}y\,[f(\vec{x},y)=0]\mid f\in\mathcal{F}_n\}\,.\end{aligned}$$

Every function in $\mathcal{F}_0$ is Σ_1. The case for $+,\cdot,S,I^n_k$ is evident; the characteristic function $\boldsymbol{\chi}_{\leq}$ is defined by the formula $\varphi_{\leq}(x,y,z)$ given by

$$\left(z = \bar{0}\vee z=\mathtt{S}(\bar{0})\right)\wedge\left(z=\mathtt{S}(\bar{0})\Leftrightarrow(x<y\vee x=y)\right).$$

Next we show that if every function in $\mathcal{F}_n$ is Σ_1 definable, then so is every function in $\mathcal{F}_{n+1}$. Let $\varphi(y_1,\dots,y_k,z)$ and $\psi_i(x_1,\dots,x_n,y)$ $(1\leq i\leq n)$ be $\boldsymbol{\Sigma}_1$ formulæ defining the k-ary function g and the n-ary functions $f_1,\dots,f_k$. The formula

$$\exists y_1\dots\exists y_k\,\Big(\bigwedge_{1\leq i\leq k}\psi_i(x_1,\dots,x_n,y_i)\wedge\varphi(y_1,\dots,y_k,z)\Big)$$

is $\boldsymbol{\Sigma}_1$ and defines $g(f_1(\vec{x}),\dots,f_k(\vec{x}))$.

Suppose g is $k+1$-ary and definable via a $\boldsymbol{\Sigma}_1$ formula $\varphi_g(\vec{x},y,z)$. The formula

$$\varphi_g(\vec{x},y,\bar{0})\wedge\forall w<y\,\exists z\,\varphi_g(\vec{x},w,\mathtt{S}(z))$$

is $\boldsymbol{\Sigma}_1$, and it defines $\vec{x}\mapsto\boldsymbol{\mu}y\,[g(\vec{x},y)=0]$.

Therefore every computable function is Σ_1. □

Theorem 11.33. (a) *A semi-computable set is* Σ_1.

(b) *A computable set is* Δ_1.

(c) *If f is computable with a computable domain, then* $\mathrm{Gr}(f)$ *is* Δ_1.

Proof. (a) By Proposition 8.35 a semi-computable set is of the form $\operatorname{dom} f$ for some computable f. As $\operatorname{dom} f$ is the projection of $\operatorname{Gr} f$ which is Σ_1, then $\operatorname{dom} f$ is Σ_1.

Part (b) follows from part (a), and part (c) follows from Proposition 8.44(c). □

Theorem 11.34. *Every Σ_1 predicate is semi-computable, and every function whose graph is Σ_1 is computable.*

Proof. A term $t(x_1,\dots,x_k)$ of $\mathcal{L}_{\mathsf{PA}}$ is—essentially—a polynomial in the variables $x_1,\dots,x_k$ with coefficients in $\mathbb{N}$, so any atomic formula $t(\vec{x}) = s(\vec{x})$ or $t(\vec{x})<s(\vec{x})$ defines an elementary computable subset of $\mathbb{N}^k$, for some k. By induction on the complexity every $\boldsymbol{\Delta}_0$ formula defines an elementary computable set, so any $\boldsymbol{\Sigma}_1$ formula defines a semi-computable set.

If f is a partial k-ary function such that $\mathrm{Gr}(f)$ is Σ_1, then $\mathrm{Gr}(f)$ is semi-computable, and hence f is computable by Proposition 8.36. □

11.C. The integers and the rationals.

The numbers 0 and 1 are definable in $(\mathbb{Z}, \cdot)$. Pell's equation $x^2 = ky^2 + 1$ has (infinitely many) integer solutions when $k > 1$ is a natural number and not a square, so $\mathbb{N}$ is the truth set in $(\mathbb{Z}, S, \cdot)$ of the formula $\varphi(z)$

$$\exists x \left(x^2 = z\right) \vee \exists x \exists y \left(y \neq 0 \wedge y \neq 1 \wedge x^2 = z \cdot y^2 + 1\right),$$

thus $\varphi(z)$ defines $\mathbb{N}$ also in $(\mathbb{Z}, +, \cdot)$. We can also use a theorem of Lagrange's [**HW79**, p. 302], asserting that every natural number is the sum of four squares, hence $\mathbb{N}$ is the truth set in $(\mathbb{Z}, +, \cdot)$ of

$$\exists y_1, y_2, y_3, y_4 \left(x = y_1 \cdot y_1 + y_2 \cdot y_2 + y_3 \cdot y_3 + y_4 \cdot y_4\right).$$

Theorem 11.35. *Multiplication is definable in the structure* $(\mathbb{N}, S, |)$ *and in the structure* $(\mathbb{Z}, S, |)$*. Thus by Exercise 11.61 addition is definable in these structures.*

Proof. For $(\mathbb{N}, S, |)$ see Exercise 11.70; for $(\mathbb{Z}, S, |)$ see [**Ric85**]. □

Theorem 11.36. $\mathbb{Z}$ *is definable in* $(\mathbb{Q}, +, \cdot)$.

The proof of this important result uses non-trivial results in algebra, and we refer the interested reader to the original paper [**Rob49**]. By Lagrange's theorem, $\mathbb{N}$ is definable in $(\mathbb{Q}, +, \cdot)$.

Remark 11.37. The formula $\varphi(t)$ used in the proof of Theorem 11.36 is:

$$\forall y, z \left(\psi(y, z, 0) \wedge \forall w \left(\psi(y, z, w) \Rightarrow \psi(y, z, w + 1)\right) \Rightarrow \psi(y, z, t)\right)$$

where $\psi(t, y, z)$ is $\exists a, b, c \left(t \cdot y \cdot z^2 + 2 = a^2 + t \cdot y^2 - y \cdot c^2\right)$. In prenex normal it becomes a $\forall\exists\forall$-formula

$$\forall x_1, x_2 \exists y_1, \ldots, y_7 \forall z_1, \ldots, z_6 [f(t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots z_6) = 0],$$

with $f \in \mathbb{Z}[t, x_1, x_2, y_1, \ldots, y_7, z_1, \ldots, z_6]$. This result has been recently improved obtaining a definition of $\mathbb{Z}$ in $\mathbb{Q}$ via a $\forall$-formula of the form $\forall x_1, \ldots, x_n [f(t, x_1, \ldots, x_n) = 0]$ with $f \in \mathbb{Z}[t, x_1, \ldots, x_n]$.

Therefore $(\mathbb{N}, +, \cdot)$ is definably interpretable in the structures

$$(\mathbb{Z}, S, \cdot), \quad (\mathbb{Z}, +, \cdot), \quad (\mathbb{N}, S, |), \quad (\mathbb{Z}, S, |), \quad (\mathbb{Q}, +, \cdot),$$

and hence these structures have a very rich family of definable sets.

11.D. Real and complex numbers.

11.D.1. *The real field.* Consider the structure $(\mathbb{R}, +, \cdot)$. The elements 0 and 1 are definable by the formulæ $\forall y(y + x = y)$ and $\forall y(y \cdot x = y)$, while the ordering $x < y$ is definable by the formula

$$\exists z\, (z \neq 0 \wedge x + z \cdot z = y)\,.$$

The sets definable in $(\mathbb{R}, +, \cdot)$ are exactly those definable in $(\mathbb{R}, +, -, \cdot, 0, 1, <)$, but the latter structure is more convenient. So from now on we focus on definability in $(\mathbb{R}, +, \cdot, -, 0, 1, <)$.

Every $z \in \mathbb{Z}$ and hence every $q \in \mathbb{Q}$ is definable in $(\mathbb{R}, +, \cdot, -, 0, 1, <)$. Recall that a real number $r \in \mathbb{R}$ is algebraic if it is the root of some polynomial with integer coefficients. Every $f \in \mathbb{Z}[X]$ yields a term $t(x)$ with just one variable x, hence saying that r is a root of f amounts to saying that r is in the truth set of the formula $t(x) = 0$. Since the set S of all roots of f is finite, we can single-out r in S by pinning-down its position with respect to the order: if $S = \{r_1 < \cdots < r_k\}$ and, for example, $r = r_3$, then r is the only real satisfying the formula

$$\begin{aligned} t(x) = 0 \wedge \exists y_1 \exists y_2 \big(&t(y_1) = 0 \wedge t(y_2) = 0 \\ &\wedge y_1 < y_2 < x \wedge \forall z\, (t(z) = 0 \wedge z < x \Rightarrow z = y_1 \vee z = y_2)\big). \end{aligned}$$

Therefore every algebraic number is definable.

Definition 11.38. The family of **semi-algebraic** subsets of dimension n is the smallest family of subsets of $\mathbb{R}^n$ containing the sets of the form

$$f(x_1, \ldots, x_n) \leq g(x_1, \ldots, x_n)$$

with f, g polynomials with coefficients in $\mathbb{R}$, and closed under intersections, unions, and complements.

It is easy to check that the semi-algebraic sets are exactly those definable with parameters in $(\mathbb{R}, +, \cdot, 0, 1, <)$ using an open formula. In Chapter **??** we shall prove that the theory of real closed fields (Definition 9.11) admits the elimination of quantifiers, and that it is a complete, decidable theory.

Remarks 11.39. (a) $(\mathbb{N}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$ show that a substructure of a decidable structure need not be decidable.

(b) By Exercise 9.22, $\mathbb{Z}$ is definable in the ring $\mathbb{R}[X]$, yet it is not definable in $\mathbb{R}$.

The following results follow rom the elimination of quantifiers for real closed fields:

Theorem 11.40 (Tarski-Seidenberg)**.** *If $\pi\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ is the projection along the first coordinate and $A \subseteq \mathbb{R}^{n+1}$ is semi-algebraic, then $\pi[A]$ is semi-algebraic.*

Theorem 11.41. *The subsets of $\mathbb{R}$ that are definable with parameters in the real field are exactly the finite unions of singletons, intervals (open, closed, half-open), and half-lines.*

Corollary 11.42. *None of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ is definable in $(\mathbb{R}, +, \cdot)$.*

Corollary 11.42 remains true if we add the function $\exp(x) = \mathrm{e}^x$. Moreover the theory of $(\mathbb{R}, +, \cdot, 0, 1, <, \exp)$ is decidable, assuming the following conjecture in number theory.

Definition 11.43. Let $\Bbbk$ be a field and let $\mathbb{F}$ be its prime subfield, that is $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ depending on the characteristic of $\Bbbk$. For each $A \subseteq \Bbbk$ let $\overline{\mathbb{F}(A)}$ be the smallest algebraically closed field containing $\mathbb{F} \cup A$. A set $A \subseteq \Bbbk$ is **algebraically independent** if $a \notin \overline{\mathbb{F}(A \setminus \{a\})}$, for all $a \in A$. If there is an algebraically independent subset of $\Bbbk$ of size n, then $\Bbbk$ has **transcendence degree over** $\mathbb{F}$ at least n.

Schanuel's conjecture. *If $z_1, \dots, z_n \in \mathbb{C}$ are linearly independent on $\mathbb{Q}$, then the transcendence degree of $\mathbb{Q}(z_1, \dots, z_n, \mathrm{e}^{z_1}, \dots, \mathrm{e}^{z_n})$ over $\mathbb{Q}$ is at least n.*

11.D.2. *The complex field.* The theory of the complex field $(\mathbb{C}, +, \cdot, 0, 1)$ is axiomatized by the axioms for algebraically closed fields of characteristic zero ACF_0 (Example 4.39).

Theorem 11.44. *Let p be a prime or $p = 0$. The theory ACF_p admits elimination of quantifiers.*

Proof. We apply Proposition 11.16. Let M, N be algebraically closed fields of characteristic p, and suppose M' and N' are substructures of M and N, respectively, and that $F\colon M' \to N'$ is an isomorphism. Thus M' and N' are rings of characteristic p and the isomorphism F extends to the quotient field. Without loss of generality we may assume that M' and N' are fields. Let $\overline{M'}$ and $\overline{N'}$ be the algebraic closure of M' computed in M and the algebraic closure of N' computed in N. Since the algebraic closure is unique, up to isomorphism, the isomorphism F extends to an isomorphism $\overline{M'} \to \overline{N'}$.

Let $\varphi(y, x_1, \dots, x_n)$ be a conjunction of atomic formulæ and negation of atomic formulæ, and let $a_1, \dots, a_n \in \overline{M'}$: we want to show that if $M \vDash \exists y \varphi[a_1, \dots, a_n]$, then $N \vDash \exists y \varphi[F(a_1), \dots, F(a_n)]$, and conversely. An atomic formula is logically equivalent to a formula of the form $t = 0$, with t a term containing only variables among $y, x_1, \dots, x_n$. Since the conjunction of two negated atomic formulæ $(t \neq 0) \wedge (s \neq 0)$ is equivalent to $t \cdot s \neq 0$, we may assume that φ is of the form

$$s \neq 0 \wedge \bigwedge_{1 \leq i \leq k} t_i = 0.$$

Suppose $M \vDash \exists y \varphi[a_1, \ldots, a_n]$: this amounts to say that there is a $b \in M$ such that is not a root of the polynomial $s[a_1, \ldots, a_n]$, yet it is a root of each polynomial $t_i[a_1, \ldots, a_n]$. Note that $b \in \overline{M'}$, hence $F(b) \in \overline{N'}$ is a root of $t_i[F(a_1), \ldots, F(a_n)]$ but it is not a root of $s[F(a_1), \ldots, F(a_n)]$. It follows that $N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)]$. The other direction

$$N \vDash \exists y \varphi[F(a_1), \ldots, F(a_n)] \Rightarrow M \vDash \exists y \varphi[a_1, \ldots, a_n]$$

is similar. □

An atomic sentence σ of the language $\mathcal{L}_{\text{Rings}}$ is logically equivalent modulo ACF_p to a sentence of the form '$t = 0$' with t a closed term, and each such sentence is decidable in ACF_p, and thus either $\text{ACF}_p \vDash \sigma$ or else $\text{ACF}_p \vDash \neg\sigma$. Therefore we obtain another proof of Theorem 4.40 that ACF_0 and ACF_p are complete.

Remark 11.45. The proof of Theorem 11.44 relies on the fact that the algebraic closure of a field is unique up to isomorphism, and this in turn depends on the axiom of choice. But since the substructures M' and N' can be taken to be countable, and since the proof of the uniqueness of the algebraic closure does not depend on choice when the field is countable, the appeal to AC can be avoided completely—see Section 28.

Sets which are definable with parameters using atomic formulæ are algebraic varieties, that is sets of the form

$$Z(f) = \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid f(\vec{z}) = 0\}$$

with $f \in \mathbb{C}[x_1, \ldots, x_n]$. Therefore the definable subsets of the complex field are the sets that can be obtained by taking unions, intersections, and complements of algebraic varieties. In particular, the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are not definable in the structure $(\mathbb{C}, +, \cdot, 0, 1)$.

Every rational number is definable in the complex field, but this result does not extend to the algebraic numbers—as observed on page 93 the set $\{\mathrm{i}, -\mathrm{i}\}$ is definable, but none of its elements is.

Working in the structure $(\mathbb{C}, +, \cdot, 0, 1, \exp)$, the set

$$\ker(\exp) = \{z \in \mathbb{C} \mid \exp(z) = 1\} = 2\mathrm{i}\pi\mathbb{Z}$$

can be defined, hence $\mathbb{Z} = \{x \in \mathbb{C} \mid x \ker(\exp) \subseteq \ker(\exp)\}$ is definable.

Exercises

Exercise 11.46. Show that:

(i) The divisibility relation $\mid$ is not definable in the structure $(\mathbb{N}, \perp)$.

(ii) Every automorphism F of $(\mathbb{N}, \mid)$ is such that $F(n \cdot m) = F(n) \cdot F(m)$.

Exercise 11.47. Show that $\langle \mathbb{N} \uplus \mathbb{Q} \times \mathbb{Z}, +, <, 0 \rangle$ is a model of Presburger arithmetic. What are its definable elements? Is the set of all its definable elements, a definable set?

Exercise 11.48. Use Theorem 4.37 to show that the theories $T_{(\mathbb{N},S)}$ and $T_{(\mathbb{N},<)}$ are complete.

Exercise 11.49. Show that the theory $T_{(\mathbb{N},<,S,0)}$ admits effective elimination of quantifiers, and hence it is a complete theory.

Exercise 11.50. For $n \in \mathbb{N}$ let $\mathcal{L}_n$ be the first-order language containing only the constant symbols c_i with $0 \leq i < n$. (In particular $\mathcal{L}_0$ is the language without non-logical symbols.) Let T_n be the theory in the language $\mathcal{L}_n$ containing all sentences $\boldsymbol{\varepsilon}_{\geq k}$ for $k \geq 1$ (see page 18). Show that:

(i) T_n admits elimination of quantifiers for $n \geq 1$, and T_0 admits elimination of quantifiers for non-closed formulæ,

(ii) T_0 and T_1 are complete theories, while for $n \geq 2$ the theory T_n is not complete.

Exercise 11.51. Complete the proof of Proposition 11.23.

Exercise 11.52. Show that the functions $\mathbb{N} \to \mathbb{N}$ defined by $g(0) = G(0) = 0$, $g(1) = G(1) = 1$ and for $n \geq 2$

$$g(n) = \text{the smallest } k \text{ such that } \forall x\, \exists y_1, \ldots, y_k\, (x = y_1^n + \cdots + y_k^n)$$

$$G(n) = \text{the smallest } k \text{ such that } \exists z\, \forall x \geq z\, \exists y_1, \ldots, y_k\, (x = y_1^n + \cdots + y_k^n)$$

are definable in $(\mathbb{N}, +, \cdot)$. (The functions g and G have been mentioned on page 68 in relation to Waring's problem (3.3) on page 29.)

Exercise 11.53. (i) Let C be the unary predicate "being a square", that is $\exists y(y^2 = x)$. Show that the map $q(x) = x^2$ is definable in $(\mathbb{N}, +, C)$.

(ii) Show that multiplication is definable in $(\mathbb{N}, +, q)$.

(iii) Show that multiplication is definable in $(\mathbb{N}, +, f)$ where $f \in \mathbb{N}[X]$ is of degree ≥ 2.

(iv) Argue that the only polynomial functions definable in $(\mathbb{N}, +)$ are those of degree ≤ 1.

Exercise 11.54. Show that $\mathbb{N}$ and multiplication are definable in $(\mathbb{Z}, +, C)$, where C is as in Exercise 11.53.

Exercise 11.55. Show that the enumeration by squares of $\mathbb{N} \times \mathbb{N}$ in Figure 12 is definable in $(\mathbb{N}, +, \cdot)$ by giving an explicit formula for such bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and for its inverses.

Exercise 11.56. Show that the bijection $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, m, k) \mapsto \boldsymbol{J}(n, \boldsymbol{J}(m, k))$ is a polynomial of degree four. Find a bijection $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ that is a polynomial of degree three. More generally, for each integer $k > 0$ construct a bijection $\mathbb{N}^k \to \mathbb{N}$ that is a polynomial of degree k.

Exercise 11.57. Let $f(n)$ be the unique $z \leq n$ such that $\frac{z(z+1)}{2} \leq n < \frac{(z+1)(z+2)}{2}$. Show that $(n)_0 = n - \frac{f(n)(f(n)+1)}{2}$ and $(n)_1 = f(n) - (n)_0$.

Exercise 11.58. Suppose that $1 < c_0, \ldots, c_{n-1} \in \mathbb{N}$ are pairwise coprime and let $a_0, \ldots, a_{n-1} \in \mathbb{N}$ be arbitrary. Let $N = \prod_{i=0}^{n-1} c_i$. Show that

(i) $x = \sum_{i=0}^{n-1} a_i (\frac{N}{c_i})^{\phi(c_i)}$ is such that $x \equiv a_i \mod c_i$, for all $0 \leq i < n$, where ϕ is the Euler function, that is $\phi(k) =$ the number of $0 < x < k$ such that x is co-prime with k;

(ii) if $x \in \mathbb{N}$ is such that $x \equiv a_i \mod c_i$, for all $0 \leq i < n$, then the following conditions are equivalent:
- $y \equiv \mod N$
- $y \equiv a_i \mod c_i$, for all $0 \leq i < n$.

Exercise 11.59. Check in detail that the function $\boldsymbol{\beta}$ is definable in the structure of arithmetic.

Exercise 11.60. Show that:

(i) $\mathcal{D}$ is the family of subsets of $\mathbb{N}^2$ that are definable in $(\mathbb{N}, S)$,

(ii) the sets in $\mathcal{D}$ are of the form $P \triangle L$ or $\mathbb{N}^2 \setminus (P \triangle L)$ where P is a finite (possibly empty) set of points and L is a finite (possibly empty) set of lines,

(iii) $\{(n, m) \mid n < m\} \notin \mathcal{D}$.

Exercise 11.61. Check that the identity (11.7) holds in $\mathbb{N}$ and in $\mathbb{Z}$ and conclude that addition is quantifier-free definable both in $(\mathbb{N}, S, \cdot)$ and in $(\mathbb{Z}, S, \cdot)$.

Exercise 11.62. Show that $<$ is definable without parameters in $(\mathbb{Q}, +, \cdot)$.

Exercise 11.63. Show that if $p, q \in \mathbb{Q}$ then the fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ are elementarily equivalent if and only if they coincide.

Exercise 11.64. Show that the real field $(\mathbb{R}, +, \cdot)$ is rigid.

Exercise 11.65. Show that the ordering is definable in $(\mathbb{Z}, +, \cdot)$.

Exercise 11.66. Show that the operation of addition $+$ and the rational field $\mathbb{Q}$ are definable in the structure $(\mathbb{C}, \cdot, \exp)$.

Exercise 11.67. Show that $\mathbb{N}$ is definable in the structures $(\mathbb{R}, +, \cdot, \sin)$, $(\mathbb{R}, +, \cdot, \cos)$, $(\mathbb{C}, +, \cdot, \exp)$.

Exercise 11.68. Consider the structure $(\mathbb{R}, +, \cdot, 0, 1, <)$. Show that:

(i) every interval (open, closed, half-open) and every half-line whose endpoints are algebraic numbers, is definable;

(ii) the functions $x \mapsto |x|$, $x \mapsto x^q$ with $q \in \mathbb{Q}$ are definable. If f and g are (partial) real-valued functions of a real variable, then also f/g is definable;

(iii) Write the formula $\varphi(x_{11}, x_{12}, x_{21}, x_{22})$ asserting that the matrix
$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$
is invertible. By elimination of quantifiers for real closed fields, there is a quantifier-free formula logically equivalent to (and with the same free variables as) φ: determine such formula.

Exercise 11.69. Consider the language of rings with an extra 1-ary function symbol. Write down sentences σ of this language so that the structure $(\mathbb{R}, +, \cdot, f)$ satisfies σ if and only if

(i) f is continuous,

(ii) f is of class C^n,

(iii) $f(x) = \mathrm{e}^x$,

(iv) $f(x) = \sin(x)$,

(v) $f(x) = \cos(x)$.

Exercise 11.70. (i) Suppose that $a, b, x, y, p \in \mathbb{N} \setminus \{0\}$ are such that:
$$\begin{array}{llll} a, b > 1 & a \perp x & a \cdot b \perp x & p \mid (\mathrm{lcm}(a, x) + 1) \\ x \perp y & b \perp y & a \cdot b \perp y & p \mid (\mathrm{lcm}(b, y) + 1)\,. \end{array}$$
Show that $p \mid (\mathrm{lcm}(a \cdot b, \mathrm{lcm}(x, y)) - 1)$.

(ii) Let $a, b, c \in \mathbb{N} \setminus \{0, 1\}$ and suppose that $\varphi \Rightarrow \psi$, where φ is the formula
$$\big[x \neq 0 \wedge a \perp x \wedge y \neq 0 \wedge b \perp y \wedge c \perp x \wedge c \perp y \wedge x \perp y \\ \wedge\ p \text{ is prime} \wedge p \mid (\mathrm{lcm}(a, x) + 1) \wedge p \mid (\mathrm{lcm}(b, y) + 1)\big]$$
an ψ is $p \mid (\mathrm{lcm}(c, \mathrm{lcm}(x, y)) - 1)$. Then $a \cdot b \equiv c \pmod p$.

(iii) Let $a, b, c \in \mathbb{N} \setminus \{0, 1\}$ and let $p > a, b, c$ be prime. Show that there are x, y satisfying φ. Conclude that the truth set of the formula $\sigma(a, b, c)$: $\forall x, y, p\, (\varphi \Rightarrow \psi)$, is $\big\{(a, b, c) \in \mathbb{N}^3 \mid c = a \cdot b\big\}$.

(iv) Use Exercise 11.61 to conclude that addition and multiplication are definable in the structure $(\mathbb{N}, |, S)$.

Exercise 11.71. Let DLO be the theory of dense linear orders without endpoints in the language $\mathcal{L}_{\mathrm{ORDR}}$ containing only $\leq$ as a binary relation symbol, and let DLO* be the same theory in the language $\mathcal{L}^*$ obtained by adding a constant symbol c to $\mathcal{L}_{\mathrm{ORDR}}$. Show that DLO admits elimination of quantifiers for non-closed formulæ, and that DLO* admits elimination of quantifiers (for all formulæ).

Deduce that if $(M, \leq) \vDash$ DLO then $\emptyset \neq X \subseteq M$ is definable with parameters $\{p_1, \ldots, p_n\} \subseteq M$ if and only if X it is a finite union of intervals[6] (closed, open, half-open) with endpoints in $\{p_1, \ldots, p_n\}$.

Conclude that DLO is decidable.

Notes and remarks

The first part of Section 11.A follows closely the book [**End01**]. The axiomatization of $(\mathbb{N}, +)$ and the elimination of quantifiers for this theory were obtained in 1929 by Presburger, a student of Tarski at the time.

The subsets of $\mathbb{N}^k$ ($k > 1$) that are definable in Presburger arithmetic have been studied in [**Woo**]. The definability of the integers in the rationals (Theorem 11.36) and the definability of addition and multiplication in $(\mathbb{N}, S, |)$ (Exercise 11.70) are due to J. Robinson. That paper asked whether multiplication is definable in the structures $(\mathbb{N}, S, \perp)$, $(\mathbb{N}, +, \perp)$, and $(\mathbb{Z}, S, |)$. The case of $(\mathbb{N}, S, \perp)$ is still open: Woods proved in [**Woo81**] that the definability of multiplication in terms of successor and co-primality is equivalent to the Erdős-Woods conjecture of Section 2.C.5. The case of $(\mathbb{N}, +, \perp)$ and $(\mathbb{Z}, S, |)$ have positive solution: the former was solved by Robinson herself, and the latter is Theorem 11.35. For a survey on definability on natural numbers see [**Bès01**].

The definability of $\mathbb{Z}$ in $\mathbb{Q}$ in the form described in Remark 11.37 is proved in [**Koe16**]: the polynomial $f(t, x_1, \ldots, x_n)$ is of degree 28 and $n = 418$. It is known that $\mathbb{Z}$ is not definable in $\mathbb{Q}$ by a quantifier-free formula, hence this result is, in some sense, optimal. It leaves open the possibility that $\mathbb{Z}$ be definable in $\mathbb{Q}$ by a $\exists$-formula: the received opinion is that this should not be the case, since it would contradict an important conjecture in number theory, known as the Bombieri-Lang conjecture. The results in Section 9.D.2 are from [**Rob51**].

The elimination of quantifiers for real closed fields (proved by Tarski in 1951) and the ensuing Tarski-Seidenberg Theorem 11.40, are crucial results for model theory and its applications to real algebraic geometry. The Tarski-Seidenberg result has been applied by Hörmander to the study of pseudo-differential operators [**HÖ5**]. Theorem 11.41 is the beginning of an important area in model theory, the study of o-minimal structures, that is real closed fields in which the definable subsets of dimension 1 are finite unions of singletons, intervals, and half-lines [**vdD98**]. The extension of Corollary 11.42 to $(\mathbb{R}, +, \cdot, \exp)$ is due to Wilkie [**Wil96**] while the proof of the decidability of this structure, modulo Schanuel's conjecture, is due to Wilkie and Macintyre [**MW96**]. Schanuel's conjecture is named after the mathematician who formulated it around 1960. It is one of the most important conjectures in number theory, settling many open questions on transcendental numbers; for example setting $z_1 = 1$ and $z_2 = \mathrm{i}\pi$ it implies that π, e are algebraically independent, hence $\pi + \mathrm{e}$, $\pi \cdot \mathrm{e}$ are both transcendental (see Example 2.2).

[6] Half-lines and the singletons $\{p_i\}$ are taken to be intervals.

12. Arithmetic and induction

12.A. Dedekind structures. $\mathcal{L}_{\mathsf{D}}$ is the language seen in Section 11.A with a unary function symbol $\mathtt{S}$ and a constant symbol $\overline{0}$. A crucial feature of the structure $(\mathbb{N}, S, 0)$ is the **second-order induction principle**

$$(\mathsf{Ind}^2) \qquad \forall I\,[0 \in I \wedge \forall x\,(x \in I \Rightarrow S(x) \in I) \Rightarrow \forall x\,(x \in I)]\,.$$

The expression *second-order* and the ensuing exponent 2 are motivated by the quantification over arbitrary subsets (see Observation 3.25(b)). In particular Ind^2 is not a first-order formula. A structure $(M, S_M, 0_M)$ satisfying Ind^2

$$\forall I \subseteq M\ [0_M \in I \wedge \forall x\,(x \in I \Rightarrow S_M(x) \in I) \Rightarrow I = M]$$

is said to be **inductive**. An inductive structure satisfying the sentences

$$\forall x\,\left(\mathtt{S}(x) \neq \overline{0}\right) \tag{12.1}$$

$$\forall x, y\,(x \neq y \Rightarrow \mathtt{S}(x) \neq \mathtt{S}(y)) \tag{12.2}$$

is a **Dedekind structure**. Clearly $(\mathbb{N}, S, 0)$ is a Dedekind structure. If $(M, S_M, 0_M)$ is inductive, then $M \setminus \{0_M\} \subseteq \operatorname{ran}(S_M)$; if it is a Dedekind structure, then $S_M \circ \cdots \circ S_M$ has no fixed points (Exercise 12.19).

Examples 12.1. (i) $\mathcal{Z}_n = (\mathbb{Z}/n\mathbb{Z}, \sigma, [0])$, where $\sigma([k]) = [k+1]$ and $[k]$ is the class of k modulo n, is an inductive structure that satisfies (12.2) but not (12.1).

(ii) $\mathcal{Z}'_m = (\{0, \dots, m-1\}, \tau, 0)$, where $m > 0$, $\tau(k) = k+1$ if $0 \leq k < m-1$ and $\tau(m-1) = m-1$ is an inductive structure that does not satisfy (12.2); $\mathcal{Z}'_m$ satisfies (12.1) if $m > 1$.

(iii) $\mathcal{Z}_{m,n} = (Z, S, a)$ is the structure with domain $\{0, \dots, m-1\} \uplus \mathbb{Z}/n\mathbb{Z}$, where $a = 0$ and S is defined by

$$S(x) = \begin{cases} x+1 & \text{if } x < m-1, \\ [0] & \text{if } x = m-1, \\ \sigma(x) & \text{if } x \in \mathbb{Z}/n\mathbb{Z}, \end{cases}$$

where σ is as in part (i). The structure $\mathcal{Z}_{m,n}$ is described by the directed graph in Figure 17. Note that $\mathcal{Z}_n = \mathcal{Z}_{0,n}$ and that $\mathcal{Z}'_m = \mathcal{Z}_{m,0}$. The structure $\mathcal{Z}_{m,n}$ is inductive; it satisfies (12.1) when $m > 0$, it satisfies (12.2) when $m = 0$ and $n > 0$.

(iv) $(\mathbb{N}, T, 0)$, where $T(n) = 2n$ is a structure that it is not inductive and that satisfies (12.1) and (12.2).

Theorem 12.2. (a) *If N is a Dedekind structure and M is an $\mathcal{L}_{\mathsf{D}}$-structure, then there is a unique morphism $F \colon N \to M$.*

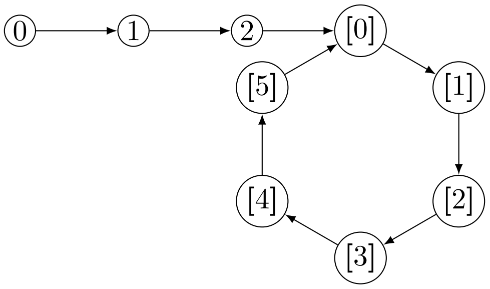


Figure 17. The structure $\mathcal{Z}_{3,6}$.

(b) *The homomorphic image of an inductive structure is an inductive structure. Conversely, every inductive structure is the homomorphic image of any Dedekind structure.*

(c) *If N and M are Dedekind structures, the unique morphism $F \colon N \to M$ as in* (a) *is an isomorphism. In particular, every Dedekind structure is isomorphic to* $(\mathbb{N}, S, 0)$.

(d) *The inductive structures are, up to isomorphism,* $(\mathbb{N}, S, 0)$ *and* $\mathcal{Z}_{m,n}$ *for* $m \geq 0$ *and* $n \geq 1$.

Proof. (a) Let us start with proving uniqueness. If $F, G \colon N \to M$ are distinct morphisms, let $I = \{x \in N \mid F(x) = G(x)\}$. Since $0_N \in I$ and by definition of morphism: if $x \in I$ then $S_N(x) \in I$, so by Ind^2 on the structure N we have that $I = N$, that is $F = G$.

To prove the existence of a morphism, argue as follows. Let $\mathcal{S}$ be the family of the subsets W of $N \times M$ such that $(0_N, 0_M) \in W$ and

$$(*) \qquad (x, y) \in W \Rightarrow (S_N(x), S_M(y)) \in W.$$

It is immediate to check that $N \times M \in \mathcal{S}$ and that $F \in \mathcal{S}$, where $F = \bigcap_{W \in \mathcal{S}} W$. Let

$$I = \{x \in N \mid \exists! y \in M\, [(x, y) \in F]\}\,.$$

Let us check by Ind^2 on N that $I = N$, so that $F \colon N \to M$ is a morphism. Clearly $(0_N, 0_M) \in F$. If $(0_N, y) \in F$ with $y \neq 0_M$, let $W = F \setminus \{(0_N, y)\}$. Since $(0_N, 0_M) \in W$, then (12.1) implies that W satisfies (*), hence $W \in \mathcal{S}$ and therefore $F \subseteq W$: a contradiction. Thus $0_N \in I$. Suppose now $x \in I$ and let $y \in M$ be the unique element such that $(x, y) \in F$, so that $(S_N(x), S_M(y)) \in F$. Towards a contradiction, suppose $(S_N(x), z) \in F$ for some $z \neq S_M(y)$ and let $W' = F \setminus \{(S_N(x), z)\}$, so that $W' \notin \mathcal{S}$. As $(0_N, 0_M) \in W'$, then (*) fails, that is there is $(x', y') \in N \times M$ such that $(x', y') \in F$ and $S_N(x') = S_N(x)$ and $S_M(y') = z$. By (12.2) $x = x'$, and since $x \in I$ it follows that $y = y'$, hence $z = S_M(y)$: a contradiction.

(b) Suppose $F\colon N \to M$ is a surjective morphism, N is an inductive structure and $I \subseteq M$ is such that $0_M \in I$ and $\forall x \in M\,(x \in I \Rightarrow S_M(x) \in I)$. Then Ind^2 applied to N proves that $F^{-1}[I] = N$, whence $I = M$.

Conversely suppose that M is inductive. Let N be a Dedekind structure and let $F\colon N \to M$ be the unique morphism given by (a). Let $I = \{y \in M \mid \exists x \in N\,(F(x) = y)\}$. Then $0_M = F(0_N) \in I$, and if $F(x) \in I$ then $S_M(F(x)) = F(S_N(x)) \in I$. Therefore $I = M$, that is F is surjective.

(c) If N and M are Dedekind structures, let $F\colon M \twoheadrightarrow N$ and $G\colon N \twoheadrightarrow M$ be surjective morphisms as of (b). Then $F \circ G\colon N \to N$ is a surjective morphism, and since $\mathrm{id}_N\colon N \to N$ is the unique morphism (a), it follows that $F \circ G = \mathrm{id}_N$, that is $F\colon M \twoheadrightarrow N$ is an isomorphism and G is its inverse.

(d) Suppose M is an inductive structure. By (b) fix a surjective morphism $F\colon \mathbb{N} \to M$. If F is injective, then F is an isomorphism, that is $(M, S_M, 0_M)$ is isomorphic to $(\mathbb{N}, S, 0)$. If F is not injective, let k be the least natural number such that $F(k) = F(m)$ for some $m < k$. Note that m is unique by minimality of k, that is $\{F(0), \dots, F(k-1)\}$ are all distinct. In particular $S_M(F(i)) = F(i+1)$ if $i + 1 < k$ and $S_M(F(k-1)) = F(m)$. Therefore M is isomorphic to $\mathcal{Z}_{m,n}$, where $n = k - 1 - m$. □

12.B. Inductive definitions. The proof of the existence of a morphism $F\colon N \to M$ in part (a) of Theorem 12.2 may seem overly indirect. Observe that the map F is recursively defined by

$$\begin{cases} F(0_N) = 0_M \\ F(S_N(x)) = S_M(F(x)). \end{cases}$$

The existence of F is apparently obvious. A seemingly convincing, but fallacious, argument is: the function F is defined in 0_N; if F is defined in $x \in N$, then it is defined in $S_N(x)$; therefore by induction F is defined on N. Under closer scrutiny, this argument does not hold water, despite its reassuring aspect: we argue about the domain of F, yet we have not yet shown that such F exist, which is what the purported argument is supposed to show! The preceding argument uses only the induction principle Ind^2 for the structure N, hence, if correct, it would show that: *If $(N, S_N, 0_N)$ is inductive and $(M, S_M, 0_M)$ is arbitrary, then there is a morphism $F\colon N \to M$.* But this is false—consider $N = \mathcal{Z}_n$ and $M = \mathcal{Z}'_n$ for $n \geq 2$.

Inductive definitions will be thoroughly studied in Section 19—right now we prove a result that is strong enough to account for most basic inductive constructions.

Theorem 12.3. *Let A and B be non-empty sets, and let $g\colon B \to A$ and $F\colon \mathbb{N} \times B \times A \to A$. There is a unique $f\colon \mathbb{N} \times B \to A$ such that*

$$\begin{cases} \quad f(0,b) = g(b) \\ f(n+1,b) = F(n,b,f(n,b)). \end{cases}$$

Proof. The proof is similar to that of Theorem 12.2. Consider the set

$$\begin{aligned} \mathcal{S} = \{W \subseteq (\mathbb{N} \times B) \times A \mid {} & ((0,b),g(b)) \in W \\ & \wedge \forall((n,b),a)\,[((n,b),a) \in W \Rightarrow ((n+1,b),F(n,b,a)) \in W]\} \end{aligned}$$

and let $f = \bigcap \mathcal{S} \subseteq (\mathbb{N} \times B) \times A$. As in the proof of Theorem 12.2, $f \in \mathcal{S}$ and $I = \mathbb{N}$ by Ind^2, where $I = \{n \in \mathbb{N} \mid \forall b \in B\, \exists! a \in A\, [((n,b),a) \in f]\}$. Therefore f is the required function. The proof of uniqueness is left to the reader. □

Whenever F does depend neither on $\mathbb{N}$ nor on B, Theorem 12.3 becomes:

Corollary 12.4. *Let A, B be non-empty sets, and let $g\colon B \to A$.*

(a) *For all $F\colon B \times A \to A$ there is a unique $f\colon \mathbb{N} \times B \to A$ such that*

$$\begin{cases} \quad f(0,b) = g(b) \\ f(n+1,b) = F(b,f(n,b)). \end{cases}$$

(b) *For all $F\colon \mathbb{N} \times A \to A$ there is a unique $f\colon \mathbb{N} \times B \to A$ such that*

$$\begin{cases} \quad f(0,b) = g(b) \\ f(n+1,b) = F(n,f(n,b)). \end{cases}$$

(c) *For all $F\colon A \to A$ there is a unique $f\colon \mathbb{N} \times B \to A$ such that*

$$\begin{cases} \quad f(0,b) = g(b) \\ f(n+1,b) = F(f(n,b)). \end{cases}$$

When g is constant, the statement of part (c) of Corollary 12.4 can be further simplified.

Corollary 12.5. *If $\bar{a} \in A$ and $F\colon A \to A$ then there is a unique $f\colon \mathbb{N} \to A$ such that*

$$\begin{cases} \quad f(0) = \bar{a} \\ f(n+1) = F(f(n)). \end{cases}$$

In other words, f is the sequence $\langle \bar{a}, F(\bar{a}), F(F(\bar{a})), \ldots \rangle$.

Example 12.6. The addition function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is obtained by letting $A = B = \mathbb{N}$, $b = 0$, $g = \mathrm{id}_{\mathbb{N}}$, and $F(k) = k+1$ in Corollary 12.4(c). Multiplication and exponentiation can be defined in a similar fashion.

Example 12.7. Given $h\colon X \to X$, letting A be the set of all functions from X to itself, letting $\bar{a} = \mathrm{id}_X$ and $F\colon A \to A$ be the map $k \mapsto h \circ k$, then Corollary 12.5 yields that there is a $f\colon \mathbb{N} \to A$ such that $\forall n \in \mathbb{N}\, \forall x \in X\, \bigl(f(n)(x) = h^{(n)}(x)\bigr)$. In other words, f is the sequence $\langle \mathrm{id}_X, h, h \circ h, h \circ h \circ h, \dots \rangle$.

Example 12.8. Let A be a non-empty set endowed with a binary operation $*$, and let $(a_n)_n$ be a sequence of elements of A. The sequence

$$s\colon \mathbb{N} \to A, \quad s(n) = (\cdots (a_0 * a_1) * \cdots * a_{n-1}) * a_n$$

is obtained from Corollary 12.4(b) by taking $B = \mathbb{N}$, $g(n) = a_n$ and $F\colon B \times A \to A$ such that $F(k, a) = a * g(k+1)$. Then there is a unique $f\colon \mathbb{N} \times B \to A$ such that

$$\begin{cases} f(0, k) = g(k) \\ f(n+1, k) = f(n, k) * g(n+1). \end{cases}$$

hence $s(n) = f(n, 0)$. This kind of constructions is very common in mathematics. For example, when $A = \mathbb{R}$, the sum of the series $\sum_{n=0}^{\infty} a_n$ is defined to be the limit (if it exists) of the sequence of the partial sums $s(k) = \sum_{n=0}^{k} a_n$.

Example 12.9. Recall that the transitive closure of $R \subseteq X \times X$ is the smallest transitive relation $\tilde{R}$ on X containing R (see page 43). It can be defined inductively by $x \mathrel{\tilde{R}} y$ if and only if $x \mathrel{R} x_1 \mathrel{R} x_2 \mathrel{R} \dots \mathrel{R} x_n = y$, that is $\tilde{R} = \bigcup_{n \in \mathbb{N}} g(n, R)$ where $g\colon \mathbb{N} \times \mathscr{P}(X \times X) \to \mathscr{P}(X \times X)$ is given by $g(0, S) = S$ and $g(n+1, S) = f(g(n, S))$, and $f(S) = S \cup \{(a, c) \mid \exists b \in X\, ((a, b), (b, c) \in S)\}$.

Recall from Section 7.A.1 that an inductive system is a triple $\mathcal{X} = (A, \mathcal{F}, X)$ where $\mathcal{F}$ is a set of operations on A and $X \subseteq A$.

An induction system $(A, \mathcal{F}, X)$ is **free** if for every $f, g \in \mathcal{F}$ we have that f is injective, $\operatorname{ran} f \cap \operatorname{ran} g = \emptyset$, and $\operatorname{ran} f \cap X = \emptyset$. Examples of free systems are $(\mathbb{N}, \{S\}, \{0\})$, and the ones in Example 7.16.

The next result is a generalization of Theorem 12.2(a), and it is proved using the same ideas as in that result.

Theorem 12.10. *Let $\mathcal{X} = (A, \mathcal{F}, X)$ be a free induction system. For any set Z, any $F\colon X \to Z$ and any collection $\{G_f \mid f \in \mathcal{F}\}$ of functions $G_f\colon Z^{n(f)} \times A^{n(f)} \to Z$ where $n(f)$ is the arity of f, there is a unique $\overline{F}\colon \overline{\mathcal{X}} \to Z$ which extends F and such that for all $f \in \mathcal{F}$ and all $x_1, \dots, x_n \in \overline{\mathcal{F}}$, with $n = n(f)$,*

$$\overline{F}(f(x_1, \dots, x_n)) = G_f(F(x_1), \dots, F(x_n), x_1, \dots, x_n).$$

12.C. The minimum principle. Ind^2 is equivalent to two other principles that are formulated in the language containing the symbol $<$: the **second-order strong induction principle**

$$(\mathsf{sInd}^2) \qquad \forall I \left[\forall x\, (\forall y\, (y < x \Rightarrow y \in I) \Rightarrow x \in I) \Rightarrow \forall x\, (x \in I)\right].$$

and the **second-order minimum principle**

$$(\mathsf{MP}^2) \qquad \forall I\,[I \neq \emptyset \Rightarrow \exists x\,(x \in I \wedge \forall y\,(y < x \Rightarrow y \notin I))]\,.$$

Proposition 12.11. *If* $(M, <, S, 0) \vDash T_{(\mathbb{N},<,S,0)}$*, then* Ind^2*,* sInd^2*, and* MP^2 *are equivalent for this structure.*

Proof. $\mathsf{Ind}^2 \Rightarrow \mathsf{sInd}^2$: Suppose $I \subseteq M$ is such that

$$\forall x \in M\,(\forall y \in M\,(y < x \Rightarrow y \in I) \Rightarrow x \in I)$$

and let $J = \{x \in M \mid \forall y < x\,(y \in I)\}$. Then $J \subseteq I$ by case assumption, and since $\forall y \in M\,(y < 0 \Rightarrow y \in I)$ holds trivially, then $0 \in J$. Suppose $x \in J$ and let $y < S(x)$: then $y < x$ or $y = x$, and in either case $y \in I$, hence $S(x) \in J$. Thus $J = M$ by Ind^2, hence $I = M$ as required.

$\mathsf{sInd}^2 \Rightarrow \mathsf{MP}^2$: Towards a contradiction suppose $\emptyset \neq I \subseteq M$ is such that

$$\forall x \in I\,\exists y \in I\,(y < x).$$

Apply strong induction to $J = M \setminus I$. Suppose $x \in M$ is such that $\forall y \in M\,(y < x \Rightarrow y \in J)$. If $x \in I$, then x would be the least element of I, hence $x \in J$. By strong induction $J = M$, so $I = \emptyset$, against our hypothesis.

$\mathsf{MP}^2 \Rightarrow \mathsf{Ind}^2$: Suppose M satisfies the minimum principle, and let $I \subseteq M$ be closed under S and such that $0 \in I$. If $I \neq M$ then let x be the minimum of $M \setminus I$. Since $x \neq 0$ then $x = S(y)$ for some y by an axiom in $T_{(\mathbb{N},<,S,0)}$, hence $y \in I$ by minimality. But then $x = S(y) \in I$: a contradiction. □

12.D. Peano arithmetic. In order to apply methods of first-order logic to arithmetic, the induction principle Ind^2 is weakened by requiring it only for truth sets of first-order formulæ. In other words we only require that

$$(\mathsf{Ind}_\varphi) \qquad \big(\varphi(\overline{0}) \wedge \forall x(\varphi(x) \Rightarrow \varphi(\mathsf{S}(x)))\big) \Rightarrow \forall x \varphi(x),$$

for all $\mathcal{L}_{\mathsf{D}}$-formulæ $\varphi(x)$ with one free variable. Given a language $\mathcal{L}$ extending $\mathcal{L}_{\mathsf{D}}$, we write $\mathsf{Ind}_{\mathcal{L}}$ (or simply Ind when $\mathcal{L}$ is clear) for the infinite list of all axioms Ind_φ with φ an $\mathcal{L}$-formula. This axiom-schema, known as **first-order induction principle** is not strong enough for proving part (c) of Theorem 12.2. In other words, a structure satisfying (12.1), (12.2) and $\mathsf{Ind}_{\mathsf{D}}$ need not be isomorphic to $(\mathbb{N}, S, 0)$. For example the $\mathcal{L}_{\mathsf{D}}$-structure with universe $M = \mathbb{N} \uplus \mathbb{Z}$ and such that $0_M = (0,0)$ and $S_M(k,i) = (k+1, i)$, satisfies (12.1), (12.2) and $\mathsf{Ind}_{\mathsf{D}}$, but it is not isomorphic to $(\mathbb{N}, S, 0)$, hence it does not satisfy (Ind^2). In analogy with what was done in Section 12.C, one can formulate the principles sInd_φ and MP_φ when φ is an $\mathcal{L}$-formula and $\mathcal{L}$ is a language containing the symbols $\mathsf{S}, \overline{0}, <$. For example MP_φ says that

$$\exists x \varphi(x) \Rightarrow \exists x(\varphi(x) \wedge \forall z(z < x \Rightarrow \neg\varphi(z))).$$

Note that the equivalence between Ind, sInd, and MP for the language $\mathcal{L}_{\mathsf{D}}$ is a logical consequence of $T_{(\mathbb{N},<,S,0)}$.

Definition 12.12. The language $\mathcal{L}_{\mathsf{PA}}$ is obtained by adding two binary function symbols $+$ and $\cdot$ and a binary relation symbol $<$ to the language $\mathcal{L}_{\mathsf{D}}$.

Peano arithmetic (PA) is the theory in the language $\mathcal{L}_{\mathsf{PA}}$ whose axioms are the statements:

$\mathsf{PA1}$: $\forall x \left(\mathtt{S}(x) \neq \overline{0}\right)$,
$\mathsf{PA2}$: $\forall x, y \ (x \neq y \Rightarrow \mathtt{S}(x) \neq \mathtt{S}(y))$,
$\mathsf{PA3}$: $\forall x \left(x + \overline{0} = x\right)$,
$\mathsf{PA4}$: $\forall x, y \ (x + \mathtt{S}(y) = \mathtt{S}(x + y))$,
$\mathsf{PA5}$: $\forall x \left(x \cdot \overline{0} = \overline{0}\right)$,
$\mathsf{PA6}$: $\forall x, y \ (x \cdot \mathtt{S}(y) = (x \cdot y) + x)$,
$\mathsf{PA7}$: $\forall x \neg \left(x < \overline{0}\right)$,
$\mathsf{PA8}$: $\forall x, y \ (x < \mathtt{S}(y) \Leftrightarrow x \leq y)$,

where $x \leq y$ is shorthand for $x < y \vee x = y$, and the first-order induction principle Ind.

The structure $(\mathbb{N}, S, 0, +, \cdot, <)$ is a model of PA, but it is far from being the only example—see Section 12.D.2. The equivalence between Ind, sInd, and MP holds also for PA. Although Ind is weaker than Ind^2, it is strong enough to prove many results on natural numbers.

12.D.1. *Some consequences of Peano's axioms.* Let PA^- be the theory with axioms $\mathsf{PA}n$ for $1 \leq n \leq 6$ plus induction for formulæ in the language $\mathcal{L}_{\mathsf{PA}}$ with $<$ removed.

Lemma 12.13. *The following statements are logical consequences of* PA^-*:*

(a) $\forall x (x = \overline{0} \vee \exists y (\mathtt{S}(y) = x))$,
(b) $\forall x (\mathtt{S}^{(n)}(x) \neq x)$ *for* $n > 0$.

Therefore PA^- *extends the theory* $T_{(\mathbb{N},S,0)}$ *from Section 11.A.1.*

Proof. Fix $(M, S, 0_M, +, \cdot)$ a model of PA^- and let us prove the result by induction.

(a) We must check that $M \vDash \varphi[0_M]$ and that for every $a \in M$, if $M \vDash \varphi[a]$ then $M \vDash \varphi[S(a)]$, where $\varphi(x)$ is $x = \overline{0} \vee \exists y (\mathtt{S}(y) = x)$. As $M \vDash \overline{0} = \overline{0}$ the base case is trivial. For the inductive step note that $S(a) \in \mathbf{T}^M_{\exists y (\mathtt{S}(y) = x)}$ and hence $M \vDash \varphi[S(a)]$.

(b) Fix $n > 0$ and apply Ind_φ where φ is $\mathtt{S}^{(n)}(x) \neq x$. Axiom $\mathsf{PA1}$ guarantees that $M \vDash \varphi[0_M]$, and if $M \vDash \varphi[a]$ that is $S^{(n)}(a) \neq a$, then $S^{(n)}(S(a)) = S(S^{(n)}(a)) \neq S(a)$, that is $M \vDash \varphi[S(a)]$. □

Proposition 12.14. *The following identities are logical consequences of* PA^-*:*

(a) $x + (y + z) = (x + y) + z$,

(b) $\overline{0} + x = x$,

(c) $\overline{1} + x = \mathsf{S}(x)$,

(d) $x + y = y + x$,

(e) $\overline{0} \cdot x = \overline{0}$,

(f) $x \cdot \mathsf{S}(\overline{0}) = \mathsf{S}(\overline{0}) \cdot x = x$,

(g) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$,

(h) $x \cdot y = y \cdot x$,

(i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Proof. Work in some model $(M, 0, S, +, \cdot)$ of PA^-.

(a) Apply $\mathsf{Ind}_{\varphi(z)}$ with $\varphi(z)$ is $\forall x, y(x + (y + z) = (x + y) + z)$. The base case, that is $M \vDash \varphi[0_M]$, holds by $\mathsf{PA3}$ as for all $a, b \in M$

$$a + (b + 0_M) = a + b = (a + b) + 0_M.$$

Assume now $M \vDash \varphi[c]$ for some c and let us argue that $M \vDash \varphi[S(c)]$. For all $a, b \in M$:

$$\begin{aligned} a + (b + S(c)) &= a + S(b + c) && \text{by } \mathsf{PA4} \\ &= S(a + (b + c)) && \text{by } \mathsf{PA4} \\ &= S((a + b) + c) && \text{by inductive assumption} \\ &= (a + b) + S(c) && \text{by } \mathsf{PA4} \end{aligned}$$

so $\varphi[S(c)]$ holds in M.

(b) Let $\varphi(x)$ be the formula $\overline{0} + x = x$ and apply Ind_φ: the base step follows from $\mathsf{PA3}$, the inductive step from $\mathsf{PA4}$.

(c) Apply $\mathsf{Ind}_{\varphi(x)}$ where $\varphi(x)$ is $\overline{1} + \mathsf{S}(x)$. By $\mathsf{PA3}$ we have the identity $\overline{1} + \overline{0} = \overline{1} = \mathsf{S}(\overline{0})$, so the base case of the induction holds. If $M \vDash \varphi[a]$ for some $a \in M$, then letting $1_M \overset{\text{def}}{=} S(0_M)$ and using part (b)

$$1_M + S(a) = S(1_M + a) = S(S(a))$$

that is: $M \vDash \varphi[S(a)]$.

(d) Apply Ind_φ where $\varphi(x)$ is the formula $\forall y\, (x + y = y + x)$. The base case $M \vDash \varphi[0_M]$ follows by $\mathsf{PA3}$ and by part (b). Assume $M \vDash \varphi[a]$ (the inductive assumption) towards proving $M \vDash \varphi[S(a)]$, that is $S(a) + b =$

$b + S(a)$ for all $b \in M$. Fix $b \in M$:

$$\begin{aligned} S(a) + b &= (1_M + a) + b && \text{by part (c)} \\ &= 1_M + (a + b) && \text{by part (a)} \\ &= 1_M + (b + a) && \text{by inductive assumption} \\ &= S(b + a) && \text{by part (c)} \\ &= b + S(a) && \text{by } \mathsf{PA4}. \end{aligned}$$

The verification of the remaining formulæ (e)–(i) is left to the reader. □

In particular, if $M \vDash \mathsf{PA}^-$, then $(M, +, 0)$ is a monoid. The order relation $x < y$ can be defined by the formula $\exists z(x + \mathtt{S}(z) = y)$, and with this definition $\mathsf{PA}^- \models \mathsf{PA7} \land \mathsf{PA8}$ (Exercise 12.29). Therefore PA^- is equivalent to PA, but the latter theory is more convenient.

Theorem 12.15. *The following facts follow from the axioms of* PA*:*

(a) $x < y \Leftrightarrow \exists z\,(x + \mathtt{S}(z) = y)$,

(b) $\forall x \forall y \forall z\,(x < y \land y < z \Rightarrow x < z)$ *(transitivity),*

(c) $\forall x \forall y\,(x < y \Leftrightarrow \mathtt{S}(x) < \mathtt{S}(y))$,

(d) $\forall x \neg\,(x < x)$ *(irreflexivity),*

(e) $\forall x\,\big(\bar{0} \neq x \Rightarrow \bar{0} < x\big)$,

(f) $\forall x \forall y\,(x < y \lor x = y \lor y < x)$ *(trichotomy),*

(g) $\forall x, y, z\,(x < y \Rightarrow x + z < y + z)$ *(monotonicity of addition),*

(h) $\forall x, y, z\,\big(z \neq \bar{0} \land x < y \Rightarrow x \cdot z < y \cdot z\big)$ *(monotonicity of multiplication).*

Proof. Work in some model $(M, S, 0, +, \cdot, <)$ of PA.

(a) Apply $\mathsf{Ind}_{\varphi(y)}$ where $\varphi(y)$ is $\forall x(x < y \Leftrightarrow \exists z\,(x + \mathtt{S}(z) = y))$. To prove $M \vDash \varphi[0]$ fix an $a \in M$: since $a < 0$ is impossible by PA7, it is enough to check that for all $b \in M$, $a + S(b) = S(a + b) \neq 0$, which follows from PA1. Suppose $M \vDash \varphi[a]$ for some $a \in M$. Then

$$\begin{aligned} a < S(b) &\Leftrightarrow a < b \lor a = b && \text{by } \mathsf{PA8} \\ &\Leftrightarrow \exists z\,(a + S(z) = b) \lor a + S(0) = S(b) && \text{(by inductive assumption)} \\ &\Leftrightarrow \exists z\,(a + S(z) = S(b)) \end{aligned}$$

that is $M \vDash \varphi[S(a)]$ holds.

(b) follows from associativity of addition: if $b = a + S(u)$ and $c = b + S(v)$, then $c = b + S(v) = (a + S(u)) + S(v) = a + (S(u) + S(v)) = a + S(S(u) + v)$, that is $a < c$.

(c) follows from commutativity of addition and $a + S(c) = b \Leftrightarrow S(a) + S(c) = S(a + S(c)) = S(b)$.

(d) PA yields $0 \not< 0$; if $a \not< a$ for some $a \in M$ then $S(a) \not< S(a)$ by part (c). Thus the result holds by induction.

(e) Apply Ind_φ where $\varphi(x)$ is $\overline{0} \doteq x \vee \overline{0} < x$. The base case $M \vDash \varphi[0]$ is immediate. Suppose that $M \vDash \varphi[a]$ for some $a \in M$, that is $0 = a \vee 0 < a$. As $a < S(a)$ by $\mathsf{PA}8$, then $0 < S(a)$, and therefore $M \vDash \varphi[S(a)]$.

(f) By transitivity and irreflexivity of $<$ it is enough to prove that $\mathsf{PA} \models \forall x, y(x < y \vee x \doteq y \vee y < x)$. We apply Ind_φ where $\varphi(x)$ is $\forall y(x < y \vee x \doteq y \vee y < x)$. The base case follows from part (e). Suppose $M \vDash \varphi[a]$ for some a. We must show that for all $b \in M$ one of the following holds: $S(a) < b$, $S(a) = b$, $b < S(a)$. By inductive assumption $a < b \vee a = b \vee b < a$: since $a < S(a)$ by $\mathsf{PA}8$, $a = b \vee b < a$ yields $b < S(a)$. If $a < b$ then $a + S(c) = b$ for some $c \in M$, so $S(a) + c = b$. If $c = 0$ then $S(a) = b$, and if $c \neq 0$ then $c = S(d)$ by Lemma 12.13 so $S(a) < b$.

(g) We apply Ind_φ, where $\varphi(z)$ is $\forall x, y(x < y \Rightarrow x + z < y + z)$. The base case follows from $\mathsf{PA}3$. Suppose $M \vDash \varphi[a]$ and let $b < c$ be elements of M. By inductive assumption and part (c), $b + S(a) = S(b + a) < S(c + a) = c + S(a)$. As b, c are arbitrary, $M \vDash \varphi[S(a)]$.

(h) We apply Ind_φ, where $\varphi(z)$ is $\forall x, y(z \neq \overline{0} \wedge x < y \Rightarrow x \cdot z < y \cdot z)$. The base case holds vacuously, so we may assume that $M \vDash \varphi[a]$ towards proving $M \vDash \varphi[S(a)]$. Let $b < c$ be elements of M. As $\mathsf{PA} \models \forall w(w \cdot \overline{1} \doteq w)$, we may assume that $a \neq 0$. Then by $\mathsf{PA}6$, the inductive assumption, and part (g) $b \cdot S(a) = b \cdot a + b < c \cdot a + b < c \cdot a + c = c \cdot S(a)$. As b, c are arbitrary, $M \vDash \varphi[S(a)]$. □

Therefore any model of PA is a commutative ordered semi-ring (Definition 9.10).

Proposition 12.16. *The following result (the algorithm of division with remainder) is logical consequence of* PA*:*

$$\forall x \, \forall y > \overline{0} \, \exists! q \, \exists! r \left[x \doteq y \cdot q + r \wedge q \leq x \wedge r < y \right].$$

In particular, for all $n \in \mathbb{N} \setminus \{0\}$, the sentence

$$\forall x \exists! r \left(\chi_n(x, r) \wedge r < \overline{n} \right)$$

is a logical consequence of PA*, where $\chi_n(x, y)$ is the formula on page 272*

$$\exists z \left(x + \underbrace{z + \cdots + z}_{n} \doteq y \ \vee \ y + \underbrace{z + \cdots + z}_{n} \doteq x \right).$$

Proof. Work in some model $(M, S, 0, +, \cdot)$ of PA. Fix $a, b \in M$ with $b > 0$. By monotonicity of multiplication $a = S(0) \cdot a \leq b \cdot a < b \cdot S(a)$, so by the minimum principle there is a least c such that $a < b \cdot c$. Since c cannot be 0, then $c = S(q)$ for some q. By trichotomy either $b \cdot q = a$ or else

$b \cdot q < a$. If the former holds then set $r = 0$. If the latter holds then $b \cdot q = b \cdot q + 0 < a < b \cdot S(q) = b \cdot q + b$ so by the minimum principle there is a least s such that $b \cdot d + e > a$. Note that $s \leq b$, and since $s = 0$ is impossible, then $s = S(r)$ for some r, hence $b \cdot q + r \leq a$. By trichotomy again either $b \cdot q + r < a$ or else $b \cdot q + r = a$: the former implies that $a \geq S(b \cdot q + r) = b \cdot q + S(r) = b \cdot q + s > a$, a contradiction. We have proved that $a = b \cdot q + r$; we must show that q and r are unique. Suppose that $a = b \cdot q_1 + r_1 = y \cdot q_2 + r_2$ with $r_1, r_2 < b$. If $q_1 < q_2$ then $b \cdot q_1 < y \cdot q_2 + r_2 = a$, and since $S(q_1) \leq q_2$ then $a = b \cdot q_1 + r_1 < b \cdot q_1 + b = b \cdot S(q_1) \leq b \cdot q_2 + r_2 = a$, a contradiction. A similar contradiction follows from $q_2 < q_1$. Therefore $q_1 = q_2 = q$. If $r_1 \neq r_2$, say $r_1 < r_2$, then $a = b \cdot q + r_1 < b \cdot q + r_2 = a$, a contradiction. Therefore $r_1 = r_2$ and hence

$$M \vDash \forall x \, \forall y > \overline{0} \, \exists! q \, \exists! r \left[x \mathrel{=\!\!=} y \cdot q + r \wedge q \leq x \wedge r < y \right]$$

If in the equation above we set $y \mathrel{=\!\!=} \overline{n}$, then since

$$x \cdot \overline{n} \mathrel{=\!\!=} \underbrace{x + \cdots + x}_{n \text{ times}}$$

we have that $M \vDash \forall x \exists! r \left(\chi_n(x, r) \wedge r < \overline{n} \right)$. □

12.D.2. *Non-standard models.* If $\mathcal{M} = (M, S_M, 0_M, +_M, \cdot_M, <_M)$ is a model of PA then $F \colon \mathbb{N} \to M$, defined recursively by $F(0) = 0_M$ and $F(n+1) = S_M(F(n))$, is an embedding of the structure $(\mathbb{N}, S, 0, +, \cdot, <)$ into $\mathcal{M}$. The **standard part of** $\mathcal{M}$ is $\operatorname{ran} F = \mathbb{N}_M = \{S_M(n) \mid n \in \mathbb{N}\}$, and it is an initial segment of $(M, <)$. If $\mathbb{N}_M = M$ then F is an isomorphism, and $\mathcal{M}$ is said to be standard; otherwise it is a **non-standard model**.

By Proposition 12.16 every model of PA is a model of Presburger's arithmetic, so if $\mathcal{M} = (M, S_M, 0_M, +_M, \cdot_M, <_M)$ is a non-standard model of PA, then M is of the form $\mathbb{N} \uplus Q \times \mathbb{Z}$ where Q is a dense linear order without endpoints, and the set $\mathbb{N}_M$ has no least upper bound by Lemma 12.13.

Theorem 12.17. *Every $\mathcal{L}_{\mathsf{PA}}$-theory T such that $(\mathbb{N}, S, 0, +, \cdot, <) \vDash T$ has a non-standard model. In particular, there is a non-standard model of* PA.

Proof. Let $\mathcal{L}$ be the language $\mathcal{L}_{\mathsf{PA}}$ augmented with a new constant symbol c, and let Δ be the theory T together with $\Sigma = \{\mathsf{S}^{(n)}(\overline{0}) < c \mid n \in \mathbb{N}\}$. If $\mathcal{M} \vDash \Delta$, then $\mathcal{M}$ must be non-standard, since $c_{\mathcal{M}}$ is larger than any element of $\mathbb{N}_{\mathcal{M}}$. Therefore it is enough to show that Δ is finitely satisfiable and then appeal to compactness (Theorem 4.46). Fix Δ_0 an arbitrary finite subtheory of Δ, and let Σ_0 be the part of Σ contained in Δ_0. Every sentence in Σ_0 is of the form $\mathsf{S}^{(k)}(\overline{0}) < c$ for some k, and being Σ_0 finite we can choose $n \in \mathbb{N}$ larger all these ks. Then letting $c_{\mathcal{M}} = n$ we have that $\mathcal{M} = (\mathbb{N}, S, 0, +, \cdot, <, c_{\mathcal{M}})$ is a model of T and Σ_0. This completes the proof. □

Remark 12.18. The induction principle says that in order to prove $\forall x\, \varphi(x)$ it is enough to show $\varphi(\overline{0})$ and $\forall x\, (\varphi(x) \Rightarrow \varphi(\mathsf{S}(x)))$. A common narrative in mathematics textbooks describes induction as a method to ascertain $\varphi(n)$ via some sort of domino effect, starting from $\varphi(0)$ and eventually reaching $\varphi(n)$. But this description is misleading for two reasons. The first reason is that it demotes induction from a significant new axiom to a mean for avoiding lengthy verifications, the second is that there are consequences of induction that cannot be proved by successive verifications starting from zero. For example, $\mathsf{S}(x) \doteq \mathsf{S}(\overline{0}) + x$ follows from the axioms of PA, so if $(M, S, 0, +, \cdot, <)$ is a non-standard model of PA and $a \in M$ is non-standard, then $S(a) = S(0) + a$, but no finite number of verifications yields this.

12.D.3. *Which functions can be captured by* PA*?* In order to proficiently develop combinatorics and number theory inside PA, it is necessary to express in $\mathcal{L}_{\mathsf{PA}}$ the sets and functions that are commonly used in these subjects. A function $f\colon \mathbb{N}^k \to \mathbb{N}$ is **representable in** PA if there is a formula $\varphi(x_1, \dots, x_k, y)$ such that for all $n_1, \dots, n_k \in \mathbb{N}$

$$\forall y \left(\varphi(\overline{n_1}, \dots, \overline{n_k}) \Leftrightarrow y \doteq \overline{f(n_1, \dots, n_k)}\right)$$

is a logical consequence of PA. (Observe that instead of $\varphi(\overline{n_1}, \dots, \overline{n_k})$ we should have written $\varphi\llbracket\overline{n_1}/x_1, \dots, \overline{n_k}/x_k\rrbracket$ to mean the sentence obtained from φ by replacing the variables $x_1, \dots, x_k$ with the numerals $\overline{n_1}, \dots, \overline{n_k}$.) The notion of representability is a strengthening of the notion of definability: if $f\colon \mathbb{N}^k \to \mathbb{N}$ is representable in PA, then its graph $\{(n_1, \dots, n_k, m) \in \mathbb{N}^{k+1} \mid f(n_1, \dots, n_k) = m\}$ is definable in $(\mathbb{N}, +, \cdot)$. In Section 24.D it is shown that *every computable function is representable in* PA, a result that greatly extend the definability results of Section 11.B. In particular there is a formula $\mathsf{Exp}(x, y, z)$ such that the following are logical consequences of PA:

- $\forall x, y \exists! z\, \mathsf{Exp}(x, y, z)$, i.e. Exp defines a function of two variables which we write as x^y;
- $\forall x \mathsf{Exp}(x, \overline{0}, \mathsf{S}(\overline{0}))$;
- $\forall x, y, z\, (\mathsf{Exp}(x, \mathsf{S}(y), z) \Rightarrow \exists w \mathsf{Exp}(x, y, w) \land w \cdot x \doteq z)$.

Therefore if $\mathcal{L}_{\mathsf{PA}^+}$ is the language obtained by adding a symbol for the exponential to $\mathcal{L}_{\mathsf{PA}}$, and if PA^+ has axioms PA1–PA8 together with the sentences $\forall x (x^{\overline{0}} \doteq \overline{1})$ and $\forall x, y (x^{\mathsf{S}(y)} \doteq x^y \cdot x)$ and the induction principle for formulæ of $\mathcal{L}_{\mathsf{PA}^+}$, then every statement σ of $\mathcal{L}_{\mathsf{PA}}$ which is provable in PA^+ is already provable in PA, and for every statement τ of $\mathcal{L}_{\mathsf{PA}^+}$ there is a statement σ of $\mathcal{L}_{\mathsf{PA}}$ such that $\mathsf{PA}^+ \models \sigma \Leftrightarrow \tau$ and $\mathsf{PA}^+ \models \tau$ iff $\mathsf{PA} \models \sigma$.

Exercises

Exercise 12.19. Show that:

(i) an inductive structure satisfies the sentence $\forall x\,(x \neq 0 \Rightarrow \exists y(\mathtt{S}(y) = x))$;

(ii) a Dedekind structure satisfies the sentences $\forall x(\mathtt{S}^{(n)}(x) \neq x)$. Thus a Dedekind structure is a model of $T_{(\mathbb{N},S,0)}$ from Section 11.A.

Exercise 12.20. Show that $T \models \mathsf{Ind}_T$, where T is one of the theories

$$T_{(\mathbb{N},S,0)},\quad T_{(\mathbb{N},<,S,0)},\quad T_{(\mathbb{N},+,<,S,0)}$$

of Section 11.A and Ind_T is the axiom-schema Ind_φ where φ is a formula of the language of T.

Exercise 12.21. Complete the details of the proof on the existence of the morphism $F\colon N \to M$ in part (a) of Theorem 12.2.

Exercise 12.22. Suppose $(N, S_N, 0_N)$ is an $\mathcal{L}_{\mathsf{D}}$-structure such that for all $\mathcal{L}_{\mathsf{D}}$-structures $(M, S_M, 0_M)$ there is a morphism $F\colon N \to M$. Show that N is a Dedekind structure, hence isomorphic to $\mathbb{N}$.

Exercise 12.23. Complete the proof of Proposition 12.14 by checking parts (e)–(i).

Exercise 12.24. Let $(N, S_N, 0_N)$ be an inductive structure. Show that:

(i) For each $x \in N$ there is a unique morphism $t_x\colon (N, S_N, 0_N) \to (N, S_N, x)$, called the **translation of order** x.

(ii) The function $a\colon N \times N \to N$ defined by $a(x, y) = t_x(y)$ is the unique function such that $a(x, 0_N) = x$ and $a(x, S_N(y)) = S_N(a(x, y))$. The operation a is called **addition on** N and is usually denoted by $+_N$.

(iii) For each $x \in N$ there is a unique map $d_x\colon N \to N$, called the **dilation of order** x such that $d_x(0_N) = 0_N$ and $d_x(S_N(y)) = d_x(y) +_N x$.

(iv) The function $m\colon N \times N \to N$ defined by $m(x, y) = d_x(y)$ is the unique function such that $m(x, 0_N) = 0_N$ and $m(x, S_N(y)) = m(x, y) +_N x$. The m is called **multiplication on** N and is usually denoted by $\cdot_N$.

(v) If $F\colon N \to M$ is a morphism of inductive structures, then F is also a morphism with respect to addition and multiplication, that is $F(x +_N y) = F(x) +_M F(y)$ and $F(x \cdot_N y) = F(x) \cdot_N F(y)$.

(vi) Addition and multiplication on $\mathcal{Z}_{m,n}$ are associative and commutative.

Exercise 12.25. Let N be an inductive structure. Show that:

(i) if $N = \mathbb{N}$ then there is a unique function $E\colon N \times N \to N$ such that $E(x, 0_N) = S_N(0_N)$ and $E(x, S_N(y)) = E(x, y) \cdot_N x$.

(ii) if $N = \mathcal{Z}_{n,m}$ there is no function E as above.

Exercise 12.26. If $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ define $\sum f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ and $\prod f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ by

$$\begin{cases} \sum f(x_1, \dots x_k, 0) = 0 \\ \sum f(x_1, \dots x_k, n+1) = f(x_1, \dots x_k, n+1) + \sum f(x_1, \dots x_k, n) \end{cases}$$

and

$$\begin{cases} \prod f(x_1, \dots x_k, 0) = 1 \\ \prod f(x_1, \dots x_k, n+1) = f(x_1, \dots x_k, n+1) \cdot \prod f(x_1, \dots x_k, n). \end{cases}$$

Show that the existence of $\sum f$ and $\prod f$ follows from Theorem 12.3.

Exercise 12.27. The ordering in a non-standard model $\mathcal{M}$ of PA is $M = \mathbb{N} \uplus L \times \mathbb{Z}$ where L is a dense linear order without endpoints. Show L is not complete; in particular is not isomorphic to $\mathbb{R}$.

Exercise 12.28. Prove in PA^+ the following:

- $\forall x, y, z(x^{y+z} \eqcirc x^y \cdot x^z)$,
- $\forall x, y, z(x^{y \cdot z} \eqcirc (x^y)^z)$,
- $\forall x, y, z((x \cdot y)^z \eqcirc x^z \cdot y^z)$,
- $\forall x, y(x > \overline{0} \wedge y > \overline{1} \Rightarrow \exists z, w(x \eqcirc y^z + w \wedge z < x \wedge w < x^z))$,
- $\forall x, y(\overline{2}^{\mathsf{S}(x)} \mid y \Rightarrow \overline{2}^x \mid y)$,
- $\forall x \exists ! y, z\left(\overline{0} < x \Rightarrow x \eqcirc \overline{2}^y(\overline{2} \cdot z + \overline{1})\right)$.

Exercise 12.29. Let $\psi(x, y)$ be $\exists z(\mathsf{S}(z) \eqcirc y)$. Show that $\forall x, y[\psi(x, \mathsf{S}(y)) \Leftrightarrow \psi(x, y) \vee x \eqcirc y]$ and $\forall x \neg \psi(x, \overline{0})$ are logical consequence of PA^-, and that any model of PA^- can be expanded is a unique way as a model of PA.

Exercise 12.30. Let $a, b\colon \mathbb{N} \to \mathbb{N}$ be defined by $a(0) = b(0) = 0$ and

$$\forall x > 0 \left(x = 2^{a(x)} \cdot b(x) \ \wedge \ \neg(2 \mid b(x))\right),$$

where $\mid$ is the divisibility relation. Show that:

(i) the functions a and b are definable in $(\mathbb{N}, +, \cdot)$;

(ii) if M is a non-standard model of $\mathrm{Th}(\mathbb{N}, +, \cdot, S, 0, <)$ then $F\colon M \to M$

$$F(x) = \begin{cases} 2 \cdot_M x & \text{if } a(x) \text{ is non-standard,} \\ x & \text{otherwise} \end{cases}$$

is an automorphism of $(M, |_M)$, but $F(x^2) \neq F(x)^2$ if $a(x)$ is non-standard.[7]

[7] Compare this to Exercise 11.46(ii).

(iii) Conclude that multiplication is not definable in $(\mathbb{N}, |)$.

[Hint: for (i) use Example 11.28.]

Notes and remarks

This section is based on the paper [**Hen60**] by Henkin, where the proof of part (a) of Theorem 12.2 is credited to Lorenzen and, independently, to Hilbert and Bernays. (See also [**Jac85**, p. 16] and [**Fef64**].) The first axiomatization of arithmetic based on the successor operation is due to Dedekind, while that based on the operations of sum and product is due to Peano.

Chapter IV

Sets, choice, and compactness

13. Ordinals and cardinals

13.A. Well-orders and ordinals. If $(P, \leq_P)$ and $(Q, \leq_Q)$ are disjoint ordered sets, define the ordering $\preceq$ on $P \cup Q$, called the sum-ordering of P and Q, by placing the elements of P before those of Q, that is $x \preceq y$ if and only if

$$(x \in P \wedge y \in Q) \vee (x, y \in P \wedge x \leq_P y) \vee (x, y \in Q \wedge x \leq_Q y).$$

If $(P', \leq_{P'}) \cong (P, \leq_P)$, $(Q', \leq_{Q'}) \cong (Q, \leq_Q)$ and $P' \cap Q' = \emptyset$, then the sum-ordering on $P' \cup Q'$ is isomorphic to the sum-ordering on $P \cup Q$. Therefore we can define the **sum** of two (not necessarily disjoint) orders

$$(P, \leq_P) + (Q, \leq_Q),$$

as the sum-ordering on the disjoint union of P and Q. In other words: the sum of orders is defined up to isomorphism. It is easy to check that he sum of orders is associative, that is

$$(P + Q) + R \cong P + (Q + R). \tag{13.1}$$

We can define several orderings on $P \times Q$. If we take the product of the structures $(P, \leq_P), (Q, \leq_Q)$ we obtain the **product ordering** defined by

$$(p_1, q_1) \trianglelefteq (p_2, q_2) \Leftrightarrow (p_1 \leq_P p_2 \wedge q_1 \leq_Q q_2).$$

The **lexicographic order** $\leq_{\text{lex}}$ on $P \times Q$ is defined by

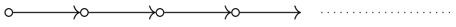
$$(p_1, q_1) \leq_{\text{lex}} (p_2, q_2) \Leftrightarrow p_1 <_P p_2 \vee (p_1 = p_2 \wedge q_1 \leq_Q q_2),$$

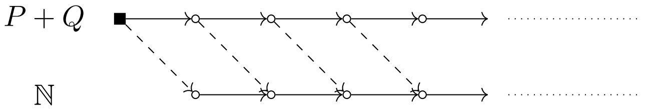
while the **antilexicographic order** $\leq_{\text{a-lex}}$ is

$$(p_1, q_1) \leq_{\text{a-lex}} (p_2, q_2) \Leftrightarrow q_1 <_Q q_2 \vee (q_1 = q_2 \wedge p_1 \leq_P p_2).$$

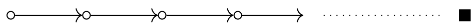
If P and Q are linear orders, then $\leq_{\text{lex}}$ and $\leq_{\text{a-lex}}$ are linear, while the product order is never linear, unless one of P and Q is a singleton or empty. For technical reasons that will be clear shortly, $P \times Q$ is endowed with the antilexicographic order. It is easy to check that multiplication of orders is associative, that is

$$(P \times Q) \times R \cong P \times (Q \times R). \tag{13.2}$$

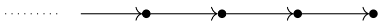
If P and Q are finite linear orders of size n and m, then $P + Q$ and $Q + P$ are linear orders of size $n + m$, and by Proposition 7.5 they are isomorphic. The assumption that P and Q are finite is crucial: if P is the ordering with exactly one element ■ and $Q = \mathbb{N}$ is 
then $P + Q$ is isomorphic to Q



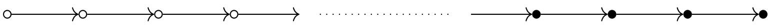
On the other hand, $Q + P$ has a maximum element,



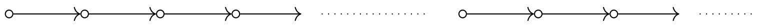
and hence it is not isomorphic to $\mathbb{N} \cong P + Q$. Note that this ordering is isomorphic to the set of reals $\{\frac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{1\}$. The linear order $\mathbb{Z}_- = \{k \in \mathbb{Z} \mid k < 0\}$ can be drawn as



thus $\mathbb{Z}_- + \mathbb{N} \cong \mathbb{Z}$. Instead $\mathbb{N} + \mathbb{Z}_-$ is the linear order with maximum and minimum isomorphic to the set of reals $\{-1 + \frac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{1 - \frac{n}{n+1} \mid n \in \mathbb{N}\}$ and its diagram is

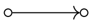


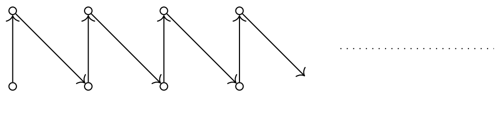
The order $\mathbb{N} + \mathbb{N}$ can be drawn as



and it is not isomorphic to either $\mathbb{Z}_- + \mathbb{N}$ or $\mathbb{N} + \mathbb{Z}_-$, but it is isomorphic to the set of reals

$$\{\tfrac{n}{n+1} \mid n \in \mathbb{N}\} \cup \{\tfrac{2n+1}{n+1} \mid n \in \mathbb{N}\}$$

and to the set $\mathbb{N} \times 2$ where 2 is the linear order with two elements .
On the other hand, $2 \times \mathbb{N}$ is isomorphic to $\mathbb{N}$



Thus $P \times Q \not\cong Q \times P$. Clearly, if P and Q are finite linear orders of size n and m respectively, then $P \times Q$ and $Q \times P$ are linear orders with nm elements, and by Proposition 7.5 they are isomorphic.

A linear order $(P, \leq)$ is a **well-order** if every $\emptyset \neq X \subseteq P$ has a minimum. Every finite linear order is a well-order, $\mathbb{N}$ is a well-order, and every subset of a well-order is a well-order with the induced relation. Conversely $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are not well-orders.

Remark 13.1. Because of the quantification over arbitrary subsets, the definition of well-order is not first-order. In Section 32 we will show that there is no sentence σ in a first-order language $\mathcal{L}$ with a binary relation symbol $\leq$ such that the models of σ are exactly the well-ordered sets.

Proposition 13.2. *If $(P, \leq)$ is a well-ordered set and $Q \subseteq P$ is an initial segment, then either $Q = P$ or else $Q = \operatorname{pred}(a, A; <)$ for some $a \in P$.*

Proof. If $Q \neq P$, then $Q = \operatorname{pred}(a, A; <)$ where $a = \min(P \setminus Q)$. □

Well-orders are much more rigid than linear orders.

Proposition 13.3. *If $(P, \leq)$ is a well-ordered set and $f \colon P \to P$ is increasing, then $\forall x \in P\, (x \leq f(x))$.*

Proof. Towards a contradiction, suppose that $\{x \in P \mid f(x) < x\} \neq \emptyset$ and let a be its minimum. Since f is increasing $f(f(a)) < f(a)$, yet $f(a) < a$ and the minimality of a imply that $f(f(a)) \geq f(a)$: a contradiction. □

Proposition 13.4. *If $(P, \leq)$ is a well-ordered set and $f \colon P \to P$ is an increasing bijection, then $\forall x \in P\, (f(x) = x)$.*

Proof. The functions f and f^{-1} are both increasing, and therefore $x \leq f(x)$ and $x \leq f^{-1}(x)$ by Proposition 13.3, thus $x = f(x)$. □

Corollary 13.5. *If $(P, \leq)$ and $(Q, \trianglelefteq)$ are isomorphic well-orders, the isomorphism $f \colon P \to Q$ is unique.*

Corollary 13.6. *If $(P, \leq)$ is a well-order and $Q \subset P$ is an initial segment, then P and Q are not isomorphic.*

Proof. By Proposition 13.2 $Q = \{x \in P \mid x < a\}$ for some $a \in P$. If $f \colon P \to Q$ is an isomorphism, then $f \colon P \to P$ is increasing and $f(a) < a$, contradicting Proposition 13.3. □

If P and Q are well-orders, let

$$Q \sqsubseteq P \Leftrightarrow Q \cong P \vee \exists a \in P\, (Q \cong \operatorname{pred} a)$$

that is, to say: $Q \sqsubseteq P$ if and only if Q is isomorphic to an initial segment of P. By Corollary 13.6 the two conditions of the disjunction are mutually exclusive, hence

$$P \sqsubseteq Q \wedge Q \sqsubseteq P \Rightarrow P \cong Q. \tag{13.3}$$

If $Q \sqsubseteq P$ but $Q \ncong P$, then we write $Q \sqsubset P$.

Theorem 13.7. *If $(P, <_P)$ and $(Q, <_Q)$ are well-ordered sets, then exactly one of the following holds:*

$$P \sqsubset Q, \qquad Q \sqsubset P, \qquad P \cong Q.$$

Proof. By Corollary 13.6 the three conditions are mutually exclusive, so it is enough to show that at least one must hold. Let

$$f = \{(p, q) \in P \times Q \mid (\operatorname{pred} p, <_P) \cong (\operatorname{pred} q, <_Q)\}.$$

If $(p, q_1), (p, q_2) \in f$, then $(\operatorname{pred} q_1, <_Q) \cong (\operatorname{pred} p, <_P) \cong (\operatorname{pred} q_2, <_Q)$ and hence $q_1 = q_2$. Similarly, if $(p_1, q), (p_2, q) \in f$, then $p_1 = p_2$. Thus f is an injective function. If $p \in \operatorname{dom}(f)$ and g is the isomorphism witnessing $(\operatorname{pred} p, <_P) \cong (\operatorname{pred} f(p), <_Q)$, and if $p' < p$, then $p' \in \operatorname{dom}(g)$ and hence $(\operatorname{pred} p', <_P) \cong (\operatorname{pred} g(p'), <_Q)$ (Exercise 7.68). In other words: $\operatorname{dom}(f)$ is an initial segment of P in the ordering $<_P$. Similarly, $\operatorname{ran}(f)$ is an initial segment of Q in the ordering $<_Q$. If $p_1, p_2 \in \operatorname{dom} f$ with $p_2 < p_1$ and g is the isomorphism between $(\operatorname{pred} p_1, <_P)$ and $(\operatorname{pred} f(p_1), <_Q)$, then $g \restriction \operatorname{pred} p_2$ is an isomorphism between $(\operatorname{pred} p_2, <_P)$ and $(\operatorname{pred} g(p_2), <_Q)$ by Exercise 7.68, hence $f(p_2) = g(p_2) <_Q f(p_1)$. From this it follows that f is an isomorphism between an initial segment of $(P, <_P)$ and an initial segment of $(Q, <_Q)$. The theorem will be proved if we show that

$$\operatorname{dom}(f) = P \vee \operatorname{ran}(f) = Q.$$

Towards a contradiction, suppose this is not true and let $\bar{p} = \min(P \setminus \operatorname{dom} f)$ and $\bar{q} = \min(Q \setminus \operatorname{ran} f)$. From what we said $f \colon (\operatorname{pred} \bar{p}, <_P) \to (\operatorname{pred} \bar{q}, <_Q)$, hence $(\bar{p}, \bar{q}) \in f$, by definition of f, a contradiction. □

Note that this "comparability" theorem among well-orders does not generalize to linear orders. For example, if $\preceq$ is the converse of $\leq$, the usual ordering on the natural numbers, then the two linear orders $(\mathbb{N}, \leq)$ and $(\mathbb{N}, \preceq)$ are not isomorphic, and neither is isomorphic to an initial segment of the other—in fact neither of them embeds into the other.

An **ordinal** is a well-ordered set, up to isomorphism; for example the natural numbers 1, 2, 3, ... can be identified with

$$\circ \qquad\qquad \circ \longrightarrow \circ \qquad\qquad \circ \longrightarrow \circ \longrightarrow \circ \qquad\qquad \cdots\cdots$$

while 0 is identified with the empty diagram. The ordinal associated with the well-ordered set P is the **order type** of P. The order type of $\mathbb{N}$ (or of any infinite subset of the natural numbers) is denoted by ω. The ordinals are denoted by lower case Greek letters α, β, γ, ... Certain non-zero ordinals (for example ω) do not have a maximum, and are called **limit ordinals**; the non-zero ordinals that are not limit are called **successor ordinals**.

The operations of addition and multiplication of ordinals are defined by means of the operations $+$ and $\times$ on the ordered sets, that is A and B are well-orders of order type α and β, then define

$$\begin{aligned} \alpha + \beta &= \text{the order type of } A + B \\ \alpha \cdot \beta &= \text{the order type of } A \times B \\ \alpha \leq \beta &\Leftrightarrow A \sqsubseteq B. \end{aligned}$$

Theorem 13.7 and (13.3) imply that $\leq$ is a linear order on the ordinals.

Proposition 13.8. *The relation $\leq$ on the ordinals is a well-order.*

Proof. Given a non-empty set of ordinals X, let $(P, \leq_P)$ be a well-order whose order type α is in X and let Q be the intersection of all initial segments of P whose order type is in X; clearly Q is an initial segment of P and if its order type β belongs to X, then β is the minimum of X. Thus it is enough to check that $\beta \in X$. When $Q = P$ then $\alpha = \beta$ and the result follows at once, thus we may assume that $Q \neq P$ and thus, by Proposition 13.2, $Q = \{x \in P \mid x <_P a\}$ for some $a \in P$. Since $a \notin Q$ and by definition of Q, there must be $Q' = \{x \in P \mid x <_P a'\}$ an initial segment of P whose order type β' is in X and such that $a \notin Q'$. But this means that $a \not<_P a'$, that is $a' \leq_P a$. By minimality of Q, it follows that $a' = a$, that is $Q' = Q$, whence $\beta = \beta'$ and therefore $\beta \in X$ as required. □

By (13.1) and (13.2) it follows that the operations of addition and multiplication of ordinals are associative. In Section 19.D other properties of the ordering, and of addition and multiplication of ordinals will be proved—for example the *right* distributive property of multiplication with respect to addition holds, that is

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

while the analogous version on the left does not hold. Addition and multiplication are increasing functions in the second variable,

$$\beta < \beta' \Rightarrow \alpha + \beta < \alpha + \beta' \qquad 0 < \alpha \wedge \beta < \beta' \Rightarrow \alpha \cdot \beta < \alpha \cdot \beta'$$

and are monotone in the first variable,

$$\alpha < \alpha' \Rightarrow \alpha + \beta \leq \alpha' + \beta \qquad \alpha < \alpha' \Rightarrow \alpha \cdot \beta \leq \alpha' \cdot \beta.$$

As with ordinary addition and multiplication of natural numbers, if α, β are order types of well-orders with at least two elements, then

$$\alpha + \beta \leq \alpha \cdot \beta.$$

Moreover, the division-with-remainder formula holds:

$$\alpha < \beta \Rightarrow \exists! \gamma < \beta \, \exists! \delta < \alpha \, (\alpha \cdot \gamma + \delta = \beta).$$

Addition and multiplication on the ordinals can be defined recursively by:

$$\alpha + \beta = \begin{cases} \alpha \\ (\alpha + \gamma) + 1 \\ \sup_{\gamma < \beta}(\alpha + \gamma) \end{cases} \qquad \alpha \cdot \beta = \begin{cases} 0 & \text{if } \beta = 0, \\ (\alpha \cdot \gamma) + \alpha & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta}(\alpha \cdot \gamma) & \text{if } \beta \text{ is limit.} \end{cases}$$

This suggests the following definition of exponentiation of ordinals:

$$\alpha^\beta = \begin{cases} 1 & \text{if } \beta = 0, \\ (\alpha^\gamma) \cdot \alpha & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta} \alpha^\gamma & \text{if } \beta \text{ is limit.} \end{cases}$$

(Table 2 in Section 19 collects the main properties of these operations.) By Exercise 13.73 it is possible to construct countable, closed subsets of $\mathbb{R}$ whose order type is

$$\omega, \quad \omega^\omega, \quad \omega^{\omega^\omega}, \quad \ldots .$$

The following example exhibits a specific closed subset of $\mathbb{R}$ of order type ω^ω—this example requires advanced notions in geometry and will not be used later, so the reader can safely skip it.

Example 13.9. An **n-dimensional hyperbolic manifold** is an n-dimensional connected manifold endowed with a complete a Riemannian metric such that every point has a neighborhood isometric to an open set of $\mathbb{H}^n$, where

$$\mathbb{H}^n = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_n \geq 0\}$$

is the hyperbolic plane with the complete Riemannian metric $\mathrm{d}s = \frac{\mathrm{d}\mathbf{x}}{x_n}$ of sectional curvature -1. To each such M it is possible to assign a positive real number $\mathrm{vol}(M)$ called volume, and

$$\{\mathrm{vol}(M) \mid M \text{ is a 3-dimensional hyperbolic manifold}\}$$

is a closed, well-orderable subset of $\mathbb{R}$ of order type ω^ω.

13.B. Induction, recursion, and well-orders*.

13.B.1. *Induction and well-orders.* Recall from Section 12.C that the second order induction principle Ind^2 is equivalent to the minimum principle

$$(\mathsf{MP}^2) \qquad \forall I \, [I \neq \emptyset \Rightarrow \exists x \, (x \in I \wedge \forall y \, (y < x \Rightarrow y \notin I))] \, .$$

The minimum principle holds for any well-ordering, not just $<$ on $\mathbb{N}$, and the proofs in Section 12.D can be recast as using the minimum principle on some appropriate well-order. For example the proof of Proposition 12.14(d) of commutativity of addition can be seen as a proof using the minimum principle on the well-order $<_{\mathrm{lex}}$ on $\mathbb{N}^2$ which has length $\omega \cdot \omega$. Suppose, towards a contradiction, that

$$I = \left\{ (n, m) \in \mathbb{N}^2 \mid n + m \neq m + n \right\}$$

is non-empty, so that by the minimum principle it has a $<_{\mathrm{lex}}$-least element (n^*, m^*). By part (c) of Proposition 12.14 $n^* \neq 0$ and $m^* \neq 0$, so $n^* = \bar{n} + 1$ and $m^* = \bar{m} + 1$ for some $\bar{n}, \bar{m}$. By minimality of (n^*, m^*) one has that $n^* + m^* \neq m^* + n^*$, $\forall k (\bar{n} + k = k + \bar{n})$ and $n^* + \bar{m} = \bar{m} + n^*$, and from these a contradiction is easily reached.

13.B.2. *Recursion and well-orders.* If f is recursively defined by

$$\begin{cases} f(0) = a \\ f(n+1) = F(n, f(n)) \end{cases}$$

then the computation of a specific value $f(\bar{n})$ depends on $\bar{n}$ many values computed before: $f(0), f(1), \ldots, f(\bar{n} - 1)$. In other words

$$f(n) = \tilde{F}(f \restriction \operatorname{pred} n) \tag{13.4}$$

where $\tilde{F}$ is a suitable functions whose domain is the collection of partial functions from $\mathbb{N}$ to $\mathbb{N}$. If the ordering $<$ on $\mathbb{N}$ is replaced by some well-order $\lhd$ on a set X, equation (13.4) is a template for the inductive definitions on an arbitrary set. For example, in order to compute a specific value of Ackermann's function $\operatorname{Ack}(m, n)$ in Section 8.D, it is enough to determine the values of $\operatorname{Ack}(m', n')$ when $(m', n') <_{\mathrm{lex}} (m, n)$ hence Ack can be defined as

$$\operatorname{Ack}(m, n) = \tilde{F} \left(\operatorname{Ack} \restriction \operatorname{pred}((m, n), <_{\mathrm{lex}}) \right)$$

where $\tilde{F}$ is defined as follows: if f is a map defined on $\operatorname{pred}((m, n), <_{\mathrm{lex}})$,

$$\tilde{F}(f) = \begin{cases} n + 1 & \text{if } m = 0, \\ f(m - 1, 1) & \text{if } m > 0 \text{ e } n = 0, \\ f(m - 1, f(m, n - 1)) & \text{if } m > 0 \text{ e } n > 0. \end{cases}$$

The template (13.4) can be extended partial orders in which every non-empty subset has a least element.[1]

[1] Such orders are dubbed well-founded and will be studied in Chapter V.

Example 13.10. Consider $M\colon \mathbb{N} \to \mathbb{N}$ defined by

$$M(n) = \begin{cases} n - 10 & \text{if } n > 100, \\ M(M(n+11)) & \text{if } n \leq 100. \end{cases}$$

At first glance is not even clear if such function is well-defined for $n \leq 100$. First of all note that $M(101) = 91$. If $91 \leq n \leq 100$, then $M(n) = M(M(n+11)) = M(n+1)$ hence

$$M(91) = M(92) = \cdots = M(100) = M(101) = 91.$$

If $80 \leq n \leq 90$, then $91 \leq n + 11 \leq 101$ hence $M(n) = M(M(n+11)) = M(91) = 91$. Repeating the argument above it is easy to check that

$$M(n) = \begin{cases} n - 10 & \text{if } n > 100, \\ 91 & \text{if } n \leq 100. \end{cases}$$

Moreover $M(n) = \tilde{F}(M \restriction \operatorname{pred}(n, \prec))$ if $n \leq 100$, where $\prec$ is the ordering on $\{0, \ldots, 101\}$ defined by

$$n \prec m \Leftrightarrow [m < n \wedge n \equiv m \mod 11] \vee [91 \leq n, m \leq 101 \wedge m < n].$$

13.C. Cardinality. Two sets X and Y are **equipotent**, in symbols

$$X \asymp Y,$$

if there is a bijection between them. The relation $\asymp$ is an equivalence relation; we say that two equipotent sets X and Y have the same **cardinality** and write

$$|X| = |Y|.$$

The cardinality of the set of all natural numbers is

$$|\mathbb{N}| = \aleph_0,$$

where $\aleph$ is *aleph*, the first letter of the Hebrew alphabet. A set X **injects into** Y, in symbols

$$X \precsim Y$$

if there is an injective function $f\colon X \to Y$; in this case we will write

$$|X| \leq |Y|.$$

The symbol $\leq$ suggests that we are dealing with an ordering: the reflexive and transitive properties are immediate, while the anti-symmetric property is ensured by the following result.

Theorem 13.11 (Cantor-Schröder-Bernstein)**.** *If $X \precsim Y$ and $Y \precsim X$ then $X \asymp Y$.*

Proof. Fix two injective functions $f\colon X \to Y$ and $g\colon Y \to X$. The ordered set $(\mathscr{P}(X), \subseteq)$ together with the function $\Phi\colon \mathscr{P}(X) \to \mathscr{P}(X)$

$$\Phi(Z) = X \setminus g[Y \setminus f[Z]]$$

satisfy Theorem 7.11's hypotheses, hence there is $Z \subseteq X$ such that $\Phi(Z) = Z$, i.e. $X \setminus Z = g[Y \setminus f[Z]]$. Since g^{-1} is a bijection between $X \setminus Z$ and $Y \setminus f[Z]$, the map $h\colon X \to Y$

$$h(x) = \begin{cases} f(x) & \text{if } x \in Z \\ g^{-1}(x) & \text{if } x \in X \setminus Z \end{cases}$$

is a bijection. □

A set is in bijection with a proper subset of itself if and only if it contains a copy of the natural numbers.

Proposition 13.12. $\mathbb{N} \precsim X \Leftrightarrow \exists Y \subset X\, (Y \asymp X)$.

Proof. Suppose $f\colon \mathbb{N} \rightarrowtail X$ and let $Y = X \setminus \{f(0)\}$. Then $g\colon X \to Y$

$$g(x) = \begin{cases} x & \text{if } x \in X \setminus \operatorname{ran} f \\ f(n+1) & \text{if } \exists n \in \mathbb{N}\, (f(n) = x). \end{cases}$$

is a bijection.

Conversely, fix $g\colon X \to Y \subset X$ is a bijection, and let $x_0 \in X \setminus \operatorname{ran} g$: then inductively define $x_{n+1} = g(x_n)$. A simple induction shows that the x_ns are distinct, hence $\mathbb{N} \precsim X$. □

If $X \neq \emptyset$ and $X \precsim Y$ then there is a surjection $Y \twoheadrightarrow X$: if $f\colon X \rightarrowtail Y$ and $x_0 \in X$, then the map $g\colon Y \to X$

$$g(y) = \begin{cases} x & \text{if } f(x) = y, \\ x_0 & \text{if } y \neq f(x) \text{ for all } x \in X \end{cases}$$

is surjective and $g \circ f = \mathrm{id}_X$. To prove the converse we need a further assumption on Y.

Proposition 13.13. *If $g\colon Y \to X$ is surjective and $\trianglelefteq$ is a well-order on Y, then there is an injection $f\colon X \to Y$ such that $g \circ f = \mathrm{id}_X$.*

In particular, if $\mathbb{N}$ surjects onto X then $X \precsim \mathbb{N}$.

Proof. Let $f(x)$ be the $\triangleleft$-least $y \in Y$ such that $g(y) = x$. □

The symbol 2 will be used to denote the cardinality of a set with two elements, for example[2] the set $\{0, 1\}$. Therefore $2 \leq |X|$ stands for "X has

[2] As explained in Chapter V, in set theory the natural number 0 is construed as the empty set $\emptyset$ and the natural number $n + 1$ is construed as the set $\{0, 1, \ldots, n\}$.

at least two elements". The cardinality of $\mathbb{N}$ is denoted with the symbol $\aleph_0$. If $X \precsim Z$ and $Y \precsim W$, then $X \times Y \precsim Z \times W$, and if $X \cap Y = Z \cap W = \emptyset$, then $X \cup Y \precsim Z \cup W$. Therefore we can define the **sum** and **product of cardinalities** as

$$|X| + |Y| = |X \uplus Y| \qquad\qquad |X| \cdot |Y| = |X \times Y|.$$

If X and Y are disjoint set, each containing at least two elements, $x_0, x_1 \in X$ and $y_0, y_1 \in Y$, let $f \colon X \cup Y \to X \times Y$ be given by $f(x) = (x, y_0)$ if $x \in X$, and for $y \in Y$

$$f(y) = \begin{cases} (x_0, y) & \text{if } y \neq y_0, \\ (x_1, y_1) & \text{if } y = y_0. \end{cases}$$

The function f is injective, so

$$2 \leq |X|, |Y| \Rightarrow |X| + |Y| \leq |X \times Y|. \tag{13.5}$$

In Section 11.B it is shown that $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ are equipotent, and hence:

Theorem 13.14. $\mathbb{N} \times \mathbb{N} \asymp \mathbb{N}$ *hence* $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$.

13.C.1. *Countable sets.* In this Section we prove some facts about countable sets that are usually taken for granted.

By definition, a set X is **finite** if and only if it is in bijection with $\{0, \dots, n-1\}$, for some $n \in \mathbb{N}$ where $\{0, \dots, n-1\} = \emptyset$ when $n = 0$. In this case we write $|X| = n$. This notation is justified by the fact that a finite set is in bijection with a unique $n \in \mathbb{N}$. This follows from part (a) of the following result, known as the *pigeonhole principle* or *Dirichlet's principle*: if we place n pigeons inside m boxes and $m < n$, then one of the boxes will contain at least two pigeons.

Theorem 13.15. *For any* $n, m \in \mathbb{N}$*:*

(a) *If* $\{0, \dots, n-1\} \precsim \{0, \dots, m-1\}$*, then* $n \leq m$*. In particular: if* $\{0, \dots, n-1\} \asymp \{0, \dots, m-1\}$*, then* $n = m$*.*

(b) $\mathbb{N}$ *is infinite, so* $\mathbb{N} \not\precsim \{0, \dots, n-1\}$*.*

Proof. (a) By induction on $n \in \mathbb{N}$. If $n = 0$ the result is trivial, so we may assume that $n = n' + 1$ and $f \colon \{0, \dots, n'\} \rightarrowtail \{0, \dots, m'\}$. Clearly $m > 0$, that is $m = m' + 1$. Let $g \colon \{0, \dots, m'\} \to \{0, \dots, m'\}$ be the bijection that exchanges $f(n')$ with m' leaving everything else unchanged. Then

$$(g \circ f) \restriction \{0, \dots, n'-1\} : \{0, \dots, n'-1\} \rightarrowtail \{0, \dots, m'-1\}$$

hence, by inductive assumption, $n' \leq m'$, whence $n = n' + 1 \leq m' + 1 = m$.

(b) If $\mathbb{N} \precsim \{0, \dots, n-1\}$ for some $n \in \mathbb{N}$, then since $\{0, \dots, n\} \subseteq \mathbb{N}$ it would follow that $\{0, \dots, n\} \precsim \{0, \dots, n-1\}$ contradicting part (a). □

Definition 13.16. A set is **countable** if it is finite, or else if it is in bijection with $\mathbb{N}$.

Remark 13.17. If $f\colon n \to X$ is a bijection and $n > 0$, then we can list the elements of X using f, that is $X = \{x_0, \dots, x_{n-1}\}$, where $x_i = f(i)$. When in a mathematical text we read: "Consider a finite set $X = \{x_0, \dots, x_{n-1}\}$ ..." it is meant that we fix a bijection between $\{0, \dots, n-1\}$ and the set X.

Proposition 13.18. *Suppose* $Y \precsim X$.

(a) *If* X *is finite then* Y *is finite and* $|Y| \leq |X|$.

(b) *If* X *is countable then* Y *is countable and* $|Y| \leq |X|$.

Proof. (a) It is enough to show that if $\emptyset \neq Y \subseteq \{0, \dots, n-1\}$ then Y is in bijection with $\{0, \dots, m-1\}$ for some $m \in \mathbb{N}$. Let $b \notin Y$ and define $f\colon \mathbb{N} \to Y \cup \{b\}$ by first listing in increasing all elements of Y, and then hitting the value b forever, that is: $f(0) = \min Y$ and

$$f(k+1) = \begin{cases} \min(Y \setminus \{0, \dots, f(k)\}) & \text{if } Y \setminus \{0, \dots, f(k)\} \neq \emptyset \\ b & \text{otherwise.} \end{cases}$$

(This recursive definition is justified by Corollary 12.5 by taking $F\colon \mathbb{N} \to Y \cup \{b\}$ to be $F(k) = \min(Y \setminus \{0, \dots, k\})$, if the set is non-empty, and $F(k) = b$ otherwise.) It is easy to check by induction that $\forall j \left(f(j) \in Y \Rightarrow \forall k < j\, (f(k) \neq f(j)) \right)$, so if $B \overset{\text{def}}{=} \{k \in \mathbb{N} \mid f(k) = b\}$ were empty, then $\mathbb{N} \precsim Y$ against Theorem 13.15. So $B \neq \emptyset$ and let $m = \min B$. Then $f\colon \{0, \dots, m-1\} \to Y$ is a bijection.

(b) By part (a) we may assume that $Y \subseteq X = \mathbb{N}$. If Y is finite, then it is countable and $|Y| < |X| = \aleph_0$, so we may assume that Y is infinite. By recursion define $f\colon \mathbb{N} \to Y$ by $f(0) = \min Y$, and $f(n) = \min(Y \setminus \{f(0), \dots, f(n-1)\})$ for $n > 0$. Then f is increasing, and hence injective, and by construction it is surjective. Therefore $|Y| = |X| = \aleph_0$. □

Proposition 13.19. *A set is countable if and only if either it is empty or else it is the surjective image of* $\mathbb{N}$.

Proof. If X is the surjective image of $\mathbb{N}$, then $X \precsim \mathbb{N}$ by Proposition 13.13, and hence X is countable by Proposition 13.18. The other direction is immediate. □

Proposition 13.20. *If the sets* X, Y *are finite, then so are*

$$X \cup Y, \quad X \times Y, \quad X^Y \asymp X^{|Y|} = \underbrace{X \times \cdots \times X}_{|Y| \text{ times}}.$$

Proof. If $Y = \{y_1, \dots, y_m\}$ then $X^Y \to X^m$, $s \mapsto (s(y_1), \dots, s(y_m))$ is a bijection. If we show that $X \times Y$ is finite for any choice of finite sets X and Y, this would yield that $X \times X = X^2$ is finite, and hence, by induction, that X^m is finite. So suppose that $n = |X|$ and $m = |Y|$. Note that

$$\{0, \dots, n-1\} \times \{0, \dots, m-1\} \subseteq \{0, \dots, k-1\} \times \{0, \dots, k-1\}$$

where $k = \max(n, m)$. If $F \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is any of the bijections seen in Section 11.B, such as $\boldsymbol{J}$ or the square enumeration, then for any k there is l such that $F[\{0, \dots, k-1\}^2] \subseteq \{0, \dots, l-1\}$. Therefore $X \times Y$ injects into some $\{0, \dots, l-1\}$ and hence it is finite.

Finally, let us show that $X \cup Y$ is finite. Since $X \cup Y = X \cup (Y \setminus X)$ we may assume that X and Y are disjoint. The result is immediate if one of the two sets is empty or it is a singleton, so we may assume that $|X|, |Y| \geq 2$. By what was argued on page 314 $X \cup Y \precsim X \times Y$, hence $X \cup Y$ is finite, as it is in bijection with a subset of $X \times Y$. □

Therefore by Theorem 13.14 and Propositions 13.18 and 13.20 we have:

Theorem 13.21. *If X, Y are countable, then so are $X \cup Y$ and $X \times Y$. Moreover, if Y is finite, then X^Y is countable.*

13.C.2. *What exactly is an ordinal number?* Although Cantor's original definition of an ordinal number as the equivalence class of well-ordered sets under the isomorphism relation has an intuitive appeal, it has two drawbacks. The first is problem has a foundational flavour. These equivalence classes are very large: for example the ordinal 1 would be the collection of all singletons, and in particular $\{1\}$, being a singleton, should belong to 1—a rather curious situation. The second, and more practical issue is that working with equivalence classes means that in proofs we must choose representatives, and check the results do not depend on these choices. A better approach is to define canonical sets that are well-ordered, and show that any well-order is isomorphic to one of those.

We define the ordinals $0, 1, 2, \dots, n, \dots$ to be the sets: $\emptyset$, $\{0\} = \{\emptyset\}$, $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$, $\dots$, $\{0, 1, \dots, n-1\}$, $\dots$. Then ω can be defined as $\mathbb{N} = \{0, 1, \dots\}$ the set of all natural numbers. Moving to larger ordinals we have $\omega + 1$ is $\{0, 1, \dots, \omega\}$ and $\omega + 2$ is $\{0, 1, \dots, \omega, \omega + 1\}$, and so on. More generally $\alpha + 1 = \alpha \cup \{\alpha\}$. The formal definition of an ordinal number α is that of a set such that the membership relation is *transitive*, that is $y \in x \in \alpha \Rightarrow y \in \alpha$, and such that $\in$ well-orders α. Thus $\beta < \alpha$ means $\beta \in \alpha$.

It can be shown that any well-ordered set is isomorphic to one and only one α, so this sleeker construction of ordinals (due to von Neumann) is completely equivalent to Cantor's original definition. The only drawback is that it requires some preliminary groundwork. We will explore this approach in Section 18.

The order type of a countable well-order is a **countable ordinal**. If α is countable then every $\beta < \alpha$ is countable as well. Every natural number and ω are countable ordinals, and it can be shown (Section 19) that the countable ordinals are closed under the operations of addition, multiplication, and exponentiation. In particular, $\omega + \omega = \omega \cdot 2$, $\omega \cdot \omega = \omega^2$, ω^ω, ω^{ω^ω}, ... are all countable ordinals. In Section 18.B we will show that not every ordinal is countable—the least uncountable ordinal is called ω_1.

13.C.3. *Finite sequences.* If X is a non-empty set, let

$$X^{<\mathbb{N}} = \{(x_0, \dots, x_{k-1}) \mid k \in \mathbb{N} \land \forall i < k \, (x_i \in X)\}$$

be the set of all finite sequences of elements from X, with the proviso that when $k = 0$ we take the empty sequence $\emptyset$, and let $[X]^{<\mathbb{N}}$ be the set of all finite subsets of X. Note that $[\mathbb{N}]^{<\mathbb{N}}$ is the ideal Fin of all finite subsets of the naturals. The function $f \colon X^{<\mathbb{N}} \to [X]^{<\mathbb{N}}$, $s \mapsto \operatorname{ran}(s)$ is surjective, and whenever $<$ is a linear order on X the function

$$g \colon [X]^{<\mathbb{N}} \to X^{<\mathbb{N}}, \qquad \{x_0 < \dots < x_n\} \mapsto (x_0, \dots, x_n)$$

is injective and such that $f \circ g$ is the identity on $[X]^{<\mathbb{N}}$. Moreover $X \precsim [X]^{<\mathbb{N}}$ via $x \mapsto \{x\}$. If X is finite then $[X]^{<\mathbb{N}} = \mathscr{P}(X)$ is also finite (Corollary 13.23) while $X^{<\mathbb{N}}$ is infinite since $\mathbb{N} \precsim X^{<\mathbb{N}}$ via the map

$$\mathbb{N} \rightarrowtail X^{<\mathbb{N}}, \qquad n \mapsto (\underbrace{\bar{x}, \dots, \bar{x}}_{n \text{ times}})$$

with $\bar{x}$ some fixed element of X.

Next we argue that $\mathbb{N}^{<\mathbb{N}} \precsim \mathbb{N}$, and since $\mathbb{N} \precsim [\mathbb{N}]^{<\mathbb{N}} \precsim \mathbb{N}^{<\mathbb{N}}$ these sets are equipotent. Examples of injective maps $\mathbb{N}^{<\mathbb{N}} \rightarrowtail \mathbb{N}$ are:

- $(n_0, \dots, n_k) \mapsto \langle\!\langle n_0, \dots, n_k \rangle\!\rangle \in \mathrm{Seq} \subseteq \mathbb{N}$ from Section 11.B,
- $(n_0, \dots, n_k) \mapsto \mathbf{p}(0)^{n_0+1} \cdots \mathbf{p}(k)^{n_k+1}$ where $\mathbf{p}(i)$ is the ith prime number (see Section 8.A.2). change!

Any bijection between $X \to \mathbb{N}$ induces bijections $X^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ and $[X]^{<\mathbb{N}} \to [\mathbb{N}]^{<\mathbb{N}}$, so

$$|X| = \aleph_0 \Rightarrow |X^{<\mathbb{N}}| = |[X]^{<\mathbb{N}}| = \aleph_0. \tag{13.6}$$

13.D. Power set. The set $\mathscr{P}(X)$ is in bijection with $\{0,1\}^X$, the set of all functions from X to $\{0,1\}$, via the correspondence sending a subset of X to its characteristic function

$$\mathscr{P}(X) \to \{0,1\}^X, \qquad Y \mapsto \chi_Y^X.$$

Theorem 13.22 (Cantor)**.** *There is no surjection from X onto $\mathscr{P}(X)$ and therefore $\mathscr{P}(X) \not\precsim X$.*

Proof. Towards a contradiction, let $f\colon X \twoheadrightarrow \mathscr{P}(X)$ be a surjection and let

$$Y = \{x \in X \mid x \notin f(x)\}.$$

Fix $\bar{x} \in X$ such that $f(\bar{x}) = Y$. Then $\bar{x} \in Y \Leftrightarrow \bar{x} \notin f(\bar{x}) = Y$: a contradiction. □

In particular, $\mathscr{P}(\mathbb{N}) \asymp \{0,1\}^{\mathbb{N}}$ is uncountable.

Corollary 13.23. *If Y is finite, then $\mathscr{P}(Y)$ is finite.*

Proof. By Proposition 13.20 when $X = \{0,1\}$ we have that $\mathscr{P}(Y) \asymp X^Y$ is finite. □

The proof of the next result is left to the reader.

Lemma 13.24. (a) $X \precsim Y \Rightarrow \mathscr{P}(X) \precsim \mathscr{P}(Y)$;

(b) $X \precsim Y \wedge Z \precsim W \Rightarrow X^Z \precsim Y^W$;

(c) $X^{(Y \uplus Z)} \asymp X^Y \times X^Z$;

(d) $(X \times Y)^Z \asymp X^Z \times Y^Z$;

(e) $(X^Y)^Z \asymp X^{Y \times Z}$.

The **exponentiation** of two cardinalities is

$$|X|^{|Y|} = |X^Y|$$

and by Lemma 13.24 the usual algebraic properties hold:

$$|X|^{(|Y|+|Z|)} = |X|^{|Y|} \cdot |X|^{|Z|} \quad \text{and} \quad \left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y| \cdot |Z|}.$$

Proposition 13.25. *Suppose $\{0,1\} \precsim Y \precsim X$ and that $X \times X \asymp X$. Then $\{0,1\}^X \asymp Y^X \asymp X^X$.*

In particular, by Theorem 13.14, we have that $\{0,1\}^{\mathbb{N}} \asymp \mathbb{N}^{\mathbb{N}}$.

Proof. Since $\{0,1\}^X \precsim Y^X \precsim X^X$ and since $\{0,1\}^X \asymp \mathscr{P}(X) \asymp \mathscr{P}(X \times X)$, it is enough to prove that $X^X \precsim \mathscr{P}(X \times X)$. But this is immediate since any $f\colon X \to X$ is just a subset of $X \times X$. □

13.E. Sets of numbers. In Section 12.A we saw that $\mathbb{N}$ can be characterized, up to isomorphism, by Dedekind's axioms (Theorem 12.2(c)) and that the addition and multiplication operations are well-defined on $\mathbb{N}$. We will now see how to construct other numerical sets, starting from $(\mathbb{N}, +, \cdot)$.

13.E.1. *The integers.* The set of integers $\mathbb{Z}$ is defined as $(\mathbb{N} \times \mathbb{N})/E_{\mathbb{Z}}$ where $E_{\mathbb{Z}}$ is the equivalence relation defined by

$$(n, m) \; E_{\mathbb{Z}} \; (h, k) \Leftrightarrow n + k = h + m.$$

The ordering $<^{\mathbb{Z}}$ and the addition and multiplication operations $+^{\mathbb{Z}}$ and $\cdot^{\mathbb{Z}}$ are defined on $\mathbb{Z}$ by

$$\begin{aligned}
[(n, m)]_{E_{\mathbb{Z}}} <^{\mathbb{Z}} [(n', m')]_{E_{\mathbb{Z}}} &\Leftrightarrow n + m' < n' + m. \\
[(n, m)]_{E_{\mathbb{Z}}} +^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n + h, m + k)]_{E_{\mathbb{Z}}}, \\
[(n, m)]_{E_{\mathbb{Z}}} \cdot^{\mathbb{Z}} [(h, k)]_{E_{\mathbb{Z}}} &= [(n \cdot h + m \cdot k, n \cdot k + m \cdot h)]_{E_{\mathbb{Z}}}.
\end{aligned}$$

The map $\mathbb{N} \to \mathbb{Z}$, $n \mapsto [(n, 0)]_{E_{\mathbb{Z}}}$, is an injective morphism with respect to the ordering and the addition and multiplication operations, hence for all intended purposes $\mathbb{N}$ can be identified with a subset of $\mathbb{Z}$, and we can forget the superscript in the order relation ${}^{\mathbb{Z}}$, and in the definition of sum and product. Integers of the form $[(n, 0)]_{E_{\mathbb{Z}}}$ are denoted by n and those of the form $[(0, n)]_{E_{\mathbb{Z}}}$ are denoted by $-n$. Clearly every $z \in \mathbb{Z}$ is either of the form n or $-n$, for $n \in \mathbb{N}$, hence the function $f \colon \mathbb{N} \to \mathbb{Z}$

$$f(n) = \begin{cases} m & \text{if } n = 2m, \\ -m & \text{if } n = 2m - 1, \end{cases}$$

is a bijection.

13.E.2. *The rationals.* The set $\mathbb{Q}$ is defined as $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/E_{\mathbb{Q}}$ where $E_{\mathbb{Q}}$ is the equivalence relation

$$(x, y) \; E_{\mathbb{Q}} \; (z, w) \Leftrightarrow x \cdot w = y \cdot z.$$

The ordering and the addition and multiplication operations on $\mathbb{Q}$ are defined as

$$\begin{aligned}
[(x, y)]_{E_{\mathbb{Q}}} <^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &\Leftrightarrow \; x \cdot w < y \cdot z, \\
[(x, y)]_{E_{\mathbb{Q}}} +^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot w + z \cdot y, y \cdot w)]_{E_{\mathbb{Q}}} \\
[(x, y)]_{E_{\mathbb{Q}}} \cdot^{\mathbb{Q}} [(z, w)]_{E_{\mathbb{Q}}} &= [(x \cdot z, y \cdot w)]_{E_{\mathbb{Q}}}
\end{aligned}$$

The map $\mathbb{Z} \to \mathbb{Q}$, $z \mapsto [(z, 1)]_{E_{\mathbb{Q}}}$, is an increasing, injective ring homomorphism, so $\mathbb{Z}$ is identified with a subset of $\mathbb{Q}$. As before, the superscript ${}^{\mathbb{Q}}$ will be dropped from the symbols of the ordering, addition, and multiplication. The rationals of the form $[(z, w)]_{E_{\mathbb{Q}}}$ are denoted by z/w and every rational number can be written as z/w with z and w coprime, and $w > 0$. Therefore $\mathbb{Q}$ is in bijection with a subset of $\mathbb{Z} \times \mathbb{Z}$ which in turns is in bijection with $\mathbb{N} \times \mathbb{N}$. Theorem 13.14 implies that $\mathbb{Q}$ is in bijection with a

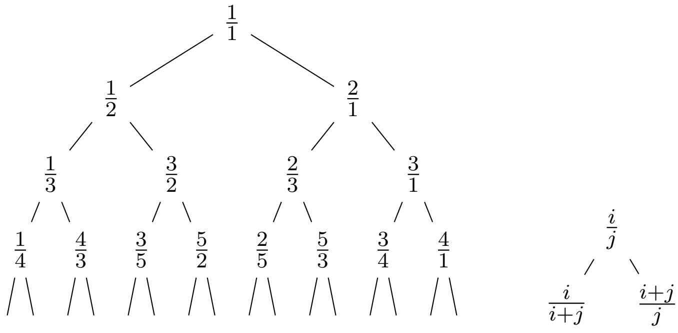


Figure 18. A tree of fractions

subset of $\mathbb{N}$ and since $\mathbb{N} \precsim \mathbb{Z} \precsim \mathbb{Q}$, the sets $\mathbb{N}$ and $\mathbb{Q}$ are in bijection, by the Cantor-Schröder-Bernstein Theorem 13.11. Therefore

$$|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0.$$

It is possible to exhibit an explicit bijection between $\mathbb{N}$ and $\mathbb{Q}_+$. Consider infinite the binary tree formed by fractions of the form $\frac{i}{j}$ subject to the following two rules: at the top of the tree there is the fraction $\frac{1}{1}$, and below a fraction $\frac{i}{j}$ we have two fractions $\frac{i}{i+j}$ and $\frac{i+j}{j}$ (see Figure 18). Let $q\colon \mathbb{N} \to \mathbb{Q}_+$ be the function enumerating the tree of fractions, from left to right and from top to bottom. Thus the first few values of q are: $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \ldots$. One checks that:

- for each $\frac{i}{j}$ the integers i and j are coprime;
- every $q \in \mathbb{Q}_+$ appears at least once in the tree;
- every $q \in \mathbb{Q}_+$ appears at most once in the tree.

The structure $(\mathbb{Q}, <)$ can be characterized up to isomorphism, as the unique countable, dense, linear order without endpoints (Theorem 13.32 below). For example $\mathbb{Q}$, $\mathbb{Q} \cup \{\pi\}$, $\overline{\mathbb{Q}} \cap \mathbb{R}$ are order isomorphic, yet it is not easy to explicitly define such an isomorphism. (Here and below $\overline{\mathbb{Q}}$ is the set of all algebraic numbers.) Therefore by Theorem 4.37

Corollary 13.26. *The theory of dense linear orders without endpoints is complete.*

Every linear order $(L, \leq)$ can be given the **interval topology** generated by the open half-lines $\{x \in L \mid x < b\}$ and $\{x \in L \mid a < x\}$, with $a, b \in L$. For example the topology on $\mathbb{R}$ is the interval topology induced by the usual ordering. An isomorphism of linear orders is a homeomorphism of the corresponding topological spaces. The function $x \mapsto \frac{1}{b-x} - \frac{1}{x-a}$ is an isomorphism between $(a; b)$ and $\mathbb{R}$, and if a and b are rationals, it is also an isomorphism between $(a;b)\cap\mathbb{Q}$ and $\mathbb{Q}$. By Theorem 13.32 $(a;b)\cap\mathbb{Q}\cong\mathbb{Q}$ even if a or b are irrationals, and moreover $((0;1)\setminus\{r\})\cap\mathbb{Q}\cong\mathbb{Q}$. On the other hand $\mathbb{R}$ and $(0;1)\setminus\{r\}$ are not isomorphic, since they are not homeomorphic topological spaces: the former is connected while the latter isn't. Therefore Theorem 13.32 cannot be generalized to uncountable orders.

Let $\mathbf{p}\colon\mathbb{N}\to\mathbb{N}$ be the function enumerating the prime numbers (Example 8.6(G)). Every element of $\mathbb{Q}_+$ distinct from 1 can be written in a unique way as $\mathbf{p}(i_1)^{n_1}\cdot\mathbf{p}(i_2)^{n_2}\cdots\mathbf{p}(i_k)^{n_k}$ with $0\leq i_1<i_2<\cdots<i_k$ and $n_1,n_2,\dots,n_k\in\mathbb{Z}\setminus\{0\}$. Then the function $\mathbb{Q}_+\to\mathbb{Z}[X]$ defined by

(13.7)
$$1\mapsto 0 \quad\text{and}\quad \mathbf{p}(i_1)^{n_1}\cdot\mathbf{p}(i_2)^{n_2}\cdots\mathbf{p}(i_k)^{n_k}\mapsto n_1X^{i_1}+n_2X^{i_2}+\cdots+n_kX^{i_k}$$

is a bijection. (Actually, it is an isomorphism of groups $(\mathbb{Q}_+,\cdot)\cong(\mathbb{Z}[X],+)$.) Since $\mathbb{Q}_+\asymp\mathbb{N}$, it follows that

$$|\mathbb{Z}[X]|=\aleph_0.$$

Every $(n_0,n_1,\dots,n_{k-1})\in\mathbb{N}^{<\mathbb{N}}$ yields a unique polynomial $n_0+n_1X+\cdots+n_{k-1}X^{k-1}\in\mathbb{N}[X]$, and conversely. Since $\mathbb{N}[X]$ is in bijection with $\mathbb{Z}[X]$, this gives a new proof of the countability of $\mathbb{N}^{<\mathbb{N}}$.

Note that $\oplus_n\mathbb{Z}$, the **direct sum** of ω copies of $\mathbb{Z}$, is isomorphic to $\mathbb{Z}[X]$ hence it has size $\aleph_0$, while $\prod_n\mathbb{Z}$, the **direct product** of ω copies of $\mathbb{Z}$, is in bijection with $\mathbb{N}^{\mathbb{N}}$ hence it is uncountable.

13.E.3. *The algebraic numbers.* The set of algebraic numbers $\overline{\mathbb{Q}}\subseteq\mathbb{C}$ is the set of all solutions of polynomials $\mathbb{Z}[X]$. Every $f\in\mathbb{Z}[X]$ yields a finite (possibly empty) set $Z(f)$ of complex numbers that are solutions of f: the set $Z(f)$ can be explicitly enumerated as $\{z_0,\dots,z_m\}$ by requiring that if $i<j$ then $|z_i|\leq|z_j|$ and if $z_i=r\mathrm{e}^{\mathrm{i}\theta}$ and $z_j=r\mathrm{e}^{\mathrm{i}\eta}$, then $0\leq\theta<\eta<2\pi$. A surjection $F\colon\mathbb{N}\times\mathbb{Z}[X]\to\overline{\mathbb{Q}}$ is defined by

$$F(n,f)=\begin{cases} z_n & \text{if } Z(f)=\{z_0,\dots,z_m\} \text{ and } n\leq m,\\ z_m & \text{if } Z(f)=\{z_0,\dots,z_m\} \text{ and } m<n,\\ 0 & \text{if } Z(f)=\emptyset.\end{cases}$$

By Theorem 13.14 $|\mathbb{N}\times\mathbb{Z}[X]|=\aleph_0$, hence there is a surjection $\tilde{F}\colon\mathbb{N}\twoheadrightarrow\overline{\mathbb{Q}}$. By Proposition 13.13 $\overline{\mathbb{Q}}\precsim\mathbb{N}$ and since $\mathbb{N}\subseteq\overline{\mathbb{Q}}$ it follows that

$$|\overline{\mathbb{Q}}|=\aleph_0.$$

13.E.4. *Real and complex numbers.* The set of **real numbers** is the Dedekind-completion of the ordered set $\mathbb{Q}$, that is

$$\mathbb{R}=\{x\in\mathscr{P}(\mathbb{Q})\mid x\text{ is a Dedekind cut}\}.$$

In other words: $x\in\mathbb{R}$ if and only if $x\notin\{\emptyset,\mathbb{Q}\}$, $\forall q\in x\,\forall p\in\mathbb{Q}(p<q\Rightarrow p\in x)$, and $\forall q\in x\exists p\in x(q<p)$. The ordering on $\mathbb{R}$ is just inclusion

between Dedekind cuts, and hence $\mathbb{R}$ is a dense linear order without end points. Addition on $\mathbb{R}$ is defined by $x +^{\mathbb{R}} y = \{p + q \mid p \in x \land q \in y\}$. The definition of multiplication $x \cdot^{\mathbb{R}} y$ is more cumbersome—see Exercise 13.71.

Let L be a linear order. A set $D \subseteq L$ is dense (in the sense of the interval topology) if and only if $\forall x, y \in L\, \exists d \in D\, (x < y \Rightarrow x < d < y)$. If L contains a dense countable set (i.e. L is separable with this topology) we will say that it is **separable**.

Theorem 13.27. *Up to isomorphism,* $(\mathbb{R}, \leq)$ *is the unique Dedekind-complete separable linear order without endpoints.*

Proof. Let $(X, \trianglelefteq)$ be a Dedekind-complete separable linear order, without endpoints, and let D a countable dense subset. Then $(D, \trianglelefteq)$ is a countable linear order without endpoints, hence by Theorem 13.32 there is an order-preserving bijection $F\colon \mathbb{Q} \to D$. For each $r \in \mathbb{R}$ we can find $p \in \mathbb{Q}$ such that $r \leq p$, hence the set $\{F(q) \mid q \in \mathbb{Q} \land q \leq r\}$ is bounded above by $F(p)$. The function F can be extended to $\mathbb{R}$ by letting

$$F(r) = \sup\{F(q) \mid q \in \mathbb{Q} \land q \leq r\}$$

where the sup is computed according to $\trianglelefteq$. Clearly $r \leq s \Rightarrow F(r) \trianglelefteq F(s)$ and if $r < s$ tale $q_1, q_2 \in \mathbb{Q}$, with $r < q_1 < q_2 < s$: then $F(r) \trianglelefteq F(q_1) \triangleleft F(q_2) \trianglelefteq F(s)$. Therefore F is increasing. We must check that F is surjective. If $x \in X$ choose $d \in D$ so that $x \triangleleft d$ and let $p \in \mathbb{Q}$ be such that $F(p) = d$. The set $A = \{r \in \mathbb{R} \mid F(r) \trianglelefteq x\}$ is bounded above by p, hence we can compute $\bar{r} = \sup A$ according $\leq$. Let us check that $F(\bar{r}) = x$. If $F(\bar{r}) \triangleleft x$, fix $d' \in D$ with $F(\bar{r}) \triangleleft d' \triangleleft x$. Let $p' = F^{-1}(d')$: then $p' \in A$ hence $p' \leq \bar{r}$, but on the other hand $F(\bar{r}) \triangleleft d'$ implies that $\bar{r} < p'$: contradiction. Similarly, the case $x \triangleleft F(\bar{r})$ yields a contradiction, and it is left to the reader. □

13.F. The real numbers and Cantor's set. For every $x \in \{0, 1\}^{\mathbb{N}}$ let

$$\Phi(x) = \sum_{n=0}^{\infty} \frac{2x(n)}{3^{n+1}}. \tag{13.8}$$

The function $\Phi\colon \{0, 1\}^{\mathbb{N}} \to [0; 1]$ is injective so $\mathscr{P}(\mathbb{N}) \precsim \mathbb{R}$. Since $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q})$ and $\mathscr{P}(\mathbb{Q}) \asymp \mathscr{P}(\mathbb{N})$, it follows that $\mathbb{R} \precsim \mathscr{P}(\mathbb{N})$. By the Cantor-Schröder-Bernstein Theorem 13.11 and Proposition 13.25:

Proposition 13.28. $\mathbb{R} \asymp \mathscr{P}(\mathbb{N})$. *In particular,* $\mathbb{R}$ *is uncountable.*

13.F.1. *Cantor's set.* The set $\operatorname{ran}(\Phi)$, where Φ is as in (13.8), is a well-known set in Analysis. In order to describe it, let us introduce a few definitions. Fix a closed interval $I = [a; b] \subset \mathbb{R}$ and fix an $r \in (0; 1)$. Remove from I the open

$$K_0 = [0;1]$$
$$K_1 = [0;\tfrac{1}{3}] \cup [\tfrac{2}{3};1]$$
$$K_2 = [0;\tfrac{1}{9}] \cup [\tfrac{2}{9};\tfrac{1}{3}] \cup [\tfrac{2}{3};\tfrac{7}{9}] \cup [\tfrac{8}{9};1]$$
$$K_3 = [0;\tfrac{1}{27}] \cup \cdots \cup [\tfrac{26}{27};1]$$

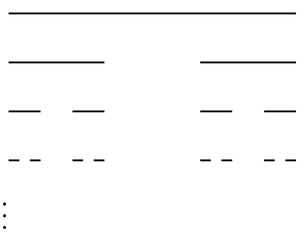
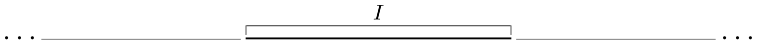


Figure 19. The construction of Cantor's set.

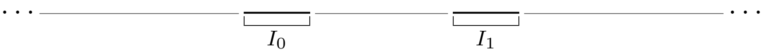
interval centered at the mid-point of I of length $r(b-a)$. We obtain thus two closed intervals

$$(13.9)\qquad \begin{aligned} I_0 &= \left[a; a + \frac{1+2r}{2}(b-a)\right] \\ I_1 &= \left[b - \frac{1+2r}{2}(b-a); b\right] \end{aligned}$$

In Figure 19 we see an example with $r = 1/2$: given a closed interval $I \subseteq \mathbb{R}$



remove the central part of I of length $1/2$ of the length of I so that I_0 and I_1 are obtained:



Cantor's ternary set defined as

$$(13.10)\qquad E_{1/3} = \bigcap_n K_n,$$

where $K_0 = [0;1]$, and $K_{n+1} \subset K_n$ is the union of 2^{n+1} closed intervals of length 3^{-n-1} obtained by applying construction (13.9) with $r = 1/3$ to each of the 2^n intervals that K_n is made of. More precisely we define $(\mathcal{K}_n)_n$ by $\mathcal{K}_0 = \{[0;1]\}$, and $\mathcal{K}_{n+1} = \{J \setminus \breve{J} \mid J \in \mathcal{K}_n\}$, where if $J = [a;b]$ then

$$\breve{J} = (a + \tfrac{b-a}{3}; b - \tfrac{b-a}{3}).$$

It is easy to check by induction that each $\mathcal{K}_n$ a collection of 2^n pairwise disjoint, closed intervals, each of length 3^{-n}, and that $K_n = \bigcup \mathcal{K}_n$. Letting $\mathcal{I}_n = \{J \setminus \breve{J} \mid J \in \mathcal{K}_n\}$, then $[0;1] \setminus K_n = \bigcup \mathcal{I}_n$ and $[0;1] \setminus E_{1/3} = \bigcup \mathcal{I}$, where $\mathcal{I} = \bigcup_{n \in \mathbb{N}} \mathcal{I}_n$. Notice that the $\mathcal{I}_n$s are pairwise disjoint, and that $\mathcal{I}$ is the collection of all connected components of the open set $[0;1] \setminus E_{1/3}$.

Remark 13.29. The construction of $E_{1/3}$ is justified by Corollary 12.4 as follows. Let A be the family of all finite sets of pairwise disjoint closed subintervals of $[0;1]$, let $a = \{[0;1]\} \in A$, and let

$$F\colon A \to A, \quad \{J_1, \dots, J_k\} \mapsto \{J_1 \setminus \breve{J}_1, \dots, J_k \setminus \breve{J}_k\}.$$

Then we have $f\colon \mathbb{N} \to A$ such that $f(n) = \mathcal{K}_n$.

It is not hard to check (Exercise 13.86) that $\operatorname{ran}(\Phi) = E_{1/3}$ hence Φ is a bijection between $2^{\mathbb{N}}$ and $E_{1/3}$. But much more is true. If $\leq$ is a linear order on A, then the **lexicographic order** on $A^{\mathbb{N}}$ is defined by

$$x \leq_{\text{lex}} y \Leftrightarrow x = y \vee \exists n\, [x(n) < y(n) \wedge \forall i < n\, (x(i) = y(i))]$$

where $<$ is the strict order induced by $\leq$. In particular $\leq_{\text{lex}}$ is a linear order on $2^{\mathbb{N}}$, and by Exercise 13.85

$$\Phi\colon (2^{\mathbb{N}}, \leq_{\text{lex}}) \to (E_{1/3}, \leq)$$

is an isomorphism, hence it is a homeomorphism between the space $2^{\mathbb{N}}$ with the interval topology induced by $\leq_{\text{lex}}$ and $E_{1/3}$ with the topology induced by $[0;1]$. In particular $2^{\mathbb{N}}$ with the interval topology is compact.[3] As the length of the intervals of $\mathcal{K}_n$ tend to 0, it follows that $E_{1/3}$ has empty interior.

In Section 26.D we show how to assign to every reasonable $X \subseteq \mathbb{R}$ a value $\lambda(X) \in [0;+\infty]$ estimating the size of X; such value called the **Lebesgue measure of** X. It can be shown that $\lambda(\emptyset) = \lambda(\{x\}) = 0$ for all $x \in \mathbb{R}$, that $\lambda(I) = b - a$ if I is an interval with endpoints $a < b$, and that $\lambda(\bigcup_n X_n) = \sum_n \lambda(X_n)$ whenever the X_ns are pairwise disjoint. Since $\mathcal{I}_n$ has 2^n open intervals of length 3^{-n-1},

$$\lambda(E_{1/3}) = 1 - \lambda(\textstyle\bigcup_n \mathcal{I}_n) = 1 - \sum_{n=0}^{\infty} \frac{2^n}{3^{n+1}} = 0.$$

If in the construction above we use $r \in (0;1)$ rather than $1/3$ and $[a;b]$ rather than $[0;1]$, we obtain the set

$$E_r(a,b) \subset [a;b],$$

which is compact, with empty interior and of measure zero.

13.G. Sets that are in bijection with $\mathbb{R}$.

[3] The interval topology on $2^{\mathbb{N}}$ is the same as the product topology of Section 14.A when $2 = \{0,1\}$ is given the discrete topology. This fact will be proved in Section 26.

13.G.1. *Product of copies of* $\mathbb{R}$. For each set X, the map sending each n-tuple $(x_0, \dots, x_{n-1}) \in X^n$ to the sequence

$$(x_0, \dots, x_{n-1}, x_{n-1}, x_{n-1}, \dots) \in X^{\mathbb{N}}$$

is injective and witness that $X^n \precsim X^{\mathbb{N}}$, hence by Theorem 13.14 and Exercise 13.24, for all $n \geq 1$

$$(\{0,1\}^{\mathbb{N}})^n \precsim (\{0,1\}^{\mathbb{N}})^{\mathbb{N}} \asymp \{0,1\}^{\mathbb{N}\times\mathbb{N}} \asymp \{0,1\}^{\mathbb{N}}$$

hence by the Cantor-Schröder-Bernstein Theorem 13.11,

$$\mathbb{R} \asymp \mathbb{R}^n \asymp \mathbb{R}^{\mathbb{N}}.$$

In particular $\mathbb{R} \asymp \mathbb{C}$, hence by Proposition 13.25 $\mathbb{R}^{\mathbb{R}} \asymp \mathscr{P}(\mathbb{R})$. This shows that the exponent $\mathbb{N}$ in the previous equation cannot be replaced with $\mathbb{R}$.

13.G.2. *The space of real-valued continuous functions on a separable space.* If $X \neq \emptyset$ is a separable space then $\mathcal{C}(X, \mathbb{R})$, the set of all continuous real-valued functions on X, is in bijection with $\mathbb{R}$; in particular $\mathcal{C}(\mathbb{R}, \mathbb{R}) \asymp \mathbb{R}$.

To see this let $Q \subseteq X$ be a countable dense set, and consider the function $\mathcal{C}(X, \mathbb{R}) \to \mathbb{R}^Q$, $f \mapsto f \restriction Q$. If $f, g \in \mathcal{C}(X, \mathbb{R})$ differ at $x_0 \in X$, then by continuity there is U non-empty open such that $x_0 \in U$ and f and g are always distinct on U. Let $q \in Q \cap U$: then $f(q) \neq g(q)$ and hence $f \restriction Q \neq g \restriction Q$. Therefore the map $f \mapsto f \restriction Q$ is injective and since $Q \precsim \mathbb{N}$, by the preceding example we have that $\mathcal{C}(X, \mathbb{R}) \precsim \mathbb{R}$. Using constant functions, $\mathbb{R} \precsim \mathcal{C}(X, \mathbb{R})$, hence $\mathcal{C}(X, \mathbb{R}) \asymp \mathbb{R}$.

13.G.3. *Separable metric spaces.* Let (X, d) be a separable metric space, and let $Q = \{q_n \mid n \in \mathbb{N}\}$ be a countable dense subset of X. The function $F \colon X \to \mathbb{R}^{\mathbb{N}}$, $F(x) \colon \mathbb{N} \to \mathbb{R}$, $n \mapsto d(x, q_n)$, is injective, hence $X \precsim \mathbb{R}$. In particular this holds when X is a (metric and separable) topological manifold or a separable normed vector space, and since $\mathbb{R}$ embeds into such X, we have another collection of sets in bijection with $\mathbb{R}$. In particular every separable **Banach space** (that is a complete, normed, vector space on $\mathbb{R}$) is in bijection with $\mathbb{R}$.

13.G.4. *Second countable spaces.* Let X be a second countable space and let $\mathcal{B} = \{V_n \mid n \in \mathbb{N}\}$ be a basis for its topology $\mathcal{T}$. The function $\mathcal{T} \to \mathscr{P}(\mathbb{N})$, $U \mapsto \{n \in \mathbb{N} \mid V_n \subseteq U\}$, is injective, hence $\mathcal{T} \precsim \mathbb{R}$. By taking complements one has that $\mathcal{C}$, the family of all closed subsets of X, can be injected into $\mathbb{R}$, that is $\mathcal{C} \precsim \mathbb{R}$.

If X is T_1 then the singletons are closed, so $X \precsim \mathbb{R}$.

13.H. Back-and-forth constructions.

13.H.1. *Dense linear orders without endpoints.* A partial isomorphisms between two orders $(X, \leq)$ and $(Y, \preceq)$ is a finite function p with $\operatorname{dom} p \subseteq X$ and $\operatorname{ran} p \subseteq Y$, such that $x_1 \leq x_2 \Leftrightarrow p(x_1) \preceq p(x_2)$, for all $x_1, x_2 \in X$.

Lemma 13.30. *Suppose p is a partial isomorphism between two linear orders $(X, \leq)$ and $(Y, \preceq)$. If $(Y, \preceq)$ is dense and without endpoints, then for all $x \in X$ there is $y \in Y$ such that $p \cup \{(x, y)\}$ is a partial isomorphism between X and Y.*

Proof. Fix $x \in X$. If $x \in \operatorname{dom} p$ pick $y = p(x)$ so that $p \cup \{(x, y)\} = p$. So we may assume that $x \notin \operatorname{dom} p = \{x_1 < \cdots < x_n\}$. If $x < x_1$ then pick y such that $y \prec p(x_1)$—this is possible, since Y has no minimum. If $x_n < x$ then pick y such that $p(x_n) \prec y$—this is possible, since Y has no maximum. If $x_i < x < x_{i+1}$ then pick y such that $p(x_i) \prec y \prec p(x_{i+1})$—this is possible since Y is dense. □

If p is a partial isomorphism between X and Y, then p^{-1} is a partial isomorphism between Y and X, so we have at once:

Lemma 13.31. *Suppose p is a partial isomorphism between two linear orders $(X, \leq)$ and $(Y, \preceq)$. If $(X, \leq)$ is dense and without first or last element, for all $y \in Y$ there is $x \in X$ such that $p \cup \{(x, y)\}$ is a partial isomorphism between X and Y.*

The next result shows that, up to isomorphisms, the set of rationals is the unique countable dense linear order without end points.

Theorem 13.32 (Cantor)**.** *Any two countable dense linear order without endpoints are isomorphic.*

Corollary 13.33. *Up to isomorphism, the countable dense linear orders are: $\mathbb{Q}$, $[0; 1] \cap \mathbb{Q}$, $[0; 1) \cap \mathbb{Q}$, $(0; 1] \cap \mathbb{Q}$.*

Proof of 13.32. Let $(X, \leq)$ and $(Y, \preceq)$ be two countable, dense linear orders without endpoints, say $X = \{x_n \mid n \in \mathbb{N}\}$ and $Y = \{y_n \mid n \in \mathbb{N}\}$. We shall construct partial isomorphisms p_n between X and Y such that $x_n \in \operatorname{dom}(p_n)$ and $y_n \in \operatorname{ran}(p_n)$, and $p_0 \subseteq p_1 \subseteq \ldots$. By construction $\bigcup_n p_n$ will be an isomorphism between X and Y.

Thus we are left to construct the p_ns. Set $p_0 = \{(x_0, y_0)\}$. Suppose we have constructed p_n as above. By the Lemma 13.30 we may find a partial isomorphism $p' \supseteq p_n$ such that $x_{n+1} \in \operatorname{dom} p'$; applying Lemma 13.31 we construct $p'' \supset p'$ such that $y_{n+1} \in \operatorname{ran} p''$. Then set $p_{n+1} = p''$. □

The construction in Theorem 13.32 is known as the *back-and-forth argument*, since we must ensure that function be defined on all x_ns (the *forth* part) and that it takes all possible values y_n (the *back* part). Using only the *forth* part of the argument, it is possible to show that:

Theorem 13.34. *Any countable linear order is embeddable in* $\mathbb{Q}$.

A linear order $(L, \leq)$ is **ultrahomogeneous** if for any pair of finite sets $A, B \subseteq L$ of the same size, there is an automorphism f of L such that $f[A] = B$. By Exercise 13.61 this is the same notion as being **interval-homogeneous**: for any two non-empty open intervals there is an automorphism mapping one onto the other. Arguing as in the proof of Theorem 13.32 and requiring that p_0 extends some given partial isomorphism we have that $\mathbb{Q}$ is homogeneous.

Theorem 13.35. *If* $A, B \subset \mathbb{Q}$ *are finite subsets of equal size, then there is an isomorphism* $f\colon (\mathbb{Q}, <) \to (\mathbb{Q}, <)$ *such that* $f[A] = B$.

13.H.2. *Countable atomless Boolean algebras and random graphs*.* A partial isomorphism between two Boolean algebras A and B is an isomorphism $p\colon A' \to B'$ where A' is a finite subalgebra of A and B' is a finite subalgebra of B. The next result is the analogue of Lemma 13.30.

Lemma 13.36. *Let* $p\colon A' \to B'$ *be a partial isomorphism between Boolean algebras* A *and* B*, and suppose* B *is atomless. Then* $\forall x \in A\, \exists y \in B$ *such that* p *can be extended to a partial isomorphism* $q\colon A'' \to B''$ *such that* $q(x) = y$*, where* A'' *and* B'' *are the Boolean algebras generated by* $A' \cup \{x\}$ *and* $B' \cup \{y\}$.

Proof. If $x \in A'$, then take $y = p(x)$ and let $A'' = A'$, $B'' = B'$, and $q = p$, so we may assume that $x \notin A'$. By Corollary 7.57 $A'' = \{(u \curlywedge x) \curlyvee (v \curlywedge x^*) \mid u, v \in A'\}$, so the atoms of A'' are the non-zero elements of

$$\{a \curlywedge x \mid a \in \mathrm{At}(A')\} \cup \{a \curlywedge x^* \mid a \in \mathrm{At}(A')\}.$$

If $a \in \mathrm{At}(A')$ and $a \curlywedge x \neq \mathbf{0}_A$, then

- either $\mathbf{0}_A < (a \curlywedge x) < a$, and hence also $\mathbf{0}_A < (a \curlywedge x^*) < a$,
- or else $a \curlywedge x = a$, that is $a \leq x$, whence $a < x$, as $x \notin A'$.

Thus the atoms of A' are split into three pairwise disjoint families:

$$\begin{aligned}\mathcal{A}_1 &= \{a \in \mathrm{At}(A') \mid \mathbf{0}_A < (a \curlywedge x) < a\}\\ \mathcal{A}_2 &= \{a \in \mathrm{At}(A') \mid a < x\}\\ \mathcal{A}_3 &= \{a \in \mathrm{At}(A') \mid a \curlywedge x = \mathbf{0}_A\}\end{aligned}$$

and hence

$$\mathrm{At}(A'') = \{a \curlywedge x \mid a \in \mathcal{A}_1\} \cup \{a \curlywedge x^* \mid a \in \mathcal{A}_1\} \cup \mathcal{A}_2 \cup \mathcal{A}_3.$$

The isomorphism $p\colon A' \to B'$ is a bijection $\mathrm{At}(A') \to \mathrm{At}(B')$, so $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$ is a partition of $\mathrm{At}(B')$, where $\mathcal{B}_i = \{p(a) \mid a \in \mathcal{A}_i\}$. As B is atomless, for each $b \in \mathcal{B}_1$ there is $\mathbf{0} < y_b < b$, so let

$$y = \bigvee(\mathcal{B}_2 \cup \{y_b \mid b \in \mathcal{B}_1\}) \in B.$$

(This element exists in B as it is the sup of a finite set.) As $b \curlywedge b' = \mathbf{0}_B$ for distinct $b, b' \in \mathrm{At}(B)$, it follows that $\forall b \in \mathcal{B}_1\, (y \curlywedge b = y_b)$, $\forall b \in \mathcal{B}_2\, (y \curlywedge b = b)$, and $\forall b \in \mathcal{B}_3\, (y \curlywedge b = \mathbf{0}_B)$. Thus

$$\{b \curlywedge y \mid b \in \mathcal{B}_1\} \cup \{b \curlywedge y^* \mid b \in \mathcal{B}_1\} \cup \mathcal{B}_2 \cup \mathcal{B}_3$$

is the set of atoms of B'', the Boolean algebra generated by $B' \cup \{y\}$. The map that is the identity on $\mathcal{A}_2 \cup \mathcal{A}_3$ and

$$a \curlywedge x \mapsto p(a) \curlywedge y, \qquad a \curlywedge x^* \mapsto p(a) \curlywedge y^*, \qquad (\text{for } a \in \mathcal{A}_1)$$

is a bijection $\mathrm{At}(A'') \to \mathrm{At}(B'')$ that can be extended to an isomorphism $q\colon A'' \to B''$. Since

$$q(a) = q(a \curlywedge x) \curlyvee q(a \curlywedge x^*) = (p(a) \curlywedge y) \curlyvee (p(a) \curlywedge y^*) = p(a)$$

for $a \in \mathcal{A}_1$, it follows that q extends p, and $q(x) = y$. □

The analogue of Lemma 13.31 is

Lemma 13.37. *Let $p\colon A' \to B'$ be a partial isomorphism between Boolean algebras A and B, and suppose A is atomless. Then $\forall y \in B \exists x \in A$ such that p can be extended to a partial isomorphism $q\colon A'' \to B''$ with $q(x) = y$, where A'' and B'' are the Boolean algebras generated by $A' \cup \{x\}$ and $B' \cup \{y\}$.*

Theorem 13.38. *Two countable atomless Boolean algebras are isomorphic.*

Proof. Let $A = \{a_n \mid n \in \mathbb{N}\}$ and $B = \{b_n \mid n \in \mathbb{N}\}$ be two Boolean algebras as in the statement of the theorem. Using Lemmata 13.36 and 13.37 we construct partial isomorphisms p_n between A and B such that $p_0 \subseteq p_1 \subseteq \dots$ and $a_n \in \operatorname{dom} p_n$ and $b_n \in \operatorname{ran} p_n$. Then function $f = \bigcup_n p_n\colon A \to B$ is a bijection, so it is enough to check that it is a homomorphism. If $x, y \in A$, fix indexes $m, n, h, k \in \mathbb{N}$ such that $x = a_m$, $y = a_n$, $x^* = a_h$ and $x \curlywedge y = a_k$. Then $x, y, x^*, x \curlywedge y \in \operatorname{dom} p_N$ where $N = \max(n, m, h, k)$ and since p_N is a partial isomorphism, $p_N(x^*) = p_N(x)^*$ and $p_N(x \curlywedge y) = p_N(x) \curlywedge p_N(y)$. Since f extends p_N one has $f(x^*) = f(x)^*$ and $f(x \curlywedge y) = f(x) \wedge f(y)$. □

By Theorem 4.37:

Corollary 13.39. *The theory of atomless Boolean algebras is complete.*

Corollary 13.40. $\mathrm{Prop}(S)$*, with S a countable set (Section 7.K.2), and the interval algebra over $\mathbb{Q}$ (Example 7.36*(b)*) are isomorphic.*

The following results are the analogues of Theorems 13.34 and 13.35, and their proof is left to the reader:

Theorem 13.41. *Every countable Boolean algebra is isomorphic to a subalgebra of the countable atomless Boolean algebra.*

Theorem 13.42. *If B is a countable, atomless Boolean algebra, and $p\colon B_1 \to B_2$ is an isomorphism with B_1, B_2 finite subalgebras of B, then there is an automorphism of B extending p.*

13.H.3. *Random graphs.* Back-and-forth constructions can be used to show also that any countable graph satisfying Rnd must be isomorphic to the countable random graph R_ω of Section 10.D, and that any countable graph embeds into it (Exercise 13.62).

Theorem 13.43. (a) *Every countable graph satisfying property Rnd of Definition 10.9 is isomorphic to* R_ω.

(b) *Every countable graph is isomorphic to an induced subgraph of* R_ω.

(c) *If $A, B \subseteq \mathrm{R}_\omega$ are finite and $f\colon A \to B$ is an isomorphism of the induced subgraphs, that is it is a bijection such that $\forall a_1, a_2 \in A\,(a_1 \mathrel{E} a_2 \Rightarrow f(a_1) \mathrel{E} f(a_2))$, then there is an automorphism $\hat{f}$ of* R_ω *such that $\hat{f} \restriction A = f$.*

Therefore by Theorem 4.37:

Corollary 13.44. *The theory of the random graph is complete.*

13.I. Recursive constructions*. As seen in Sections 11.B, 12.B and 8, inductive definitions are interesting from the logical point of view, and are quite common in mathematics. Some inductive constructions can be carried out in the transfinite.

13.I.1. *Transfinite recursion and derived sets.*

Definition 13.45. The **derivative** of a topological space X is

$$X' = \{x \in X \mid x \text{ is not isolated } X\}.$$

As $X \setminus X' = \bigcup \{\{x\} \mid \{x\} \text{ open in } X\}$ it follows that X' is closed in X. A topological space is **perfect** if it has no isolated points, that is if it coincides with its derivative. The empty set and the intervals of $\mathbb{R}$ are examples of perfect spaces, while $\mathbb{N}$ with the discrete topology (that is: the induced topology as a subset of $\mathbb{R}$) is not perfect, since its derived set is empty. Also the set $\{1 - 2^{-n} \mid n \in \mathbb{N}\} \cup \{1\}$, which has order type $\omega + 1$, isn't perfect, as its derivative is $\{1\}$, which itself isn't perfect, since its derivative is empty. Starting from X one defines $X^{(n)}$ by applying the derivation process n-times to X. The set $X^{(\omega)} = \bigcap_n X^{(n)}$ need not be perfect, hence this procedure can be carried into the transfinite by setting

$$\begin{aligned} X^{(0)} &= X \\ X^{(\alpha+1)} &= (X^{(\alpha)})' \\ X^{(\lambda)} &= \bigcap_{\alpha<\lambda} X^{(\alpha)} \qquad \text{when } \lambda \text{ is limit.} \end{aligned}$$

Thus the $X^{(\alpha)}$ form a decreasing sequence of closed sets, that is $X^{(\beta)} \subseteq X^{(\alpha)}$ when $\alpha < \beta$; if $X^{(\bar{\alpha})} = X^{(\bar{\alpha}+1)}$ then $X^{(\bar{\alpha})} = X^{(\beta)}$ for all $\beta > \bar{\alpha}$, and we will say that the derivation procedure terminates. The smallest such $\bar{\alpha}$ is the **Cantor-Bendixson rank** of X and it is denoted by $\|X\|_{\mathrm{CB}}$.

The sets $X^{(\|X\|_{\mathrm{CB}})} = \bigcap_\nu X^{(\nu)}$ and $X \setminus X^{(\|X\|_{\mathrm{CB}})}$ are, respectively, the **perfect kernel** and the **scattered part** of X. A space without isolated point coincides with its perfect kernel. At the other extreme of the spectrum are the **scattered spaces**, whose perfect kernel is empty. The map o^X defined on $X \setminus X^{(\|X\|_{\mathrm{CB}})}$ by

$$o^X(x) = o(x) = \text{the unique } \alpha < \|X\|_{\mathrm{CB}} \text{ such that } x \in X^{(\alpha)} \setminus X^{(\alpha+1)}$$

is the **order of isolation** of x in X. Therefore

$$X^{(\alpha)} = X \setminus \{x \in X \mid o(x) < \alpha\}.$$

Proposition 13.46. *In a second countable space there is no increasing sequence of open sets of length ω_1, i.e. there are no open sets U_α $(\alpha < \omega_1)$ such that $\alpha < \beta \Rightarrow U_\alpha \subset U_\beta$. Similarly there is no decreasing sequence of closed sets of length ω_1, i.e. there are no closed sets C_α $(\alpha < \omega_1)$ such that $\alpha < \beta \Rightarrow C_\alpha \supset C_\beta$.*

Proof. Let X be a topological space, and let $\{V_n \mid n \in \mathbb{N}\}$ be a basis for it. Towards a contradiction, suppose there are U_α $(\alpha < \omega_1)$ as above, then the map $\{\alpha \mid \alpha < \omega_1\} \to \mathbb{N}$

$$\alpha \mapsto \min\{n \in \mathbb{N} \mid V_n \subseteq U_{\alpha+1} \wedge V_n \nsubseteq U_\alpha\}$$

would be injective, against the definition of ω_1.

The case for closed sets is obtained by taking complements. □

Fix a second countable topological space X with base $\{U_n \mid n \in \mathbb{N}\}$. For each subspace $C \subseteq X$ we can define its derivative C' by taking C to be the ambient space, and the map $F_C \colon C \setminus C' \rightarrowtail \mathbb{N}$

$$F_C(x) = \min\{n \in \mathbb{N} \mid U_n \cap C = \{x\}\}$$

is injective. In particular, letting $C_0 = X$ and $C_\alpha = X^{(\alpha)}$, then the C_αs are a decreasing sequence of closed sets hence $\|X\|_{\mathrm{CB}} < \omega_1$ by Proposition 13.46, and $X^{(\|X\|_{\mathrm{CB}})}$ is perfect. Moreover, if $P \subseteq X$ is perfect, then $P \subseteq X^{(\alpha)}$ for all α and in particular $P \subseteq X^{(\|X\|_{\mathrm{CB}})}$. The map

$$F\colon \bigcup_{\alpha<\|X\|_{\mathrm{CB}}} X^{(\alpha)} \setminus X^{(\alpha+1)} \to \{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \times \mathbb{N}, \quad x \mapsto (o(x), F_{C^{(o(x))}}(x))$$

is injective. Since $\|X\|_{\mathrm{CB}} < \omega_1$, there is $g\colon \{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \rightarrowtail \mathbb{N}$, and composing F with the map $\{\alpha \mid \alpha < \|X\|_{\mathrm{CB}}\} \times \mathbb{N} \rightarrowtail \mathbb{N} \times \mathbb{N}$, $(\nu, i) \mapsto (g(\nu), i)$, we obtain

$$X \setminus X^{(\|X\|_{\mathrm{CB}})} = \bigcup_{\alpha<\|X\|_{\mathrm{CB}}} X^{(\alpha)} \setminus X^{(\alpha+1)} \precsim \mathbb{N} \times \mathbb{N} \asymp \mathbb{N}.$$

We have thus proved:

Theorem 13.47 (Cantor-Bendixson). *Every second countable space X can be partitioned as $X = P \cup S$, where P is closed and perfect, and S is countable and open.*

In particular, every closed set C of $\mathbb{R}$ can be decomposed as $C = P \cup S$, with P perfect and S countable. We will show in Section 26 that every non-empty perfect set $P \subseteq \mathbb{R}$ contains a copy of $2^{\mathbb{N}}$ and hence it is equipotent to $\mathbb{R}$.

The construction of the $X^{(\alpha)}$ is a definition by recursion, but of a more general kind than the one seen so far,[4] since we had to deal with limit stages. A function $f\colon \mathrm{Ord} \to A$, where Ord is the collection of all ordinals, is defined by recursion if it is the unique solution to

$$\begin{aligned} f(0) &= a \\ f(\alpha+1) &= F(\alpha, f(\alpha)) \\ f(\lambda) &= G(\lambda, (f(\alpha))_{\alpha<\lambda}) \qquad\qquad \text{if } \lambda \text{ is limit,} \end{aligned}$$

where $a \in A$, $F\colon \mathrm{Ord} \times A \to A$, and G is defined on pairs of the form $(\lambda, (x_\alpha)_{\alpha<\lambda})$ with λ limit and $x_\alpha \in A$. In many cases we may assume that F does not depend on α, i.e. that $F\colon A \to A$. For example, if X is a topological space and

$$A = \mathscr{P}(X), \quad a = X, \quad F(Y) = Y', \quad G(\lambda, (Y_\alpha)_{\alpha<\lambda}) = \bigcap_{\alpha<\lambda} Y_\alpha,$$

we recover the construction of the $X^{(\alpha)}$s.

The study of recursive definitions on the ordinals will be take upon in Section 19 in Chapter V.

[4] *It's life, Jim, but not as we know it.*—Mr. Spock, *Star Trek*

13.J. An interesting countable ordinal*.

work in progress

Lemma 13.48. $\forall \alpha < \omega_1 \, (\omega^\alpha < \omega_1)$.

In this section $(\nu_n)_{n\in\mathbb{N}}$ denote the ordinals defined as follows: $\nu_0 = \omega$, $\nu_n = \omega^{\nu_n}$. By induction on n, ν_n is countable, and hence so is

$$\varepsilon_0 = \sup_n \nu_n .$$

The ordinal ε_0 is closed under exponentiation, that is:

$$\alpha, \beta < \varepsilon_0 \Rightarrow \alpha^\beta < \varepsilon_0 .$$

13.J.1. *Hydras.* The battle between Hercules and the hydra is described in Example 1.2—it is a game between these two players where at each round Hercules chops off a head of the hydra, and the monster regenerates n new parts of itself. The game terminates when there is nothing left of the hydra, and Hercules is declared to be the winner.

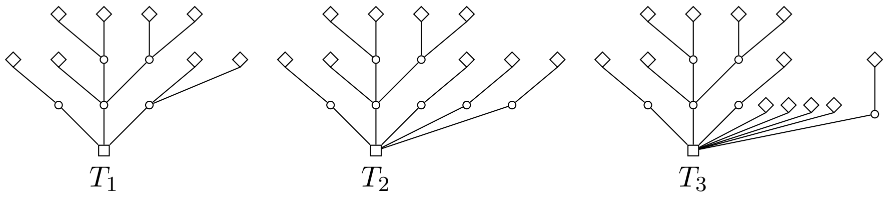
A hydra is a finite tree T whose maximal nodes are called **heads** and the minimum is called **root**. If $t \in T$ then the set $\uparrow t$ is usually denoted by $T_{\lfloor t \rfloor}$, that is

$$T_{\lfloor t \rfloor} = \{u \in T \mid t \leq u\}.$$

The game starts with a hydra $T = T_0$. At round n of the game the hydra is a non-empty tree T_n, and Hercules removes one of the heads $h \in T_n$:

- if h is the root, the game is over and Hercules wins;
- if h is immediately above the root, then $T_{n+1} = T_n$;
- if t is the immediate predecessor of h, and s is the immediate predecessor of t, then T_{n+1} is obtained from $T^* = T_n \setminus \{h\}$ by attaching to s n-copies of $T^*_{\lfloor t \rfloor}$.

Thus if the original hydra is the tree $T = T_0$ of Figure 1 on page 3, and Hercule's moves are as in Example 1.2, the hydra in the first three rounds is:



We prove that no matter what strategy Hercules follows, he kills the hydra in finitely many steps. To this end we assign an ordinal $o(T)$ to each hydra (i.e. finite tree) $T \neq \emptyset$, in such a way that

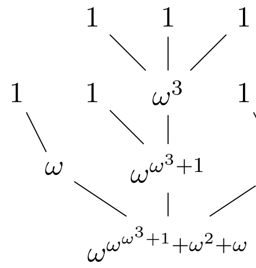
$$o(T_0) > o(T_1) > o(T_2) > \dots$$

Therefore in finitely many steps we reach $T_n = \emptyset$.

We label each node of T with an ordinal, and set $o(T)$ to be the label of its root. The labelling procedure is defined starting from the maximal elements of T (the heads) and moving downwards towards the root—as T is finite, this labelling procedure is well-defined:

- every maximal node is labelled with $1 = \omega^0$;
- if t is a node that has n immediate successors, and $\alpha_1 \geq \cdots \geq \alpha_n$ are the labels of these nodes, then t is labelled with $\omega^{\alpha_1 + \cdots + \alpha_n}$.

Therefore the labelling of the hydra of Example 1.2 is



so $o(T_0) = \omega^{\omega^{\omega^3+1}+\omega^2+\omega}$, and the reader can easily verify that

$$o(T_0) > o(T_1) = \omega^{\omega^{\omega^2\cdot 2+1}+\omega^2+\omega}$$

$$> o(T_2) = \omega^{\omega^{\omega^2\cdot 2+1}+\omega\cdot 4} > o(T_3) = \omega^{\omega^{\omega^2\cdot 2+1}+\omega\cdot 3+3}$$

Observe that the label of t in T is

$$o(T^*) < o$$

13.J.2. *Goodstein's sequences.*

13.J.3. *The consistency of* PA.

Exercises

Exercise 13.49. Show that:

(i) if $(P, \leq_P)$ and $(Q, \leq_Q)$ are linear orders, then $P + Q$ and $P \times Q$ are linear orders. Show with a counterexample that this does not hold if the product ordering is used instead of the lexicographic ordering;

(ii) if Q' is an initial segment of Q, then $P + Q'$ and $P \times Q'$ are initial segments of $P + Q$ and $P \times Q$, respectively. Show with a counterexample that if P' is an initial segment of P, then it does not follow that $P' + Q$ and $P' \times Q$ are initial segments of $P + Q$ and $P \times Q$.

(iii) $P + P \cong P \times 2$.

Exercise 13.50. Show that

(i) If $(P, \leq)$ is a well-order and $Q \subseteq P$, then Q with the induced order is a well-order.

(ii) Propositions 13.2, 13.3 and 13.4 do not hold if the well-order $(P, \leq)$ is replaced by $\mathbb{Q}$ or $\mathbb{R}$.

Exercise 13.51. Complete the proof that $q \colon \mathbb{N} \to \mathbb{Q}_+$ on page 320 is a bijection. Show that

(i) the denominator of $q(n)$ is the numerator of $q(n+1)$, hence $q(n) = \frac{f(n)}{f(n+1)}$, for some $f \colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$

(ii) the function f satisfies the recurrence relations: $f(0) = 1$, $f(2n+1) = f(n)$, and $f(2n+2) = f(n) + f(n+1)$.

Exercise 13.52. Compute the cardinality of the sets $\mathcal{X}_i \subseteq \mathscr{P}(\mathbb{N})$ $(i = 0, \dots, 3)$:

- $\mathcal{X}_0 = \{X \subseteq \mathbb{N} \mid X \text{ is cofinite}\} = \{X \subseteq \mathbb{N} \mid \mathbb{N} \setminus X \in [\mathbb{N}]^{<\mathbb{N}}\}$,
- $\mathcal{X}_1 = \{X \subseteq \mathbb{N} \mid X \text{ is infinite}\}$,
- $\mathcal{X}_2 = \{X \subseteq \mathbb{N} \mid X \text{ is coinfinite}\} = \{X \subseteq \mathbb{N} \mid \mathbb{N} \setminus X \text{ is infinite}\}$,
- $\mathcal{X}_3 = \{X \subseteq \mathbb{N} \mid X \text{ is infinite and coinfinite}\}$.

Exercise 13.53. Suppose $(L, \preceq)$ is a linear order and that each $X_n \subseteq L$ $(n \in \mathbb{N})$ is either finite, or else $(X_n, \preceq) \cong (\mathbb{N}, \leq)$. Show, without assuming AC_ω, that $\bigcup_n X_n$ is countable.

move in §14

Exercise 13.54. Show that $f \colon [\mathbb{N}]^{<\mathbb{N}} \to \mathbb{N}$ is a bijection, where $f(\emptyset) = 0$ and if $X = \{k_0 < \dots < k_n\}$ then $f(X) = 2^{k_0} + \dots + 2^{k_n}$.

In the next two exercises the linear orders with one and two elements are denoted by 1 and 2.

Exercise 13.55. Consider the following list of uncountable linear orders:

$L_0 = \mathbb{R} + \mathbb{R}$	$L_1 = \mathbb{R} \times \mathbb{R}$	$L_2 = [0;1) \times \mathbb{Z}$	$L_3 = \mathbb{R} + 2 + \mathbb{R}$
$L_4 = \mathbb{Q} \times \mathbb{R}$	$L_5 = \mathbb{R} \setminus \mathbb{Q}$	$L_6 = [0;1) \times \mathbb{N}$	$L_7 = \mathbb{R} + 1 + \mathbb{R}$
$L_8 = [0;1)$	$L_9 = (0;1] \times \mathbb{N}$	$L_{10} = [0;1] \times \mathbb{Z}$	$L_{11} = \mathbb{R} + (\omega + 1) + \mathbb{R}$
$L_{12} = \mathbb{R} \times \mathbb{Q}$	$L_{13} = (0;1] \times \mathbb{Z}$	$L_{14} = (0;1) \cup (1;2)$	$L_{15} = (0;1] \cup (2;3)$
$L_{16} = \mathbb{R} \setminus \mathbb{Z}$	$L_{17} = (0;1) \times \mathbb{Z}$	$L_{18} = (0;1] \cup [2;3)$	$L_{19} = \bigcup_{n \in \mathbb{Z}} (2n; 2n+1)$

$$L_{20} = (0;1] \cup \left\{2 - (n+1)^{-1} \mid n \in \mathbb{N}\right\} \cup [2;3)$$

For each pair $0 \leq i < j \leq 20$ determine whether L_i and L_j are isomorphic or not.

Exercise 13.56. Consider the following list of countable linear orders:

$$\mathbb{Q}, \quad \mathbb{Q}+\mathbb{Q}, \quad \mathbb{Q}+1+\mathbb{Q}, \quad \mathbb{Q}+2+\mathbb{Q}, \quad \mathbb{Q}\times\mathbb{Z}, \quad \mathbb{Z}\times\mathbb{Q}, \quad \mathbb{Q}\setminus\mathbb{Z}.$$

For each pair, determine whether they are isomorphic or not.

Exercise 13.57. Use Theorem 13.32 to prove that given A, B countable dense subsets of $\mathbb{R}$ there is an auto-homeomorphism f of $\mathbb{R}$ which is increasing, and such that $f[A] = B$. In particular, there is an increasing auto-homeomorphism of $\mathbb{R}$ mapping the irrational numbers onto the transcendental numbers.

Exercise 13.58. Let $L \neq \emptyset$ be a countable linear order, and recall Corollary 13.33. Show that:

(i) If $Q \in \{\mathbb{Q}, \mathbb{Q}\cap[0;1), \mathbb{Q}\cap(0;1]\}$ then $Q \times L$ is dense and determine to which order it is isomorphic.

(ii) If $Q = \mathbb{Q}\cap[0;1]$ and L is dense then $Q \times L$ is dense and determine which of the four orders above it is isomorphic to.

Exercise 13.59. Let $\mathcal{I}$ be a collection of pairwise disjoint intervals of $\mathbb{R}$. For $I, J \in \mathcal{I}$ set $I \lhd J \Leftrightarrow \sup I \leq \inf J$. Show that:

(i) $\mathcal{I}$ is countable and $(\mathcal{I}, \lhd)$ is a strict linear order.

(ii) If the elements in $\mathcal{I}$ are open sub-intervals of $[a;b]$ with disjoint closures, i.e. $I \neq J \Rightarrow \mathrm{Cl}(I) \cap \mathrm{Cl}(J) = \emptyset$, and $\bigcup \mathcal{I}$ is dense in $[a;b]$, then $(\mathcal{I}, \lhd) \cong (\mathbb{Q}, <)$.

(iii) If the elements of $\mathcal{I}$ are closed sub-intervals of $(a;b)$ such that $\bigcup \mathcal{I}$ is dense in $(a;b)$, then $(\mathcal{I}, \lhd) \cong (\mathbb{Q}, <)$. Conclude that here is no $\mathcal{I}$ as above such that $\bigcup \mathcal{I} = (a;b)$.

(iv) If $\mathcal{I}$ is the collection of open intervals removed from $[0;1]$ in the construction of $E_{1/3}$ (see page 323), and $D \subseteq (0;1)$ is countable dense, then there is a continuous monotone function $f\colon [0;1] \to [0;1]$ such that $f[E_{1/3}] = [0;1]$ and on each $I \in \mathcal{I}$ the function f is constant and attains value in D.

(v) Show that:

- q^- is the immediate predecessor of q^+ in $(\mathrm{Down}(\mathbb{Q}), \subseteq)$, where $q^- = \{x \in \mathbb{Q} \mid x < q\}$ and $q^+ = q^- \cup \{q\} = {\downarrow} q$.
- $(\mathrm{Down}(\mathbb{Q}), \subseteq) \cong (E_{1/3}, \leq)$.

[Hint: $(\mathcal{I}, \lhd) \cong (\mathbb{Q}, <)$, where $\mathcal{I}$ is as in (iv).]

Exercise 13.60. Consider $\mathbb{N}^{\mathbb{N}}$ with the topology induced by the lexicographic order $\leq_{\mathrm{lex}}$. Show that

(i) $D = \{h \in \mathbb{N}^{\mathbb{N}} \mid \exists k\, \forall n \geq k\, (h(n) = 0)\}$ is countable and dense in $\mathbb{N}^{\mathbb{N}}$, and $(D, \leq_{\mathrm{lex}}) \cong ([0;1) \cap \mathbb{Q}, \leq)$.

(ii) $\mathbb{N}^{\mathbb{N}}$ is homeomorphic to $[0;1)$.

Exercise 13.61. Show that:

(i) a linear order is ultrahomogeneous if and only if it is interval-homogeneous;

(ii) $\mathbb{R} \setminus \mathbb{Z}$ is homogeneous, but not ultrahomogeneous.

Exercise 13.62. Prove Theorem 13.43.

Exercise 13.63. Show every dense, Dedekind-complete linear order with at least two elements is uncountable.

Exercise 13.64. Fix a bijection $\mathbb{N} \to \{(A, B) \mid A, B \in [\mathbb{N}]^{<\mathbb{N}} \wedge A \cap B = \emptyset\}$, $n \mapsto (A_n, B_n)$. Fix an increasing sequence $(x_n)_n$ of non-zero natural numbers such that $\max(A_n \cup B_n) < x_n$. Show that the graph $(\mathbb{N}, E)$

$$\forall m < k \; (m \mathrel{E} k \Leftrightarrow \exists n \; (k = x_n \wedge m \in A_n))$$

satisfies Rnd.

Exercise 13.65. Show that:

(i) there is an order $(P, \leq)$ satisfying the following property: given finite and pairwise disjoint sets $A, B, C \subseteq P$ such that

$$\forall a \in A \, \forall b \in B \, \forall c \in C \; (b \nleq a \wedge c \nleq a \wedge b \nleq c)\,,$$

there is $p \in P \setminus (A \cup B \cup C)$ such that

$$\forall a \in A \, \forall b \in B \, \forall c \in C \; (a \leq p \leq b \wedge p \nleq c \wedge c \nleq p)\,.$$

Such $(P, \leq)$ is called a **random order**;

(ii) two countable random orders are isomorphic,

(iii) every countable order embeds into a countable random order.

Exercise 13.66. In analogy with the case of the random graph and order, define and construct a random object for each kind of structure:

(i) directed graph,

(ii) transitive relation,

(iii) irreflexive relation,

(iv) binary relation.

In each case state and prove a result analogous to Theorem 13.43.

Exercise 13.67. Show that there is a $\mathcal{C} \subseteq \mathscr{P}(\mathbb{N})$ such that $(\mathcal{C}, \subset)$ is isomorphic to $(\mathbb{R}, <)$.

Exercise 13.68. Compute the order type of X and X_k with $k \in \mathbb{N}$:

$$X = \left\{ \tfrac{m\cdot(n+1)-1}{n+1} \mid n, m \in \mathbb{N} \right\}$$

$$X_k = \left\{ \tfrac{m\cdot(n+1)-1}{n+1} \mid n \in \mathbb{N} \wedge 0 \leq m < k \right\}$$

Exercise 13.69. Consider the set $\mathbb{N}[X]$ of polynomials in a variable X with coefficients in $\mathbb{N}$ ordered under eventual dominance: $f \prec g \Leftrightarrow \exists M \forall x > M\,(f(x) < g(x))$. Show that $\prec$ is a well-order of type ω^ω and explicitly describe the isomorphism $F\colon (\mathbb{N}[X], \prec) \to (\omega^\omega, <)$.

Exercise 13.70. Show that the sum and product of cardinalities are commutative, associative operations, and that multiplication is distributive with respect to addition.

Exercise 13.71. If $x, y \in \mathbb{R}$ and $x, y > 0$ set

$$x \cdot y = \{p \in \mathbb{Q} \mid \exists q, r \in \mathbb{Q}\,(0 < q \in x \wedge 0 < r \in y \wedge p \leq q \cdot r)\}$$

and if x, y are not both positive,

$$x \cdot y = \begin{cases} 0 & \text{if } x = 0 \text{ or } y = 0, \\ -\big((-x) \cdot y\big) & \text{if } x < 0 \text{ and } y > 0, \\ -\big(x \cdot (-y)\big) & \text{if } x > 0 \text{ and } y < 0, \\ (-x) \cdot (-y) & \text{if } x < 0 \text{ and } y < 0, \end{cases}$$

where $-x = \{p \in \mathbb{Q} \mid \exists s \in \mathbb{Q} \forall q \in x\,(p + q < s < 0)\}$. Check that the operation is well-defined and that $(\mathbb{R}, +, \cdot, <)$ is an ordered Archimedean field.

Exercise 13.72. Suppose X and Y are finite sets. Show that $|X \uplus Y| = |X| + |Y|$, $|X \times Y| = |X| \cdot |Y|$ and $|X^Y| = |X|^{|Y|}$, where the operations of addition, multiplication, and exponentiation on natural numbers are defined recursively as in Section 12.B.

Exercise 13.73. Show that A is equipotent with $\mathbb{R}$, for any $A \subseteq \mathbb{R}^n$ such that $\operatorname{Int}(A) \neq \emptyset$.

Exercise 13.74. Check that the proof of Theorem 13.34 shows that every countable ordinal can be embedded in $\mathbb{R}$ as a closed set. In other words, for all $\alpha < \omega_1$ there is an order preserving $f\colon \alpha \to \mathbb{Q}$ with $\operatorname{ran}(f)$ a closed subset of $\mathbb{R}$.

Exercise 13.75. Show that there is no increasing or decreasing function $f\colon \omega_1 \to \mathbb{R}$.

Exercise 13.76. Let $X \asymp Y \asymp \mathbb{N}$. Show that the following subsets of X^Y are equipotent with $\mathbb{R}$:

$$\mathcal{F}_0 = \{f \mid f \text{ is bijective}\} \quad \mathcal{F}_1 = \{f \mid f \text{ is injective}\} \quad \mathcal{F}_2 = \{f \mid f \text{ is surjective}\}.$$

Conclude that $\mathcal{F}_3 \asymp \mathcal{F}_4 \asymp \mathbb{R}$, where

$$\mathcal{F}_3 = \{f \in \mathbb{N}^{\mathbb{N}} \mid f \text{ is monotone}\}, \qquad \mathcal{F}_4 = \{f \in \mathbb{N}^{\mathbb{N}} \mid f \text{ is increasing}\}.$$

Exercise 13.77. For any $f \in 2^{\mathbb{N}}$ consider the linear order

$$L_f = \mathbb{Z} + f(0) + \mathbb{Z} + f(1) + \mathbb{Z} + f(2) + \mathbb{Z} + \dots$$

obtained by taking ω copies of $\mathbb{Z}$ in which the n-th copy is separated from the $n+1$-st by a single point if and only if $f(n) = 1$. Show that $L_f \cong L_g$ if and only if $f = g$. Conclude that there are $|\mathbb{R}|$-many pairwise non-isomorphic countable linear orders.

Exercise 13.78. For each $n \geq 2$ construct a graph G_n on $\mathbb{N}$ satisfying $\neg \textsc{Rnd}_n \wedge \bigwedge_{j<n} \textsc{Rnd}_j$ as defined on page 259. Conclude that $\Sigma_{\textsc{RndGrph}}$ is not finitely axiomatizable.

Exercise 13.79. Show that if $(L, <)$ is a separable linear order, then $L \precsim \mathscr{P}(\mathbb{N})$.

In the following exercises, alternative proofs of the Cantor-Schröder-Bernstein Theorem 13.11 are presented.

Exercise 13.80. Suppose that $f\colon A \to B$ is injective and that $B \subset A$. Let $C_0 = A \setminus B$ and $C_{n+1} = f[C_n]$. Show that

$$h\colon A \to B, \qquad h(x) = \begin{cases} f(x) & \text{if } x \in \bigcup_n C_n \\ x & \text{otherwise} \end{cases}$$

is a bijection. Use this to infer the Cantor-Schröder-Bernstein Theorem.

Exercise 13.81. Given two injective functions $f\colon A \to B$ and $g\colon B \to A$ consider the sets

$$\begin{aligned} A_0 &= A & B_0 &= B \\ A_{n+1} &= g[B_n] & B_{n+1} &= f[A_n]. \end{aligned}$$

Show that $h\colon A \to B$ is a bijection:

$$h(x) = \begin{cases} g^{-1}(x) & \text{if } x \in \bigcup_n A_{2n+1} \setminus A_{2n+2}, \\ f(x) & \text{otherwise.} \end{cases}$$

Exercise 13.82. Suppose that $f\colon A \to B$ and $g\colon B \to A$ are injective functions and that $A \cap B = \emptyset$. If $a' = g(f(a))$ we say that a' is the immediate successor of a and that a is the immediate predecessor of a'. Fix $a \in A$. Define a_n with $n \geq 0$ by letting $a_0 = a$ and $a_{n+1} =$ the immediate successor of a_n. If the immediate predecessor of a exists, denote it with a_{-1}; if the immediate predecessor of a_{-1} exists, denote it with a_{-2}; if the immediate predecessor of a_{-2} exists, denote it with a_{-3}; and so on. Suppose a is such that there is a least $n < 0$ such that a_n is defined: then either

$$a_n \notin \operatorname{ran}(g) \tag{13.11a}$$

or else

$$a_n \in \operatorname{ran}(g) \text{ and } g^{-1}(a_n) \notin \operatorname{ran}(f) \tag{13.11b}$$

Let A_0 be the set of all a satisfying (13.11b). Check that $h\colon A \to B$ is a bijection

$$h(a) = \begin{cases} f(a) & \text{if } a \in A_0, \\ g^{-1}(a) & \text{otherwise.} \end{cases}$$

Exercise 13.83. In a commutative unitary semi-ring $(R, +, \cdot, 0, 1)$ (see Definition 9.10 on 241) define the relation $x \leq y \Leftrightarrow \exists z\, (x + z = y)$. Suppose $a \in R$ is such that

$$a + 1 = a \tag{13.12a}$$

$$x + y \leq x \Rightarrow y \cdot a \leq x. \tag{13.12b}$$

Show that:

(i) $x + y \leq x \Rightarrow x + y = x$;

(ii) $x \leq y \wedge y \leq x \Rightarrow x = y$, that is $\leq$ is a partial order on R;

(iii) The conjunction of (13.12a) and (13.12b) is equivalent to

$$x + y = x \Leftrightarrow y \cdot a \leq x. \tag{13.12c}$$

Moreover a is the unique element of R satisfying (13.12c).

(iv) $a + a = a$ and $a \cdot a = a$;

Exercise 13.84. (i) Show that if $X \uplus Y \precsim X$ then $Y \times \mathbb{N} \precsim X$.

(ii) Let R be the collection of all equivalence classes modulo the relation $\asymp$ of equipotence among sets. Use part (i) together with Exercise 13.83 to give an alternative proof of the Cantor-Schröder-Bernstein Theorem 13.11 and of Theorem 13.14.

Exercise 13.85. Show that:

(i) the series (13.8) converges to a real number in $[0; 1]$;

(ii) if $\forall i < n\ (x(i) = y(i))$ and $x(n) = 0$ and $y(n) = 1$, then $\Phi(x) < \Phi(y) \leq \Phi(x) + 3^{-n}$.

Exercise 13.86. Fix a natural number $b > 1$. The **base-b expansion** of $x \in [0, 1]$ is the sequence $(n_0, n_1, n_2, \dots) \in \{0, \dots, b-1\}^{\mathbb{N}}$ such that

$$x = \sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}}.$$

(i) Verify that if: $\forall i < k(n_i = m_i)$, $n_k = m_k + 1$, and $\forall i > k(n_i = 0 \wedge m_i = b - 1)$, then

$$\sum_{i=0}^{\infty} \frac{n_i}{b^{i+1}} = \sum_{i=0}^{\infty} \frac{m_i}{b^{i+1}} \in [0,1]$$

hence the base-b expansion of an $x \in [0,1]$ is not unique.

(ii) Show that if x admits an expansion that it is not eventually 0 or eventually $b-1$, then such expansion is unique.

(iii) Show that $E_{1/3}$, the Cantor set, is the set of reals in $[0;1]$ admitting an expansion in base 3 in which the digit 1 does not occur, and that $E_{1/3} = \operatorname{ran}(\Phi)$.

Exercise 13.87. Show that for any $a < b$ and any $0 < r < 1$ the set $E_r(a,b)$ is compact, with empty interior, $\lambda(E_r(a,b)) = 0$ and that there is a homeomorphism $f\colon [0;1] \to [a;b]$ such that $f[E_{1/3}] = E_r(a,b)$.

Exercise 13.88. We give an alternative proof of the fact that $\mathbb{R}$ is uncountable. Suppose $(0;1) = \{r_n \mid n \in \mathbb{N}\}$, and for each n let $d_{n,m} \in \{0,\dots,9\}$ be the mth digit of the decimal expansion of r_n. Argue that the real number $r \in (0;1)$ with decimal expansion $0.e_0e_1e_2\dots$ where $e_n = 2$ if $d_{n,n}$ is odd and $e_n = 3$ if $d_{n,n}$ is even, is not of the form r_m.

Notes and remarks

Set theory was invented by Cantor around 1870 in order to study a problem in the theory of trigonometric series posed by Riemann, see [**Coo93**].

The Cantor-Schröder-Bernstein Theorem 13.11 was stated (without proof) by Cantor in 1887 and in 1895 he obtained this result as corollary of the fact that every set can be well-ordered. Schröder published an incorrect proof in 1896, while Bernstein gave a correct proof a year later. In any case, the first correct proof of this result dates back to 1887 and it is due to Dedekind, but sadly his name is not associated to this result. The proof of Theorem 13.11 sketched in Exercise 13.11 is attributed to J. König, while Exercises 13.83 and 13.84 are form [**Cra11**].

The proof that $\mathscr{P}(\mathbb{N})$ is uncountable (Theorem 13.22) uses the celebrated diagonal method, a technique used (implicitly or explicitly) in many other proofs that $\mathbb{R}$ is uncountable. For a proof of this result that does not use the diagonal method see page 393.

Exercise 13.57 can be considerably strengthened: given A, B countable dense subsets of the real line, there is an auto-homeomorphism f of $\mathbb{R}$ mapping monotonically A onto B and such that f is the restriction of an entire function on the complex plane [**BS70, SR74**].

The result in Example 13.9 is form [**Thu82**]. The function in Example 13.10 is known McCarthy's 91 function, form the name of the computer scientist that defined it 1970. This function (like other generalizations introduced by Knuth) are of importance in theoretical computer science, in particular in the study of termination of programs [**Man03**]. Exercise 13.51 is from [**CW00**].

14. The axiom of choice, the well-ordering principle, and Zorn's lemma.

In mathematics it is customary to denote a set of objects by using some indexing method, so that a collection $\mathcal{A}$ of sets is often denoted by $\mathcal{A} = \{A_i \mid i \in I\}$, with I some set of indexes. Careless use of indexed symbols can hide delicate problems. For example, suppose $\mathcal{A}$ is a non-empty family of non-empty sets, that is to say: $\mathcal{A} = \{A_i \mid i \in I\}$ where $I \neq \emptyset$ and $\forall i \in I\,(A_i \neq \emptyset)$. It is tempting to restate the second clause as "there is $a_i \in A_i$", but writing "a_i" subsumes the existence of a function f assigning $f(i) = a_i \in A_i$ to each $i \in I$. In other words, we moved from "$\forall i \in I \exists x\,(x \in A_i)$" to "$\exists f\, \forall i \in I\,(f(i) \in A_i)$" swapping the order of quantifiers. The **axiom of choice**, in symbols AC, certifies the legitimacy of this swapping of quantifiers. Since $\{A_i \mid i \in I\} \subseteq \mathscr{P}(X)$ where $X = \bigcup_{i \in I} A_i$, it can be stated as follows:

(AC) For each set $X \neq \emptyset$ there is $f\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$ such that $\forall Y \subseteq X\,(\emptyset \neq Y \Rightarrow f(Y) \in Y)$.

The title *Axiom* refers to the fact that this a genuinely new principle, one that cannot be derived from the other axioms of set theory that will be introduced in Section V of the next Chapter. Another equivalent (Exercise 14.41) way of stating AC involves cartesian products:

(14.1) If $\{A_i \mid i \in I\} \neq \emptyset$ and $A_i \neq \emptyset$ for all $i \in I$, then $\bigtimes_{i \in I} A_i \neq \emptyset$.

The axiom of choice has an innocent-looking formulation, and many mathematicians consider it to be *obviously true.* Yet AC is equivalent to several, seemingly unrelated statements, some of which are far from being obvious.[5]

First we prove a technical result. Recall that a function on an ordered set $f\colon P \to P$ is progressive if $x \leq f(x)$ for all $x \in P$, and that $X^{\blacktriangledown} = \{y \in P \mid \forall x \in X\,(x \leq y)\}$, for any $X \subseteq P$.

Theorem 14.1. *Suppose $(P, \leq)$ is an ordered set and $G\colon \{C \subseteq P \mid C$ is a chain$\} \to P$ is such that $G(C) \in C^{\blacktriangledown}$. Then any progressive $f\colon P \to P$ has a fixed point.*

Proof. If $f\colon P \to P$ had no fixed points, then we define by induction on the ordinals an increasing sequence $p_\alpha \in P$, by letting $p_{\alpha+1} = f(p_\alpha)$ and $p_\lambda = G(\{p_\alpha \mid \alpha < \lambda\})$ for λ limit. Since there are more ordinals than points in P, a contradiction is reached. □

Remark 14.2. There is a sticky point in the proof above: we must be sure that there is no injective map from the collection of all ordinals into P, and this will follow easily from the axioms of set theory presented in Chapter V.

[5] The axiom of choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?—Jerry Bona

Theorem 14.3. *The following are equivalent:*

(a) ***Zorn's Lemma****: an ordered set such that every chain has an upper bound has a maximal element;*

(b) *the* ***well-ordering principle****: every set can be well-ordered;*

(c) *the axiom of choice.*

Proof. (a)⇒(b). Given a set X, we must find a well-order of X. Let

$$\mathcal{P} = \{(A, R) \mid A \subseteq X \wedge R \text{ is a well-order of } A\}$$

and for $(A, R), (B, S) \in \mathcal{P}$ set $(A, R) \trianglelefteq (B, S)$ if and only if $(A, R) = (B, S) \vee (A, R) \lhd (B, S)$ where

$$(A, R) \lhd (B, S) \Leftrightarrow A \subset B \wedge R \subset S \wedge \forall b \in B \setminus A\, \forall a \in A\, (a\ S\ b)$$

In other words: S extends R by placing the elements of $B \setminus A$ after those of A. Thus $(A, R) \lhd (B, S)$ if there is $b \in B$ such that $A = \operatorname{pred}(b, B; S)$. If $\{(A_i, R_i) \mid i \in I\}$ is a chain in $\mathcal{P}$ then $\bigcup_{i\in I} R_i$ well-orders $\bigcup_{i\in I} A_i$, so there is a maximal $(\bar{A}, \bar{R}) \in \mathcal{P}$. Towards a contradiction, suppose $\bar{A} \neq X$ and fix $b \in X \setminus \bar{A}$. Let $S = \bar{R} \cup \{(a, b) \mid a \in \bar{A}\} \cup \{(b, b)\}$. Then $(\bar{A} \cup \{b\}, S) \in \mathcal{P}$ and $(\bar{A}, \bar{R}) \lhd (\bar{A} \cup \{b\}, S)$, against the maximality of $(\bar{A}, \bar{R})$. Therefore $\bar{R}$ is a well-order of X.

(b)⇒(c). Given a non-empty X we must find a choice function $f \colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. Given a well-ordering $\preceq$ of X, set $f(Y)$ to be the $\preceq$-least element of Y.

(c)⇒(a). Let $(P, \leq)$ be an ordered set such that every chain has an upper bound, and towards a contradiction suppose it has no maximal elements. Let $\mathcal{C}$ be the collection of all non-empty chains of P. By hypothesis $C^{\blacktriangledown} \neq \emptyset$ for all $C \in \mathcal{C}$, so by AC let $G \colon \mathcal{C} \to P$, $G(C) \in C^{\blacktriangledown}$. By case assumption $A_x = \uparrow x \setminus \{x\} = \{y \in P \mid x < y\}$ is non-empty for all $x \in P$, so by AC there is $f \colon P \to P$ such that $f(x) \in A_x$. The function f is progressive, so it has a fixed point by Theorem 14.1. But $x < f(x)$ by construction: a contradiction. □

Lemma 14.4 (Krull). *Assuming* AC, *any ring*[6] *contains a maximal ideal.*

Proof. Let R be a ring and let $\mathcal{I} = \{I \subseteq R \mid I \text{ is a proper ideal of } R\}$. If $\mathcal{C} \subseteq \mathcal{I}$ is a chain, then $\bigcup \mathcal{C}$ is an ideal of R. Moreover $\bigcup \mathcal{C}$ is proper: if, towards a contradiction, $1 \in \bigcup \mathcal{C}$ then $1 \in I \in \mathcal{C}$ against the fact that every $I \in \mathcal{C} \subseteq \mathcal{I}$ is proper. Thus $\bigcup \mathcal{C} \in \mathcal{I}$. The assumption of Zorn's Lemma hold, so there is a maximal $I \in \mathcal{I}$. □

[6] The assumption that we are dealing with a *ring*, i.e. there is a multiplicative identity cannot be relaxed to *rng* or to *group*—see Exercise 14.39.

As the lattice of ideals of R containing a given proper ideal I is isomorphic to the lattice of ideals of R/I, we have

Corollary 14.5. *Assuming* AC*, a proper ideal of a ring is contained in a maximal ideal.*

Definition 14.6. The **Boolean prime ideal principle** (BPI) is the statement: any proper ideal in a Boolean algebra is contained in a prime ideal.

Krull's Lemma implies that every Boolean algebra has a maximal (that is: prime) ideal, so BPI follows from AC. By Exercise 14.40 BPI is equivalent to the seemingly weaker statement: every Boolean algebra has a prime ideal.

14.A. Tychonoff's theorem. Given functions $F_i\colon X \to Y_i$ $(i \in I)$ from a set X to topological spaces Y_i with topology $\mathcal{T}_i$, we can endow X with the **topology induced by the functions** F_i, namely the smallest topology that makes all F_i continuous. This topology exists since the lattice of topologies is complete, and

$$\mathcal{S} = \{F_i^{-1}[U] \mid i \in I \wedge U \in \mathcal{T}_i\}$$

is a subbase for it. A base for this topology is obtained by taking all finite intersections of sets in $\mathcal{S}$:

$$\{F_{i_1}^{-1}[U_{i_1}] \cap \cdots \cap F_{i_n}^{-1}[U_{i_n}] \mid i_1, \ldots, i_n \in I \wedge U_{i_j} \in \mathcal{T}_{i_j}\}.$$

When $X = \bigtimes_{i\in I} Y_i$ and $F_i\colon X \to Y_i$, $f \mapsto f(i)$, the resulting topology is called the **product topology** or **Tychonoff topology**. By construction the product topology is the coarsest topology on X that makes each projection $X \to Y_i$, $f \mapsto f(i)$ continuous. The basic open sets are of the form

$$(\bigtimes_{j=1}^{n} U_{i_j}) \times (\bigtimes_{i\in I\setminus\{i_1,\ldots,i_n\}} Y_i),$$

where $U_{i_j} \in \mathcal{T}_{i_j}$ and $i_1, \ldots, i_n \in I$. The **box topology** on $\bigtimes_{i\in I} Y_i$ is the topology generated by the sets $\{\bigtimes_{i\in I} U_i \mid \forall i \in I\,(U_i \text{ open in } Y_i)\}$. When I is finite the product and box topologies coincide, but when I is infinite the box topology is strictly finer than the product topology.

Example 14.7. Consider $\mathbb{R}^I = \bigtimes_{i\in I}\mathbb{R}$ with $I = \mathbb{R}$. The product topology is the topology of pointwise convergence—$f_n \to f$ if and only if $f_n(x) \to f(x)$ for all $x \in \mathbb{R}$. A basic open set is of the form

$$\{f \in \mathbb{R}^{\mathbb{R}} \mid f(x_i) \in U_i, \text{ for } i = 1, \ldots, n\}$$

with $\{x_1, \ldots, x_n\} \subseteq \mathbb{R}$ and the U_is open intervals of $\mathbb{R}$.

A basic open set in the topology of uniform convergence is of the form $\{f \in \mathbb{R}^{\mathbb{R}} \mid \forall x \in \mathbb{R}\,|f(x) - g(x)| < \varepsilon\}$ for some given $g \in \mathbb{R}^{\mathbb{R}}$ and $\varepsilon \in \mathbb{R}_{>0}$. The topology of uniform convergence is strictly finer than the pointwise topology. A basic open set in the topology of uniform convergence is open in the box topology, but not in the product topology. On the other hand an open set in the box topology need not be open in the topology of uniform convergence.

Let's agree that from now on the spaces $\bigtimes_{i\in I} Y_i$ and Y^I are endowed with the *product topology*, and the former is denoted by $\prod_{i\in I} Y_i$.

Theorem 14.8 (Tychonoff). *Assuming* AC*, the product of compact spaces is compact, that is: if X_i is compact for all $i \in I$, then $X = \prod_{i\in I} X_i$ is compact.*

We present two proofs of this theorem. The first one relies on the following result, known as the Alexander's subbase Lemma.

Lemma 14.9. *Assume* AC*. Suppose that a topological space X has a subbase $\mathcal{S}$ such that every open covering $\mathcal{V} \subseteq \mathcal{S}$ admits a finite subcovering. Then X is compact.*

Proof. Let $\mathcal{S}$ be as above. Since

$$\mathcal{B} = \{U_0 \cap \cdots \cap U_n \mid U_0, \ldots, U_n \in \mathcal{S} \wedge n \in \mathbb{N}\}$$

is a base, towards a contradiction we may assume that there is a covering $\mathcal{U}^* \subseteq \mathcal{B}$ of X that has no finite subcovering. Order by inclusion

$$\mathfrak{F} = \{\mathcal{U} \subseteq \mathcal{B} \mid \mathcal{U} \supseteq \mathcal{U}^* \text{ is a covering of } X \text{ without a finite subcovering}\}.$$

Claim 14.9.1. *If $\mathfrak{C} \subseteq \mathfrak{F}$ is a chain, then $\bigcup \mathfrak{C} \in \mathfrak{F}$.*

Proof of the Claim. $\bigcup \mathfrak{C}$ is a covering of X containing $\mathcal{U}^*$. If $\bigcup \mathfrak{C}$ had a subcovering $\{U_0, \ldots, U_n\}$, choose $\mathcal{U}_i \in \mathfrak{F}$ such that $U_i \in \mathcal{U}_i$. As $\mathfrak{C}$ is a chain, $\mathcal{U}_0 \cup \cdots \cup \mathcal{U}_n = \mathcal{U}_j$, for some suitable $j \leq n$. Thus $\mathcal{U}_j$ has a finite subcovering, against the fact that $\mathcal{U}_j \in \mathfrak{C} \subseteq \mathfrak{F}$. □

By Zorn's Lemma there is a maximal $\overline{\mathcal{U}} \in \mathfrak{F}$. Fix $U \in \overline{\mathcal{U}}$, and let $S_0, \ldots, S_n \in \mathcal{S}$ be such that $U = S_0 \cap \cdots \cap S_n$.

Claim 14.9.2. *$S_i \in \overline{\mathcal{U}}$, for some $i \leq n$.*

Proof of the Claim. If $S_i \notin \overline{\mathcal{U}}$, then by maximality there is a finite $\mathcal{U}_i \subseteq \overline{\mathcal{U}}$ such that $\mathcal{U}_i \cup \{S_i\}$ is a covering of X, that is $\mathcal{U}_i$ is a covering of $X \setminus S_i$. Therefore if $\{S_0, \ldots, S_n\} \cap \overline{\mathcal{U}} = \emptyset$, then $\mathcal{U}_0 \cup \cdots \cup \mathcal{U}_n \cup \{U\} \subseteq \overline{\mathcal{U}}$ would be a finite cover of X, against our assumption. □

Therefore for all $U \in \overline{\mathcal{U}}$ there is $V \in \overline{\mathcal{U}} \cap \mathcal{S}$ such that $U \subseteq V$. So $\overline{\mathcal{U}} \cap \mathcal{S}$ is a covering of X and $\overline{\mathcal{U}} \cap \mathcal{S} \subseteq \mathcal{S}$, so it has a finite subcovering $\mathcal{V}$; but $\mathcal{V} \subseteq \overline{\mathcal{U}}$, against our assumption that $\overline{\mathcal{U}}$ has no finite subcovering. □

First proof of Tychonoff's Theorem 14.8. Let $X = \prod_{i \in I} X_i$, and let $\mathcal{T}_i$ be a compact topology on X_i. The family

$$\mathcal{S} = \{U \times \mathsf{X}_{i \in I \setminus \{j\}} X_i \mid j \in I \wedge U \in \mathcal{T}_j\}$$

is a sub-base for the topology of X, so by Lemma 14.9 it is enough to show that any covering $\mathcal{U} \subseteq \mathcal{S}$ has a finite subcovering. Fix such $\mathcal{U}$, and let $\mathcal{V}_i = \{V \in \mathcal{T}_i \mid F_i^{-1}[V] \in \mathcal{U}\} \subseteq \mathscr{P}(X_i)$. Note that $\bigcup_{i \in I} \{F_i^{-1}[V] \mid V \in \mathcal{V}_i\} = \mathcal{U}$: the inclusion from left-to-right follows from the definition of $\mathcal{V}_i$, while the other inclusion follows from $\mathcal{U} \subseteq \mathcal{S}$. If $\mathcal{V}_j$ is a covering of X_j, for some j, then by compactness there would be a subcovering $\{V_0, \dots, V_n\} \subseteq \mathcal{V}_j$ and therefore $\{F_j^{-1}[V_k] \mid 0 \leq k \leq n\} \subseteq \mathcal{U}$ would be a finite subcovering of X. Thus, towards a contradiction, we may assume that $\mathcal{V}_i$ does not cover X_i, for any $i \in I$. Choose $x_i \in X_i \setminus \bigcup \mathcal{V}_i$ so that letting $f(i) = y_i$ we have that $f \in X \setminus \bigcup_{i \in I} \{F_i^{-1}[U] \mid U \in \mathcal{V}_i\} = X \setminus \bigcup \mathcal{U} = \emptyset$, a contradiction. □

14.B. Filters in topology. In this section X is a topological space, and $\mathcal{V}_x$ is the filter of the neighborhoods of $x \in X$.

Lemma 14.10. *For $\mathcal{F}$ a proper filter on X and $x \in X$, the following are equivalent:*

(a) $x \in \bigcap_{A \in \mathcal{F}} \mathrm{Cl}(A)$.

(b) $\forall A \in \mathcal{F} \, \forall U \in \mathcal{V}_x \, (A \cap U \neq \emptyset)$.

(c) $\mathcal{C} = \{A \cap U \mid A \in \mathcal{F}, U \in \mathcal{V}_x\}$ *is a family of non-empty sets, closed under finite intersections.*

(d) *There is a proper filter $\mathcal{G}$ extending $\mathcal{F} \cup \mathcal{V}_x$.*

Proof. It is immediate that (a), (b), and (c) are equivalent. If (c) holds, then $\mathcal{G} = \{G \subseteq X \mid \exists C \in \mathcal{C} \, (C \subseteq G)\}$ is a proper filter extending $\mathcal{F} \cup \mathcal{V}_x$, so (d) holds. Conversely any $\mathcal{G}$ as in (d) extends $\mathcal{C}$ so (c) holds. □

Definition 14.11. For $x \in X$ and $\mathcal{F}$ a proper filter on X, we say that

- x is a **cluster point for** $\mathcal{F}$ if any of the equivalent conditions of Lemma 14.10 is met;
- $\mathcal{F}$ **converges to** x if $\mathcal{V}_x \subseteq \mathcal{F}$.

Lemma 14.12. *Let $\mathcal{F}$ be a proper filter on X. If $\mathcal{F}$ converges to x, then x is a cluster point of $\mathcal{F}$. If $\mathcal{F}$ is an ultrafilter, then $\mathcal{F}$ converges to x if and only if x is a cluster point of $\mathcal{F}$.*

Proof. If $\mathcal{F}$ converges to x, then (b) of Lemma 14.10 shows that x is a cluster point of $\mathcal{F}$. Conversely, if x is a cluster point of the ultrafilter $\mathcal{F}$, then $\mathcal{F} \cup \mathcal{V}_x$ is contained in a proper filter, which must be $\mathcal{F}$ by maximality. Therefore $\mathcal{V}_x \subseteq \mathcal{F}$, that is $\mathcal{F}$ converges to x. □

Lemma 14.13. *X is Hausdorff if and only if each proper filter on X converges to at most one point.*

Proof. If X is Hausdorff then for distinct $x_0, x_1 \in X$ there are disjoint $U_i \in \mathcal{V}_{x_i}$, so that no proper filter can extend $\mathcal{V}_{x_0} \cup \mathcal{V}_{x_1}$, and hence cannot converge to both x_0, x_1. Conversely, if $\mathcal{F}$ is a proper filter converging to distinct x_0, x_1 then $\mathcal{V}_{x_0} \cup \mathcal{V}_{x_1} \subseteq \mathcal{F}$, so $\forall U_0 \in \mathcal{V}_{x_0} \forall U_1 \in \mathcal{V}_{x_1} (U_0 \cap U_1 \neq \emptyset)$, that is X is not Hausdorff. □

Filters can be used to characterize compactness.

Theorem 14.14. *X is compact if and only if every proper filter has at least one cluster point.*

Proof. Suppose X is compact and $\mathcal{F}$ is a proper filter. Since $\{\mathrm{Cl}(A) \mid A \in \mathcal{F}\}$ has the finite intersection property, then $\bigcap\{\mathrm{Cl}(A) \mid A \in \mathcal{F}\} \neq \emptyset$, and hence any of its elements are cluster points of $\mathcal{F}$.

Conversely, suppose $\mathcal{C}$ is a family of closed sets with the finite intersection property, and let us prove that $\bigcap \mathcal{C} \neq \emptyset$. Without loss of generality we may assume that $\mathcal{C}$ is closed under finite intersections. Let $\mathcal{F} = \{A \subseteq X \mid \exists C \in \mathcal{C}\, (C \subseteq A)\}$ be the filter generated by $\mathcal{C}$. Then $\emptyset \neq \bigcap\{\mathrm{Cl}(A) \mid A \in \mathcal{F}\} \subseteq \bigcap\{\mathrm{Cl}(A) \mid A \in \mathcal{C}\} = \bigcap \mathcal{C}$, that is X is compact. □

Corollary 14.15. *Assume* BPI. *A space X is compact if and only if each ultrafilter converges to at least one point. A space X is compact and Hausdorff if and only if each ultrafilter converges to exactly one point.*

Proof. If X is compact and $\mathcal{U}$ is an ultrafilter on X, then $\mathcal{U}$ has at least one cluster point, so $\mathcal{U}$ converges to at least one point. For the converse we apply Theorem 14.14: let $\mathcal{F}$ be a filter on X, and by BPI let $\mathcal{U} \supseteq \mathcal{F}$ be an ultrafilter. Then $\mathcal{U}$ converges to some x, so x is a cluster point for $\mathcal{F}$. □

The next result is Tychonoff's Theorem 14.8 stated in a more articulated form.

Theorem 14.16. *Suppose the X_i $(i \in I)$ are compact spaces, and let $X = \prod_{i \in I} X_i$. Then* AC *implies that X is compact. If the spaces X_i are* T_2 *then* AC *can be weakened to* BPI.

Proof. If $X = \emptyset$ then it is trivially compact, so we may assume otherwise. By Theorem 14.14 we must prove that every proper filter $\mathcal{F}$ on X has a cluster point. By BPI let $\mathcal{U}$ be an ultrafilter on X extending $\mathcal{F}$; it is enough to show that $\mathcal{U}$ converges to some $\bar{x}$ which therefore will be a cluster point of $\mathcal{F}$. Let $\pi_i \colon X \to X_i$, $f \mapsto f(i)$, be the projection on the i-th coordinate. Since $\mathcal{U}_i = \{\pi_i[A] \mid A \in \mathcal{U}\}$ is an ultrafilter on X_i, then by compactness

$$C_i = \{y \in X_i \mid \mathcal{U}_i \text{ converges to } y\}$$

is non-empty. By AC choose $\bar{x}_i \in C_i$, for all $i \in I$. As $\mathcal{V}_{\bar{x}_i} \subseteq \mathcal{U}_i$, then any basic open neighborhood of $\bar{x} \in X = \times_{i\in I} X_i$ is in $\mathcal{U}$, where $\bar{x}$ is the function $i \mapsto \bar{x}_i$. Therefore $\mathcal{U}$ converges to $\bar{x}$.

If the X_is are Hausdorff, then the C_is are singletons so picking $\bar{x}_i$ does not require choice. □

Tychonoff's theorem, even restricted to T_1 spaces, implies AC (Exercise 28.12). On other hand, the next result shows that Tychonoff's theorem for T_2 spaces yields the existence of prime ideals in any Boolean algebra (and hence BPI by Exercise 14.40).

Theorem 14.17. *Suppose that the product of finite, discrete spaces is compact. Then every Boolean algebra has a prime ideal.*

Proof. We must show that if B is a Boolean algebra, then there is a homomorphism $h \colon B \to \mathbf{2} = \{\mathbf{0}, \mathbf{1}\}$. Let $\mathcal{A}$ be the set of all Boolean finite subalgebras of B and let X_A be the set of all homomorphisms $h \colon A \to \mathbf{2}$ with $A \in \mathcal{A}$. Since A is finite then X_A is finite, and so is $Y_A = X_A \cup \{*\}$ where $*$ is a point that does not belong to any of the X_As. By assumption $\prod_{A\in\mathcal{A}} Y_A$ is compact, where each Y_A is endowed with the discrete topology. Moreover $A \mapsto *$ witnesses that $\times_{A\in\mathcal{A}} Y_A$ is non-empty. For $A \in \mathcal{A}$ consider the set

$$\begin{aligned} C_A &= \{f \in \times_{A\in\mathcal{A}} Y_A \mid f_A \neq *\} \\ &= \{f \in \times_{A\in\mathcal{A}} Y_A \mid f_A \colon A \to \mathbf{2} \text{ is a homomorphism}\} \end{aligned}$$

where f_A is $f(A)$. By Proposition 7.43 the set C_A is non-empty, and it is closed, in fact: clopen. Therefore $\prod_{A\in\mathcal{A}} X_A = \bigcap_{A\in\mathcal{A}} C_A$ is closed and hence compact. Moreover for any $A_1, \ldots, A_n \in \mathcal{A}$, the Boolean algebra A generated by $A_1 \cup \cdots \cup A_n$ is finite (Corollary 7.58), so belongs to $\mathcal{A}$, and $C_{A_1} \cap \cdots \cap C_{A_n} = C_A \neq \emptyset$, so by compactness $\prod_{A\in\mathcal{A}} X_A$ is non-empty. For $A_1 \subseteq A_2$ in $\mathcal{A}$ the set

$$F(A_1, A_2) = \{f \in \times_{A\in\mathcal{A}} X_A \mid f_{A_1} = f_{A_2} \restriction A_1\}$$

is closed (in fact: clopen) and non-empty, so by compactness

$$F = \bigcap \{F(A_1, A_2) \mid A_1 \subseteq A_2 \wedge A_1, A_2 \in \mathcal{A}\} \neq \emptyset.$$

Pick $f \in F$ and define $h \colon B \to \mathbf{2}$ as follows: for each $b \in B$ let

$$h(b) = f_A(b) \text{ for some/any } A \in \mathcal{A} \text{ such that } b \in A.$$

If $b \in A_1, A_2 \in \mathcal{A}$ pick $A_3 \in \mathcal{A}$ containing $A_1 \cup A_2$; as $f \in F(A_1, A_3) \cap F(A_2, A_3)$ then $f_{A_3} \restriction A_2 = f_{A_2}$ and $f_{A_3} \restriction A_1 = f_{A_1}$ so $f_{A_1}(b) = f_{A_3}(b) =$

$f_{A_2}(b)$, so that the definition of h is fully justified. Towards a contradiction, suppose h is not a homomorphism: then there are $b_1, b_2 \in B$ such that $h(b_1^*) \neq 1 - h(b_1)$ or $h(b_1 \curlywedge b_2) \neq \min(h(b_1), h(b_2))$. If A is the subalgebra of B generated by $\{b_1, b_2\}$, then $h \restriction A \in X_A$, so h respects the operations on b_1, b_2. □

14.C. Ultrafilters and Stone's theorem. The **Stone space**[7] of a Boolean algebra B is

$$\mathrm{St}(B) = \{U \subseteq B \mid U \text{ is an ultrafilter of } B\}.$$

In the proof of Theorem 7.47 we defined a function

$$\mathfrak{A}\colon B \to \mathscr{P}(\mathrm{At}(B)), \qquad \mathfrak{A}(b) = \{a \in \mathrm{At}(B) \mid a \leq b\}.$$

The map $\mathrm{At}(B) \to \{U \in \mathrm{St}(B) \mid U \text{ is principal}\}$, $a \mapsto \uparrow a$, is a bijection, so we can identify principal ultrafilters with atoms. If a Boolean algebra is atomic then every ultrafilter is principal, so, modulo this identification, $\mathfrak{A}\colon B \to \mathscr{P}(\mathrm{St}(B))$ becomes $\mathfrak{A}(b) = \{U \in \mathrm{St}(B) \mid b \in U\}$.

Theorem 14.18 (BPI). *$\mathfrak{U}\colon B \to \mathscr{P}(\mathrm{St}(B))$, $\mathfrak{U}(b) = \{U \in \mathrm{St}(B) \mid b \in U\}$ is an injective homomorphism of Boolean algebras.*

Proof. $\mathfrak{U}(\mathbf{0}_B) = \emptyset$ and $\mathfrak{U}(\mathbf{1}_B) = \mathrm{St}(B)$, since no ultrafilter contains $\mathbf{0}_B$ and every ultrafilter contains $\mathbf{1}_B$. Suppose $U \in \mathfrak{U}(b) \cup \mathfrak{U}(c)$: then either $b \in U$ or $c \in U$, and since $b, c \leq b \curlyvee c$ in either case we obtain that $b \curlyvee c \in U$, that is $U \in \mathfrak{U}(b \curlyvee c)$. Conversely, if $U \in \mathfrak{U}(b \curlyvee c)$, that is $b \curlyvee c \in U$, then either $b \in U$ or else $c \in U$, as U is prime, hence $U \in \mathfrak{U}(b) \cup \mathfrak{U}(c)$. It follows that

$$\forall b, c \in B\, (\mathfrak{U}(b \curlyvee c) = \mathfrak{U}(b) \cup \mathfrak{U}(c)).$$

No ultrafilter contains both b and b^*, hence $\mathfrak{U}(b) \cap \mathfrak{U}(b^*) = \emptyset$. Conversely, if $U \notin \mathfrak{U}(b)$, then $b^* \in U$ and hence $U \in \mathfrak{U}(b^*)$. Thus

$$\forall b \in B\, (\mathfrak{U}(b^*) = \mathrm{St}(B) \setminus \mathfrak{U}(b)).$$

For every $b \neq \mathbf{0}_B$, the set $\{c \in B \mid b \leq c\}$ is a proper filter that by BPI can be extended to an ultrafilter, so

$$\forall b \in B \setminus \{\mathbf{0}_B\}\, (\mathfrak{U}(b) \neq \emptyset).$$

It follows that $\ker \mathfrak{U} = \{\mathbf{0}_B\}$, hence $\mathfrak{U}$ is an injective homomorphism. □

An immediate corollary is **Stone's representation theorem** for Boolean algebras, a result extending Corollary 7.48(a).

Theorem 14.19 (BPI). *Every Boolean algebra is isomorphic to an algebra of sets.*

[7] In Section 25.B the set $\mathrm{St}(B)$ will be endowed with a topology, whence the name *space*.

14.D. The compactness theorem for propositional calculus. In Section 7.K.2 we constructed $\mathrm{Prop}(S)$ the set of all propositions with the letters in S, and defined what it means for a valuation $v\colon S \to \mathbf{2} = \{\mathbf{0}, \mathbf{1}\}$ to be a model for a set of propositions. We also defined an equivalence relation on $\mathrm{Prop}(S)$

$$\mathrm{p} \mathrel{\models\!\!\!\dashv} \mathrm{q} \Leftrightarrow \forall v\,(v(\mathrm{p}) = v(\mathrm{q}))$$

and showed that $\mathrm{Prop}(S)/{\models\!\!\!\dashv}$ is a Boolean algebra with maximum $\top$ the set of all tautologies and minimum $\bot$ the set of all propositional contradictions.

A set $\Gamma \subseteq \mathrm{Prop}(S)$ is **satisfiable** if it has a model, i.e. there is a valuation v such that $v(\mathrm{p}) = \mathbf{1}$ for all $\mathrm{p} \in \Gamma$; we say that it is **finitely satisfiable** if every finite subset of Γ is satisfiable. The following result, known as the **Compactness Theorem for propositional calculus**, is an immediate consequence of Theorem 4.46, but can be proved directly.

Theorem 14.20. *Assume* BPI. *If* $\Gamma \subseteq \mathrm{Prop}(S)$ *is finitely satisfiable, then it is satisfiable.*

Proof. The assumption on Γ amounts to say that $\bot \neq [\mathrm{p}_1 \wedge \ldots \wedge \mathrm{p}_n]$ for each $\mathrm{p}_1, \ldots, \mathrm{p}_n \in \Gamma$. In other words, the filter generated by $\{[\mathrm{p}] \mid \mathrm{p} \in \Gamma\}$ is proper. By BPI, let D be an ultrafilter extending this filter, and let $v\colon S \to \mathbf{2}$ defined by $v(\mathrm{p}) = \mathbf{1} \Leftrightarrow [\mathrm{p}] \in D$. Therefore $\mathrm{p} \in \Gamma$ implies that $[\mathrm{p}] \in F \subseteq D$, hence $v(\mathrm{p}) = \mathbf{1}$. Thus we have shown that Γ is satisfiable. □

Corollary 14.21. *Assume* BPI *and let* $\Gamma \subseteq \mathrm{Prop}(S)$. *If* $\Gamma \models \mathrm{p}$ *then* $\Delta \models \mathrm{p}$ *for some finite* $\Delta \subseteq \Gamma$.

Proof. Towards a contradiction, suppose that $\Delta \not\models \mathrm{p}$, for all finite $\Delta \subseteq \Gamma$, and let v_Δ be a function satisfying Δ but such that $v_\Delta(\mathrm{p}) = \mathbf{0}$. Then v_Δ satisfies $\Delta \cup \{\neg\mathrm{p}\}$. It follows that

$$\forall \Delta \subseteq \Gamma\,(\Delta \text{ finite } \Rightarrow \Delta \cup \{\neg\mathrm{p}\} \text{ is satisfiable})$$

and hence by the Compactness Theorem let v be a model of $\Gamma \cup \{\neg\mathrm{p}\}$. But, by assumption, every model of Γ must satisfy p: a contradiction. □

Compactness for propositional logic can be used to prove that every partial order can be extended to a total order.

Theorem 14.22 (BPI). *Every strict order* $\prec$ *on a set* X *can be extended to a strict total order* $\lhd$ *on* X, *that is*

$$\forall x, y \in X\,(x \prec y \Rightarrow x \lhd y)\,.$$

Proof. Let $(X, \prec)$ be a strict order: by Proposition 7.4 we may assume that X is infinite. Consider the propositional calculus $\mathrm{Prop}(S)$ where $S = X \times X$, and let $\Gamma \subseteq \mathrm{Prop}(S)$ be the set

$$\{\neg(x,x) \mid x \in X\} \cup \{(x,y) \vee (y,x) \mid x,y \in X, x \neq y\}$$
$$\cup \{\big((x,y) \wedge (y,z)\big) \Rightarrow (x,z) \mid x,y,z \in X\}.$$

The idea is that a propositional letter (x,y) asserts that x precedes y in a strict order on X. Any $v\colon S \to \mathbf{2}$ defines a relation $\lhd = \lhd_v$ on X

$$x \lhd y \Leftrightarrow v(\mathrm{A}) = \mathbf{1}, \text{ where } \mathrm{A} = (x,y) \in S$$

and, conversely, every binary relation $\lhd$ defines a function $v = v_\lhd$. Then v satisfies Γ if and only if $\lhd$ is a strict linear order on X. Moreover, if v satisfies $\Gamma \cup \Delta$, where $\Delta = \{(x,y) \mid x \prec y\}$, then the induced ordering $\lhd$ extends $\prec$. Thus, by Theorem 14.20, it is enough to show that $\Gamma \cup \Delta$ is finitely satisfiable.

Let $\Gamma_0 \cup \Delta_0$ be finite, with $\Gamma_0 \subseteq \Gamma$ and $\Delta_0 \subseteq \Delta$. Let X_0 be the set of all $x \in X$ occurring in some letter of $\Gamma_0 \cup \Delta_0$. The set X_0 is finite, and by Proposition 7.4 there is a strict total order $\lhd$ on X_0 extending $\prec$ on X_0. Let $v\colon S \to \{\mathbf{0}, \mathbf{1}\}$ be a function such that

$$\forall x,y \in X_0\ (v(x,y) = \mathbf{1} \Leftrightarrow x \lhd y)\,.$$

Let us check that $v(\mathrm{p}) = 1$ for all $\mathrm{p} \in \Gamma_0 \cup \Delta_0$. If $\mathrm{p} = \neg(x,x) \in \Gamma_0$, then $x \in X_0$, and the thesis follows at once from the failure of $x \lhd x$. If $\mathrm{p} = (x,y) \vee (y,x) \in \Gamma_0$ then $x \neq y$, hence either $x \lhd y$ or else $y \lhd x$, that is either $v(x,y) = \mathbf{1}$ or else $v(y,x) = \mathbf{1}$; thus $v(\mathrm{p}) = \mathbf{1}$. If $\mathrm{p} = ((x,y) \wedge (y,z)) \Rightarrow (x,z) \in \Gamma_0$ and, towards a contradiction, $v(\mathrm{p}) = \mathbf{0}$, then $v(x,y) = v(y,z) = \mathbf{1}$ and $v(x,z) = \mathbf{0}$, that is $x \lhd y$ and $y \lhd z$, but $\neg(x \lhd z)$: a contradiction. If $\mathrm{p} \in \Delta_0$ then $\mathrm{p} = (x,y)$ and $x \prec y$, so $x \lhd y$, whence $v(\mathrm{p}) = \mathbf{1}$. Therefore v satisfies $\Gamma_0 \cup \Delta_0$. As $\Gamma_0 \cup \Delta_0$ is arbitrary, it follows that $\Gamma \cup \Delta$ is finitely satisfiable, as required. □

Taking $\prec$ as the empty order on X we have:

Corollary 14.23 (BPI). *Every set can be totally ordered.*

Corollary 14.24. BPI *implies the axiom of choice for finite sets* $\mathsf{AC}^{\mathrm{Fin}}$*: if $\mathcal{A} \neq \emptyset$ is a family of non-empty finite sets, then there is a choice function on $\mathcal{A}$.*

Proof. Let $X = \bigcup \mathcal{A}$ and let $\leq$ be a linear order on X. If $A \in \mathcal{A}$, then A is a finite subset of X, so we can choose its least element. □

14.D.1. *Applications to combinatorics.* In 1935 Philip Hall proved the following result on bipartite graphs (Section 10), known as Hall matching theorem.

Theorem 14.25. *If $(A \uplus B, E)$ is a bipartite graph with A finite, and such that*

$$(14.2) \qquad a_1, \dots, a_n \in A \text{ distinct} \Rightarrow n \leq |\{b \in B \mid \exists i < n\,(b\ E\ a_i)\}| < \aleph_0.$$

Then there is an injective $f\colon A \to B$ such that $a\ E\ f(a)$ for all $a \in A$.

The finiteness assumption on A can be removed.

Theorem 14.26 (BPI). *Let $(A \uplus B, E)$ be a bipartite graph satisfying* (14.2). *Then there is an injective $f\colon A \to B$ such that $a\ E\ f(a)$ for all $a \in A$.*

Proof. Consider the propositional calculus $\mathrm{Prop}(A \times B)$. For each $a \in A$ the set $\{b \in B \mid a\ E\ b\}$ is finite of size $n(a) \geq 1$, so by Corollary 14.24 we can fix an enumeration $(b^a_1, \dots, b^a_{n(a)})$ of this set. For distinct $a, a' \in A$ and $b \in B$ let $\mathrm{p}_a, \mathrm{q}_{a,a',b} \in \mathrm{Prop}(A \times B)$ be defined by

$$\begin{aligned}\mathrm{p}_a &= \big(\bigvee\nolimits_{1 \leq i \leq n(a)} (a, b^a_i)\big) \wedge \big(\bigwedge\nolimits_{1 \leq i < j \leq n(a)} \neg \big((a, b^a_i) \wedge (a, b^a_j)\big)\big),\\ \mathrm{q}_{a,a',b} &= \neg[(a,b) \wedge (a', b)].\end{aligned}$$

If v is a valuation such that $v(\mathrm{p}_a) = \mathbf{1}$, then there is a unique $b \in B$ such that $a\ E\ b$ and $v(a,b) = \mathbf{1}$; similarly, if $v(\mathrm{q}_{a,a',b}) = \mathbf{1}$ then $v(a,b) = \mathbf{1}$ and $v(a', b) = \mathbf{1}$ cannot both be true. By Theorem 14.25 the set $\Phi \subseteq \mathrm{Prop}(A \times B)$ of all p_as and $\mathrm{q}_{a,a',b}$s is finitely satisfiable, so by Theorem 14.20, there is a valuation v satisfying Γ. Then set $f(a)$ to be the unique b such that $v(a, b) = \mathbf{1}$. □

Theorem 14.27 (BPI). *Suppose $F\colon A \to \mathscr{P}(B)$ is such that $F(a)$ is finite for any $a \in A$. If $|F(a_1) \cup \dots \cup F(a_n)| \geq n$ for any distinct $a_1, \dots, a_n \in A$, then there is an injective $f\colon A \to B$ such that $f(a) \in F(a)$ for all $a \in A$.*

Proof. Without loss of generality we may assume that $A \cap B = \emptyset$, so consider the bipartite graph on $A \cup B$ with $a\ E\ b \Leftrightarrow b \in F(a)$. The result follows from Theorem 14.26. □

Every finitely generated vector space has a basis, and any two basis are in bijection. The axiom of choice implies that this result holds for arbitrary vector spaces.

Proposition 14.28. *Let V be a vector space over a field $\Bbbk$.*

(a) AC *implies that V has a basis.*

(b) BPI *implies that if $A, B \subseteq V$ are bases, then $A \asymp B$.*

Proof. (a) Any maximal linearly independent set is a basis, so apply Zorn's Lemma to the family $\{X \subseteq V \mid X \text{ is linearly independent}\}$ ordered under inclusion.

(b) As B is a basis of V, any non-zero $\mathbf{v}$ can be written in a unique way as $\mathbf{v} = \alpha_1 \mathbf{b}_1 + \cdots + \alpha_n \mathbf{b}_n$, with $\mathbf{b}_1, \dots, \mathbf{b}_n \in B$ and $\alpha_1, \dots, \alpha_n \in \Bbbk \setminus \{0_{\Bbbk}\}$. Thus for any $\mathbf{a} \in A$ there is a non-empty finite $F(\mathbf{a}) \supseteq B$ such that $\mathbf{a}$ is a linear combination of the vectors in $F(\mathbf{a})$ with non-zero scalars. By basic linear algebra $F(\mathbf{a}_1) \cup \cdots \cup F(\mathbf{a}_n)$ has size $\geq n$, so $A \precsim B$ by Theorem 14.27. Similarly $B \precsim A$ so the result follows by the Cantor-Schröder-Bernstein Theorem. □

A **transcendence basis** for a field a maximal, algebraically independent set (Definition 11.43). By BPI every field $\Bbbk$ can be embedded in an algebraically closed field $\overline{\Bbbk}$ (Theorem **??**), and the intersection $\Bbbk^{\mathrm{alg}}$ of all algebraically closed subfields of $\overline{\Bbbk}$ containing $\Bbbk$ is called the **algebraic closure** of $\Bbbk$. Therefore an algebraically independent set B is a basis if and only if $\Bbbk^{\mathrm{alg}}$ is the smallest algebraically closed field containing the prime subfield and B. In analogy with Proposition 14.28 we have

Proposition 14.29. *If $\Bbbk$ is a field,*

(a) AC *implies that $\Bbbk$ has a transcendence basis.*

(b) BPI *implies that any two transcendence bases are in bijection.*

14.E. Countable choices. The axiom of choice has many important applications throughout mathematics (see Section 28) but it has also a few counterintuitive consequences, involving subsets on $\mathbb{R}$ that most mathematicians would consider to be pathological (see Section 28.B). For this reason it is customary to keep close tabs on the applications of this axiom. Several weakenings of AC have been introduced. One of these is the **axiom of countable choices** AC_ω, stating that for any family $\{A_n \mid n \in \mathbb{N}\}$ of non-empty sets, there is a sequence $(a_n)_n$ such that $a_n \in A_n$ for all n.

Theorem 14.30. *Assume AC_ω. If X is infinite then $\mathbb{N} \precsim X$.*

Proof. As X is infinite, $\emptyset \neq \mathcal{G}_n \stackrel{\text{def}}{=} \{g \mid g \colon n \rightarrowtail X\}$ for every $n \in \mathbb{N}$. By AC_ω fix $g_n \in \mathcal{G}_n$. Define by recursion $f \colon \mathbb{N} \to X$

$$\begin{cases} f(0) = g_1(0) \\ f(n+1) = g_{n+2}(i) \end{cases}$$

where $i = \min\{k \leq n+1 \mid g_{n+2}(k) \notin \{f(0), \dots, f(n)\}\}$. Since $\operatorname{ran}(g_{n+2})$ has $n+2$ elements, at least one of these does not belong to $\{f(0), \dots, f(n)\}$ hence f is well defined. A simple induction shows that f is injective. □

Thus AC_ω and Proposition 13.12 imply that a set is infinite if and only if it is in bijection with a proper subset of itself. This is the property Dedekind used to define infinity, hence sets that are in bijection with a proper subset of themselves are called **Dedekind-infinite**; a set which is not in bijection with a proper subset of itself is called **Dedekind-finite**.

Theorem 14.31. *Assume* AC_ω. *If* $X_n \precsim \mathbb{N}$ *for all* $n \in \mathbb{N}$, *then* $\bigcup_{n\in\mathbb{N}} X_n \precsim \mathbb{N}$, *that is to say: countable union of countable sets is countable.*

Proof. Let $N\colon \bigcup_n X_n \to \mathbb{N}$, $x \mapsto \min\{n \in \mathbb{N} \mid x \in X_n\}$. By AC_ω choose $f_n\colon X_n \rightarrowtail \mathbb{N}$ and define $F\colon \bigcup_n X_n \rightarrowtail \mathbb{N}\times\mathbb{N}$, $F(x) = (N(x), f_{N(x)}(x))$. □

Remark 14.32. Theorems 14.30 and 14.31 are not provable without choice. For example it is consistent that there exist infinite sets that are Dedekind-finite, i.e. sets X such that $n \precsim X$ for all $n \in \mathbb{N}$, yet X does not contain a sequence $(x_n)_n$ of distinct elements. Such sets can be taken to be subset of $\mathbb{R}$. No infinite, Dedekind-finite set can be well-orderable.

Similarly, in the absence of choice, the countable union of countable sets need not be countable. In fact in absence of choice, it may happen that $\mathbb{R}$ is the countable union of countable sets!

The principle $\mathsf{AC}_\omega(\mathbb{R})$ is obtained by requiring that $A_n \subseteq \mathbb{R}$ in the statement of AC_ω. It is used even in basic calculus courses, for example when proving the equivalence between continuity and sequential continuity. Recall that $f\colon \mathbb{R}\to\mathbb{R}$ is sequentially continuous in $\bar{x}$ if $f(x_n) \to f(\bar{x})$ for all sequences $x_n \to \bar{x}$. Every continuous function is continuous is sequentially continuous and by $\mathsf{AC}_\omega(\mathbb{R})$ it can be shown that

(14.3) *For every* $f\colon \mathbb{R}\to\mathbb{R}$ *and all* $\bar{x} \in \mathbb{R}$, *if* f *is sequentially continuous in* $\bar{x}$, *then* f *is continuous in* $\bar{x}$.

In fact (14.3) is *equivalent* to $\mathsf{AC}_\omega(\mathbb{R})$—see Exercise 28.19. On the other hand its global version:

(14.4) *For all* $f\colon \mathbb{R}\to\mathbb{R}$, *if* f *is sequentially continuous in* every *point, then it is continuous on* $\mathbb{R}$

is provable without choice [**Her06**, pag. 30]. This is not surprising: statement (14.3) is of the form

$$\forall f\, \forall \bar{x}\, \left(\varphi_{\text{seq. cont.}}(f,\bar{x}) \Rightarrow \varphi_{\text{cont.}}(f,\bar{x})\right)$$

and it is stronger than (14.4) which is of the form

$$\forall f\, \left(\forall \bar{x}\, \varphi_{\text{seq. cont.}}(f,\bar{x}) \Rightarrow \forall \bar{x}\, \varphi_{\text{cont.}}(f,\bar{x})\right).$$

Another subtle application of $\mathsf{AC}_\omega(\mathbb{R})$ occurs in the construction of the Lebesgue measure (Section 26.D). One of the first results proved in measure theory is that the union of countably many null sets is null, and since countable sets are null, this implies that $\mathbb{R}$ cannot be the countable union of countable sets. But as we observed this (highly pathological!) situation could occur if AC_ω is eschewed entirely, so this shows that $\mathsf{AC}_\omega(\mathbb{R})$ is indeed crucial for having a decent theory of integration.

14.F. What exactly is a cardinal number? The definition of cardinality of a set given in Section 13.C is similar to the notion of ordinal number presented in Section 13.A, $|X|$ is $\{Y \mid Y \asymp X\}$, the equivalence class of X under the equipotence relation. Many of the shortcomings of the naïve definition of ordinals highlighted in Section 13.C.2 can be repeated for the concept of cardinality.

Let us assume for the rest of this section the axiom of choice. As every set can be well-ordered, we can define the cardinality of X to be the smallest ordinal $|X|$ in bijection with it. An ordinal that is not in bijection with any smaller ordinal is called a **cardinal**, so under AC the cardinality of any set is a cardinal. Every natural number is a cardinal, and so is ω, which we denote as $\aleph_0$. The smallest uncountable ordinal is ω_1, which is also denoted by $\aleph_1$; more generally, $\aleph_{n+1}$ is the smallest cardinal bigger than $\aleph_n$.

The **cardinality of the continuum** is the cardinality of $\mathbb{R}$, or equivalently, of any set in bijection with it, like $\mathscr{P}(\omega)$ or $2^{\mathbb{N}}$. By Theorem 13.22 the cardinality of the continuum is uncountable, that is $2^{\aleph_0} \geq \aleph_1$. Cantor conjectured that inequality could be replaced by an equality, and dubbed the ensuing statement the **continuum hypothesis**

$$(\mathsf{CH}) \qquad 2^{\aleph_0} = \aleph_1 .$$

The formula above asserts that the type of infinity of the real numbers is the smallest kind of uncountable infinity, so it can be restated as

$$\forall X \subseteq \mathbb{R} \left(|X| \leq \aleph_0 \vee X \asymp R \right).$$

(Clearly in the formula above the set $\mathbb{R}$ can be replaced by any other set equipotent with it.) This is a reasonable sounding statement, since for all sets $X \subseteq \mathbb{R}$ encountered in practice, either X is countable or else X is in bijection with $\mathbb{R}$—Cantor proved this when X is open or closed, and the result was later extended to all Borel sets by Alexandroff. Despite its innocent look, the continuum hypothesis cannot be proved nor disproved from the usual axioms system for set theory—see Sections 39 and 41.

14.F.1. *Equivalents of the continuum hypothesis.* The continuum hypothesis has many applications throughout mathematics. It can be used to prove facts in analysis, geometry, algebra, ..., that otherwise would not be provable. Some of these facts turn out to be equivalent to CH itself, for example Theorem 14.33 and Corollary 14.38.

Theorem 14.33 (Erdős). CH *is equivalent to: there is an uncountable family $\mathcal{F}$ of entire functions such that for all $z \in \mathbb{C}$ the set $\{f(z) \mid f \in \mathcal{F}\}$ is countable.*

It is convenient to restate this result in a slightly more general form. Let κ be an infinite cardinal. A family $\mathcal{F}$ of entire functions is κ-small iff $|\{f(z) \mid f \in \mathcal{F}\}| < \kappa$ for all $z \in \mathbb{C}$. If $|\mathcal{F}| < \kappa$ then $\mathcal{F}$ is κ-small, and Theorem 14.33 says that $\neg\mathsf{CH}$ is equivalent to the fact that every ω_1-small family is countable, and thus follows from the next two propositions.

Proposition 14.34. *If $\kappa < 2^{\aleph_0}$ then every κ-small family is of cardinality $< \kappa$. In particular: $\omega_1 < 2^{\aleph_0}$ implies that every ω_1-small family is countable.*

Proof. Towards a contradiction, suppose $\mathcal{F}$ is κ-small and $|\mathcal{F}| \geq \kappa$. By passing to a subfamily if needed, we may assume that $\{f_\alpha \mid \alpha < \kappa\}$ is an enumeration without repetitions of $\mathcal{F}$. For each $\alpha < \beta < \kappa$ let $E_{\alpha,\beta} = \{z \in \mathbb{C} \mid f_\alpha(z) = f_\beta(z)\}$. By standard facts on holomorphic functions $E_{\alpha,\beta} \cap \{z \in \mathbb{C} \mid |z| \leq n\}$ is finite, for all $n \in \mathbb{N}$, so $E_{\alpha,\beta}$ is countable. Therefore $\bigcup_{\alpha<\beta<\kappa} E_{\alpha,\beta}$ has size $\leq \kappa < |\mathbb{C}|$. Let $w \in \mathbb{C} \setminus \bigcup_{\alpha<\beta<\kappa} E_{\alpha,\beta}$. Then the values $f_\alpha(w)$ are all distinct, against κ-smallness. □

Corollary 14.35. *If $\{f(z) \mid f \in \mathcal{F}\}$ is finite for all $z \in \mathbb{C}$ then $\mathcal{F}$ is finite.*

Proposition 14.36. CH *implies that there is an uncountable family of entire functions that is ω_1-small.*

Proof. Fix $\{z_\alpha \mid \alpha < \omega_1\}$ an enumeration without repetitions of $\mathbb{C}$. We construct entire functions f_α with $\alpha < \omega_1$ so that

$$(*) \qquad \alpha < \beta \Rightarrow f_\beta(z_\alpha) \in \mathbb{Q} + \mathrm{i}\mathbb{Q}$$

Given any $z \in \mathbb{C}$, let $\alpha < \omega_1$ such that $z = z_\alpha$: then $\{f_\beta(z_\alpha) \mid \beta < \omega_1\} \subseteq \{f_\beta(z_\alpha) \mid \beta \leq \alpha\} \cup \mathbb{Q} + \mathrm{i}\mathbb{Q}$. Therefore $\{f_\alpha \mid \alpha < \omega_1\}$ is ω_1-small.

The construction of the f_α is by recursion. Let f_0 be any arbitrary entire function. Suppose $0 < \beta < \omega_1$ and that $\{f_\alpha \mid \alpha < \beta\}$ has been constructed. Let $\nu \ni n \mapsto g_n$ and $\nu \ni n \mapsto w_n$, where $\nu \leq \omega$, be some enumeration without repetitions of the sets $\{f_\alpha \mid \alpha < \beta\}$ and $\{z_\alpha \mid \alpha < \beta\}$. To be more specific, if $\alpha \leq \omega$ take $\nu = \alpha$, and $g_n = f_n$ and $w_n = z_n$; if $\omega < \alpha$ fix some bijection between α and ω and use it to relabel the functions and points. We construct f_β such that

$$\forall n \in \omega \left(f_\beta(w_n) \in \mathbb{Q} + \mathrm{i}\mathbb{Q} \wedge f_\beta(w_n) \neq g_n(w_n) \right)$$

so that $(*)$ holds, and f_β differs from all f_α with $\alpha < \beta$. The following elementary fact will come handy.

Claim 14.36.1. *For every $a, b \in \mathbb{C}$ with $b \neq 0$, and for every ε positive and real, there is $c \in \mathbb{C}$ such that $a + bc \in \mathbb{Q} + \mathrm{i}\mathbb{Q}$ and $|c| < \varepsilon$.*

Proof. The map $h \colon \mathbb{C} \to \mathbb{C}$, $z \mapsto a + bz$ is a homeomorphism. By density choose $d \in \mathbb{Q} + \mathrm{i}\mathbb{Q} \cap \{w \in \mathbb{C} \mid |w - a| < \varepsilon|b|\}$. Then $c = h^{-1}(d)$ is as required. □

The function f_β will be of the form

$$\begin{aligned} f_\beta(z) &= \textstyle\sum_{i<\nu} c_i(\prod_{j<i}(z-w_j)) \\ &= c_0 + c_1(z-w_0) + c_2(z-w_0)(z-w_1) + \cdots \end{aligned}$$

with $|c_n| < 2^{-n}$ so that the series converges and f_β is indeed an entire function. Note that for every $n < \nu$,

$$f_\beta(w_n) = \textstyle\sum_{i \leq n} c_i(\prod_{j<i}(z-w_j)),$$

since all terms $\prod_{j<i}(w_n - w_j)$ are zero when $i > n$. We construct inductively the c_ns so that

$$f_\beta(w_n) \in \mathbb{Q} + \mathrm{i}\mathbb{Q} \setminus \{f_\beta(w_m) \mid m < n\}$$

so that $(*)$ holds. This can be done since the value $f_\beta(w_m)$ does not depend on c_n when $m < n$. Let $c_0 = 0$, and suppose $c_0, \ldots, c_n$ have been constructed. As

$$f_\beta(w_{n+1}) = \underbrace{\textstyle\sum_{i=0}^{n} c_i \prod_{j<i}(w_{n+1} - w_j)}_{a} + c_{n+1} \underbrace{(w_{n+1} - w_0) \cdots (w_{n+1} - w_n)}_{b}$$

we can apply the Claim to find the desired c_{n+1}. □

The next result shows that the continuum hypothesis is equivalent to a statement in elementary geometry. In order to simplify the notation, it is convenient to introduce the following definition. For S an arbitrary set, a line in S^n parallel to the i-th direction, with $i < n$, is a set of the form

$$\{(a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{n-1}) \in S^n \mid x \in S\}$$

for some $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n-1} \in S$. Thus in $\mathbb{R}^2$ a line parallel to the 0-th direction is an horizontal line, i.e. parallel to the x-axis, and a line parallel to the 1-st direction is an vertical line, i.e. parallel to the y-axis.

Theorem 14.37 (Sierpiński)**.** *For every set S, the following are equivalent:*

(a) $|S| \leq \omega_1$.

(b) *There is a partition $S^2 = A_0 \cup A_1$ such that for $i = 0, 1$ every line parallel to the i-th direction intersects A_i in a* countable *set.*

(c) *There is a partition $S^3 = A_0 \cup A_1 \cup A_2$ such that for $i = 0, 1, 2$ every line parallel to the i-th direction intersects A_i in a* finite *set.*

Proof. (a)⇔(b) Let $\trianglelefteq$ be a well-order of S of order type $\leq \omega_1$, and let A_0 be $\trianglelefteq$ and A_1 its complement, that is $A_1 = \{(x, y) \in S^2 \mid y \triangleleft x\}$. A line parallel to the 0-th direction is the set of $\trianglelefteq$-predecessors of some $s \in S$, hence it is countable.

Conversely, suppose there is a partition as in the statement, and towards a contradiction suppose $|S| > \omega_1$. Let $Y \subset S$ be a set of size ω_1. As the vertical sections of A_1 are countable, for every $x \in S$ there is $f(x) \in Y$ such that $(x, f(x)) \notin A_1$, and therefore $(x, f(x)) \in A_0$. As $|S| > |Y| = \omega_1$, there is an uncountable $X \subseteq S$ such that the map $x \mapsto f(x)$ is constant on X, and let $y \in Y$ be this constant value. Then $X \subseteq \{x \in S \mid (x, y) \in A_0\}$, against the assumption that the horizontal sections of A_0 are countable.

(a)⇔(c) Suppose $S = \{r_\alpha \mid \alpha < \omega_1\}$: we must construct A_0, A_1, A_2 as in part (c). For each $\gamma < \omega_1$ choose an injection $j_\gamma \colon \gamma + 1 \to \omega$. Given $(x_0, x_1, x_2) \in S^3$, let $\alpha, \beta, \gamma \in \omega_1$ such that $\{x_0, x_1, x_2\} = \{r_\alpha, r_\beta, r_\gamma\}$, and without loss of generality we may assume that $\alpha, \beta \leq \gamma$ and that $j_\gamma(\alpha) \leq j_\gamma(\beta)$. For $i < 3$ define

$$A_i = \{(x_0, x_1, x_2) \in S^3 \mid i \text{ is least such that } r_\alpha = x_i\}$$

This defines a partition of S^3 in three disjoint sets A_0, A_1, A_2, so it is enough to show verify the finiteness condition. Consider a line L parallel to the 0-th axis, say $L = \{(x, b, c) \mid x \in S\}$. If $(x, b, c) \in A_0$, then $x = r_\alpha$ and $\{b, c\} = \{r_\beta, r_\gamma\}$, for some β, γ such that $\alpha, \beta \leq \gamma$ and $j_\gamma(\alpha) \leq j_\gamma(\beta)$. Since $j_\gamma(\beta) \in \omega$, there are finitely many possibilities for $j_\gamma(\alpha)$ and hence for x. Thus $L \cap A_0$ is finite. The case for A_1 and A_2 is similar.

Conversely suppose there is a partition $S^3 = A_0 \cup A_1 \cup A_2$ as in part (c), and that $|S| \geq \aleph_2$. Fix $U, V, W \subseteq S$ of size $\aleph_0, \aleph_1, \aleph_2$, respectively. For each $(u, v) \in U \times V$ the set $B(u, v) = \{z \in S \mid (u, v, z) \in A_2\}$ is finite, and as $\bigcup_{(u,v) \in U \times V} B(u, v)$ is of size $\leq \aleph_1$, there is $c \in W$ such that

$$\forall (u, v) \in U \times V\ [(u, v, c) \notin A_2].$$

For each $u \in U$ the set $B'(u) = \{y \in S \mid (u, y, c) \in A_1\}$ is finite, so $\bigcup_{u \in U} B'(u)$ is countable, so there is $b \in V$ such that

$$\forall u \in U\ [(u, b, c) \notin A_1].$$

As $\{x \in S \mid (x, b, c) \in A_0\}$ is finite, then there is $a \in U$ such $(a, b, c) \notin A_0$. By construction (a, b, c) cannot belong to A_1 or to A_2, contradicting the fact that $A_0 \cup A_1 \cup A_2 = S^3$. □

Corollary 14.38. CH *is equivalent to either of the following:*

- *There is a partition of the* $\mathbb{R}^2 = A_0 \cup A_1$ *such that for* $i = 0, 1$ *every line parallel to the i-th direction intersects* A_i *in a* countable *set.*
- *There is a partition of* $\mathbb{R}^3 = A_0 \cup A_1 \cup A_2$ *such that for* $i = 0, 1, 2$ *every line parallel to the i-th direction intersects* A_i *in a* finite *set.*

The proof of Theorem 14.37 shows that $|S| \leq \aleph_0$ if and only if there is a partition $S^2 = A_0 \cup A_1$ such that every line parallel to the i-th direction has finite intersection with A_i, so we cannot replace *countable* with *finite* in part (b) of Theorem 14.37. One could ask what is so special about dimension

2 and 3, and the fact that the intersections be finite or countable. It turns put that positing the existence of a partition of $\mathbb{R}^3 = A_0 \cup A_1 \cup A_2$ such that every line parallel to i-direction has *countable* intersection with A_i $(i < 3)$ is equivalent to positing the existence of a partition of $\mathbb{R}^4 = A_0 \cup A_1 \cup A_2 \cup A_3$ such that every line parallel to the i-th direction has *finite* intersection with A_i $(i < 4)$, and either statement is equivalent to $2^{\aleph_0} \leq \aleph_2$. More generally, by a theorem of Sikorski $|S| \leq \aleph_n$ is equivalent to either one of the following statements:

- there is a partition of $S^{n+2} = A_0 \cup \cdots \cup A_{n+1}$ such that every line parallel to the i-th direction has *finite* intersection with A_i;
- there is a partition of $S^{n+1} = A_0 \cup \cdots \cup A_n$ such that every line parallel to the i-th direction has *countable* intersection with A_i.

14.G. From naïve set theory to axiomatic set theory. As we have remarked before, the definition of ordinals and cardinals as quotients modulo suitable equivalence relations yield huge equivalence classes. In naïve set theory, that is to say: in the elementary, non-axiomatic presentations of set theory, as usually presented in mathematics textbooks, these questions are not usually addressed. But lighthearted use of very large collections of objects is prone to serious problems that hinder the technical development of the discipline. These problems show up as *antinomies* or *paradoxes*. Let us see two of these, one related to the notion of ordinal number, the second to cardinality.

14.G.1. *Burali-Forti's paradox.* By Proposition 13.8, $(\mathrm{Ord}, \leq)$ is a well-order, with Ord the set of all ordinals. Note that if $(P, \leq_P)$ is a well-order of order type $\alpha \in \mathrm{Ord}$, then P is isomorphic to $\{\beta \in \mathrm{Ord} \mid \beta < \alpha\}$ via the map that sends x to the order type of the initial segment $\{y \in P \mid y <_P x\}$. Therefore, if $\Omega \in \mathrm{Ord}$ is the order type of $(\mathrm{Ord}, \leq)$, then the well-order Ord is isomorphic to its initial segment $\{\alpha \in \mathrm{Ord} \mid \alpha < \Omega\}$, against Corollary 13.6.

14.G.2. *Cantor's paradox.* If X is the set of all sets, then $\mathscr{P}(X) \subseteq X$, hence there should be a surjection from X onto $\mathscr{P}(X)$, against Theorem 13.22.

As the unconsidered usage of very large collections (the set of all sets, the set of all ordinals,. . .) leads to logical contradictions, it is necessary to put on firm grounds the mathematical constructions seen in the previous pages, starting from set theory itself. The plan is to sort the aggregates of objects into two regions: the *small collection* called *sets* and *large collections* called *proper classes*. The first region is inhabited by the sets usually encountered in mathematics ($\mathbb{N}$, $\mathbb{R}$, differentiable manifolds, etc.), while the dangerously large collections (the set of all sets, the set of all ordinals, . . .) will be relegated to the second region. In Chapter V we shall see how axiomatic set theory delimits the range of the notion of set, wiping out these logical antinomies.

14.G.3. *A crash course in set theory.* If the reader is too impatient to see what will be happen in the next Chapter (or, more likely, if the reader is too lazy to read it), we list now the main ideas.

Theorem 13.14 says that $\omega \times \omega$ is in bijection with ω, and this fact generalizes to all infinite cardinals, that is (Theorem 18.28)

$$\boxed{\text{If } \kappa \text{ is an infinite cardinal, then } \kappa \times \kappa \asymp \kappa.}$$

For A a well-orderable set, let $|A|$ be the smallest ordinal α in bijection with A. Thus assuming the axiom of choice, the notion of 'cardinality of a set' is well-defined. If we relinquish AC, the definition cardinality requires some further notions in set theory (Section 20.C). The operations on cardinals are defined as above, that is $\kappa + \lambda$ is the cardinal in bijection with the (well-orderable) set $\kappa \uplus \lambda$, and $\kappa \cdot \lambda$ is the cardinal in bijection with the (well-orderable) set $\kappa \times \lambda$. Thus if κ and λ are infinite cardinals

$$\boxed{\kappa + \lambda = \kappa \cdot \lambda = \max \{\kappa, \lambda\}.}$$

Also (13.6) can be generalized to all infinite cardinals (Theorem 18.31)

$$\boxed{|X| = \kappa \geq \aleph_0 \Rightarrow |X^{<\mathbb{N}}| = \kappa}$$

that is: if X is infinite and well-orderable then $X \asymp X^{<\mathbb{N}}$. If we do not assume some form of choice, we cannot exclude that X be infinite, that is $n \precsim X$ for all $n \in \mathbb{N}$, yet $\omega \not\precsim X$. In other words: X has more than n elements, for all $n \in \mathbb{N}$, yet it does not contain an infinite sequence of distinct elements. Since $\mathbb{N} \precsim X^{<\mathbb{N}}$, such an X would contradict the formula above. In absence of choice we can only prove that

$$\boxed{\emptyset \neq X \Rightarrow X^{<\mathbb{N}} \asymp (X^{<\mathbb{N}})^{<\mathbb{N}}}$$

These results will be relevant when looking at arbitrary first-order languages. For example: if the set of non-logical symbols of $\mathcal{L}$ has size $\leq \kappa$, then the set of all $\mathcal{L}$-terms and $\mathcal{L}$-formulæ are well-orderable and of size $\leq \kappa$.

Given a family $\mathcal{F}$ of operations on a non-empty set X, the closure of $Y \subseteq X$ is the smallest $\bar{Y} \subseteq X$ such that $Y \subseteq \bar{Y}$ and $\bar{Y}$ is closed under all $f \in \mathcal{F}$, and it is denoted with $\mathrm{Cl}_{\mathcal{F}}(Y)$. For example, if X is a ring and $\mathcal{F} = \{+, -, \cdot\}$, and $0_X \in Y \subseteq X$, then $\bar{Y} = \mathrm{Cl}_{\mathcal{F}}(Y)$ is the smallest subring of X containing Y. If X is well-orderable, then $\bar{Y}$ is of size $\leq \max(\aleph_0, |Y|)$. (We need to take in account $\aleph_0$ since Y could be finite, yet $\bar{Y}$ could be infinite.)

More generally (Theorem 21.18)

> If $\mathcal{F}$ is a collection of operations on X, and X and $\mathcal{F}$ are well-orderable and $|\mathcal{F}| \leq |X|$, then $\mathrm{Cl}_{\mathcal{F}}(Y)$ is well-orderable and for all $Y \subseteq X$
> $$|\mathrm{Cl}_{\mathcal{F}}(Y)| = \max(\aleph_0, |Y|, |\mathcal{F}|).$$

Exercises

Exercise 14.39. Show that $(\mathbb{Q}, +)$ has no maximal proper subgroups. Conclude that the rng $(\mathbb{Q}, +, *)$ where $a * b = 0$ for all $a, b \in \mathbb{Q}$ has no maximal ideals.

Exercise 14.40. Show that BPI follows from: every Boolean algebra has a prime ideal.

Exercise 14.41. Prove that the following statements are equivalent to AC:

(i) the axiom of choice for families of pairwise disjoint sets: if $\mathcal{A} \neq \emptyset$ is a family of non-empty, pairwise disjoint sets, then there is $f \colon \mathcal{A} \to \bigcup \mathcal{A}$ such that $\forall A \in \mathcal{A}\, (f(A) \in A)$;

(ii) if $\mathcal{A} \neq \emptyset$ is a family of non-empty, pairwise disjoint sets, then there is a **transversal for** $\mathcal{A}$, that is a $T \subseteq \bigcup \mathcal{A}$ such that $A \cap T$ is a singleton, for all $A \in \mathcal{A}$;

(iii) the formula (14.1);

(iv) if $f \colon X \twoheadrightarrow Y$ then there is a left inverse for f, that is there is $g \colon Y \rightarrowtail X$ such that $\forall y \in Y\, (f \circ g(y) = y)$;

(v) every set X is **projective**, that is to say: for every $f \colon X \to Y$ and every surjection $g \colon Z \twoheadrightarrow Y$ there is $h \colon X \to Z$ such that $f = g \circ h$;

(vi) every set is contained in a projective set;

(vii) if a set R is a binary relation, then there is a function f such that $\mathrm{dom}(f) = \mathrm{dom}(R)$ and $\forall x \in \mathrm{dom}(R)\, (x, f(x)) \in R$.

Exercise 14.42. Let $F_{i,j}$ be non-empty sets, with $(i, j) \in I \times J$. Show that:

(i) $\bigcap_{i \in I} \bigcup_{j \in J} F_{i,j} \supseteq \bigcup_{f \in {}^I J} \bigcap_{i \in I} F_{i,f(i)}$ and $\times_{i \in I} \bigcup_{j \in J} F_{i,j} \supseteq \bigcup_{f \in {}^I J} \times_{i \in I} F_{i,f(i)}$;

(ii) AC implies that
$$\bigcap_{i \in I} \bigcup_{j \in J} F_{i,j} = \bigcup_{f \in {}^I J} \bigcap_{i \in I} F_{i,f(i)} \quad \text{and} \quad \times_{i \in I} \bigcup_{j \in J} F_{i,j} = \bigcup_{f \in {}^I J} \times_{i \in I} F_{i,f(i)};$$

(iii) both statements, for arbitrary $I, J, F_{i,j}$,

$$\bigcap_{i\in I}\bigcup_{j\in J} F_{i,j} \subseteq \bigcup_{f\in {}^I J}\bigcap_{i\in I} F_{i,f(i)} \quad\text{and}\quad \bigtimes_{i\in I}\bigcup_{j\in J} F_{i,j} \subseteq \bigcup_{f\in {}^I J} \bigtimes_{i\in I} F_{i,f(i)}$$

imply AC.

Exercise 14.43. Show that if F is a proper filter of a Boolean algebra B and $\mathsf{BPI}(B)$ holds, then $F = \bigcap\{D \in \mathrm{St}(B) \mid F \subseteq D\}$.

Notes and remarks

Theorem 14.1 was proved around 1950 by Bourbaki and independently by Witt and for this reason it is known as the Bourbaki-Witt fixed point theorem. The presentation of Tychonff's theorem follows [**Cie97**].

15. The compactness theorem

15.A. Ultraproducts. We want to generalize the cartesian product construction. Given non-empty sets A_i $(i \in I \neq \emptyset)$ and a filter $\mathcal{F}$ on I consider the equivalence relation $\sim_{\mathcal{F}}$ on $\bigtimes_{i\in I} A_i$

$$f \sim_{\mathcal{F}} g \Leftrightarrow \{i \in I \mid f(i) = g(i)\} \in \mathcal{F}.$$

The relation $\sim_{\mathcal{F}}$ is clearly reflexive and symmetric; transitivity follows from $\{i \in I \mid f(i) = h(i)\} \supseteq \{i \in I \mid f(i) = g(i)\} \cap \{i \in I \mid g(i) = h(i)\}$ and the closure of $\mathcal{F}$ under intersections and supersets. The **reduced product of the A_is modulo** $\mathcal{F}$ is the quotient

$$\prod_{\mathcal{F}} A_i \overset{\text{def}}{=} \bigtimes_{i\in I} A_i / {\sim_{\mathcal{F}}}.$$

If $\mathcal{F} = \mathscr{P}(I)$ then $\prod_{\mathcal{F}} A_i$ is a singleton; if $\mathcal{F} = \{I\}$ then $\prod_{\mathcal{F}} A_i$ can be identified with $\bigtimes_{i\in I} A_i$; if $\mathcal{F}$ is proper and $\{i_0\} \in \mathcal{F}$ for some $i_0 \in I$, then $\prod_{\mathcal{F}} A_i \to A_{i_0}$, $[f] \mapsto f(i_0)$, is a bijection. When $\mathcal{F}$ is an ultrafilter, the reduced product is called an **ultraproduct**. If the sets A_i are the same set A we speak of a **reduced power** and write $A^I/\mathcal{F}$; if $\mathcal{F}$ is an ultrafilter we will speak of **ultrapower**.

Remark 15.1. The construction of reduced power is similar to the construction of $L^p(X, \mu)$ spaces in analysis, where starting from a measurable space one takes the quotient set

$$\left\{f \mid f \colon X \to \mathbb{R} \text{ is } \mu\text{-measurable and } \textstyle\int_X |f(x)|^p \,\mathrm{d}x < +\infty\right\}$$

taking $f \sim_{\mathcal{F}} g$ where $\mathcal{F} = \{Y \subseteq X \mid \mu(X \setminus Y) = 0\}$ is the filter of all sets whose complement is null. (In case μ is a probability measure $\mathcal{F} = \{Y \subseteq X \mid \mu(Y) = 1\}$.) The addition, multiplication and the ordering on

$L^p(X, \mu)$ are defined by: $[f] + [g] = [f + g]$ and $[f] \cdot [g] = [f \cdot g]$, where $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$, and $[f] < [g]$ if and only if $\{x \in X \mid f(x) < g(x)\} \in \mathcal{F}$. If the measure concentrates on a point $\bar{x} \in X$, that is $\mathcal{F} = \{Y \subseteq X \mid \bar{x} \in Y\}$ is a principal ultrafilter, then $L^p(X, \mu)$ is isomorphic to $\mathbb{R}$.

If the A_is are endowed with some (algebraic or relational) structure, the reduced product is endowed with the same structure as well. Let us see two specific examples when $\mathcal{F}$ is a proper, non-trivial, non-principal filter on $I = \mathbb{N}$.

15.A.1. *Ultrapower of* $(\mathbb{N}, \leq)$. Let us fix a filter $\mathcal{F}$ on $\mathbb{N}$ and consider the reduced power $\mathbb{N}^{\mathbb{N}}/\mathcal{F}$ with the ordering

$$[f] \trianglelefteq [g] \Leftrightarrow \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in \mathcal{F}$$

If $\{n \mid f(n) = f'(n)\}, \{n \mid g(n) = g'(n)\}, \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in \mathcal{F}$ then

$$\begin{aligned} &\{n \in \mathbb{N} \mid f'(n) \leq g'(n)\} \supseteq \\ &\qquad \{n \mid f(n) = f'(n)\} \cap \{n \mid g(n) = g'(n)\} \cap \{n \in \mathbb{N} \mid f(n) \leq g(n)\} \in \mathcal{F} \end{aligned}$$

hence the definition of $\trianglelefteq$ does not depend on the representative. Similarly, one verifies that $\trianglelefteq$ is reflexive, antisymmetric, and transitive on $\mathbb{N}^{\mathbb{N}}/\mathcal{F}$, i.e. $(\mathbb{N}^{\mathbb{N}}/\mathcal{F}, \trianglelefteq)$ is an ordered set.

By assumption $\mathcal{F}$ contains the Fréchet filter, hence if $f, g \in \mathbb{N}^{\mathbb{N}}$ agree from some point on, then $f \sim_{\mathcal{F}} g$. If $\mathcal{F}$ is the Fréchet filter, then the ordering is not total.

Suppose now that $\mathcal{F}$ is an ultrafilter. For each pair $f, g \in \mathbb{N}^{\mathbb{N}}$ the sets

$$\{n \mid f(n) < g(n)\}, \quad \{n \mid f(n) = g(n)\}, \quad \{n \mid f(n) > g(n)\}$$

form a partition of the natural numbers, hence one and only one of the following condition holds:

$$[f] \triangleleft [g], \quad [f] = [g], \quad [g] \triangleleft [f].$$

In other words, $\triangleleft$ is a linear order on $\mathbb{N}^{\mathbb{N}}/\mathcal{F}$.

Moreover, if $\mathcal{F}$ is non-principal, then $\triangleleft$ is not a well-order on $\mathbb{N}^{\mathbb{N}}/\mathcal{F}$: if $f_k(n) = |n - k|$ then $\ldots [f_2] \triangleleft [f_1] \triangleleft [f_0]$ is an infinite descending chain.

15.A.2. *Ultraproduct of fields.* If the $\mathcal{A}_n = \Bbbk_n$ are fields, define the operations of addition and multiplication on $\prod_{\mathcal{F}} \Bbbk_n$ by letting

$$[f] + [g] = [f + g] \qquad \text{and} \qquad [f] \cdot [g] = [f \cdot g]$$

where the sequences $f + g$ and $f \cdot g$ are defined by

$$(f + g)(n) = f(n) +_n g(n) \qquad \text{and} \qquad (f \cdot g)(n) = f(n) \cdot_n g(n),$$

and the operations $+_n$ and $\cdot_n$ on the right-hand side are addition and multiplication in the field $\Bbbk_n$. With these operations we get a commutative ring—the identity elements for sum and product are the equivalence classes of the sequences $n \mapsto 0_{\Bbbk_n}$ and $n \mapsto 1_{\Bbbk_n}$, respectively, and will be denoted with $\mathbf{0}$ and $\mathbf{1}$.

Suppose that $[f] \neq \mathbf{0} \neq [g]$, but $[f] \cdot [g] = \mathbf{0}$. This means that $\{n \mid f(n) = 0_{\Bbbk_n}\} \notin \mathcal{F}$ and $\{n \mid g(n) = 0_{\Bbbk_n}\} \notin \mathcal{F}$, but

$$\{n \mid f(n) \cdot g(n) = 0_{\Bbbk_n}\} = \{n \mid f(n) = 0_{\Bbbk_n}\} \cup \{n \mid g(n) = 0_{\Bbbk_n}\} \in \mathcal{F},$$

that is $\mathcal{F}$ is not prime.

Conversely if $\mathcal{F}$ is prime, that is an ultrafilter, then $\prod_{\mathcal{F}} \Bbbk_n$ is a field. In fact if $[f] \neq \mathbf{0}$, then $A \overset{\text{def}}{=} \{n \mid f(n) \neq 0_{\Bbbk_n}\} \in \mathcal{F}$ so we can define

$$f'(n) = \begin{cases} f(n) & \text{if } n \in A, \\ 1_{\Bbbk_n} & \text{otherwise,} \end{cases}$$

so that $[f] = [f']$ and $\forall n\, (f'(n) \neq 0_{\Bbbk_n})$. If $g(n)$ is the element of $\Bbbk_n$ such that $f'(n) \cdot g(n) = 1_{\Bbbk_n}$, then $\forall n\, (f'(n) \cdot g(n) = 1_{\Bbbk_n})$, that is $[f] \cdot [g] = \mathbf{1}$.

If $\mathcal{F}$ is the ultrafilter generated by some $n_0 \in \mathbb{N}$, the function $\prod_{\mathcal{F}} \Bbbk_n \to \Bbbk_{n_0}$, $[f] \mapsto f(n_0)$ is an isomorphism of fields. If instead $\mathcal{F}$ is non-principal, the ultraproduct need not be isomorphic to one of its factors. For example suppose that the fields $\Bbbk_n$ have finite characteristic and that the characteristic tends to infinity, that is $\lim_{n\to\infty} \operatorname{char}(\Bbbk_n) = \infty$. Fix an $m > 0$ and let $[f]$ be a non-zero element of the ultraproduct—from what we have seen above, we may assume that $f(n) \neq 0_{\Bbbk_n}$, for all $n \in \mathbb{N}$. The element

$$m[f] \overset{\text{def}}{=} \underbrace{[f] + \cdots + [f]}_{m}$$

is the equivalence class of the function $mf \in \mathsf{X}_n \Bbbk_n$ defined by

$$n \mapsto mf(n) \overset{\text{def}}{=} \underbrace{f(n) + \cdots + f(n)}_{m}$$

Let M be such that $\forall n \geq M\, (\operatorname{char}(\Bbbk_n) > m)$ hence $\forall n \geq M\, (m \cdot f(n) \neq 0_{\Bbbk_n})$. The sequence

$$g(n) = \begin{cases} mf(n) & \text{if } n \geq M \\ 1_{\Bbbk_n} & \text{otherwise} \end{cases}$$

is equivalent to mf as $\mathcal{F}$ is not principal, hence $\mathbb{N} \setminus M \in \mathcal{F}$. It follows that $m[f]$ is not null. Being m and $[f]$ arbitrary, we have verified that $\prod_{\mathcal{F}} \Bbbk_n$ is of characteristic 0.

15.B. The fundamental theorem of ultraproducts.

Theorem 15.2 (Łos). *Let $\mathcal{A}_i = (A_i; \dots)$ be $\mathcal{L}$-structures, with $i \in I$, and let U be an ultrafilter on I. Let $\lhd_i$ be a well-order on A_i. For every formula $\varphi(x_1, \dots, x_n)$ and every $g_1, \dots, g_n \in \mathsf{X}_{i \in I} A_i$*

$$\prod_U \mathcal{A}_i \vDash \varphi[[g_1], \dots, [g_n]] \quad \Leftrightarrow \quad X_{\varphi, g_1, \dots, g_n} \in U,$$

where $X_{\varphi, g_1, \dots, g_n} = \{i \in I \mid \mathcal{A}_i \vDash \varphi[g_1(x), \dots, g_n(x)]\}$.

Proof. The proof is by induction on the complexity of φ. If φ is atomic, the result follows from the definition of $\prod_U \mathcal{A}_i$. For the other cases, suppose fo simplicity that n, the number of free variables of φ is at most 2. If $\varphi = \neg\psi$, then

$$\begin{aligned}\prod_U \mathcal{A}_i \vDash \varphi[[g_1], [g_2]] &\Leftrightarrow \prod_U \mathcal{A}_i \nvDash \psi[[g_1], [g_2]] \\ &\Leftrightarrow X_{\psi, g_1, g_2} \notin U \\ &\Leftrightarrow X_{\varphi, g_1, g_2} \in U\end{aligned}$$

where in the last passage we used that $X_{\varphi, g_1, g_2} = I \setminus X_{\psi, g_1, g_2}$.

If $\varphi = \psi \vee \chi$, then

$$\begin{aligned}\prod_U \mathcal{A}_i \vDash \varphi[[g_1], [g_2]] &\Leftrightarrow \big(\prod_U \mathcal{A}_i \vDash \psi[[g_1], [g_2]]\big) \vee \big(\prod_U \mathcal{A}_i \vDash \chi[[g_1], [g_2]]\big) \\ &\Leftrightarrow X_{\psi, g_1, g_2} \in U \ \vee \ X_{\chi, g_1, g_2} \in U \\ &\Leftrightarrow X_{\psi, g_1, g_2} \cup X_{\chi, g_1, g_2} \in U \\ &\Leftrightarrow X_{\psi \vee \chi, g_1, g_2} \in U\end{aligned}$$

where we used that $X_{\psi \vee \chi, g_1, g_2} = X_{\psi, g_1, g_2} \cup X_{\chi, g_1, g_2}$.

Suppose now $\varphi = \exists y \psi$. If $\prod_U \mathcal{A}_i \vDash \varphi[[g_1], [g_2]]$ then there is $h \in \mathsf{X}_{i \in I} A_i$ such that $\prod_U \mathcal{A}_i \vDash \psi[[h], [g_1], [g_2]]$ hence, by inductive hypothesis, $X_{\psi, h, \bar{g}} \in U$. As $X_{\varphi, g_1, g_2} \supseteq X_{\psi, h, g_1, g_2}$, it follows that $X_{\varphi, g_1, g_2} \in U$. Conversely, suppose that $X_{\varphi, g_1, g_2} \in U$. Let $h \in \mathsf{X}_{i \in I} A_i$ be the function

$$h(i) = \begin{cases} \text{the } \lhd_i\text{-least } a \text{ such that } \mathcal{A}_i \vDash \psi[a, g_1(i), g_2(i)] & \text{if } i \in X_{\varphi, g_1, g_2}, \\ a_i^* & \text{otherwise,} \end{cases}$$

where a_i^* is the $\lhd_i$-least element of A_i. Then X_{φ, g_1, g_2} is contained in X_{ψ, h, g_1, g_2} (in fact: the two sets are the same) hence $X_{\psi, h, g_1, g_2} \in U$. By inductive assumption, this implies that $\prod_U \mathcal{A}_i \vDash \psi[[h], [g_1], [g_2]]$ hence $\prod_U \mathcal{A}_i \vDash \varphi[[g_1], [g_2]]$. □

Corollary 15.3. *Let $\mathcal{A}$ be a well-orderable structure, let U be an ultrafilter on I, and let $\pi \colon \mathcal{A} \to \prod_U \mathcal{A}$ be the map defined by $\pi(a) = [c_a]$ where $c_a \colon I \to \{a\}$.*

Then π is an elementary embedding. In particular $\mathcal{A}$ is elementarily equivalent to any of its ultrapowers.

We are now ready to prove the compactness theorem for first-order logic, Theorem 4.46.

Theorem 15.4. *Assume* AC. *If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is finitely satisfiable, then it is satisfiable.*

Proof. The result is trivial if Σ is finite, so we may assume otherwise. Then Σ does not belong to $I = \{i \subseteq \Sigma \mid i \text{ is finite}\}$. By AC for any $i \in I$ choose $\mathcal{A}_i \vDash i$. Let $S(i) = \{j \in I \mid i \subseteq j\}$. As $S(i_1) \cap \cdots \cap S(i_n) = S(i_1 \cup \cdots \cup i_n)$, then $\{S(i) \mid i \in I\} \subseteq \mathscr{P}(I)$ is a base for a proper filter F on I. Let $U \supseteq F$ be an ultrafilter extending F. We want to show that for each σ in Σ

$$\textstyle\prod_U \mathcal{A}_i \vDash \sigma.$$

This follows at once from Łos' Theorem and from $\{i \in I \mid \mathcal{A}_i \vDash \sigma\} \supseteq S(\{\sigma\}) \in F \subseteq U$. □

Remark 15.5. Does the Compactness Theorem 15.4 depend on the axiom of choice? The answer is: it depends on the language $\mathcal{L}$. More to the point:

- if the set of non-logical symbols of $\mathcal{L}$ is countable (or more generally: it is well-orderable), then compactness is provable without any appeal to the axiom of choice;
- if $\mathcal{L}$ is arbitrary, then the compactness theorem follows BPI. In fact the compactness theorem for arbitrary languages is equivalent to BPI.

The proof of Theorem 15.4 given above uses the full axiom of choice, but in Chapter VII we will present a different proof compactness that vindicates the two points above. For the time being let us observe that all the consequences of Theorem 15.4 (that is Theorem 4.46) presented in Sections 4.K, 4.L used countable languages, so none of them requires choice.

15.C. More applications of compactness.

Definition 15.6. The **elementary diagram** of $\mathcal{A}$ is the set of all sentences that hold in $(\mathcal{A}, a)_{a\in A}$,

$$\mathrm{EDiag}(\mathcal{A}) = \mathrm{Th}((\mathcal{A}, a)_{a\in A}).$$

The **diagram of** $\mathcal{A}$ is the set of all atomic and negated-atomic formulæ that are true in $(\mathcal{A}, a)_{a\in A}$

$$\mathrm{Diag}(\mathcal{A}) = \mathrm{EDiag}(\mathcal{A}) \cap \big(\mathrm{AtFml}(\mathcal{L}_A) \cup \{\neg\psi \mid \psi \in \mathrm{AtFml}(\mathcal{L}_A)\}\big).$$

Theorem 15.7. *The following are equivalent:*

(a) $\mathcal{A} \preccurlyeq \mathcal{B}$,

(b) *there is an expansion* $\tilde{\mathcal{B}}$ *of* $\mathcal{B}$ *in the language* $\mathcal{L}_A = \mathcal{L} \cup \{\mathring{a} \mid a \in A\}$ *such that* $\tilde{\mathcal{B}} \vDash \mathrm{EDiag}(\mathcal{A})$.

Proof. (a) ⇒ (b): If $\pi\colon \mathcal{A} \to \mathcal{B}$ is elementary, then letting $(\mathring{a})^{\tilde{\mathcal{B}}} = \pi(a)$ for $a \in A$, we obtain the expansion $\tilde{\mathcal{B}} = (\mathcal{B}, \pi(a))_{a \in A}$. Let us check that $\tilde{\mathcal{B}} \vDash \sigma$ for all $\sigma \in \mathrm{EDiag}(\mathcal{A})$. If $\sigma \in \mathrm{Sent}(\mathcal{L}_A)$ then σ is of the form $\varphi(\!|\mathring{a}_1/x_1, \dots, \mathring{a}_n/x_n|\!)$, where $\varphi(x_1, \dots, x_n)$ is an $\mathcal{L}$-formula, therefore

$$\begin{aligned}(\mathcal{A}, a)_{a \in A} \vDash \sigma &\Leftrightarrow \mathcal{A} \vDash \varphi[a_1, \dots, a_n]\\ &\Leftrightarrow \mathcal{B} \vDash \varphi[\pi(a_1), \dots, \pi(a_n)]\\ &\Leftrightarrow \tilde{\mathcal{B}} \vDash \sigma.\end{aligned}$$

(b) ⇒ (a): Suppose that $\tilde{\mathcal{B}}$ is an $\mathcal{L}_A$-structure satisfying $\mathrm{EDiag}(\mathcal{A})$. Then, for each pair $a_1, a_2 \in A$

$$a_1 \neq a_2 \;\Leftrightarrow\; (\mathring{a}_1 \neq \mathring{a}_2) \in \mathrm{EDiag}(\mathcal{A}) \;\Leftrightarrow\; \tilde{\mathcal{B}} \vDash \mathring{a}_1 \neq \mathring{a}_2 \;\Leftrightarrow\; (\mathring{a}_1)^{\tilde{\mathcal{B}}} \neq (\mathring{a}_2)^{\tilde{\mathcal{B}}}.$$

Therefore $\pi\colon A \to B$, $\pi(a) = (\mathring{a})^{\tilde{\mathcal{B}}}$, is an injective function. If $\varphi(x_1, \dots, x_n)$ is an $\mathcal{L}$-formula and $a_1, \dots, a_n \in A$, then

$$\begin{aligned}\mathcal{A} \vDash \varphi[a_1, \dots, a_n] &\Leftrightarrow \varphi(\!|\mathring{a}_1/x_1, \dots, \mathring{a}_n/x_n|\!) \in \mathrm{EDiag}(\mathcal{A})\\ &\Leftrightarrow \tilde{\mathcal{B}} \vDash \varphi(\!|\mathring{a}_1/x_1, \dots, \mathring{a}_n/x_n|\!)\\ &\Leftrightarrow \mathcal{B} \vDash \varphi[\pi(a_1), \dots, \pi(a_n)].\end{aligned}$$

Thus π is elementary. □

The same proof yields:

Theorem 15.8. *The following are equivalent:*

(a) $\mathcal{A} \subseteq \mathcal{B}$,

(b) *there is an expansion* $\tilde{\mathcal{B}}$ *of* $\mathcal{B}$ *in the language* $\mathcal{L}_A = \mathcal{L} \cup \{\mathring{a} \mid a \in A\}$ *such that* $\tilde{\mathcal{B}} \vDash \mathrm{Diag}(\mathcal{A})$.

Notes and remarks

Exercises

Exercise 15.9. Suppose R is a ring, D a filter on a set $I \neq \emptyset$, and $J = \{f \in R^I \mid \exists X \in D \, \forall i \in X \, f(i) = 0_R\}$. Show that

(i) J is a two-sided ideal of the ring R^I and that the reduced power R^I/D is isomorphic to the quotient ring R^I/J.

(ii) Assuming D is an ultrafilter on I, then
- R does not have zero-divisors if and only if J is a prime ideal of R^I;
- R is a division ring if and only if J is a maximal ideal of R^I.

Exercise 15.10. Show that a group G is (left-)orderable if and only if every finitely generated subgroup of G is (left-)orderable. Conclude that if $G_0 \subseteq G_1 \subseteq \dots$ are (left-)orderable groups, then $\bigcup_{n \in \mathbb{N}} G_n$ is (left-)orderable.

Exercise 15.11. In this exercise we give a new proof of Stone's Theorem 14.18. Let $\mathcal{L}$ be the language $\{X, \mathcal{F}, \mathring{\in}, C, U, I\}$ where

- $X, \mathcal{F}$ are 1-ary relational symbols,
- $\mathring{\in}, C$ are 2-ary relational symbols,
- U, I are 3-ary relation symbols

Find a finite $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ such that every model of Σ is isomorphic to a structure with universe $X \cup \mathcal{F}$, where $X \neq \emptyset$, $X \cap \mathcal{F} = \emptyset$, $\mathcal{F} \subseteq \mathscr{P}(X)$ is a subalgebra, the relation $\mathring{\in}$ is interpreted as membership between elements of X and elements of $\mathcal{F}$, while the sets C, I and U are, respectively, the graphs of the functions complementation, intersection, and union in $\mathcal{F}$. Let B be an boolean algebra and let $\tilde{\mathcal{L}} = \mathcal{L} \cup \{\mathring{b} \mid b \in B\}$. Show that $\mathrm{Diag}(B) \cup \Sigma$ is a finitely satisfiable set of $\tilde{\mathcal{L}}$-sentences. Conclude that B is isomorphic to a subalgebra of $\mathscr{P}(X)$, for some set X.

Exercise 15.12. Use Exercise 7.96 to prove that every distributive lattice is isomorphic to a sublattice of some $\mathscr{P}(X)$.

Exercise 15.13. Prove the Four Color Theorem 10.7 for plane maps with infinitely many regions, that is: any graph that does not contain neither K_5 nor $\mathrm{K}_{3,3}$ as minor is 4-colorable.

Chapter V

Basic set theory

16. The axioms

A set is completely characterized by its elements—two sets with the same elements coincide:

(∗) Suppose that A and B are sets and that, for every x, $x \in A$ if and only if $x \in B$. Then $A = B$.

This principle, known as the axiom of extensionality, is the foundation of set theory. Another characteristic of the conception of set is that given a property φ, it is possible to consider the set $\{x \mid \varphi(x)\}$ of all x that satisfy φ. This set is completely determined because of (∗). It seems reasonable to postulate that:

(∗∗) If φ is a property, then the set $\{x \mid \varphi(x)\}$ exists.

Yet Bertrand Russell in 1901 showed that (∗∗) contradicts (∗)! To see this, consider the property $\varphi(x)$ asserting "x is a set and $x \notin x$", and let

$$\mathrm{R} = \{x \mid x \notin x\}. \tag{16.1}$$

By (∗∗) R is a set, so either $\mathrm{R} \notin \mathrm{R}$ or else $\mathrm{R} \in \mathrm{R}$. But

(16.2a) $\mathrm{R} \in \mathrm{R}$ implies that $\mathrm{R} \notin \mathrm{R}$ and

(16.2b) $\mathrm{R} \notin \mathrm{R}$ implies that $\mathrm{R} \in \mathrm{R}$,

a contradiction. Russell's paradox, like the Burali-Forti and Cantor paradoxes (Sections 14.G.1 and 14.G.2 in Chapter **??**) use (∗∗) to define collections that are very "large", but never appeal to sets encountered in mathematical practice. In order to resolve these contradictions, several axiomatic theories have been introduced, each one precisely delimiting the admissible set-theoretic constructions. The theory that we are going to present is known Morse-Kelly set theory (MK).

16.A. Sets and classes. The primitive notions are that of a **class**, and **membership** $\in$ between classes. A class A is a **set** if and only if there is a class B to which A belongs, that is $\exists B(A \in B)$. A class that is not a set is a **proper class**. In naïve set theory, it is customary to distinguish between *sets* (or classes) and *objects*, but the notion of set (and class) is so general that it is possible to avoid objects that are not sets or classes. In other words, we may assume from now on that the *elements of a class are themselves classes*, in fact sets. The principle $(*)$ can be extended to cover the case when A and B are classes (rather than sets).

Axiom of Extensionality. *If A and B are classes and $\forall x(x \in A \Leftrightarrow x \in B)$, then $A = B$.*

In order to adequately formalize $(**)$, the ambiguous concept of *property* is replaced with the rigorous notion **formula of set theory**. The language of set theory is the first-order language $\mathcal{L}_\in$ with only one binary predicate $\in$. Thus its atomic formulæ are of the form $x \in y$ and $x = y$.[1] We will abbreviate $\neg(x \in y)$ with $x \notin y$. Let $\mathrm{Set}(x)$ be the formula asserting that x is a set:

$$\exists y\,(x \in y)\,. \tag{Set(x)}$$

The following axiom-schema crystallizes the principle $(**)$.

Axiom of Comprehension. *Let $\varphi(x, y_1, \dots, y_n)$ be a formula in which the variable x occurs free, and let A be a variable different from $x, y_1, \dots, y_n$. Then*

$$\forall y_1 \dots \forall y_n \exists A\, \forall x\big(x \in A \Leftrightarrow (\mathrm{Set}(x) \wedge \varphi(x, y_1, \dots, y_n))\big).$$

The class A defined by φ and $y_1, \dots, y_n$ is the class of all *sets* x such that $\varphi(x, y_1, \dots, y_n)$ holds. By extensionality, the class A is unique and it is denoted by $\{x \mid \varphi(x, y_1, \dots, y_n)\}$.

Remark 16.1. In mathematics, every time it is proved that

$$\forall x_1 \dots \forall x_n \exists! y\, \varphi(x_1, \dots, x_n, y)$$

a new symbol $\mathsf{t}(x_1, \dots, x_n)$ is introduced, denoting the unique y satisfying $\varphi(x_1, \dots, x_n, y)$. This $\mathsf{t}(x_1, \dots, x_n)$ is called a **defined term**, and it is a term of a language *extending* $\mathcal{L}_\in$. Therefore

$$\{\mathsf{t}(x_1, \dots, x_n) \mid x_1 \in X_1, \dots, x_n \in X_n\} \tag{16.3}$$

[1] We should really write $x \mathrel{\scriptstyle =} y$, rather than $x = y$, but as the only terms of in set theory are the variables, we can safely blur the distinction between these two notions.

is shorthand for the class

$$\{y \mid \exists x_1 \dots \exists x_n \, (x_1 \in X_1 \wedge \cdots \wedge x_n \in X_n \wedge \varphi(x_1, \dots, x_n, y))\},$$

where φ is the formula defining $\mathtt{t}$.

Let's go back to Russell's paradox. By the axiom of comprehension, the class $\mathrm{R} = \{x \mid x \notin x\}$ exists and the implication in (16.2a) shows that $\mathrm{R} \in \mathrm{R}$ cannot hold, hence $\mathrm{R} \notin \mathrm{R}$. If R were a set, we could apply (16.2b) and obtain a contradiction as before. (If instead R is a proper class and the problem disappears.) It follows that R *is a proper class.*

If A is a class, $\{x \in A \mid \varphi(x, y_1, \dots, y_n)\}$ is the class determined by the formula $x \in A \wedge \varphi(x, y_1, \dots, y_n)$, that is $\{x \in A \mid \varphi(x, y_1, \dots, y_n)\} = \{x \mid x \in A \wedge \varphi(x, y_1, \dots, y_n)\}$. The usual set-theoretic operations apply to classes as well: if A and B are classes, then $A \cap B = \{x \mid x \in A \wedge x \in B\}$, $A \cup B = \{x \mid x \in A \vee x \in B\}$, $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ and $A \mathbin{\triangle} B = (A \setminus B) \cup (B \setminus A)$ are classes. From the axiom of extensionality, it follows that $A \cap B = B \cap A$, $A \cup B = B \cup A$ and $A \mathbin{\triangle} B = B \mathbin{\triangle} A$.

The axiom of comprehension guarantees the existence of many classes, but by itself it does not guarantee the existence of *sets.*

Axiom of Set-existence. $\exists x \, \mathrm{Set}(x)$.

The class A is a **subclass** of B, i.e. A is contained in B, in symbols $A \subseteq B$, if $\forall x \, (x \in A \Rightarrow x \in B)$. If $A \subseteq B$ and $A \neq B$, then A is a proper subclass of (or: is properly contained in) B and write $A \subset B$.

Axiom of Power-set. *For every set A there is a set P such that*

$$\forall B \, (B \subseteq A \Leftrightarrow B \in P) \, .$$

In other words: if A is a set, every subclass of it is a set, and the class of all subsets of A is itself a set. The set P as above is denoted with $\mathscr{P}(A)$ and it is called **power-set** of A. Note that $\mathscr{P}(x)$ is a defined term in the sense of Remark 16.1.

Corollary 16.2. *If B is a set and $A \subseteq B$ then A is a set. Equivalently: if A is a proper class and $A \subseteq B$ then B is a proper class.*

If A is a set, then also $A^{\neq} = \{x \in A \mid x \neq x\}$ is a set. No x can belong to $A^{\neq}$ and by the axiom of extensionality, any empty class must be equal to $A^{\neq}$. In other words, $A^{\neq}$ does not depend on A and it is called **empty set**, and it is denoted with $\emptyset$.

Give two sets x and y, the axiom of comprehension guarantees the existence of $\{x, y\}$, and by extensionality $\{x, y\} = \{y, x\}$. We require that this class be a set:

Axiom of Pairing. *If x and y are sets, then $\{x, y\}$ is a set.*

It is not required that x and y be distinct—if x and y coincide, we will write $\{x, x\}$ as $\{x\}$, called the **singleton** of x. The axiom of comprehension applied to the formula $x = x_1 \vee \cdots \vee x = x_n$ guarantees the existence of $\{x_1, \dots, x_n\}$; by the axiom of union that we will see shortly, it can be shown that $\{x_1, \dots, x_n\}$ is a set (Exercise 16.15(iii)).

If x and y are sets, the **ordered pair** (x, y) is defined as

$$(x, y) \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}. \tag{16.4}$$

Proposition 16.3. *For all sets x, y, z, w, we have $(x, y) = (z, w) \Leftrightarrow x = z \wedge y = w$.*

Proof. Suppose that $(x, y) = (z, w)$: we must to check that $x = z$ and $y = w$. If $x = y$ then $\{\{x\}\} = (x, y) = (z, w) = \{\{z\}, \{z, w\}\}$, hence $\{x\} = \{z, w\} = \{z\}$, that is $x = z = w$. It follows that $x = y \Rightarrow z = w$ and since the converse implication follows similarly, it can be shown that

$$x \neq y \quad \text{and} \quad z \neq w. \tag{16.5}$$

Since $\{x\} \in (x, y) = (z, w) = \{\{z\}, \{z, w\}\}$, it follows that either $\{x\} = \{z\}$ or else $\{x\} = \{z, w\}$, hence either $x = z$ or $x = z = w$. The second possibility must be discarded because of (16.5), hence $x = z$. From $\{x, y\} \in (x, y) = (z, w) = (x, w)$ it follows that either $\{x, y\} = \{x\}$ or $\{x, y\} = \{x, w\}$. The former cannot hold by (16.5), and by the latter we obtain $y \in \{x, w\}$, that is either $y = x$ or $y = w$: again by (16.5) it follows that $y = w$.

The converse implication is immediate. □

Remark 16.4. The definition in (16.4) is due to Kuratowski. It is not the only possible definition of ordered pair, but it is probably the simplest. The first such definition was given by Wiener in 1914, $(x, y)_{\mathrm{W}} = \{\{\emptyset, \{x\}\}, \{\{y\}\}\}$. Another definition of ordered pair is a variant of the one by Kuratowski: $(x, y)_{\mathrm{K}'} = \{x, \{x, y\}\}$. The disadvantage of this definition is that it requires the axiom of foundation (defined below) in order to prove its adequacy—see Exercise 16.21.

If $A \in B$ it is reasonable to consider A to be simpler than B. From this point of view, the empty set is the simplest of all sets. If the elements of a set are simpler than the set itself, then no set should belong to itself.

Axiom of Foundation. *If A is a non-empty class there is a $B \in A$ such that $A \cap B = \emptyset$.*

Remark 16.5. If $A \in A$ for some class A, then A would be a set and hence $\{A\}$ would exist. By the axiom of foundation there should be a set $B \in \{A\}$ such that $B \cap \{A\} = \emptyset$. Then B should be A and by assumption $A \in A = B$

and therefore $A \in B \cap \{A\}$: a contradiction. Similarly there are no sets A and B such that $A \in B$ and $B \in A$.

Since no set can belong to itself, Russell's class R in (16.1) is the class of *all* sets, and it is usually denoted by V:

$$\mathrm{V} \overset{\text{def}}{=} \{x \mid x = x\}. \tag{16.6}$$

For this reason, V is called the **universe of all sets** or **total class**.

The operations of generalized unions and intersections are defined as follows:

$$\bigcup A = \bigcup_{x \in A} x = \{y \mid \exists x \in A (y \in x)\}$$
$$\bigcap A = \bigcap_{x \in A} x = \{y \mid \forall x \in A (y \in x)\},$$

with the proviso that when $A = \emptyset$ then $\bigcap A = \emptyset$. Since $\bigcap A \subseteq x$ for all $x \in A$, Corollary 16.2 implies that $\bigcap A$ is always a set.

Axiom of Union. *If A is a set, then $\bigcup A$ is also a set.*

Thus, if x and y are sets, then $\{x, y\}$ is also a set by the axiom of pairing, hence $x \cup y \overset{\text{def}}{=} \bigcup\{x, y\}$ is also a set.

The **cartesian product** of two classes A and B is the class $A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$, which exists by comprehension.

Proposition 16.6. *If A and B are sets, then $A \times B$ is also a set.*

Proof. It is enough to find a set containing $A \times B$. If $x \in A$ and $y \in B$, then $\{x\}, \{x, y\} \subseteq A \cup B$, and hence $(x, y) = \{\{x\}, \{x, y\}\} \subseteq \mathscr{P}(A \cup B)$. It follows that $A \times B \subseteq \mathscr{P}(\mathscr{P}(A \cup B))$, so we are done. □

16.B. Infinite sets. The constructions seen so far enable us to construct infinitely many sets. Starting from $\emptyset$ and using pairing and unions we obtain

$$\{\emptyset\} = \mathbf{S}(\emptyset),\ \{\emptyset, \{\emptyset\}\} = \mathbf{S}(\{\emptyset\}),\ \{\emptyset, \{\emptyset\},\ \{\emptyset, \{\emptyset\}\}\} = \mathbf{S}(\{\emptyset, \{\emptyset\}\}),\ \ldots$$

where

$$\mathbf{S}(x) = x \cup \{x\}$$

is called the **successor** of x. The sets in the list above are all distinct, thus the class V is infinite. Let's introduce the following definition: a class I is **inductive** if

$$\emptyset \in I \wedge \forall x\, (x \in I \Rightarrow \mathbf{S}(x) \in I)\,.$$

Inductive *classes* exist, for example V, but what about inductive *sets*?

Axiom of Infinity. *There is an inductive set.*

Let $\mathcal{I}$ be the class of all inductive sets and let

$$\mathbb{N} \overset{\text{def}}{=} \bigcap \mathcal{I}. \tag{16.7}$$

Thus $\mathbb{N}$ is the smallest set containing $\emptyset$ and closed under the successor operation. Define $0 = \emptyset$, $1 = \mathbf{S}(0)$, $2 = \mathbf{S}(1) = \mathbf{S}(\mathbf{S}(0))$, ...

Proposition 16.7. *$\mathbb{N} \in \mathcal{I}$ and if $n \in \mathbb{N}$, then either $n = 0$ or else $n = \mathbf{S}(m)$ for some $m \in \mathbb{N}$.*

Proof. It is easy to check that $\mathbb{N} \in \mathcal{I}$. Let $n \in \mathbb{N} \setminus \{0\}$ and suppose, towards a contradiction, that $n \neq \mathbf{S}(m)$ for all $m \in \mathbb{N}$. Then $J = \mathbb{N} \setminus \{n\}$ would be an inductive set, that is $J \in \mathcal{I}$. This implies that $J \supseteq \bigcap \mathcal{I} = \mathbb{N}$, but by construction $J \subset \mathbb{N}$: a contradiction. □

We are now ready to prove Ind^2 the second-order induction principle for $\mathbb{N}$ seen in Section 12.A.

Proposition 16.8. *Suppose that $0 \in I \subseteq \mathbb{N}$ and $\forall n\, (n \in I \Rightarrow \mathbf{S}(n) \in I)$. Then $I = \mathbb{N}$.*

Proof. $I \in \mathcal{I}$, therefore $I \supseteq \mathbb{N}$. □

16.C. Relations and functions. A **binary relation** (or simply: a relation) is a class whose elements are ordered pairs. A relation F is **functional** if $(x, y), (x, y') \in F$ implies that $y = y'$; sometimes we use the term **class-function** instead of functional relation. A **function** is a set which is a functional relation. We often write $x \mathrel{R} y$ instead of $(x, y) \in R$ and whenever R is a functional relation, $R(x)$ denotes the unique y (if it exists) such that $(x, y) \in R$. The **composition of R with S** is the class

$$R \circ S \overset{\text{def}}{=} \{(x, z) \mid \exists y\, ((x, y) \in S \wedge (y, z) \in R)\}$$

and the **converse of R** is

$$\breve{R} = \{(x, y) \mid (y, x) \in R\}.$$

Although the definition of $R \circ S$ (and of $\breve{R}$) makes sense for all classes, it is particularly important when R and S are functional relations: in this case also $R \circ S$ is a functional relation and $(R \circ S)(x) = R(S(x))$.

The **domain**, the **range**, and the **field** of a class R are, respectively,

$$\operatorname{dom}(R) = \{x \mid \exists y\, (x, y) \in R\} \qquad \operatorname{ran}(R) = \{y \mid \exists x\, (x, y) \in R\}$$
$$\operatorname{fld}(R) = \operatorname{dom}(R) \cup \operatorname{ran}(R).$$

Proposition 16.9. *If R is a set, then $\operatorname{dom}(R)$, $\operatorname{ran}(R)$, $\operatorname{fld}(R)$ are sets.*

Proof. In order to show that $\mathrm{dom}(R)$ is a set, it is enough to find a set containing $\mathrm{dom}(R)$: if $x \in \mathrm{dom}(R)$ then $x \in \{x\} \in (x, y) \in R$, for some y, hence $x \in \bigcup(\bigcup R)$, and therefore $\mathrm{dom}(R) \subseteq \bigcup(\bigcup R)$. The argument for $\mathrm{ran}(R)$ and $\mathrm{fld}(R)$ are similar. □

Proposition 16.10. *Let $\mathcal{F}$ be a class of functions upward directed under $\subseteq$. Then $\bigcup \mathcal{F}$ is a functional relation.*

Proof. $\bigcup \mathcal{F}$ is a class of ordered pairs. Suppose that $(x, y), (x, z) \in \bigcup \mathcal{F}$, hence $(x, y) \in f$ and $(x, z) \in g$, for some $f, g \in \mathcal{F}$. Let $h \in \mathcal{F}$ be such that $f, g \subseteq h$: then $(x, y), (x, z) \in h$ hence $y = z$. □

The next result amplify Remark 16.5.

Theorem 16.11. *There is no functional relation F such that $\mathrm{dom}\, F = \mathbb{N}$ and $F(\mathbf{S}(n)) \in F(n)$ for all $n \in \mathbb{N}$.*

Proof. Suppose there is such an F. Since $\emptyset \neq \mathrm{ran}\, F$, there is $y \in \mathrm{ran}\, F$ such that $y \cap \mathrm{ran}\, F = \emptyset$ by the axiom of foundation. Let $n \in \mathbb{N}$ be such that $y = F(n)$. But $F(\mathbf{S}(n)) \in F(n) \cap \mathrm{ran}\, F$: a contradiction. □

For F and A arbitrary classes, the **point-wise image** of A via F is the class

$$F[A] = F``A = \{y \mid \exists x \in A\, (x, y) \in F\}.$$

The notation $F``A$ is used whenever the square brackets are already used for some other concepts (e.g. equivalence classes). The **pre-image** of A via F is $F^{-1}[A] = \{x \mid \exists y \in A\, (x, y) \in F\}$, while $F \restriction A = \{(x, y) \in F \mid x \in A\}$ is the **restriction of F to A**. If both F and A are proper classes, it may happen that $F[A]$ be a proper class: for example if F is the identity functional relation

$$\mathrm{id} \overset{\mathrm{def}}{=} \{(x, x) \mid x \in \mathrm{V}\}$$

then $\mathrm{id}[A] = A$ is not a set. We write id_A for $\mathrm{id} \restriction A$. If R is a relation on a class X and $Y \subseteq X$, we denote the induced relation $R \cap (Y \times Y)$ by $R \restriction Y$ or even R, if there is no danger of confusion.

By Exercise 16.15(v) if F is a set then also $F[A]$ is a set, but what happens if F is a proper class and A a set? Small classes are sets, and since every element of A corresponds at most one element of $F[A]$, this class should be a set.

Axiom of Replacement. *If F is a functional relation and A is a set, then $F[A]$ is a set.*

This completes the list of the axioms of MK.

If F is a (class-)function with domain A and range contained in B, we say that F is a (class-)function from A to B and write $F\colon A \to B$. The collection of all these F is denoted with ${}^{A}B$ or B^{A}.

Remark 16.12. Both notations B^A and ${}^AB$ are used in set theory, but only the latter is common in other parts of mathematics. The reason for using ${}^AB$ is that in certain situations B^A is ambiguous: for example ${}^{2}3$ is the class (actually: the set, by Proposition 16.13) of all maps from the set $2 = \{0, 1\}$ to the set $3 = \{0, 1, 2\}$, while 3^2 is the number 9. When there is no danger of confusion we will freely use B^A.

Proposition 16.13. *If A and B are sets, then B^A is a set.*

Proof. $B^A \subseteq \mathscr{P}(A \times B)$. □

If F is an injective (class-)function, then $\breve{F}$ is also a (class-)function, denoted by F^{-1}, and it is called the inverse (class-)function. In this case F and F^{-1} are inverses of each other, that is

$$\forall x \in \operatorname{dom}(F)\, [(F^{-1} \circ F)(x) = x] \quad \text{and} \quad \forall x \in \operatorname{ran}(F)\, [(F \circ F^{-1})(x) = x].$$

The point-wise image of A via F^{-1} coincides with the preimage of A via F, hence the notation $F^{-1}[A]$ is unambiguous. We retool the notions seen in Section 13.C to classes: given two classes A and B, we will say that A **embeds into** B, $A \precsim B$ if there is an injective functional-relation $F\colon A \rightarrowtail B$; if F is bijective we will say that A and B are **equipotent**, $A \asymp B$.

The axiom of replacement yields:

Proposition 16.14. *If A is a proper class and $A \precsim B$, then B is a proper class as well.*

16.D. Sequences and strings. In mathematics the notation F_x is often used in place of $F(x)$—when writing "a_i $(i \in I)$" or "$(a_i)_{i\in I}$" we are really positing the existence of a function a with domain I mapping $i \in I$ to a_i. For example it is common practice in mathematics to use "indexed sets" to denote a family of sets—e.g we write $\mathcal{A}$ as $\{A_i \mid i \in I\}$. This can always be achieved—set $I = \mathcal{A}$ and take $i \mapsto A_i$ to be the identity map id_I. This notation is very handy when dealing with the **disjoint union of the sets** A_i: choose $A'_i \asymp A_i$ so that these new sets are pairwise disjoint, and we take their union. For example take $A'_i = \{i\} \times A_i$. When A and B are sets or classes, their disjoint union is

$$A \uplus B = (\{0\} \times A) \cup (\{1\} \times B). \tag{16.8}$$

In order to concisely describe the function with domain I mapping $i \in I$ to a_i we shall write either $I \ni i \mapsto a_i$ or else $\langle a_i \mid i \in I\rangle$. This notation is particularly handy when $I \in \mathbb{N}$, that is when we deal with **finite sequences**, or **strings**. For example, $s = \langle a_0, a_1, \dots, a_{n-1} \rangle$ is the function with domain $n = \{0, 1, \dots, n-1\}$ that assigns a_i to $i < n$; the ordinal $n = \operatorname{dom}(s)$ is called the **length** of s and it is denoted with $\operatorname{lh} s$. In calculus, the word **sequence** means function with domain $\mathbb{N}$, but in set theory it simply means function, so $\langle a_i \mid i \in I \rangle$ is an I-sequence of sets. With a slight abuse of terminology we speak of sequences even when I is a proper class and $\langle a_i \mid i \in I \rangle$ is a class-function.

Although the sequence $\langle a, b \rangle$ of length 2 and the ordered pair (a, b) are essentially the same, they are distinct sets. The advantage in using sequences rather than pairs becomes evident when we must talk about n-tuples: if we defined[2] a tuple by $(a_1, a_2, \dots, a_n) \overset{\text{def}}{=} ((a_1, a_2, \dots, a_{n-1}), a_n)$, then its length would not be well-defined. Another drawback of the usual definition of ordered pair is that the cartesian product is non-associative, hence the expression $X \times \cdots \times X$ is ambiguous—for example: when we write $\mathbb{R}^3$ do we mean $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$ or $\mathbb{R} \times (\mathbb{R} \times \mathbb{R})$? In order to avoid petty (and trivial) ambiguities, it is best to declare that X^n be the class of all functions from n into X, rather than the cartesian product $X \times \cdots \times X$, and that $X^n \times X^m$ stands for the collection X^{n+m}. In accordance with Section 3.E, for any class X let

$$X^{<\mathbb{N}} = \{s \mid s \text{ is a finite string and } \operatorname{ran}(s) \subseteq X\}. \tag{16.9}$$

Then $X^{<\mathbb{N}}$ is a set if and only if X is a set.

A **finitary function** or **operation** on a class X is a functional relation $f \colon X^n \to X$ where $n = \operatorname{ar}(f) \in \mathbb{N}$ is called **arity** of f. If $n = 0$ then $f \colon \{\emptyset\} \to X$, hence f is completely determined by the value $f(\emptyset) \in X$. Thus 0-ary functions on X can be identified with the elements of X. If f is an operation on X, by notational simplicity we will write either $f(\vec{x})$ or $f(x_0, \dots, x_{n-1})$ rather than the more correct, but baroque, $f(\langle x_0, \dots, x_{n-1} \rangle)$.

The definition of ordered pair can be extended to proper classes: if A and B are classes and at least one among them is a proper class, set

$$\langle A, B \rangle \overset{\text{def}}{=} A \uplus B.$$

Since $A = \{x \mid (0, x) \in \langle A, B \rangle\}$ and $B = \{x \mid (1, x) \in \langle A, B \rangle\}$, the class $\langle A, B \rangle$ codes both A and B. More generally, if we assign a class A_i to each $i \in I$, and at least one of the A_i's is a proper class, define the sequence $\langle A_i \mid i \in I \rangle$ to be the class

$$A = \{(i, a) \mid i \in I \wedge a \in A_i\}$$

and, with abuse of language, we will write $I = \operatorname{dom}(A)$.

Recall the axiom of choice, introduced in Section 14.

[2] This is the approach that will be used in Section 39—see Definition 39.1.

Axiom of Choice. *If $\mathcal{A}$ is a non-empty set and if $\forall A \in \mathcal{A}\,(A \neq \emptyset)$, then there exists $f\colon \mathcal{A} \to \bigcup \mathcal{A}$ such that $\forall A \in \mathcal{A}\,(f(A) \in A)$.*

A map f as above is called a **choice function for $\mathcal{A}$**; a **choice function on** X, where X is a non-empty set, is an $f\colon \mathscr{P}(X) \to X$ such that $f \restriction \mathscr{P}(X) \setminus \{\emptyset\}$ is a choice function for $\mathscr{P}(X) \setminus \{\emptyset\}$. Letting $X = \bigcup \mathcal{A}$ we can reformulate AC as: "For every set $X \neq \emptyset$ there is a choice function on X." Recall that if I is a set and $\langle A_i \mid i \in I\rangle$ is a sequence of sets, the **generalized cartesian product** is

$$\mathsf{X}_{i\in I} A_i = \{f \mid f \text{ is a function, } \operatorname{dom}(f) = I \text{ and } \forall i \in I\,(f(i) \in A_i)\}.$$

Therefore if $A_i = A$ for all $i \in I$, then $\mathsf{X}_{i\in I} A_i = A^I$. If $A_{i_0} = \emptyset$ for some $i_0 \in I$, then $\mathsf{X}_{i\in I} A_i = \emptyset$. The converse: "if $I \neq \emptyset$ is a set and $A_i \neq \emptyset$ for all $i \in I$, then $\mathsf{X}_{i\in I} A_i \neq \emptyset$" is equivalent to AC (Exercise **??**). Note that when the A_i are all equal to some fixed set $A \neq \emptyset$, then AC is not needed to prove that $\mathsf{X}_{i\in I} A_i = A^I$ is non-empty, as witnessed by any constant function $i \mapsto a \in A$.

The theory obtained by adding the axiom of choice to MK is denoted by $\mathsf{MK} + \mathsf{AC}$. By requiring a uniform method for extracting an element from a non-empty set, we obtain a strengthening of AC known as the **axiom of global choice**

$$(\mathsf{AGC}) \qquad \exists F\,(F\colon \mathrm{V} \setminus \{\emptyset\} \to \mathrm{V} \wedge \forall x\,(x \neq \emptyset \Rightarrow F(x) \in x))\,.$$

We have little use for such principle and, unless otherwise stated, in this book when appealing to choice we mean the "local version" AC, or some weakening of it.

Exercises

Exercise 16.15. Show that:

(i) if A is a set, then $A \cap B$ is a set,

(ii) if B is a proper class then $A \cup B$ is a proper class,

(iii) if $x_1, \ldots, x_n$ are sets, then also $\{x_1, \ldots, x_n\}$ is a set,

(iv) $\mathrm{V} \setminus x$ is a proper class, for every set x,

(v) if f is a set, then so is $f``A$,

(vi) $\{\{x\} \mid x \in \mathrm{V}\}$ is a proper class;

(vii) if $y \neq \emptyset$ is a set, then $\{x \mid x \asymp y\}$ is a proper class.

(viii) Give an example of a proper class A such that $\bigcup A$ is a proper class.

Exercise 16.16. Show that:

(i) if A is a proper class or if $B = \emptyset \neq A$, then $B^A = \emptyset$,

(ii) if $A \neq \emptyset$ is a set and B is a proper class, then B^A is a proper class,

(iii) if $A = \emptyset$, then $B^A = \{\emptyset\}$.

Exercise 16.17. Show that

(i) X is a set if and only if $X^{<\mathbb{N}}$ is a set,

(ii) if X is a proper class, then X^n $(n \neq 0)$ is a proper class,

(iii) a class R is a binary relation if and only if it coincides with its double converse $\breve{\breve{R}}$,

(iv) if $\breve{R}$ is a proper class, then so is R.

Exercise 16.18. Find formulæ $\varphi(x)$ and $\psi(x)$ stating that "x is of the form $\{y, z\}$, with $y \neq z$" and "x is an ordered pair."

Exercise 16.19. Formalize in $\mathcal{L}_\in$ the following axioms of MK: Powerset, Pairing, Foundation, Union, Infinity, and Replacement.

Exercise 16.20. Show that if $\langle A_i \mid i \in I \rangle$ is a sequence of non-empty classes and $I \neq \emptyset$ is in bijection with a natural number, then $\mathsf{X}_{i \in I} A_i \neq \emptyset$.

Exercise 16.21. Show that:

$$\{\{\emptyset, \{x\}\}, \{\{y\}\}\} = \{\{\emptyset, \{z\}\}, \{\{w\}\}\} \Rightarrow x = z \wedge y = w \qquad \text{and}$$
$$\{x, \{x, y\}\} = \{z, \{z, w\}\} \Rightarrow x = z \wedge y = w.$$

(For the second implication use the axiom of foundation.) Therefore the definitions of order pair $(x, y)_{\mathrm{W}}$ and $(x, y)_{\mathrm{K}'}$ in Remark 16.4 are adequate.

Exercise 16.22. Show that there is no formula $\varphi(x, y, \vec{w})$ such that MK proves:

$$\exists \vec{w} \big[\forall x\, (\mathrm{Set}(x) \Rightarrow \exists! y\, \varphi(x, y, \vec{w})) \wedge \forall y \exists x (\mathrm{Set}(x) \wedge \varphi(x, y, \vec{w}))\big].$$

In other words, in MK there is no definable surjective map from V, the class of all sets, onto the collection of all classes. In layman's terms: are more classes than sets.

17. The theories MK, ZF, and NGB

The axiomatization of set theory was introduced in order to resolve the antinomies spawned by Russell's paradox. A possible axiomatization is the one seen in the preceding section—the theory MK—that talks about certain mathematical objects called classes. These split into two sub-collections: the "small" ones, that is sets, and the "large" ones, that is the proper classes. The axioms of MK are:

Extensionality: $\forall x \forall y\, (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.

Comprehension (axiom schema): For all $\mathcal{L}_\in$ formulæ

$$\varphi(x, y_1, \dots, y_n)$$

in which x occurs free, and for all variables A different from $x, y_1, \dots, y_n$,

$$\forall y_1 \dots \forall y_n \exists A\, \forall x\, (x \in A \Leftrightarrow \mathrm{Set}(x) \land \varphi(x, y_1, \dots, y_n))\,.$$

Existence of sets: $\exists x \exists y (x \in y)$.

Power-set: $\forall x\, (\exists y\, (x \in y) \Rightarrow \exists z \exists w\, (z \in w \land \forall t\, (t \in z \Leftrightarrow t \subseteq x)))$.

Pairing: $\forall x \forall y\, (\exists a\, (x \in a) \land \exists b\, (y \in b) \Rightarrow \exists z \exists c\, (z \in c \land z = \{x, y\}))$.

Foundation: $\forall A\, (A \neq \emptyset \Rightarrow \exists x\, (x \in A \land x \cap A = \emptyset))$.

Union: $\forall x\, (\mathrm{Set}(x) \Rightarrow \exists u\, (\mathrm{Set}(u) \land u = \bigcup x))$.

Infinity: $\exists x\, (\mathrm{Set}(x) \land \emptyset \in x \land \forall y\, (y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Replacement:

$$\forall F \forall A\, \bigl((\forall x \in \mathrm{dom}(F)\, \exists! y\, (x, y) \in F \land \mathrm{Set}(A)\bigr) \Rightarrow \mathrm{Set}(F``A)\bigr)\,. \tag{17.1}$$

The axioms above are only partially formalized in the language $\mathcal{L}_\in$ since we have used defined terms like $\subseteq$, $\{x, y\}$, $\cap$, $\emptyset$, $\bigcup$, $\mathbf{S}$, $F``A$, $\mathrm{dom}(F)$, and the formula $\mathrm{Set}(x)$. We leave to the reader the burden of removing these definite symbols (Exercise 16.19). Moreover we have used capital and lower case letters, in an attempt to make the meaning of the axioms more transparent. For example, in the case of the axiom of replacement, the letter F suggests that we are working with a function (to be precise: a functional relation). In the axiom of comprehension the letters (i.e. the variables) $y_1, \dots, y_n$ denote parameters, while the capital letter A is used for the class $\{x \mid \varphi(x, y_1, \dots, y_n)\}$ whose existence is postulated by the axiom.

It is possible to formulate MK in a two-sorted language—see Section 9.C. Formally we have a binary relation symbol $\in$ and two disjoint lists of variables $x_0, x_1, x_2, \dots$ for sets, and $X_0, X_1, X_2, \dots$, for classes. Here is how the axioms of MK look like. Note the axiom of set existence follows logically from $\exists x(x = x)$, but on the other hand an axiom stating that sets are classes must be added.

Sets are classes: $\forall x\, \exists X\, (x = X)$.

Extensionality: $\forall X \forall Y\, (\forall z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y)$.

Comprehension (axiom schema): For $\varphi(x, Y_1, \dots, Y_n, z_1, \dots, z_m)$ an $\mathcal{L}_\in$ formula in which x occurs free, and for all variables A different from $Y_1, \dots, Y_n$,

$$\forall Y_1 \dots \forall Y_n \forall z_1 \dots \forall z_m \exists A\, \forall x\, (x \in A \Leftrightarrow \varphi(x, Y_1, \dots, Y_n, z_1, \dots, z_m))\,.$$

Power-set: $\forall x \exists y \forall z\, (z \in y \Leftrightarrow \forall w (w \in z \Rightarrow w \in x))$.

Pairing: $\forall x \forall y \exists z \forall w \, (w \in z \Leftrightarrow w = x \vee w = y)$.

Foundation: $\forall X \, (\exists y (y \in X) \Rightarrow \exists y \, (y \in X \wedge \neg \exists w (w \in y \wedge w \in X)))$.

Union: $\forall x \exists u \forall y \, (y \in u \Leftrightarrow \exists z (z \in x \wedge y \in z))$.

Infinity: $\exists x \, (\emptyset \in x \wedge \forall y \, (y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Replacement: $\forall F \forall a \, \big(\big(\forall x \in \operatorname{dom}(F) \, \exists! y (x, y) \in F \big) \Rightarrow \exists b (b = F``a) \big)$.

17.A. The Zermelo-Frænkel axioms. Another axiomatization of set theory is due to Zermelo and Frænkel, and it generally known with the acronym ZF. Just like MK, it is formulated in the language $\mathcal{L}_\in$, hence the notion of formula of set theory remains the same, but, contrarily to MK, it is a theory that talks only about sets. Proper classes in ZF are formulæ describing a collection without formal counterpart in the theory. For example: instead of the class of all groups one considers the formula $\gamma(x)$ asserting that x is a group, that is x is an ordered pair $(G, *)$, where G is a non-empty set and $*$ is a binary operation on G inducing a group structure. Similarly, the class of all topological spaces is the formula $\tau(x)$ stating that x is an ordered pair $(X, \mathcal{O})$ where X is a non-empty set and $\mathcal{O}$ is a topology on X. In particular, the class V of all sets has no right to exists in ZF. The axioms of extensionality and foundation are exactly as in MK; the axioms of pairing, powerset, union, and infinity are *essentially* as in MK, except that we do not need to state that we are dealing with sets:

Pairing: $\forall x \forall y \exists z \, (z = \{x, y\})$.

Power-set: $\forall x \exists y \forall z \, (z \in y \Leftrightarrow z \subseteq x)$.

Union: $\forall x \exists y \forall z \, (z \in y \Leftrightarrow \exists u \, (u \in x \wedge z \in u))$.

Infinity: $\exists x \, (\emptyset \in x \wedge \forall y \, (y \in x \Rightarrow \mathbf{S}(y) \in x))$.

The axiom-schema of comprehension is replaced by

Separation (axiom schema): *For any $\varphi(x, B, y_1, \ldots, y_n)$ such that x occurs free in it, and for any variable A different from $x, B, y_1, \ldots, y_n$,*

$$\forall y_1 \ldots \forall y_n \forall B \exists A \forall x \, (x \in A \Leftrightarrow x \in B \wedge \varphi(x, B, y_1, \ldots, y_n)) \, .$$

In other words: for any set B and any formula φ the set $A = \{x \in B \mid \varphi(x, y_1, \ldots, y_n)\}$ exists. The axiom of replacement is supplanted by the following axiom-schema:

Replacement (axiom-schema): *For any* $\varphi(x, y, A, z_1, \dots, z_n)$ *and any variable* B *different from* $x, y, A, z_1, \dots, z_n$,

$$\forall A \forall z_1 \dots \forall z_n \left(\forall x \left(x \in A \Rightarrow \exists ! y \varphi(x, y, A, z_1, \dots, z_n)\right) \Rightarrow \exists B \forall y \left(y \in B \Leftrightarrow \exists x \left(x \in A \wedge \varphi(x, y, A, z_1, \dots, z_n)\right)\right)\right).$$

In other words: given sets $A, z_1, \dots, z_n$, if the formula φ defines a function $x \mapsto y$ on the set A, then there is a set B whose elements are exactly all these y.

Note that (17.1) is a single axiom, while the axiom-schema of replacement[3] of ZF is an infinite list of statements. Russell's paradox is disarmed by ZF as follows. First of all the collection R in (16.1) was not defined using the axiom of separation, thus we cannot infer that it is a set, i.e. a legitimate object in ZF. In fact ZF proves that: $\neg \exists x \forall y \, (y \notin y \Rightarrow y \in x)$. To see this, suppose, towards a contradiction, that such a set x exists: then $x = \mathrm{R}$, and the implications (16.2a) and (16.2b) would still be valid, leading to a contradiction. It follows that R is *not* a set, hence Russell's paradox vanishes.

17.B. The von Neumann-Gödel-Bernays axioms. There is a third approach to axiomatic set theory, due to von Neumann and developed by Gödel and Bernays, aptly named NGB. As in the case of MK, the theory NGB deals with both sets and classes. The axioms of this theory are more easily stated in a two-sorted language: as before, upper case letters range on classes, while lower case letters range over sets. If we wanted to stick to the usual one sorted language, we should replace each occurrence of quantification over sets $\exists x \, \varphi(x)$ and $\forall x \, \varphi(x)$ with $\exists X \, (\mathrm{Set}(X) \wedge \varphi(X))$ and $\forall X \, (\mathrm{Set}(X) \Rightarrow \varphi(X))$.

Sets are classes: $\forall x \, \exists X \, (x = X)$,

Classes belonging to classes are sets: $\forall X \, \forall Y \, (X \in Y \Rightarrow \exists x \, (x = X))$,

Extensionality: $\forall X \forall Y \, (\forall z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y)$,

Pairing: $\forall x \forall y \exists z \forall w \, (w \in z \Leftrightarrow w = x \vee w = y)$.

A formula is **predicative** if the only quantified variables are set-variables.

Predicative comprehension (axiom schema): If x is free in the predicative formula $\varphi(x, y_1, \dots, y_n, Z_1, \dots, Z_m)$, and X does not occur in φ, then

$$\forall y_1, \dots, y_n, Z_1, \dots, Z_m \exists X \forall x (x \in X \Leftrightarrow \varphi(x, y_1, \dots, y_n, Z_1, \dots, Z_m)).$$

Separation: $\forall x \forall Y \exists z \forall w \, (w \in z \Leftrightarrow w \in x \wedge w \in Y)$, that is: the intersection of a class with a set is a set.

Power-set: $\forall x \exists y \forall z \, (z \in y \Leftrightarrow z \subseteq x)$.

[3] In order to tell apart the axiom of replacement in MK (a single statement) from the one in ZF (an infinite list of statements), the former is called **strong replacement**.

Foundation: $\forall X\,(\exists y\,(y \in X) \Rightarrow \exists y\,(y \in X \wedge \forall z\,(z \notin y \cap X)))$.

Union: $\forall x \exists y \forall z\,(z \in y \Leftrightarrow \exists u\,(u \in x \wedge z \in u))$.

Infinity: $\exists x\,(\emptyset \in x \wedge \forall y\,(y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Replacement: $\forall F \forall a \bigl[\forall x\,(x \in a \Rightarrow \exists! y\,(x,y) \in F) \Rightarrow \exists b \forall y\,(y \in b \Leftrightarrow \exists x\,(x \in a \wedge (x,y) \in F))\bigr]$.

17.C. MK vs NGB vs ZF. Although the vast majority of the objects studied in mathematics are sets, it is often useful to be able to speak of the class of all groups, or the class of all topological spaces, or the class of all finite sets—this is particularly relevant when using the language of categories (Section 22). For this reason some mathematicians prefer a theory like MK or NGB over ZF. On the other hand these theories do not seem to be very satisfactory either, since it is not possible to construct aggregates such as classes-of-classes like $\mathscr{P}(\mathrm{V})$, or classes-of-classes-of-classes like $\mathscr{P}(\mathscr{P}(\mathrm{V}))$, etc. These very large aggregates occur in various part of mathematics, for example the topology on the class of all ordinals (Section 21.D), the category of all categories (Section 22), the topology on the class of all $\mathcal{L}$-structures (Section 15), and so on. Actually if we extend ZF by adding strong forms of the axiom of infinity it is possible to capture the concept of class, of class-of-classes, class-of-classes-of-classes,... and much more. For this reason research in set theory takes place for the most part in ZF or in some extension of it.

The axioms of MK that we presented form an infinite list, and the same is true were of ZF and NGB. In Chapter VIII we will prove that for ZF and MK this is not an accident, since these theories are not finitely axiomatizable, while, quite surprisingly, NGB is finitely axiomatizable.

In MK and NGB it is possible to prove theorems of the form

$$\exists X\,(\neg\,\mathrm{Set}(X) \wedge \ldots X \ldots) \tag{17.2}$$

and

$$\forall X\,(\neg\,\mathrm{Set}(X) \Rightarrow \ldots X \ldots) \tag{17.3}$$

that is statements of the form: “There is a proper class X such that ...” and “For all proper classes X it happens that ...”. Clearly in MK and NGB one can prove much more complex statements, like: “For each proper class X there is a proper class Y such that ...”. In ZF one might prove existential statements as in (17.2): in this case we must *explicitly produce a formula* defining the proper class X with the required properties. In MK and in NGB the burden is lighter and we may prove (17.2) by contradiction: assuming no proper class X satisfies the required property, a contradiction is argued in MK or in NGB. In ZF statements of the form (17.3) are problematic: a “theorem” of this kind must be proved case-by-case, one for each formula

φ defining the class X. The ensuing result is a *scheme of theorems* or a *metatheorem.*

The discussion above may suggest that the difference between MK and ZF pertains only to proper classes, and that the theorems about sets be the same in either theory. Every statement on sets provable in ZF is also a theorem of MK, but not conversely: there are statements on the natural numbers that are provable in MK, but not in ZF. In fact these can be taken to be of the form

$$\forall n \in \mathbb{N}\ P(n)$$

where P is a recursive predicate. Admittedly, statements of this form are quite rare, and by and large, a result about *sets* proved in MK is also provable in ZF, essentially with the same proof. On the other hand, any statement about *sets* proved in NGB, can be proved inside ZF.

17.D. Set theory as a foundation for mathematics. In the remaining sections we shall show how to reconstruct mathematics within axiomatic set theory, giving a rigorous proof of even the simplest results. In particular, the results in Chapter I, III and **??** will be shown to be provable in MK, in NGB, and in ZF. Let us see how.

The structure $\langle \mathbb{N}, \mathbf{S}, 0\rangle$ is inductive (Proposition 16.8), hence by what was said at the end of Section 12.A, the two operations $+$ and $\cdot$ are defined on $\mathbb{N}$, and satisfy the recursive definitions of sum and product. In Section 18 we shall define ordinals (and cardinals) and their ordering; the set $\mathbb{N}$ will be an ordinal and we will check that its ordering satisfies the minimum principle, enabling us to recover all results from Section 12. In particular, it is possible to define the bijection $\boldsymbol{J}\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ of (8.1) on page 204, hence one can prove that $\mathbb{N} \times \mathbb{N} \asymp \mathbb{N}$ (Theorem 13.14). The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are defined as in Section 13, and hence $\mathbb{N} \asymp \mathbb{Z} \asymp \mathbb{Q}$, and $\mathscr{P}(\mathbb{N}) \asymp \mathbb{R} \asymp \mathbb{C}$, and $\mathscr{P}(\mathbb{N})$ is uncountable.

The definition of first-order language, term, formula, will be given in Section 30.B, and the satisfaction relation will be given in Section 31.A: the ancillary notions (such as: free/bound occurrences of variables, etc.) are particular cases of results on finite strings of Section 23.

Exercises

Exercise 17.1. Let σ be the statement $\exists x' \exists x \forall y (y \notin x \wedge x \in x')$, that the assertion that empty set exists. Clearly σ is a theorem of both ZF and MK. Consider the following theories

T_1: σ + pairing axiom + powerset axiom,

T_2: σ + union axiom + powerset axiom,

T_3: σ + pairing axiom + union axiom + powerset axiom.

Which of the theories above proves the existence of a set with 5 elements?

Exercise 17.2. Show that in the presence of the other axioms of MK, the axiom of replacement (17.1) is equivalent to its injective version: *If F is an injective functional relation and A is a set, then $F[A]$ is a set.*

Prove a similar result for ZF.

Exercise 17.3. Show that NGB can be formalized using one sort of variables.

Exercise 17.4. In this exercise, let's assume that both MK and NGB are formulated in a two sorted language. Show that:

(i) every axiom of ZF is provable in NGB;

(ii) every axiom of NGB is provable in MK.

Notes and remarks

The axiomatization of set theory was completed only in the first half of the twentieth century, and it is the cooperative effort of many mathematicians, including Zermelo, Frænkel, von Neumann, Gödel, Bernays, Kelley and Morse. An excellent textbook in set theory covering ZF is [**Lev02**], while for NGB see [**Men15**]. The theory MK was developed independently by Kelley and Morse: the appendix of the book on general topology by Kelley [**Kel55**] contains a list of axioms equivalent to the ones presented here, while the Morse's monograph [**Mor65**] gives a detailed (and fairly idiosyncratic) presentation of the axioms of MK. The exposition in this book follows closely [**Mon69**].

18. Ordered sets and ordinals

The notions seen in Section 7 (pre-orders, equivalence relations, ...) can be recast in the language of classes. For example, we say that $R \subseteq X \times X$ is reflexive on the class X if $x \mathrel{R} x$ that is $(x, x) \in R$ for all $x \in X$, but we will refrain from writing

$$\langle X, R\rangle \vDash \forall x\, (x \mathrel{R} x)$$

since, as we shall see in Section 31.A, the satisfaction relation is defined only for structures that are *sets*.

The following notion is of interest only when dealing with proper classes.

Definition 18.1. $R \subseteq X \times X$ is **left-narrow** if $\{y \in X \mid y \mathrel{R} x\}$ is a set, for all $x \in X$.

Therefore an order $\leq$ on a proper class X is left-narrow if

$$\operatorname{pred}(x, X; \leq) = \{y \in X \mid y < x\}$$

is a set for all $x \in X$. Similarly, an equivalence relation E on a proper class X is left-narrow if every equivalence class is a set, hence the quotient[4] $X/E = \{[x]_E \mid x \in X\}$ can be defined. Extending the definitions in Section 13.A to classes, if $\langle X_0, \leq_0\rangle$ and $\langle X_1, \leq_1\rangle$ are ordered classes, we can define two orderings on $X_0 \times X_1$: the **product order** and the **lexicographic order** $\leq_{\mathrm{lex}}$. These constructions can be generalized: if $\langle I, \preccurlyeq\rangle$ is an ordered set and $\langle X_i, \leq_i\rangle$ with $i \in I$ are ordered classes, the product order on $\bigtimes_{i\in I} X_i$ is defined by

$$f \trianglelefteq g \Leftrightarrow \forall i \in I\,(f(i) \leq_i g(i))$$

while the lexicographic order is defined by

$$f \leq_{\mathrm{lex}} g \Leftrightarrow \exists i \in I \Big(\forall j \in I\,(j \prec i \Rightarrow f(j) = g(j)) \wedge f(i) \leq_i g(i)\Big),$$

where '$j \prec i$' means '$j \preccurlyeq i \wedge j \neq i$'. The ordering on $\biguplus_{i\in I} X_i = \bigcup_{i\in I} \{i\} \times X_i$ is defined by

$$(i,x) \leq_{\mathrm{lex}} (j,y) \Leftrightarrow (i \prec j \vee (i = j \wedge x \leq_i y))\,.$$

Definition 18.2. A relation $R \subseteq X \times X$ on a class X is **well-founded** if every non-empty subclass of X contains an R^*-minimal element, where $R^* = R \setminus R^{-1}$ is the strict part of R:

$$\forall Y \subseteq X\,(Y \neq \emptyset \Rightarrow \exists y \in Y\, \forall z \in Y\,((z,y) \in R \Rightarrow (y,z) \in R)).$$

If R is not well-founded on X we will say that it is **ill-founded**.

The axiom of foundation implies that $\{(x,y) \in \mathrm{V} \mid x \in y\}$ is irreflexive and well-founded, and since $\{y \mid y \in x\} = x$ is a set for all $x \in \mathrm{V}$, it is left-narrow.

A total, well-founded, left-narrow order is a **well-order**; if R is a well-order, then $R \setminus \mathrm{id}$ is a **strict well-order**. If R is a well-order on A and $B \subseteq A$ then R (or better: $R \cap B \times B$) is a well-order on B.

A class is well-orderable if it has a well-order. The implication (b)⇒(c) in the proof of Theorem 14.3 shows that:

Theorem 18.3. *If the class X is well-orderable, then there is a choice class-function on X.*

The following result is a straightforward generalization of Propositions 13.3 and 13.4 and Corollaries 13.5 and 13.6.

Theorem 18.4. *Let $\langle A, \leq\rangle$ be a well-ordered class.*

- *If $f\colon A \to A$ is increasing, then $\forall a \in A\,(a \leq f(a))$; if moreover f is bijective then $f = \mathrm{id}_A$.*

[4] In Section 20.C a method to define X/E when E is not left-narrow will be given.

- *If $\langle A, \leq \rangle$ and $\langle B, \trianglelefteq \rangle$ are isomorphic well-ordered classes, then the isomorphism is unique.*
- *If $a \in A$, then $\langle A, \leq \rangle$ and $\langle \mathrm{pred}(a, A; \leq), \leq \rangle$ are not isomorphic.*

18.A. Ordinals. We now give a rigorous treatment of ordinal numbers, which were already informally introduced in Section 13.A.

Definition 18.5. A class A is **transitive** if $\bigcup A \subseteq A$, that is if

$$\forall a \forall x \left((a \in A \wedge x \in a) \Rightarrow x \in A \right).$$

An **ordinal** is a transitive set such that all of its elements are transitive. The ordinals are usually denoted with lower case Greek letters α, β, ... and

$$\mathrm{Ord}$$

is the class of the ordinals.

The proof of the next result is straightforward, and it is left to the reader.

Proposition 18.6. (a) *If x is a transitive set, then $\bigcup x$ and $\mathbf{S}(x)$ are transitive.*

(b) *If $\alpha \in \mathrm{Ord}$ then $\alpha \subseteq \mathrm{Ord}$ and $\mathbf{S}(\alpha) \in \mathrm{Ord}$.*

(c) *If x is a set of ordinals, then $\bigcup x \in \mathrm{Ord}$.*

Proposition 18.7. Ord *is a proper class.*

Proof. The class Ord is transitive: if it were a set, then it would be an ordinal, hence Ord $\in$ Ord, against the axiom of foundation. □

Theorem 18.8. *Two ordinals are $\in$-comparable, that is for $\alpha, \beta \in \mathrm{Ord}$ exactly one of the following possibilities holds:*

$$\alpha \in \beta \ \vee \ \alpha = \beta \ \vee \ \beta \in \alpha.$$

Proof. The axiom of foundation implies that two distinct possibilities cannot hold simultaneously, so we are left to prove that at least one holds. We must show that

$$A = \{\alpha \in \mathrm{Ord} \mid \exists \beta \in \mathrm{Ord}\, (\alpha \notin \beta \ \wedge \ \alpha \neq \beta \ \wedge \ \beta \notin \alpha)\}$$

is empty. If $A \neq \emptyset$, by foundation there is $\bar{\alpha} \in A$ such that

$$\bar{\alpha} \cap A = \emptyset. \tag{18.1}$$

Then $B = \{\beta \in \mathrm{Ord} \mid \beta \notin \bar{\alpha} \ \wedge \ \beta \neq \bar{\alpha} \ \wedge \ \bar{\alpha} \notin \beta\}$ is a non-empty class, and again by foundation there is $\bar{\beta} \in B$ such that $\bar{\beta} \cap B = \emptyset$. If $\gamma \in \bar{\alpha}$ then (18.1) implies that $\gamma \notin A$, hence in particular $\bar{\beta} \in \gamma \ \vee \ \bar{\beta} = \gamma \ \vee \ \gamma \in \bar{\beta}$. The first two possibilities and the transitivity of $\bar{\alpha}$ imply that $\bar{\beta} \in \bar{\alpha}$, contradicting $\bar{\beta} \in B$. Therefore $\gamma \in \bar{\beta}$. Since γ is arbitrary, we obtain $\bar{\alpha} \subseteq \bar{\beta}$. Similarly $\bar{\beta} \subseteq \bar{\alpha}$ hence $\bar{\alpha} = \bar{\beta}$ a contradiction. □

Corollary 18.9. *The membership relation $\in$ is a strict well-order on* Ord*, and hence on every ordinal α.*

For this reason we stipulate that

$$\boxed{\alpha < \beta \text{ means } \alpha \in \beta, \text{ and } \alpha \leq \beta \text{ means } \alpha \in \beta \vee \alpha = \beta.}$$

If $\emptyset \neq A \subseteq \mathrm{Ord}$, then the $\in$-minimal element of A is the minimum of A. From Theorem 18.4 we get:

Proposition 18.10. (a) *If $f \colon \alpha \to \beta$ is increasing, then $\gamma \leq f(\gamma)$ for all $\gamma \in \alpha$, and $\alpha \leq \beta$.*

(b) *If $f \colon \alpha \to \beta$ is an isomorphism, then $\alpha = \beta$ and f is the identity.*

Similarly, if $f \colon \mathrm{Ord} \to \mathrm{Ord}$ is increasing then $\gamma \leq f(\gamma)$ and if moreover f is surjective, then it is the identity.

Notation. We will write $A \leq \mathrm{Ord}$ in lieu of "$A \in \mathrm{Ord} \vee A = \mathrm{Ord}$" and use the letter Ω to denote such a class A. In other words, either $\Omega \in \mathrm{Ord}$ or else $\Omega = \mathrm{Ord}$.

Any ordinal α yields a well-order $\langle \alpha, \leq \rangle$ and if $\beta \in \alpha$, then $\beta = \mathrm{pred}(\beta, \alpha; \leq)$. Theorem 18.4 implies that $\langle \alpha, \leq \rangle \cong \langle \beta, \leq \rangle$ if and only if $\alpha = \beta$.

Let $\langle X, \trianglelefteq \rangle$ be a well-ordered class and let

$$A = \{\alpha \in \mathrm{Ord} \mid \exists x \in X\, (\langle \alpha, \leq \rangle \cong \langle \mathrm{pred}(x), \trianglelefteq \rangle)\}$$

be the class of the ordinals isomorphic to some initial segment of X. Suppose $f \colon \langle \alpha, \leq \rangle \to \langle \mathrm{pred}(x), \trianglelefteq \rangle$ is the isomorphism witnessing $\alpha \in A$. If $\beta \in \alpha$ then $f \restriction \beta \colon \langle \beta, \leq \rangle \to \langle \mathrm{pred}(f(\beta)), \trianglelefteq \rangle$ is an isomorphism, hence $\beta \in A$. It follows that A is a transitive class of ordinals, hence $A \leq \mathrm{Ord}$. Let $F \colon A \to X$ be the functional relation that sends $\alpha \in A$ to the unique $x \in X$ such that $\langle \alpha, \leq \rangle \cong \langle \mathrm{pred}(x), \trianglelefteq \rangle$. It is immediate to check that $\mathrm{ran}(F)$ is an initial segment of X. If, towards a contradiction, $\mathrm{ran}(F) \neq X$, then $\mathrm{ran}(F) = \mathrm{pred}(\bar{x}, \trianglelefteq)$, for some $\bar{x} \in X$. Since $A \asymp \mathrm{pred}(\bar{x}, \trianglelefteq)$, it follows that $A \in \mathrm{Ord}$ hence $A \in A$ by definition of A: a contradiction. Therefore F is surjective. By Theorem 18.4 and what we just proved we have the following:

Theorem 18.11. *Every well-ordered set is isomorphic to a unique ordinal, and every well-ordered proper class is isomorphic to* Ord*. Moreover the isomorphism is unique.*

Theorems 18.8 and 18.11 yield:

Theorem 18.12. *If $\langle A, \leq \rangle$ and $\langle B, \preceq \rangle$ are well-ordered classes, then exactly one of the following holds:*

(1) $\exists a \in A\,(\langle \mathrm{pred}(a), \leq \rangle \cong \langle B, \preceq \rangle)$

(2) $\exists b \in B\,(\langle \mathrm{pred}(b), \preceq \rangle \cong \langle A, \leq \rangle)$

(3) $\langle A, \leq \rangle \cong \langle B, \preceq \rangle$.

In particular, any two well-ordered proper classes are isomorphic.

If $\langle X, \preceq \rangle$ is a well-ordered class, its **order type** is the unique $\Omega \leq \mathrm{Ord}$ isomorphic to $\langle X, \preceq \rangle$ and it is denoted by $\mathrm{ot}\,\langle X, \preceq \rangle$ or simply with $\mathrm{ot}(X)$ if the ordering is clear from the context. In particular $\mathrm{ot}(A) = \mathrm{Ord}$ for all proper classes $A \subseteq \mathrm{Ord}$. The unique isomorphism $\langle \Omega, \leq \rangle \to \langle X, \preceq \rangle$ is the **enumerating function**.

Proposition 18.13. *If* $\emptyset \neq A \subseteq \mathrm{Ord}$ *then* $\min A = \bigcap A$.

Proof. By foundation if $\bar{\alpha} \in A$ is such that $\bar{\alpha} \cap A = \emptyset$, then $\forall \alpha \in A\,(\bar{\alpha} \subseteq \alpha)$, so $\bigcap A = \bar{\alpha} = \min A$. □

A particular case of Theorem 16.11 is

Corollary 18.14. *There is no descending chain of ordinals, that is to say* $\neg \exists f\,(f \colon \mathbb{N} \to \mathrm{Ord} \wedge \forall n (f(\mathbf{S}(n)) < f(n)))$.

Lemma 18.15. (a) *Every natural number is an ordinal.*

(b) *If* $n \in \mathbb{N}$ *and* $x \in n$ *then* $x \in \mathbb{N}$.

Proof. (a) Towards a contradiction, suppose $X = \mathbb{N} \setminus \mathrm{Ord}$ is non-empty, and let $n \in X$ be such that $n \cap X = \emptyset$. Since 0 is an ordinal, it follows that $n \neq 0$ hence, by Proposition 16.7 $n = \mathbf{S}(m)$ for some $m \in \mathbb{N}$. Then $m \in \mathrm{Ord}$ and therefore $\mathbf{S}(m) \in \mathrm{Ord} \cap \mathbb{N}$: a contradiction.

(b) Towards a contradiction, suppose $X = \{n \in \mathbb{N} \mid \exists x \in n\,(x \notin \mathbb{N})\}$ is non-empty, and let $\bar{n} \in X$ be such that $\bar{n} \cap X = \emptyset$. Fix $\bar{x} \in \bar{n}$ such that $\bar{x} \in \bar{n} \setminus \mathbb{N}$. By Proposition 16.7, $\bar{n} = \mathbf{S}(\bar{m})$ for some $\bar{m} \in \mathbb{N}$, hence either $\bar{x} \in \bar{m}$ or else $\bar{x} = \bar{m}$. It is immediate to check that either way a contradiction is obtained. □

An ordinal α is **successor** if $\alpha = \mathbf{S}(\beta)$, for some β. Clearly $\alpha < \mathbf{S}(\alpha)$ and there is no β such that $\alpha < \beta < \mathbf{S}(\alpha)$. In other words $\mathbf{S}(\alpha)$ is the immediate successor of α in the ordering given by $\in$. If an ordinal is not a successor and it is not 0, it is **limit**.

In set theory it is customary to denote $\mathbb{N}$ by ω.

Theorem 18.16. ω *is the smallest limit ordinal.*

Proof. ω is an ordinal by Lemma 18.15, and by Proposition 16.7 there are no limit ordinals smaller than ω. It is enough to check that ω is not a successor.

If, towards a contradiction, $\omega = \mathbf{S}(\alpha)$, then $\alpha \in \omega$, hence $\mathbf{S}(\alpha) \in \omega$, that is $\omega \in \omega$: a contradiction. □

Proposition 18.17. (a) *$\alpha < \beta \Leftrightarrow \alpha \subset \beta$;*

(b) *$\alpha \leq \beta \Leftrightarrow \alpha \subseteq \beta$;*

(c) *$\alpha < \beta \Leftrightarrow \mathbf{S}(\alpha) \leq \beta$;*

(d) *$\alpha < \beta \Leftrightarrow \mathbf{S}(\alpha) < \mathbf{S}(\beta)$;*

(e) *$x \subseteq \alpha \Rightarrow (\bigcup x = \alpha \vee \bigcup x < \alpha)$;*

(f) *$\bigcup(\mathbf{S}(\alpha)) = \alpha$;*

(g) *$\alpha = \mathbf{S}(\bigcup \alpha) \vee \alpha = \bigcup \alpha$;*

(h) *$\bigcup \alpha = \alpha \Leftrightarrow (\alpha = 0 \vee \alpha$ limit$) \Leftrightarrow \langle \alpha, < \rangle$ has no maximum.*

Proof. (a) If $\alpha \in \beta$ then $\alpha \subseteq \beta$ by transitivity. The axiom of foundation implies $\alpha \neq \beta$, hence $\alpha \subset \beta$. Conversely, suppose $\alpha \subset \beta$: foundation implies that $\beta \notin \alpha$ and since $\beta \neq \alpha$ it follows that $\alpha \in \beta$.

(b) is similar to (a).

(c) Let $\alpha < \beta$. Since $\beta \in \mathbf{S}(\alpha)$ is impossible, then either $\beta = \mathbf{S}(\alpha)$ or $\mathbf{S}(\alpha) \in \beta$. The converse implication is immediate.

(d) is similar to (c).

(e) $\bigcup x$ is an ordinal by Proposition 18.6 hence it is comparable to α. But $\alpha \in \bigcup x$ implies that $\alpha \in \beta \in x \subseteq \alpha$, for some β: a contradiction. Therefore $\bigcup x \leq \alpha$.

(f) $\beta \in \bigcup \mathbf{S}(\alpha)$ if an only if either $\beta \in \gamma \in \alpha$ for some γ or else $\beta \in \alpha$. Therefore $\beta \in \bigcup \mathbf{S}(\alpha) \Leftrightarrow \beta \in \alpha$.

(g) As $\mathbf{S}(\alpha) \supseteq \alpha$ then $\alpha = \bigcup \mathbf{S}(\alpha) \supseteq \bigcup \alpha$ by part (f). If $\bigcup \alpha < \alpha$, then by (c) $\mathbf{S}(\bigcup \alpha) \leq \alpha$, hence it is enough to prove that the strict inequality does not hold: if $\mathbf{S}(\bigcup \alpha) \in \alpha$ then $\bigcup \alpha \in \mathbf{S}(\bigcup \alpha)$ implies that $\bigcup \alpha \in \bigcup \alpha$, a contradiction.

(h) follows from (f) and (g). □

Thus λ is limit if and only if $\lambda = \bigcup \lambda > 0$.

Proposition 18.18. *If $A \subseteq \mathrm{Ord}$ is a set, then $\bigcup A = \sup A$.*

Proof. The result follows from the following three easy facts: the first is that $\bigcup A$ is the smallest set containing every $\alpha \in A$, the second is that $\bigcup A$ is an ordinal, the third is that $\leq$ and $\subseteq$ agree on the ordinals. □

18.B. Cardinals. A class is **finite** if is in bijection with a natural number, otherwise is said to be **infinite**. Since natural numbers are sets, finite classes are sets and proper classes are infinite.

Definition 18.19. A **cardinal** is an ordinal κ that is not in bijection with any $\alpha < \kappa$. Cardinals are usually denoted with greek letters such κ, λ, ... and Card is the class of cardinals.

A class X is **well-orderable** if there is a well-order on X—equivalently, by Theorem 18.11, if X is in bijection with some $\Omega \leq \mathrm{Ord}$. By Exercise 18.42, if X is well-orderable and Y is in bijection with (or even if it is surjective image of) X, then Y is well-orderable; conversely, if Y is well-orderable and $X \precsim Y$, then X is well-orderable.

Definition 18.20. If X is a well-orderable *set*, the **cardinality of** X is the smallest ordinal $|X|$ in bijection with X. In particular, $|\alpha|$ is the smallest ordinal $\beta \asymp \alpha$, so $|\alpha| \leq \alpha$.

Thus, the cardinality of a set (if it exists, i.e. if the set is well-orderable) is a cardinal. The axiom of choice is equivalent to the statement that every set is well-orderable (Theorem 14.3) hence $|X|$ is defined for *every set* X if AC is assumed. Theorem 13.15 implies that every natural number is cardinals, and that ω is the first infinite cardinal. On the other hands, $\mathbf{S}(\omega)$, $\mathbf{S}(\mathbf{S}(\omega))$, $\mathbf{S}(\mathbf{S}(\mathbf{S}(\omega)))$, ... are not cardinals (Proposition 18.22).

Proposition 18.21. *If κ and λ are cardinals,*

(a) $\kappa = \lambda$ *if and only if* $\kappa \asymp \lambda$,

(b) $\kappa \leq \lambda$ *if and only if* $\kappa \precsim \lambda$. *In particular: if X and Y are well-orderable, then* $|X| \leq |Y| \Leftrightarrow \exists f(f\colon X \rightarrowtail Y)$.

Proof. (a) Suppose that $\kappa \asymp \lambda$ and that $\kappa \neq \lambda$, e.g. $\kappa < \lambda$. Then λ would be in bijection with a smaller ordinal, a contradiction.

(b) Towards a contradiction suppose $\kappa \precsim \lambda$ and $\lambda < \kappa$. Then $\mathrm{id}_\lambda \colon \lambda \rightarrowtail \kappa$ so by the Cantor-Schröder-Bernstein Theorem 13.11 $\kappa \asymp \lambda$, hence $\kappa = \lambda$ by part (a), a contradiction. □

Proposition 18.22. (a) *If $\alpha \geq \omega$ then* $|\alpha| = |\mathbf{S}(\alpha)|$,

(b) $|\alpha| \leq \beta \leq \alpha \Rightarrow |\alpha| = |\beta|$,

(c) $|\alpha| = |\beta|$ *if and only if* $\alpha \asymp \beta$,

(d) $|\alpha| \leq |\beta|$ *if and only if* $\alpha \precsim \beta$.

Proof. (a) The function $\mathbf{S}(\alpha) \to \alpha$ which is the identity on $\alpha \setminus \omega$ and sending $n \mapsto \mathbf{S}(n)$, if $n < \omega$, and $\alpha \mapsto 0$ is a bijection.

(b) Let $f\colon \alpha \to |\alpha|$ be a bijection. Since $f\colon \alpha \to \beta$ is injective and β injects into α, then $|\alpha| = |\beta|$ by the Cantor-Schröder-Bernstein 13.11 and Proposition 18.21.

(c) and (d) follow from Proposition 18.21. □

The only examples of cardinals we have encountered so far are the natural numbers and ω, hence it is natural to ask whether there exist larger cardinals. By Cantor's Theorem 13.22, $\mathscr{P}(\omega)$ is not countable, so if we want an uncountable cardinal we could well-order $\mathscr{P}(\omega)$ and compute its cardinality. A well-ordering of $\mathscr{P}(\omega)$ requires AC, so the question is: can we prove the existence of an uncountable cardinal without choice? The answer is affirmative, and actually for any set X there is a least ordinal κ that does not inject into X, and in fact κ is a cardinal. (This cardinal will come handy in Section 20.B.) Here are the details.

Given a set X, let

$$A = \{(\alpha, f) \mid \alpha \in \mathrm{Ord} \wedge f\colon \alpha \rightarrowtail X\}.$$

For each $(\alpha, f) \in A$ let $W_{(\alpha,f)}$ be the well-order on $\mathrm{ran}(f) \subseteq X$ induced by f, that is

$$x \mathrel{W_{(\alpha,f)}} y \Leftrightarrow f^{-1}(x) \leq f^{-1}(y).$$

Thus $f\colon \langle \alpha, \leq\rangle \to \langle \mathrm{ran}(f), W_{(\alpha,f)}\rangle$ is an isomorphism. If $(\alpha, f), (\beta, g) \in A$ and $W_{(\alpha,f)} = W_{(\beta,g)}$ then $g^{-1} \circ f\colon \langle \alpha, \leq\rangle \to \langle \beta, \leq\rangle$ is an isomorphism, hence $\alpha = \beta$ and $f = g$ by Proposition 18.10. In other words: the function

$$A \to \mathscr{P}(X \times X), \qquad (\alpha, f) \mapsto W_{(\alpha,f)} \tag{18.2}$$

is injective, hence A is a set by the replacement and power-set axioms. Its projection on the first coordinate $B = \{\alpha \in \mathrm{Ord} \mid \alpha \precsim X\}$ is a transitive set, hence it is an ordinal. The ordinal B is the smallest ordinal that does not embed into X and it is called the **Hartogs' number** of the set X, denoted by

$$\mathrm{Hrtg}(X).$$

By taking the inverse of the function in (18.2) a surjection $\mathscr{P}(X \times X) \twoheadrightarrow A$ is obtained, and composing with the projection $A \twoheadrightarrow \mathrm{Hrtg}(X)$ we obtain the surjection $\mathscr{P}(X \times X) \twoheadrightarrow \mathrm{Hrtg}(X)$. Let us show that $\mathrm{Hrtg}(X)$ is a cardinal: towards a contradiction, if $|\mathrm{Hrtg}(X)| \in \mathrm{Hrtg}(X)$, then $\mathrm{Hrtg}(X) \precsim |\mathrm{Hrtg}(X)| \precsim X$, a contradiction. We have proved the following

Theorem 18.23. *For any set X, $\mathrm{Hrtg}(X)$ is the smallest ordinal that does not inject into X, and it is a cardinal. Moreover $\mathscr{P}(X \times X)$ surjects onto $\mathrm{Hrtg}(X)$.*

Definition 18.24. $\alpha^+ = \mathrm{Hrtg}(\alpha)$.

Thus α^+ is the smallest cardinal strictly larger than α, and if $\alpha \geq \omega$, then $\alpha^+ = \bigcup\{\beta \mid |\beta| = |\alpha|\} = \{\beta \mid |\beta| \leq |\alpha|\}$. In Section 18.C we will show (Theorem 18.28) that $\alpha \times \alpha \asymp \alpha$, for all $\alpha \geq \omega$, hence

$$\forall \alpha \geq \omega \left(\mathscr{P}(\alpha) \twoheadrightarrow \alpha^+\right). \tag{18.3}$$

As $\mathbb{R} \asymp \mathscr{P}(\omega)$ surjects onto ω^+ but ω does not, we obtain another proof of the fact that $\mathbb{R}$ is uncountable.

Theorem 18.25. *If X is a set of cardinals, then* $\sup X$ *is a cardinal.*

Proof. If $\lambda = \bigcup X$ were not a cardinal, then $|\lambda| < \lambda$ hence $|\lambda| < \kappa \leq \lambda$ for some $\kappa \in X$ and hence $|\kappa| = |\lambda|$, that is κ would not be a cardinal, a contradiction. □

Corollary 18.26. Card *is a proper class, and it is closed in* Ord.

18.C. Cardinal arithmetic.

Definition 18.27. Cardinal addition and **cardinal multiplication** are the binary operations Card × Card → Card defined by

$$\kappa + \lambda = |\{0\} \times \kappa \cup \{1\} \times \lambda| \qquad\qquad \kappa \cdot \lambda = |\kappa \times \lambda|.$$

These operations are well defined since $\kappa \uplus \lambda = \{0\} \times \kappa \cup \{1\} \times \lambda$ and $\kappa \times \lambda$ are well-ordered by the lexicographic order. By (13.5),

$$2 \leq \kappa, \lambda \Rightarrow \kappa + \lambda \leq \kappa \cdot \lambda. \tag{18.4}$$

Note that by part (a) of Proposition 18.22, this formula holds even with one of the two cardinals is 1 and the other is $\geq \omega$. Thus if κ and λ are cardinals and either $2 \leq \min(\kappa, \lambda)$ or else $1 = \min(\kappa, \lambda)$ and $\omega \leq \max(\kappa, \lambda)$, then

$$\max(\kappa, \lambda) \leq \kappa + \lambda \leq \kappa \cdot \lambda \leq \max(\kappa, \lambda) \cdot \max(\kappa, \lambda). \tag{18.5}$$

The **Gödel well-ordering $<_{\mathrm{G}}$ on** Ord × Ord is defined by

$$(\alpha, \beta) <_{\mathrm{G}} (\gamma, \delta) \Leftrightarrow$$
$$\Big[\max(\alpha, \beta) < \max(\gamma, \delta) \vee \big(\max(\alpha, \beta) = \max(\gamma, \delta) \wedge (\alpha, \beta) <_{\mathrm{lex}} (\gamma, \delta)\big)\Big].$$

The ordering $<_{\mathrm{G}}$ coincides with the ordering on ω given by the square enumeration (see pag. 203), and if $\alpha < \beta$ then $\alpha \times \alpha$ is an initial segment of $\beta \times \beta$.

Theorem 18.28. *Let κ be an infinite cardinal. Then* $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) = \kappa$ *and* $|\kappa \times \kappa| = \kappa$.

Proof. The function $\langle \kappa, < \rangle \to \langle \kappa \times \kappa, <_{\mathrm{G}} \rangle$, $\alpha \mapsto (\alpha, 0)$, is increasing hence $\kappa \leq \mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}})$. Therefore it is enough to show by induction on $\kappa \geq \omega$ that $\mathrm{ot}(\kappa \times \kappa, <_{\mathrm{G}}) \leq \kappa$, hence $|\kappa \times \kappa| = \kappa$.

Let $\alpha < \kappa$. If $\alpha < \omega$, then $|\alpha \times \alpha| < \omega$ by Proposition 13.20. If instead $\omega \leq \alpha$, then $\omega \leq |\alpha| < \kappa$ hence, by inductive assumption, $|\alpha| \times |\alpha|$ is of size $|\alpha|$. As $|\alpha| \times |\alpha|$ is in bijection with $\alpha \times \alpha$, we have that $|\alpha \times \alpha| < \kappa$. Therefore we have proved that $\forall \alpha < \kappa\, (|\alpha \times \alpha| < \kappa)$. Fix $\alpha, \beta < \kappa$. The set $\operatorname{pred}(\alpha, \beta)$ of all $<_{\mathrm{G}}$-predecessors of (α, β) is included in $\nu \times \nu$, where $\nu = \max\{\alpha, \beta\} + 1$, hence $|\operatorname{pred}(\alpha, \beta)| \leq |\nu \times \nu| < \kappa$. We have thus shown that $\forall \alpha, \beta < \kappa\, (\operatorname{ot} \operatorname{pred}(\alpha, \beta) < \kappa)$, hence $\operatorname{ot}(\kappa \times \kappa, <_{\mathrm{G}}) \leq \kappa$. □

From (18.5) and Theorem 18.28 we get

Corollary 18.29. *If κ and λ are cardinals different from 0 and at least one among κ and λ is infinite, then*

$$\max(\kappa, \lambda) = \kappa + \lambda = \kappa \cdot \lambda.$$

In other words: the sum and multiplication of cardinals are trivial operations. Using Theorem 18.28, Proposition 13.25 can be restated as follows.

Proposition 18.30. *If $2 \leq \kappa \leq \lambda$ and λ is an infinite cardinal, then ${}^{\lambda}2 \asymp {}^{\lambda}\kappa \asymp {}^{\lambda}\lambda$.*

In absence of the axiom of choice it is not possible to prove that ${}^{\kappa}X$ is well-orderable when $\kappa \geq \omega$ and X has at least two elements—for example if AC fails ${}^{\omega}2$ may not be in bijection with any ordinal. We will now prove (without appealing to AC) that ${}^{n}\kappa$ is well-orderable when $n < \omega$.

Let X be an infinite set which has the same size as its square, and let $f \colon X \times X \to X$ be a bijection witnessing this. By Theorem 12.3 define by recursion on $n \geq 1$ bijections $j_n \colon {}^{n}X \to X$ as follows. Let $j_1(\langle x \rangle) = x$ for all $x \in X$, and since the function ${}^{n+1}X \to {}^{n}X \times X$, $s \mapsto (s \restriction n, s(n))$, is a bijection, it is possible to define j_{n+1} via the diagram

$$\begin{tikzcd}
{}^{n+1}X \arrow[r] \arrow[rrr, bend left, "j_{n+1}"] & {}^{n}X \times X \arrow[r] & X \times X \arrow[r] & X \\
s \arrow[r, mapsto] & (s \restriction n, s(n)) \arrow[r, mapsto] & (j_n(s \restriction n), s(n)) \arrow[r, mapsto] & f(j_n(s \restriction n), s(n))
\end{tikzcd}$$

Therefore ${}^{n}X \asymp X$ for all $n > 0$. Moreover given $\bar{x} \in X$ the function $j_\omega \colon {}^{<\omega}X \to \omega \times X$

$$j_\omega(s) = \begin{cases} (0, \bar{x}) & \text{if } s = \emptyset, \\ (n, j_n(s)) & \text{if } \operatorname{lh}(s) = n > 0, \end{cases}$$

is injective. If $\omega \precsim X$ then $\omega \times X \precsim X \times X \asymp X$, so ${}^{<\omega}X \precsim X$. We have thus shown that

Theorem 18.31. *Let X be an infinite set such that $X \times X \asymp X$. Then $\forall n > 0\, ({}^{n}X \asymp X)$. Moreover, $\omega \precsim X$ implies ${}^{<\omega}X \asymp X$.*

In particular, if X is well-orderable and infinite, then $|{}^{<\omega}X| = |X|$.

Definition 18.32. If $\langle X, \lhd\rangle$ is a well-ordered set and $\alpha \in \mathrm{Ord}$, let

$$[X]^{\alpha} = \{Y \subseteq X \mid \mathrm{ot}\langle Y, \lhd\rangle = \alpha\}\,.$$

Replacing $=$ with $\leq$ and $<$ in the formula above, the definition of $[X]^{\leq\alpha}$ and $[X]^{<\alpha}$ is obtained.

Every $x \in [\kappa]^n$ can be written as $x = \{\alpha_0, \dots, \alpha_{n-1}\}$ with $\alpha_0 < \dots < \alpha_{n-1} < \kappa$, and therefore it can be identified with the sequence $\langle\alpha_0, \dots, \alpha_{n-1}\rangle \in {}^{n}\kappa$. Such identification yields an injection $[\kappa]^n \rightarrowtail {}^{n}\kappa$ that extends to $[\kappa]^{<\omega} \rightarrowtail {}^{<\omega}\kappa$. Therefore for $n > 0$

$$\kappa \leq |[\kappa]^n| \leq \left|[\kappa]^{<\omega}\right| \leq \left|{}^{<\omega}\kappa\right| = \kappa$$

that is $\kappa = |[\kappa]^n| = |[\kappa]^{<\omega}|$.

Corollary 18.33. *If X is infinite and well-orderable, then also $[X]^n$ and $[X]^{<\omega}$ are well-orderable, and $|[X]^n| = |[X]^{<\omega}| = |X|$ if $n > 0$.*

The well-orderability assumption in Theorem 18.31 is essential, since by Theorems 14.3 and 20.11 "$X \asymp X \times X$ for *every* infinite X" implies that every set is well-orderable. Corollary 18.35 shows that, regardless of choice, there are *arbitrarily large* sets that are in bijection with their own square.

Proposition 18.34. *${}^{<\omega}X \asymp \omega \times {}^{<\omega}X \asymp {}^{<\omega}({}^{<\omega}X)$ for every set X.*

Proof. If $X = \emptyset$ then ${}^{<\omega}X = \emptyset$ and the result is trivial. If $X = \{x_0\}$ is a singleton, then ${}^{<\omega}X \asymp \omega$ and the result follows from Theorem 18.31. If X has at least two distinct elements x_0, x_1, given $s \in {}^{<\omega}X$ let

$$s' = x_0^{(\mathrm{lh}\, s)} {}^\frown \langle x_1\rangle {}^\frown s.$$

The map ${}^{<\omega}X \to {}^{<\omega}X$, $s \mapsto s'$ is injective, and so is the map

$${}^{<\omega}({}^{<\omega}X) \to {}^{<\omega}X, \quad \langle s_0, \dots, s_n\rangle \mapsto s'_0 {}^\frown s'_1 {}^\frown \dots {}^\frown s'_n.$$

Since ${}^{<\omega}X \precsim \omega \times {}^{<\omega}X$ and

$$\omega \times {}^{<\omega}X \to {}^{<\omega}({}^{<\omega}X), \quad (n, s) \mapsto \langle \underbrace{s, \dots, s}_{n+1 \text{ times}} \rangle,$$

is injective, the result follows from the Cantor-Schröder-Bernstein Theorem 13.11. □

Corollary 18.35. *For any set X there is a set Y such that $X \precsim Y$ and such that $Y \asymp {}^{<\omega}Y$ and hence $Y \asymp Y \times Y$.*

Proof. Take $Y = {}^{<\omega}X$. □

The set Y in Corollary 18.35 can be taken to be transitive—Exercise 20.25.

18.D. Applications.

18.D.1. *Vector spaces.* Suppose V is a non-trivial vector space on a field $\Bbbk$. If V is well-orderable, then $\Bbbk$ is also well-orderable, and V has a **basis** (Exercise 20.24). Conversely, if $\Bbbk$ is well-orderable and V has a well-orderable basis, then V is well-orderable. To see this suppose $|\Bbbk| = \kappa$ and that $\{\mathbf{e}_\alpha \mid \alpha \in \lambda\}$ is a basis of V, where λ is a cardinal. For every $\mathbf{v} \in V$ there is a unique finite set $I = I(\mathbf{v}) = \{\alpha_0, \ldots, \alpha_{n-1}\} \subseteq \lambda$ and a unique sequence of non-zero scalars $s = s(\mathbf{v}) \in {}^n\Bbbk \setminus \{0_\Bbbk\}$ such that

$$\mathbf{v} = \sum_{i<n} s(i)\mathbf{e}_{\alpha_i}.$$

(When $\mathbf{v} = \mathbf{0}$ then $I(\mathbf{v}) = s(\mathbf{v}) = \emptyset$.) The map

$$V \to [\lambda]^{<\omega} \times {}^{<\omega}(\Bbbk \setminus \{0_\Bbbk\}), \quad \mathbf{v} \mapsto (I(\mathbf{v}), s(\mathbf{v}))$$

is injective, and since $[\lambda]^{<\omega}$ and ${}^{<\omega}(\Bbbk \setminus \{0_\Bbbk\})$ are well-orderable, then V is well-orderable. If $\max(\kappa, \lambda) \geq \omega$ then $|[\lambda]^{<\omega} \times {}^{<\omega}(\Bbbk \setminus \{0_\Bbbk\})| = \max(\kappa, \lambda)$, so $|V| \leq \max(\kappa, \lambda)$. Since $\Bbbk \precsim V$ and $\lambda \precsim V$ we have that

$$|V| = \begin{cases} \kappa^\lambda & \text{if } \kappa, \lambda < \omega, \\ \max(\kappa, \lambda) & \text{otherwise.} \end{cases}$$

Suppose $\{\mathbf{e}_\alpha \mid \alpha \in \lambda\}$ and $\{\mathbf{e}'_\alpha \mid \alpha \in \lambda'\}$ are bases of V, with λ, λ' cardinals. If $\lambda < \omega$, then $\lambda = \lambda'$ by elementary linear algebra; if $\omega \leq \lambda < \lambda'$, choose a finite set $I_\alpha \subseteq \lambda'$ for each $\alpha < \lambda$ so that $\mathbf{e}_\alpha$ is in the span of $\{\mathbf{e}'_\beta \mid \beta \in I_\alpha\}$, and hence $I = \bigcup_{\alpha<\lambda} I_\alpha$ is of size λ and $\{\mathbf{e}'_\alpha \mid \alpha \in I\}$ generates V, contradicting the assumption that $\{\mathbf{e}'_\alpha \mid \alpha \in \lambda'\}$ is a base. Therefore if V is well-orderable two bases have the same size, and the cardinality of any such base is called the **dimension** of V, in symbols $\dim(V)$.

Corollary 18.36. *If V, W are well-orderable vector spaces over a well-orderable field $\Bbbk$, and $|V|, |W| > |\Bbbk|$, then*

$$V \cong W \Leftrightarrow \dim(V) = \dim(W) \Leftrightarrow |V| = |W|.$$

Remark 18.37. The axiom of choice is equivalent to the fact that every vector space has a basis ($\mathsf{AC}(2)$ of Section 28.C), while the statement "two bases of the same vector space are in bijection" follows from a weakening of AC (see Exercise 32.10).

18.D.2. *Free groups.* Recall from Section 9.E that any equational theory admits a free model over X, for any set X. The free group $\boldsymbol{F}(X)$ is the set of all sequences $\langle x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}\rangle$ where $x_i \in X$ and $\varepsilon_i \in \{-1, 1\}$ for all $1 \leq i \leq n$, with the proviso that if $x_i = x_{i+1}$ then $\varepsilon_i = \varepsilon_{i+1}$. Thus $\boldsymbol{F}(X)$ can be identified with a subset of $(\{1,-1\}\times X)^{<\omega}$, while X is identified with a subset of $\boldsymbol{F}(X)$ via $x\mapsto(1,x)$. It follows that if X is well-orderable, so is $\boldsymbol{F}(X)$, and if $|X|=\kappa\geq\omega$, then $|\boldsymbol{F}(X)|=\kappa$. Any map f from a set X to a group G can be uniquely extended to a homomorphism $\hat{f}\colon\boldsymbol{F}(X)\to G$, and if $X\precsim Y$ then $\boldsymbol{F}(X)$ can be identified with a subgroup of $\boldsymbol{F}(Y)$.

If X is well-orderable, then the **rank** of $\boldsymbol{F}(X)$ is the cardinality of X. If $X\asymp Y$ then $\boldsymbol{F}(X)$ is isomorphic to $\boldsymbol{F}(Y)$, and the unique (up to isomorphism) free group of rank $\kappa\neq 0$ is denoted by $\boldsymbol{F}_\kappa$. If $X\precsim Y$ then $\boldsymbol{F}(X)$ is isomorphic to a subgroup of $\boldsymbol{F}(Y)$, but the converse does not hold: the free group $\boldsymbol{F}_2$ contains subgroups isomorphic to each $\boldsymbol{F}_n$ with $1\leq n\leq\omega$; for example, the subgroup generated by $\{a^nba^{-n}\mid n\in\omega\}$ is isomorphic to $\boldsymbol{F}_\omega$. The following result summarizes what we just said. (The axiom of choice is needed for this result—see Section 28.C.)

Proposition 18.38. *Assume* AC. *If X,Y are infinite sets, then $|X|=|Y|\Leftrightarrow\boldsymbol{F}(X)\cong\boldsymbol{F}(Y)\Leftrightarrow|\boldsymbol{F}(X)|=|\boldsymbol{F}(Y)|$.*

Exercises

Exercise 18.39. Show that the lexicographic ordering on $2\times\mathrm{Ord}$ is total, every non-empty subclass has a minimum, but it is not left-narrow, hence it is not a well-order.

Exercise 18.40. Let $R\subseteq X\times X$ be a transitive,[5] left-narrow relation. Then R is well-founded if and only if every non-empty sub-*set* of X has an R-minimal element.

Exercise 18.41. Show that:

(i) if R is a reflexive relation on X, then R is a set if and only if X is a set;

(ii) if $\sim$ is an equivalence relation on a set X, then $X/{\sim}$ is a set.

(iii) The relation of equipotence between sets (see page 376) is an equivalence relation that is not left-narrow on V.

Exercise 18.42. Show that for X a class the following conditions are equivalent: (1) X is well-orderable; (2) $\exists\Omega\leq\mathrm{Ord}\,\exists F\,(F\colon\Omega\twoheadrightarrow X)$; (3) $X\precsim\mathrm{Ord}$.

Exercise 18.43. If $\langle A,<\rangle$ is a well-ordered class in which every element different from the minimum has an immediate predecessor, then its order type is $\leq\omega$, and hence A is a set.

[5] By Exercise 19.23 the transitivity assumption can be removed.

Exercise 18.44. Let $I \subseteq \Omega \leq \mathrm{Ord}$.

(i) Suppose that $\bigl(\forall \beta \in \Omega \, (\beta < \alpha \Rightarrow \beta \in I)\bigr) \Rightarrow \alpha \in I$, for all $\alpha \in \Omega$. Show that $I = \Omega$.

(ii) Suppose that
- $0 \in I$,
- $\forall \alpha \in \Omega\bigl(\exists \beta (\alpha = \mathbf{S}(\beta) \, \wedge \, \beta \in I) \Rightarrow \alpha \in I\bigr)$,
- $\forall \alpha \in \Omega\bigl((\alpha \text{ limit and } \forall \beta < \alpha \; \beta \in I) \Rightarrow \alpha \in I\bigr)$.

  Show that $I = \Omega$.

Exercise 18.45. Show that

(i) $<_{\mathrm{G}}$ is a well-ordering on $\mathrm{Ord} \times \mathrm{Ord}$ and that
- if $\alpha < \beta$ then $\alpha \times \alpha$ is an initial segment of $\beta \times \beta$,
- the class-function $\nu \mapsto \mathrm{ot}\langle \nu \times \nu, <_{\mathrm{G}} \rangle$ is increasing and continuous;

(ii) if $F \colon \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ is the class-function witnessing the isomorphism between $\langle \mathrm{Ord} \times \mathrm{Ord}, <_{\mathrm{G}} \rangle$ and $\langle \mathrm{Ord}, < \rangle$, then for any $\alpha, \beta \in \mathrm{Ord}$
- $F(\alpha, \beta) \geq \max(\alpha, \beta)$ and
- $F(\alpha, \beta) = \max(\alpha, \beta) \Rightarrow \alpha = 0 \wedge (\beta \in \{0, 1\} \vee \beta \text{ is limit})$.

Exercise 18.46. Show that if λ is limit and $\lhd_\alpha$ is a well-order on X_α for all $\alpha < \lambda$, then the following is a well-order on $\bigcup_{\alpha < \lambda} X_\alpha$: $x \lhd_\lambda y$ iff

$$\min \{\alpha \mid x \in X_\alpha\} < \min \{\alpha \mid y \in X_\alpha\} \;\vee\; \exists \alpha \, (x, y \in X_\alpha \setminus \bigcup_{\beta < \alpha} X_\beta \wedge x \lhd_\alpha y).$$

Exercise 18.47. Show that:

(i) if X surjects onto Y, then $Y \precsim \mathscr{P}(X)$,

(ii) $\kappa^+ \precsim \mathscr{P}(\mathscr{P}(\kappa))$,

(iii) there is a surjection $\{\mathscr{Y} \in \mathscr{P}(\mathscr{P}(X)) \mid \subseteq \text{ well-orders } \mathscr{Y}\} \twoheadrightarrow \mathrm{Hrtg}(X)$, and hence $\mathrm{Hrtg}(X) \precsim \mathscr{P}(\mathscr{P}(\mathscr{P}(X)))$.

Exercise 18.48. Let G be an ordered abelian group. Show that if $A, B \subseteq G$ are well-ordered, then $A + B = \{a + b \mid a \in A, b \in B\}$ is well-ordered.

Notes and remarks

The literature on orders is enormous. Ordinals are the only kind of orderings that admit a general structure theorem—for all the other orderings there are very few general results. The original definition of ordinal (due to Cantor) as the isomorphism class of well-orders has the disadvantage that every non-null ordinal would be a proper class—this is the same problem that arises with the naive definition of cardinality, as equivalence class of equipotent sets (see Section 20.C). The modern definition of ordinal as a transitive set whose elements are transitive sets is due to von Neumann.

19. Recursive constructions

We now start a systematic study of recursive constructions, a topic that was introduced in Section 12.B. By Theorem 12.3, given non-empty sets A and B, and functions $g\colon B \to A$ and $F\colon \omega \times B \times A \to A$, there is a unique $f\colon \omega \times B \to A$ such that

$$\begin{cases} \quad f(0, b) = g(b) \\ f(n+1, b) = F(n, b, f(n, b)). \end{cases}$$

In the proof of Theorem 12.3, the function f is obtained by taking the intersection of a suitable collection of subsets of $(\omega \times B) \times A$. This works fine as long as A and B are *sets*, but when A or B are *proper classes* we only show that for each n the function $f_n\colon B \to A$, $b \mapsto f(n, b)$, can be defined by comprehension; the sticky point is to define the sequence of the f_ns, or—equivalently—the function f. Rather than approximating f *top-down* as in the proof of Theorem 12.3, we approximate f *bottom-up*, pretty much like what was done in Example 7.15 for constructing the subgroup of a group generated by a set.

Theorem 19.1. *Let A be a* class*, let $\bar{a} \in A$, and let $F\colon \omega \times A \to A$ be a functional relation. There is a unique function $G\colon \omega \to A$ such that*

$$\begin{cases} \quad G(0) = \bar{a} \\ G(\mathbf{S}(n)) = F(n, G(n)). \end{cases}$$

Proof. Let

$$\mathcal{G} = \bigl\{p \mid \exists m \in \omega \bigl[p\colon m \to A \land (0 < m \Rightarrow p(0) = \bar{a}) \\ \land \forall n\ (\mathbf{S}(n) < m \Rightarrow p(\mathbf{S}(n)) = F(n, p(n)))\bigr]\bigr\}$$

Claim. *If $p, q \in \mathcal{G}$ then $p \cup q$ is a function.*

Proof. Suppose that $p, q \in \mathcal{G}$ and $p \cup q$ is not a function. Then there is a least $n \in \operatorname{dom}(p) \cap \operatorname{dom}(q)$ witnessing $p(n) \neq q(n)$. Clearly $n \neq 0$ since $p(0) = \bar{a} = q(0)$, and hence $n = \mathbf{S}(k)$ for some $k \in \omega$. Then

$$p(n) = F(k, p(k)) = F(k, q(k)) = q(n),$$

where the second equality follows from minimality of n. □

By an argument as in Proposition 16.10, $G = \bigcup \mathcal{G} \subseteq \omega \times A$ is a functional relation, and hence a function by replacement. Since $\{(0, \bar{a})\} \in \mathcal{G}$, it follows that $G \neq \emptyset$ and $G(0) = \bar{a}$. Moreover if $\mathbf{S}(n) \in \operatorname{dom}(G)$ for some $n \in \omega$, then $G(\mathbf{S}(n)) = p(\mathbf{S}(n))$ for some $p \in \mathcal{G}$ hence $G(\mathbf{S}(n)) = F(n, p(n)) = F(n, G(n))$. Thus G is a (possibly partial) function satisfying the statement of the theorem. We must show that $\operatorname{dom}(G) = \omega$. Towards a contradiction, suppose $\bar{n}$ is least such that $\bar{n} \notin \mathrm{dom}(G)$. Since $0 \in \mathrm{dom}(G)$ then $\bar{n} = \mathbf{S}(\bar{m})$ for some $\bar{m}$. It is easy to check that

$$p \stackrel{\text{def}}{=} G \cup \{(\bar{n}, F(\bar{m}, G(\bar{m})))\} \in \mathcal{G}$$

hence $p \subseteq G$, and therefore $\bar{n} \in \mathrm{dom}(G)$: a contradiction.

We are left to show that the function G is unique: if G' were another function satisfying the theorem, then let $\bar{n}$ be least such that $G(\bar{n}) \neq G'(\bar{n})$. Clearly $\bar{n} \neq 0$ hence $\bar{n} = \mathbf{S}(\bar{m})$ for some $\bar{m}$, and therefore, by minimality of $\bar{n}$,

$$G(\bar{n}) = F(\bar{m}, G(\bar{m})) = F(\bar{m}, G'(\bar{m})) = G'(\bar{n}),$$

contradiction! □

Theorem 19.4 in Section 19.B is a substantial generalization of Theorem 19.1, but the reason for proving first a special case is not just a pedagogical one, as the proof of the general Recursion Theorem requires Proposition 19.2 which follows from Theorem 19.1.

19.A. Transitive closure.

19.A.1. *Transitive closure of a class.* The **transitive closure** of a class X is

$$\mathrm{TC}(X) = \Bigl\{ y \mid \exists n \in \omega \, \exists f \in {}^{\mathbf{S}(n)}\mathrm{V} \bigl[f(0) \in X \wedge \\ y = f(n) \wedge \forall i < n \, f(\mathbf{S}(i)) \in f(i) \bigr] \Bigr\}.$$

In other words: $y \in \mathrm{TC}(X)$ if and only if there are $x_0, \dots, x_n$ in V such that

$$y = x_0 \in x_1 \in \cdots \in x_n \in X.$$

If $z \in y$ and $f \in {}^{\mathbf{S}(n)}\mathrm{V}$ witnesses that $y \in \mathrm{TC}(X)$, then $f \cup \{(\mathbf{S}(n), z)\}$ witnesses that $z \in \mathrm{TC}(X)$. Therefore $\mathrm{TC}(X)$ is transitive, it contains X, and if $Y \supseteq X$ is transitive, then $\mathrm{TC}(X) \subseteq Y$. Thus $\mathrm{TC}(X)$ is the smallest transitive class containing X.

19.A.2. *Transitive closure of a relation.* The **transitive closure** of $R \subseteq X \times X$ where X is a class, is the relation

$$\tilde{R} = \Bigl\{ (x, y) \in X \times X \mid \exists n > 0 \, \exists f \in {}^{\mathbf{S}(n)}X \bigl[x = f(0) \wedge \\ y = f(n) \wedge \forall i < n \, (f(i), f(\mathbf{S}(i))) \in R \bigr] \Bigr\}$$

In other words: $x \, \tilde{R} \, y$ if and only if there are $x_0, \dots, x_n$ in X such that

$$x = x_0 \, R \, x_1 \, R \cdots R \, x_{n-1} \, R \, x_n = y.$$

By construction $\tilde{R}$ is the smallest transitive relation on X extending R—see page 43.

Proposition 19.2. *R is left-narrow on X if and only if $\tilde{R}$ is left-narrow on X.*

Proof. Since $R \subseteq \tilde{R}$ it is enough to check that $\tilde{R}$ is left-narrow if so is R. Fix a $\bar{x} \in X$.

Claim 19.2.1. *There is a sequence of sets $\langle Z_n \mid n \in \omega \rangle$ such that*

$$\begin{aligned} Z_0 &= \{y \in X \mid y \mathrel{R} \bar{x}\} \\ Z_{n+1} &= \{y \in X \mid \exists z \in Z_n \,(y \mathrel{R} z)\} = \bigcup_{z \in Z_n} \{y \in X \mid y \mathrel{R} z\}. \end{aligned}$$

Proof. Apply Theorem 19.1 when $A = \mathrm{V}$, $\bar{a} = Z_0$, and $F(n, a) = \{x \in X \mid \exists y \in a \,(x \mathrel{R} y)\}$. Then $G(n) = Z_n$. □

By replacement $\bigcup_{n \in \omega} Z_n$ is a set, and it is equal to $\{y \in X \mid y \mathrel{\tilde{R}} \bar{x}\}$. □

Proposition 19.3. *R is well-founded on X if and only if $\tilde{R}$ is well-founded on X.*

Proof. Since $R \subseteq \tilde{R}$ it is enough to check that if R is well-founded then so is $\tilde{R}$. Fix $\emptyset \neq Y \subseteq X$ and show that there is an $\tilde{R}$-minimal element in Y. A path from Y to itself is a finite sequence $\langle z_0, \ldots, z_n \rangle$ in X such that $z_0, z_n \in Y$ and $z_i \mathrel{R} z_{i+1}$ for $i < n$. Let

$$\bar{Y} = \{x \in X \mid \exists s \,(s \text{ is a path from } Y \text{ in itself and } x \in \operatorname{ran} s)\}$$

be the class of points visited by a path from Y to itself. By construction $Y \subseteq \bar{Y}$ and let $\bar{y}$ be an R-minimal element of $\bar{Y}$. Moreover no element of $\bar{Y} \setminus Y$ is R-minimal, hence $\bar{y} \in Y$. Let us check that $\bar{y}$ is $\tilde{R}$-minimal in Y. If, towards a contradiction, $\bar{x} \mathrel{\tilde{R}} \bar{y}$ for some $\bar{x} \in Y$ distinct from $\bar{y}$, then there is a path $\langle z_0, \ldots, z_{n+1} \rangle$ from Y in itself with $z_0 = \bar{x}$ and $z_{n+1} = \bar{y}$ and $n > 1$. Therefore $z_n \mathrel{R} \bar{y}$, against R-minimality of $\bar{y}$. □

19.B. The Recursion Theorem. Theorems 12.3 and 19.1 are not enough for many applications. For example, we might need both $G(n)$ and n in order to compute $G(\mathbf{S}(n))$—if G is the factorial function, then $G(\mathbf{S}(n)) = G(n) \cdot \mathbf{S}(n)$. Or maybe the value $G(\mathbf{S}(n))$ might depend on some (or all) values $G(k)$ for $k \leq n$. Moreover we often need to define a function by recursion on a well-founded relation, rather than just on ω.

Theorem 19.4. *Let X and Z be classes, let $R \subseteq X \times X$ be irreflexive, left-narrow and well-founded, and let $F\colon Z \times X \times \mathrm{V} \to \mathrm{V}$. Then there is a unique $G\colon Z \times X \to \mathrm{V}$ such that for all $(z, x) \in Z \times X$*

$$G(z, x) = F(z, x, G \restriction \{(z, y) \mid y \mathrel{R} x\}). \tag{19.1}$$

Proof. Suppose that $G, G' \colon Z \times X \to \mathrm{V}$ satisfy (19.1) and that $G \neq G'$. Fix a $\bar{z} \in Z$ such that $Y = \{x \in X \mid G(\bar{z}, x) \neq G'(\bar{z}, x)\} \neq \emptyset$ and let $\bar{x} \in Y$ be an R-minimal element of Y. Then

$$G \restriction \{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\} = G' \restriction \{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\}$$

and let $\bar{p}$ be this functional relation. Since R is left-narrow, then $\bar{p}$ is a set by replacement, so $G(\bar{z}, \bar{x}) = F(\bar{z}, \bar{x}, \bar{p}) = G'(\bar{z}, \bar{x})$: a contradiction. Thus uniqueness is established.

Let $\mathcal{G}$ be the class of all functions p such that

(i) $\mathrm{dom}(p) \subseteq Z \times X$,

(ii) $\forall (z, x) \in \mathrm{dom}(p) \, \forall y \in X \, (y \mathrel{R} x \Rightarrow (z, y) \in \mathrm{dom}(p))$,

(iii) $\forall (z, x) \in \mathrm{dom}(p) \, (p(z, x) = F(z, x, p \restriction \{(z, y) \mid y \mathrel{R} x\}))$.

Note that (ii) is equivalent to the seemingly stronger condition

$$\forall (z, x) \in \mathrm{dom}(p) \, (\{z\} \times \{y \in X \mid y \mathrel{\tilde{R}} x\} \subseteq \mathrm{dom}(p)),$$

where $\tilde{R}$ is the transitive closure of R.

Claim 19.4.1. *If $p, q \in \mathcal{G}$ then $p \cup q$ is a function, and $p \cup q \in \mathcal{G}$.*

Proof. Towards a contradiction suppose that

$$\{x \in X \mid \exists z \in Z \, ((z, x) \in \mathrm{dom}(p) \cap \mathrm{dom}(q) \ \wedge \ p(z, x) \neq q(z, x))\}$$

is non-empty, and by well-foundedness let $\bar{x}$ be an R-minimal element of this class. Let $\bar{z} \in Z$ be such that $(\bar{z}, \bar{x}) \in \mathrm{dom}(p) \cap \mathrm{dom}(q)$ and $p(\bar{z}, \bar{x}) \neq q(\bar{z}, \bar{x})$. By (ii) $\{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\} \subseteq \mathrm{dom}(p) \cap \mathrm{dom}(q)$ and by R-minimality of $\bar{x}$

$$p \restriction \{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\} = q \restriction \{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\} \overset{\mathrm{def}}{=} \bar{r}$$

hence, by (iii), $p(\bar{z}, \bar{x}) = F(\bar{z}, \bar{x}, \bar{r}) = q(\bar{z}, \bar{x})$, against our assumption. It is easy to check that $p \cup q \in \mathcal{G}$. □

The class $G = \bigcup \mathcal{G}$ is a functional relation with domain $\subseteq Z \times X$ satisfying (19.1) for all $(z, x) \in \mathrm{dom}(G)$, so it is enough to show that $\mathrm{dom}(G) = Z \times X$. If $Z \times X \setminus \mathrm{dom}(G) \neq \emptyset$, let $\bar{x}$ be an R-minimal element of $\{x \in X \mid \exists z \in Z \ (z, x) \notin \mathrm{dom}(G)\}$ and let $\bar{z} \in Z$ be such that $(\bar{z}, \bar{x}) \notin \mathrm{dom}(G)$. By Proposition 19.2 the relation $\tilde{R}$ is left-narrow, and hence

$$\bar{p} \overset{\mathrm{def}}{=} G \restriction \{(\bar{z}, y) \mid y \mathrel{\tilde{R}} \bar{x}\}$$

is a set by the axiom of replacement. It is easy to check that $\bar{p} \in \mathcal{G}$ and that also

$$\bar{p} \cup \{((\bar{z}, \bar{x}), F(\bar{z}, \bar{x}, \bar{p} \restriction \{(\bar{z}, y) \mid y \mathrel{R} \bar{x}\}))\} \in \mathcal{G}.$$

Therefore $(\bar{z}, \bar{x}) \in \mathrm{dom}(G)$, against our assumption. It follows that G is the class-function we were looking for. □

Remarks 19.5. (a) The reason to use $\tilde{R}$ rather than R in the definition of $\bar{p}$ is to ensure condition (ii) so that $\bar{p} \in \mathcal{G}$.

(b) The hypothesis that R be irreflexive can be removed, but then in the statement and the proof the sets of the form $\{(z, y) \mid y \mathrel{R} x\}$ should be replaced by $\{(z, y) \mid y \mathrel{R} x \land \neg(x \mathrel{R} y)\}$.

(c) Theorem 19.4 is formulated and proved in MK, and says that for each class-function F there is a unique class-function G with certain properties. The statement and proof work in NGB without any changes. If we want to state (and prove) Theorem 19.4 in ZF, we must employ the longer phrasing: given formulæ φ_X, φ_Z, φ_R and φ_F that define, respectively, the classes X, Z, the relation $R \subseteq X \times X$, and the functional relation $F \colon Z \times X \times \mathrm{V} \to \mathrm{V}$ as in the statement, then there is a formula φ_G that defines the functional relation G satisfying (19.1). If moreover ψ is another formula defining a class-function G' satisfying (19.1) then $G = G'$, that is the formulæ φ_G and ψ are logically equivalent.

Thus in ZF we do not have a *single statement* but a *schema of theorems*, one for each choice of φ_X, φ_Z, φ_R and φ_F: for each choice of formulæ it is possible to construct explicitly a formula φ_G.

19.C. Applications and examples. Let us see some examples of functions constructed via Theorem 19.4.

19.C.1. *The transitive closure of a set.* The transitive closure was defined for all classes in Section 19.A.1. If x is a set, then $\mathrm{TC}(x)$ can be defined using Theorem 19.1 as $\mathrm{TC}(x) = \bigcup_{n\in\omega} x_n$ with $x_0 = x$ and $x_{n+1} = \bigcup x_n$. Equivalently, $\mathrm{TC}(x)$ can be defined using Theorem 19.4 by $\in$-recursion as

$$\mathrm{TC}(x) = x \cup \bigcup_{y \in x} \mathrm{TC}(y).$$

Thus if $M \neq \emptyset$ is a transitive set then the map $\mathscr{P}(M) \to \mathscr{P}(M)$, $x \mapsto \mathrm{TC}(x)$, is a closure operator in the sense of Section 7.A.

19.C.2. *Rank of a well-founded relation.* If R is an irreflexive, left-narrow, and well-founded relation on X, then the functional relation defined by

$$\varrho_{R,X}(x) = \bigcup \{\mathbf{S}(\varrho_{R,X}(y)) \mid y \mathrel{R} x\}$$

is called **rank of R on X**.

Proposition 19.6. $\mathrm{ran}(\varrho_{R,X})$ *is an initial segment of* Ord*, that is either* $\mathrm{ran}(\varrho_{R,X}) \in \mathrm{Ord}$ *or else* $\mathrm{ran}(\varrho_{R,X}) = \mathrm{Ord}$*. Moreover* $x \mathrel{R} y \Rightarrow \varrho_{R,X}(x) < \varrho_{R,X}(y)$*, and* $\varrho_{R,X}(x) = \inf\{\alpha \mid \forall y \left(y \mathrel{R} x \Rightarrow \varrho_{R,X}(y) < \alpha\right)\}$.

Proof. If $\varrho_{R,X}(y) \in \mathrm{Ord}$ for each y such that $y \mathrel{R} x$, then $\varrho_{R,X}(x) \in \mathrm{Ord}$ by Proposition 18.6, hence $\mathrm{ran}(\varrho_{R,X}) \subseteq \mathrm{Ord}$. Towards a contradiction, suppose there is $\bar{x} \in X$ and an α such that $\alpha \in \varrho_{R,X}(\bar{x}) \setminus \mathrm{ran}(\varrho_{R,X})$, and take $\bar{x}$ to

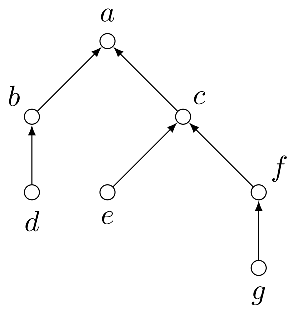


Figure 20.

be R-minimal such. Then there would exist $y \mathrel{R} \bar{x}$ such that $\alpha < \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y))$. Since $\alpha \notin \operatorname{ran} \boldsymbol{\varrho}_{R,X}$ then $\alpha < \boldsymbol{\varrho}_{R,X}(y)$, against the R-minimality of $\bar{x}$.

The rest of the proof is left to the reader. □

Thus $\boldsymbol{\varrho}_{R,X}(x) = 0$ if and only if x is R-minimal in X and $\boldsymbol{\varrho}_{R,X}(x) = \alpha$ if and only if x is R-minimal in $X \setminus \{y \in X \mid \boldsymbol{\varrho}_{R,X}(y) < \alpha\}$. The rank function yields a complexity to each $x \in X$—the complexity of x is the least value bigger than the complexity of the ys such that $y \mathrel{R} x$. For example, if R is a relation on $X = \{a, b, c, d, e, f, g\}$ described by the directed graph (see Section 7.C) of Figure 20 then $\boldsymbol{\varrho}_{R,X}(d) = \boldsymbol{\varrho}_{R,X}(e) = \boldsymbol{\varrho}_{R,X}(g) = 0$, $\boldsymbol{\varrho}_{R,X}(b) = \boldsymbol{\varrho}_{R,X}(f) = 1$, $\boldsymbol{\varrho}_{R,X}(c) = 2$ and $\boldsymbol{\varrho}_{R,X}(a) = 3$.

19.C.3. *The Mostowski collapse.* If R is an irreflexive, left-narrow, well-founded relation on X, then the function with domain X defined by

$$\boldsymbol{\pi}_{R,X}(x) = \{\boldsymbol{\pi}_{R,X}(y) \mid y \mathrel{R} x\}$$

is the **Mostowski collapse**. The class $\overline{X} = \operatorname{ran}(\boldsymbol{\pi}_{R,X})$ is called the **transitive collapse of** R **and** X. One checks that $\overline{X}$ is transitive and that $\forall x, y \in X\, (x \mathrel{R} y \Rightarrow \boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y))$.

For example, if R and X are as in Figure 20, $\boldsymbol{\pi}_{R,X}(d) = \boldsymbol{\pi}_{R,X}(e) = \boldsymbol{\pi}_{R,X}(g) = \emptyset$, $\boldsymbol{\pi}_{R,X}(b) = \boldsymbol{\pi}_{R,X}(f) = \{\emptyset\} = 1$ and $\boldsymbol{\pi}_{R,X}(c) = \{0, 1\} = 2$ and $\boldsymbol{\pi}_{R,X}(a) = \{1, 2\}$.

Definition 19.7. A relation $R \subseteq X \times X$ is **extensional on** X if

$$\forall x, y \in X\, (\forall z \in X\, (z \mathrel{R} x \Leftrightarrow z \mathrel{R} y) \Rightarrow x = y)\,.$$

Proposition 19.8. *Let R be an irreflexive, left-narrow, well-founded relation on the class X.*

(a) *If R is extensional on X, then $\boldsymbol{\pi}_{R,X}$ is injective and $\boldsymbol{\pi}_{R,X} \colon \langle X, R\rangle \to \langle \overline{X}, \in \rangle$ is an isomorphism.*

(b) *If R is a strict well-order on X, the functions $\boldsymbol{\pi}_{R,X}$ and $\boldsymbol{\varrho}_{R,X}$ coincide.*

Proof. (a) Let us check that $\boldsymbol{\pi}_{R,X}$ is injective. Towards a contradiction, let $\bar{x}$ be R-minimal such that $\boldsymbol{\pi}_{R,X}(\bar{x}) = \boldsymbol{\pi}_{R,X}(\bar{y})$, for some $\bar{y} \neq \bar{x}$. Let $z \mathrel{R} \bar{x}$: since $\boldsymbol{\pi}_{R,X}(z) \in \boldsymbol{\pi}_{R,X}(\bar{x}) = \boldsymbol{\pi}_{R,X}(\bar{y})$, there is a $w \mathrel{R} \bar{y}$ such that $\boldsymbol{\pi}_{R,X}(z) = \boldsymbol{\pi}_{R,X}(w)$. By minimality of $\bar{x}$, then $z = w$. Therefore $\forall z\,(z \mathrel{R} \bar{x} \Rightarrow z \mathrel{R} \bar{y})$. Similarly, if $z \mathrel{R} \bar{y}$ then there exists $w \mathrel{R} \bar{x}$ such that $\boldsymbol{\pi}_{R,X}(z) = \boldsymbol{\pi}_{R,X}(w)$ hence $z = w$, that is $\forall z\,(z \mathrel{R} \bar{y} \Rightarrow z \mathrel{R} \bar{x})$. Thus, by extensionality, $\bar{y} = \bar{x}$, against our assumption. It follows that $\boldsymbol{\pi}_{R,X}$ is a bijection between X and $\overline{X}$.

If $\boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y) = \{\boldsymbol{\pi}_{R,X}(z) \mid z \mathrel{R} y\}$, then by injectivity $x \mathrel{R} y$. Therefore $\forall x, y \in X\,(x \mathrel{R} y \Leftrightarrow \boldsymbol{\pi}_{R,X}(x) \in \boldsymbol{\pi}_{R,X}(y))$.

(b) Suppose that $\boldsymbol{\varrho}_{R,X}(y) = \boldsymbol{\pi}_{R,X}(y)$, for all $y \mathrel{R} x$. Then $\boldsymbol{\pi}_{R,X}(x) = \{\boldsymbol{\pi}_{R,X}(y) \mid y \mathrel{R} x\} = \{\boldsymbol{\varrho}_{R,X}(y) \mid y \mathrel{R} x\}$ is a set of ordinals. If $\boldsymbol{\pi}_{R,X}(z) \in \boldsymbol{\pi}_{R,X}(y) \in \boldsymbol{\pi}_{R,X}(x)$, then $z \mathrel{R} y \mathrel{R} x$, whence $z \mathrel{R} x$, that is $\boldsymbol{\pi}_{R,X}(x)$ is transitive, hence an ordinal. By construction $\boldsymbol{\pi}_{R,X}(x)$ is the sup of the ordinals $\mathbf{S}(\boldsymbol{\pi}_{R,X}(y)) = \mathbf{S}(\boldsymbol{\varrho}_{R,X}(y))$ with $y \mathrel{R} x$, that is $\boldsymbol{\pi}_{R,X}(x) = \boldsymbol{\varrho}_{R,X}(x)$. □

19.C.4. *The $\aleph$ function.* By Corollary 18.26 $\mathrm{Card}\setminus\omega$ is a proper class hence its transitive collapse is Ord. The enumerating function of $\mathrm{Card} \setminus \omega$ is denoted with the first letter of the Hebrew alphabet $\aleph$ (pronunced "aleph"), and satisfies the following definition:

$$\aleph_0 = \omega, \qquad \aleph_{\mathbf{S}(\alpha)} = (\aleph_\alpha)^+, \qquad \aleph_\lambda = \sup_{\alpha<\lambda} \aleph_\alpha, \text{ if } \lambda \text{ is limit.}$$

Thus $\aleph_0 = \omega$, $\aleph_1 = \omega^+$, ... We often write ω_α instead of $\aleph_\alpha$, so ω_1 is the first uncountable ordinal, ω_2 is the least ordinal of size bigger than ω_1, and so on.

19.C.5. *Fixed points of continuous functions.*

Lemma 19.9. *If $f\colon \mathrm{Ord} \to \mathrm{Ord}$ is increasing and continuous, then*

$$\forall\alpha\exists\bar{\alpha} > \alpha\,(f(\bar{\alpha}) = \bar{\alpha})\,.$$

Proof. Define inductively the sequence $\langle \alpha_n \mid n \in \omega\rangle$ by $\alpha_0 = \mathbf{S}(\alpha)$ and $\alpha_{\mathbf{S}(n)} = f(\alpha_n)$, and let $\bar{\alpha} = \sup_n \alpha_n$. If $f(\alpha_0) = \alpha_0$, then $\forall n\,(\alpha_0 = \alpha_n)$ and hence $\bar{\alpha} = \alpha_0$. If instead $\alpha_0 < f(\alpha_0) = \alpha_1$, then $\alpha_n < \alpha_{\mathbf{S}(n)}$ and therefore $\bar{\alpha}$ is limit. Then

$$f(\bar{\alpha}) = \sup\nolimits_{\nu<\bar{\alpha}} f(\nu) = \sup\nolimits_n f(\alpha_n) = \sup\nolimits_n \alpha_{\mathbf{S}(n)} = \bar{\alpha}.$$

In any case $\bar{\alpha}$ is the least fixed point for f bigger than α. □

Since $\aleph\colon \mathrm{Ord} \to \mathrm{Ord}$ is increasing and continuous, there are cardinals κ such that $\kappa = \aleph_\kappa$, and the least such cardinal is the supremum of

$$\aleph_0, \quad \aleph_{\aleph_0}, \quad \aleph_{\aleph_{\aleph_0}}, \quad \aleph_{\aleph_{\aleph_{\aleph_0}}}, \quad \ldots .$$

$$\alpha \dotplus \beta = \begin{cases} \alpha & \text{if } \beta = 0, \\ \mathbf{S}(\alpha \dotplus \gamma) & \text{if } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta}(\alpha \dotplus \gamma) & \text{if } \beta \text{ is limit,} \end{cases}$$

$$\alpha \cdot \beta = \begin{cases} 0 & \text{if } \beta = 0, \\ (\alpha \cdot \gamma) \dotplus \alpha & \text{if } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta} \alpha \cdot \gamma & \text{if } \beta \text{ is limit,} \end{cases}$$

$$\alpha^{\cdot\beta} = \begin{cases} 1 & \text{if } \beta = 0, \\ \alpha^{\cdot\gamma} \cdot \alpha & \text{if } \beta = \mathbf{S}(\gamma), \\ \sup_{\gamma<\beta} \alpha^{\cdot\gamma} & \text{if } \beta \text{ is limit.} \end{cases}$$

Table 1. The recursive definition of addition, multiplication, exponentiation on the ordinals.

19.D. Ordinal arithmetic. The operations of ordinal addition, multiplication, and exponentiation were defined in Section 13. Every cardinal is an ordinal, and this could cause some ambiguity: for example the term $\omega + 1$ could either mean ω, the result of *cardinal* addition, or else it could denote $\mathbf{S}(\omega)$, the result of *ordinal* addition. For this reason we write $\alpha \dotplus \beta$, $\alpha \cdot \beta$, and $\alpha^{\cdot\beta}$ for the operations of ordinal addition, multiplication, and exponentiation. They are functions Ord × Ord → Ord defined by recursion, as in Table 1. When $\alpha, \beta \in \omega$ the definitions of $\alpha \dotplus \beta$ and $\alpha \cdot \beta$ boil-down to the definitions of addition and multiplication on $\mathbb{N}$, so they commute by Theorem 12.15; moreover ordinal and cardinal operations agree on the finite cardinals, but differ on the infinite cardinals (Exercises 19.29 and 19.30). Table 2 collects some of the properties of ordinal operations, some of which we have seen in Section 13. They can all be proved by transfinite induction. For example, for the first property, argue by induction on β' that $\forall \beta < \beta' \, (\alpha \dotplus \beta < \alpha \dotplus \beta')$. The case $\beta' = 0$ holds trivially, so we may assume that β' is successor or limit. If $\beta' = \mathbf{S}(\beta'') > \beta$ then $\beta'' \geq \beta$: by inductive assumption $\alpha \dotplus \beta \leq \alpha \dotplus \beta''$ and

$$\alpha \dotplus \beta'' < \mathbf{S}(\alpha \dotplus \beta'') = \alpha \dotplus \beta',$$

whence the result. If β' is limit and $\beta' > \beta$, then

$$\alpha \dotplus \beta' = \sup_{\gamma<\beta'} \alpha \dotplus \gamma \geq \alpha \dotplus \mathbf{S}(\beta) > \alpha \dotplus \beta.$$

This concludes the proof that $\forall \beta, \beta' \, (\beta < \beta' \Rightarrow \alpha \dotplus \beta < \alpha \dotplus \beta')$.

For each α the class-function Ord → Ord, $\beta \mapsto \alpha \dotplus \beta$ is increasing and continuous, so there is a proper class of γ such that $\alpha \dotplus \gamma = \gamma$. Similarly there is a proper class of γ such that $\alpha \cdot \gamma = \gamma$, and a proper class of γ such

$\beta < \beta' \Rightarrow \alpha \dotplus \beta < \alpha \dotplus \beta'$
If $\lambda = \bigcup \lambda = \sup_{i \in I} \lambda_i$, then $\alpha \dotplus \lambda = \bigcup(\alpha \dotplus \lambda) = \sup_{i \in I} \alpha \dotplus \lambda_i$
$(\alpha \dotplus \beta) \dotplus \gamma = \alpha \dotplus (\beta \dotplus \gamma)$
$\alpha < \alpha' \Rightarrow \alpha \dotplus \beta \leq \alpha' \dotplus \beta$
$0 \dotplus \beta = \beta$
$\beta \geq \omega \Rightarrow 1 \dotplus \beta = \beta$
$\beta \leq \alpha \dotplus \beta$
$\alpha \leq \beta \Leftrightarrow \exists! \gamma\, (\alpha \dotplus \gamma = \beta)$
If $\alpha \neq 0$ then $\beta < \beta' \Rightarrow \alpha \cdot \beta < \alpha \cdot \beta'$
If $\lambda = \bigcup \lambda = \sup_{i \in I} \lambda_i$ then $\alpha \cdot \lambda = \bigcup(\alpha \cdot \lambda) = \sup_{i \in I} \alpha \cdot \lambda_i$
$\alpha \cdot (\beta \dotplus \gamma) = \alpha \cdot \beta \dotplus \alpha \cdot \gamma$
$0 \cdot \beta = 0$ and $1 \cdot \beta = \beta$
$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$
$\alpha < \alpha' \Rightarrow \alpha \cdot \beta \leq \alpha' \cdot \beta$
$\lambda = \bigcup \lambda \Leftrightarrow \exists \nu (\omega \cdot \nu = \lambda)$
$\lambda = \bigcup \lambda \Rightarrow 2 \cdot \lambda = \lambda$
If $\alpha > 1$ then $\beta < \beta' \Rightarrow \alpha^{\cdot \beta} < \alpha^{\cdot \beta'}$
If $\alpha > 0$ then $\alpha^{\cdot (\beta \dotplus \gamma)} = \alpha^{\cdot \beta} \cdot \alpha^{\cdot \gamma}$
$(\alpha^{\cdot \beta})^{\cdot \gamma} = \alpha^{\cdot (\beta \cdot \gamma)}$
$\alpha < \alpha' \Rightarrow \alpha^{\cdot \beta} \leq \alpha'^{\cdot \beta}$
$1^{\cdot \beta} = 1$
If $\bigcup \beta = \beta$ then $0^{\cdot \beta} = 1$; if β is a successor then $0^{\cdot \beta} = 0$
If $\alpha > 1$ then $\beta \leq \alpha^{\cdot \beta}$
If $1 < \alpha$ then $\forall \beta \exists! \gamma \leq \beta \exists! \delta < \alpha \exists! \varepsilon < \alpha^{\cdot \gamma}\, (\alpha^{\cdot \gamma} \cdot \delta \dotplus \varepsilon = \beta)$

Table 2. Some properties of ordinal operations.

that $\alpha^{\cdot \gamma} = \gamma$. In fact there is a proper class of **additively indecomposable ordinals**, i.e. ordinals γ such that $\alpha, \beta < \gamma \Rightarrow \alpha \dotplus \beta < \gamma$; similarly, there is a proper class of **multiplicatively indecomposable ordinals**, i.e. ordinals γ such that $\alpha, \beta < \gamma \Rightarrow \alpha \cdot \beta < \gamma$ and a proper class of **exponentially indecomposable ordinals**, i.e. ordinals γ such that $\alpha, \beta < \gamma \Rightarrow \alpha^{\cdot \beta} < \gamma$ (Exercise 19.33). The exponentially indecomposable ordinals bigger than ω are called **$\boldsymbol{\epsilon}$-numbers** and the smallest of them is

$$\boldsymbol{\epsilon}_0 = \sup\{\omega, \omega^{\omega}, \omega^{\omega^{\omega}}, \omega^{\omega^{\omega^{\omega}}}, \ldots\}.$$

19.E. The von Neumann hierarchy. The ordinal $\boldsymbol{\varrho}_{R,X}(x)$, when $X = \mathrm{V}$ and R is the $\in$ relation, is called **rank of** x and it is denoted by $\operatorname{rank}(x)$. From the definition it follows that

$$x \in y \Rightarrow \operatorname{rank}(x) < \operatorname{rank}(y) \qquad x \subseteq y \Rightarrow \operatorname{rank}(x) \leq \operatorname{rank}(y),$$

and by induction it follows that $\operatorname{rank}(\alpha) = \alpha$.

Proposition 19.10. (a) $\operatorname{rank}(\mathscr{P}(x)) = \mathbf{S}(\operatorname{rank}(x))$.

(b) $\operatorname{rank}(\bigcup x) = \sup\{\operatorname{rank}(y) \mid y \in x\}$.

Proof. (a) Since $x \in \mathscr{P}(x)$ it follows that $\mathbf{S}(\operatorname{rank}(x)) \leq \operatorname{rank}(\mathscr{P}(x))$. Conversely, if $y \subseteq x$, then $\mathbf{S}(\operatorname{rank}(y)) \leq \mathbf{S}(\operatorname{rank}(x))$ and hence $\operatorname{rank}(\mathscr{P}(x)) = \sup\{\mathbf{S}(\operatorname{rank}(y)) \mid y \subseteq x\} \leq \mathbf{S}(\operatorname{rank}(x))$.

(b) If $y \in x$ then $y \subseteq \bigcup x$, so $\sup\{\operatorname{rank}(y) \mid y \in x\} \leq \operatorname{rank}(\bigcup x)$. Conversely, if $z \in y \in x$ then $\mathbf{S}(\operatorname{rank}(z)) \leq \operatorname{rank}(y)$ hence $\mathbf{S}(\operatorname{rank}(z)) \leq \sup\{\operatorname{rank}(y) \mid y \in x\}$. As z is arbitrary, then $\operatorname{rank}(\bigcup x) \leq \sup\{\operatorname{rank}(y) \mid y \in x\}$. □

Definition 19.11. Let $\mathrm{V}_\alpha = \{x \mid \operatorname{rank}(x) < \alpha\}$. The **von Neuman hierarchy** is the class function $\langle \mathrm{V}_\alpha \mid \alpha \in \mathrm{Ord}\rangle$.

As $\operatorname{rank}(\alpha) = \alpha$ it follows that $\mathrm{V}_\alpha \cap \mathrm{Ord} = \alpha$.

Theorem 19.12. V_α *is a transitive set and*

$$\mathrm{V}_\alpha = \textstyle\bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta). \tag{19.2}$$

Proof. If $y \in x \in \mathrm{V}_\alpha$ then $\operatorname{rank}(y) < \operatorname{rank}(x) < \alpha$ and therefore $y \in \mathrm{V}_\alpha$. Thus V_α is a transitive class. By induction on α let us show that V_α is a set and that (19.2) holds. Suppose the result holds for all $\beta < \alpha$: then $\{\mathscr{P}(\mathrm{V}_\beta) \mid \beta < \alpha\}$ is a set, hence it is enough to prove (19.2). If $y \in x$ then $\operatorname{rank}(y) < \operatorname{rank}(x)$ so that $x \subseteq \mathrm{V}_{\operatorname{rank}(x)}$, and therefore $\operatorname{rank}(x) < \alpha \Rightarrow x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$. Conversely, if $x \in \bigcup_{\beta<\alpha} \mathscr{P}(\mathrm{V}_\beta)$, then $x \subseteq \mathrm{V}_\beta$, for some $\beta < \alpha$ and therefore $\operatorname{rank}(y) < \beta$ for all $y \in x$, which implies $\operatorname{rank}(x) \leq \beta < \alpha$. □

Corollary 19.13. (a) $\mathrm{V}_0 = \emptyset$.

(b) *If* $\alpha < \beta$ *then* $\mathrm{V}_\alpha \in \mathrm{V}_\beta$ *and* $\mathrm{V}_\alpha \subset \mathrm{V}_\beta$.

(c) $\mathrm{V}_{\mathbf{S}(\alpha)} = \mathscr{P}(\mathrm{V}_\alpha)$.

(d) $\mathrm{V}_\lambda = \bigcup_{\alpha<\lambda} \mathrm{V}_\alpha$, *when* λ *is limit.*

(e) $\mathrm{V} = \bigcup_{\alpha\in\mathrm{Ord}} \mathrm{V}_\alpha$.

Therefore the universe V is the increasing union of the transitive sets V_α, each of which belongs to the successive sets, and the least such set is empty (see Figure 21). As $|\mathrm{V}_{n+1}| = 2^n$ for all $n \in \omega$, then $\mathrm{V}_\omega \asymp \omega$, and $\mathrm{V}_{\omega+1} \asymp \mathscr{P}(\omega) \asymp \mathbb{R}$. In V_ω there is (an isomorphic copy of) any finite structure (graph, group, ring, ...), and V_ω is the universe where finite combinatorics takes place. Its elements are the **hereditarily finite sets**, that is those sets whose transitive closure is finite. If $x, y \in \mathrm{V}_\alpha$ then $\{x, y\} \in \mathrm{V}_{\alpha+1}$ and $(x, y) \in \mathrm{V}_{\alpha+2}$, so $\mathbb{N} \times \mathbb{N} \subseteq \mathrm{V}_\omega$.

Remark 19.14. One would expect that $\mathbb{Z}$ and $\mathbb{Q}$ be subsets of V_ω, yet the usual construction yields that, *e.g.* $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/E_{\mathbb{Z}} \subseteq \mathrm{V}_{\omega+2}$. As we are taking

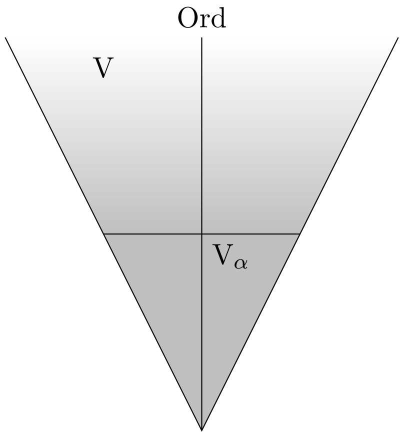


Figure 21. The universe V and the hierarchy of V_αs.

quotients of a countable set, it is possible to choose canonical representatives in the equivalence classes. For example if we re-define

$$\mathbb{Z} = \{(n, 0) \mid n \in \omega\} \cup \{(0, n) \mid n \in \omega\}$$

$$\mathbb{Q} = \{(z, w) \in (\mathbb{Z} \setminus \{0\})^2 \mid z, w \text{ relatively prime and } w > 0\} \cup \{(0, 0)\},$$

then $\mathbb{Z}, \mathbb{Q} \subseteq \mathrm{V}_\omega$, and hence $\mathbb{R} \subseteq \mathscr{P}(\mathbb{Q}) \subseteq \mathrm{V}_{\omega+1}$.

Every object usually encountered in classical mathematics (finite combinatorics, real and complex analysis, ...) can be construed as an element of $\mathrm{V}_{\omega+\omega}$, but this does not mean that the study of V_α for large α is irrelevant for classical mathematics. In fact the answer to many natural questions in classical mathematics are strictly related to questions regarding properties of V_α for very large αs.

19.F. Models of set theory. A structure for $\mathcal{L}_\in$, the first-order language used to formulate MK, NGB, and ZF, is a pair $\langle M, E\rangle$ where M is a non-empty set[6] and $E \subseteq M \times M$. It can be quite difficult to determine which sentences are true in an arbitrary $\mathcal{L}_\in$-structure $\langle M, E\rangle$. If E is extensional on M, i.e. if $\langle M, E\rangle$ models the axiom of extensionality, and if E is well-founded on M, then $\langle M, E\rangle$ is isomorphic to a unique $\langle \overline{M}, \in\rangle$ with $\overline{M}$ transitive. A particular kind of transitive structures are the $\langle \mathrm{V}_\alpha, \in\rangle$ (simply denoted by V_α), for $\alpha > 0$. The following question comes up:

Which axioms of set theory are true in V_α?

Theorem 19.15.

(a) *All axioms of* ZFC *except the axiom of infinity hold in* V_ω.

[6] The requirement of focusing on sets rather than classes will be explained in Chapter VIII.

(b) *All axioms of* ZF *except possibly for replacement hold in* V_λ*, if* $\lambda > \omega$ *is limit.*

(c) *Assuming choice, then* AC *holds in* V_λ*, if* λ *is limit.*

Remarks 19.16. (a) For the sake of simplicity, Theorem 19.15 is stated for (sub-theories of) ZF, but a similar statement could be formulated for MK or NGB (Exercise 19.31).

(b) Theorem 19.15 suggest the following question: are there ordinals α such that V_α is a model of ZF or MK? The answer will be presented in Section 21.F after enough cardinal arithmetic is developed.

(c) Although a direct proof of Theorem 19.15 is possible, we will follow a more general route, since this will be useful later in the book (Sections 24.B and 37).

19.F.1. *A hierarchy of formulæ.*

Definition 19.17. An $\mathcal{L}_\in$-formula is Δ_0 if it belongs to the smallest class containing all atomic formulæ and closed under connectives and **bounded quantifications**, that is

- atomic formulæ are Δ_0,
- if φ, ψ are Δ_0 then so are $\neg\varphi$ and $\varphi \odot \psi$, where $\odot$ is any binary connective,
- if φ is Δ_0 then so is $\forall y(y \in x \Rightarrow \varphi)$ and $\exists y(y \in x \wedge \varphi)$,

and nothing else is a Δ_0-formula.

We write $\forall y \in x\, \varphi$ and $\exists y \in x\, \varphi$ instead of $\forall y(y \in x \Rightarrow \varphi)$ and $\exists y(y \in x \wedge \varphi)$. Table 3 lists some Δ_0-formulæ. Checking that they are indeed Δ_0 is straightforward. For example, $\mathsf{Trans}(x)$ is Δ_0 since it is $\forall y \in x\, \forall z \in y\, (z \in x)$.

Definition 19.18. A $\mathcal{L}_\in$-formula is Σ_1 if it is of the form $\exists x\, \varphi$ with φ a Δ_0-formula; it is Π_1 if it is of the form $\forall x\, \varphi$ with φ a Δ_0-formula.

Thus the negation of a Π_1-formula is (logically equivalent to) a Σ_1-formula, and conversely.

Definition 19.19. Let M be a non-empty set. We say that $\varphi(x_1, \dots, x_n)$ is:

- **upward absolute between** M **and** V if
$$\forall a_1, \dots, a_n \in M\, \big((\langle M, \in\rangle \vDash \varphi[a_1, \dots, a_n]) \Rightarrow \varphi(a_1, \dots, a_n)\big);$$
- **downward absolute between** M **and** V if
$$\forall a_1, \dots, a_n \in M\, \big(\varphi(a_1, \dots, a_n) \Rightarrow (\langle M, \in\rangle \vDash \varphi[a_1, \dots, a_n])\big);$$

$\mathsf{Trans}(x)$, i.e. x is transitive	$x = \{y, z\}$
$\mathsf{Ord}(x)$, i.e. x is an ordinal	$x = (y, z)$
$\mathsf{Op}(x)$, i.e x is an ordered pair	$f \colon x \to y$
$\mathsf{Rel}(x)$, i.e. x is a relation	$y = \mathrm{dom}(x)$
$\mathsf{Fn}(x)$, i.e. x is a function	$y = \mathrm{ran}(x)$
$\mathsf{Seq}(x)$, i.e. x is a finite sequence	$\mathbf{S}(x) = y$
x is an injective function	$f(x) = g(y)$
x is a reflexive relation	$g = f \restriction x$
x is a symmetric relation	$f(x) = y$
x is a transitive relation	$f``x = y$
$x \subseteq y$	$z = x \times y$
$z = x \cup y$	$z = x \setminus y$
$z = x \cap y$	

Table 3. Some Δ_0-formulæ.

- **absolute between** M **and** V if it is both upward and downward absolute, that is

$$\forall a_1, \dots, a_n \in M \left((\langle M, \in \rangle \vDash \varphi[a_1, \dots, a_n]) \Leftrightarrow \varphi(a_1, \dots, a_n) \right),$$

where $\varphi(a_1, \dots, a_n)$ stands for $\varphi(\!|a_1/x_1, \dots, a_n/x_n|\!)$.

From the definition it follows that φ is upward absolute between M and V if and only if $\neg\varphi$ is downward absolute between M and V, and that if φ and ψ are upward/downward absolute, then so are $\varphi \wedge \psi$ and $\varphi \vee \psi$. Therefore the collection of formulæ that are absolute between M and V is closed under all connectives.

An easy induction on the complexity of formulæ shows that:

Lemma 19.20. *A quantifier-free formula is absolute between a transitive* $M \neq \emptyset$ *and* V.

Lemma 19.21. *Suppose* M *is a non-empty transitive set.*

(a) *Every* Δ_0 *formula is absolute between* M *and* V.

(b) *Every* Σ_1 *formula is upward absolute between* M *and* V*, and every* Π_1 *formula is downward absolute between* M *and* V.

Proof. (a) By Lemma 19.20 it is enough to consider formulæ of the form $\forall y \in x_i \, \varphi(y, x_1, \dots, x_n)$. Fix $a_1, \dots, a_n \in M$. By the inductive hypothesis, and since M is transitive,

$$\begin{aligned}\langle M,\in\rangle \vDash \forall y\in x_i\,\varphi[\vec{a}] &\Leftrightarrow \forall b\in M\,(b\in a_i \Rightarrow \langle M,\in\rangle\vDash\varphi[b,\vec{a}])\\ &\Leftrightarrow \forall b\in a_i\,\langle M,\in\rangle\vDash\varphi[b,\vec{a}]\\ &\Leftrightarrow \forall y\in a_i\,\varphi(\vec{a}).\end{aligned}$$

(b) It is enough to prove that Σ_1 formulæ are upward absolute. Suppose that $\varphi(y_1,\dots,y_k,x_1,\dots,x_n)$ is Δ_0, that $a_1,\dots,a_n\in M$, and that $\langle M,\in\rangle\vDash\exists y_1,\dots,y_k\,\varphi[a_1,\dots,a_n]$. Fix $b_1,\dots,b_k\in M$ such that $\langle M,\in\rangle\vDash\varphi[b_1,\dots,b_k,a_1,\dots,a_n]$. By part (a) $\varphi(b_1,\dots,b_k,a_1,\dots,a_n)$ holds, and hence $\exists y_1,\dots,y_k\,\varphi(a_1,\dots,a_n)$. □

Thus the meaning of a Δ_0 formula in a transitive structure $\langle M,\in\rangle$ is the same as in V, and in particular it applies to all formulæ of Table 3.

Theorem 19.22. *Suppose $M\neq\emptyset$ is a transitive set. Then*

(a) *$\langle M,\in\rangle$ satisfies the axioms of extensionality and foundation.*

(b) *If $\{a,b\}\in M$ for all $a,b\in M$, then $\langle M,\in\rangle$ satisfies the axiom of pairing.*

(c) *If $\bigcup a\in M$ for all $a\in M$, then $\langle M,\in\rangle$ satisfies the axiom of union.*

(d) *If $\forall a\in M\ (\mathscr{P}(a)\cap M\in M)$, then $\langle M,\in\rangle$ satisfies the power-set axiom.*

(e) *If $\omega\in M$ then $\langle M,\in\rangle$ satisfies the axiom of infinity.*

(f) *If $\forall a\in M\,\forall b\subseteq a\,(b\in M)$, then $\langle M,\in\rangle$ satisfies the axiom schema of separation.*

(g) *If for all $a\in M$ and all $f\colon a\to M$ there is $b\in M$ such that* $\operatorname{ran} f\subseteq b$, *then $\langle M,\in\rangle$ satisfies the axiom schema of replacement.*

(h) *$\langle M,\in\rangle\vDash$* AC *if and only if $\forall\mathcal{A}\in M\,(\forall A\in\mathcal{A}\,(A\neq\emptyset)\Rightarrow\exists f\in M\,(f$ is a choice function for $\mathcal{A}))$.*

Proof. (a) The axioms of extensionality and foundations are the universal closure of the Δ_0-formulæ

$$\forall z\in x\,(z\in y)\wedge\forall z\in y\,(z\in x)\Rightarrow x=y$$
$$\exists y\in x\,(y=y)\Rightarrow\exists y\in x\,\forall z\in y\,(z\notin x)$$

so they are downward absolute. Both axioms hold in V and therefore hold in $\langle M,\in\rangle$.

(b) and (c) follow from the fact that $z=\{x,y\}$ and $v=\bigcup u$ are Δ_0 formulæ.

(d) Fix $a\in M$ and let $b\overset{\text{def}}{=}\mathscr{P}(a)\cap M$. As $z\subseteq x$ is Δ_0, then $\langle M,\in\rangle$ satifies $\forall z(z\subseteq x\Leftrightarrow z\in y)$, where x and y are given the values a and b.

(e) The axiom of infinity is $\exists x\,\varphi(x)$ where $\varphi(x)$ is the Δ_0-formula $\emptyset\in x\wedge\forall y\in x\,(\mathbf{S}(y)\in x)$, so by absoluteness $\langle M,\in\rangle$ satisfies the axiom of infinity if and only if $\exists x \in M\, \varphi(x)$. As ω satisfies φ, if $\omega \in M$ then $\langle M, \in\rangle$ satisfies the axiom of infinity.

(f) We must show that given $\varphi(x, y, \vec{w})$, and given $a, \vec{c} \in M$ to be assigned to the variables $y, \vec{w}$, the set $b = \{d \in a \mid \langle M, \in\rangle \vDash \varphi[d, a, \vec{c}]\}$ belongs to M. But this follows at once by the assumption and by $b \subseteq a$.

(g) We must show that given $\varphi(x, y, z, \vec{w})$ and given $a, \vec{c} \in M$ to be assigned to the variables $z, \vec{w}$, if $\langle M, \in\rangle \vDash \forall x \in z\, \exists! y\, \varphi[a, \vec{c}]$ then there is $b \in M$ such that $\langle M, \in\rangle \vDash \forall x \in z\, \exists y \in v\, \varphi[a, \vec{c}, b]$, with b assigned to the variable v. Then $\varphi, a, \vec{c}$ yield a function $f\colon a \to M$, and by case assumption there is $b \in M$ such that $\operatorname{ran} f \subseteq b$. This is the b we were looking for.

(h) The result follows from the straightforward verification that $\varphi(f, x)$ saying "$x \neq \emptyset$, every element of x is non-empty, and $f\colon x \to \bigcup x$ is a choice function" is Δ_0. □

Proof of Theorem 19.15. (a) It is enough to check that replacement and choice hold in V_ω. As we shall see (Exercise 21.52), every V_n is finite, hence every element of V_ω is finite. It follows that every $x \in \mathrm{V}_\omega$ is well-orderable, hence AC holds by Theorem 18.3. Moreover, if $A \in \mathrm{V}_\omega$ and $F\colon A \to \mathrm{V}_\omega$, then $F``A$ is finite, $F``A = \{a_0, \dots, a_{n-1}\}$. For every $i < n$, let $m_i < \omega$ be such that $a_i \in \mathrm{V}_{m_i}$. Then $F``A \subseteq \mathrm{V}_m$, where $m = \max\{m_0, \dots, m_{n-1}\}$, hence $F``A \in \mathrm{V}_{m+1}$.

(b) Since $\omega \in \mathrm{V}_\lambda$ we apply Theorem 19.22(e).

(c) If $\mathcal{A} \in \mathrm{V}_\lambda$ is a non-empty family of non-empty sets, by AC there is a choice function $f\colon \mathcal{A} \to \bigcup \mathcal{A}$. If $\alpha < \lambda$ is such that $\mathcal{A} \in \mathrm{V}_{\alpha+1}$ then $f \in \mathrm{V}_{\alpha+3}$ so we are done by Theorem 19.22(h). □

Exercises

Exercise 19.23. Generalize Exercise 18.40 by showing that if X is a class, $R \subseteq X \times X$ is left-narrow on X, and every non-empty sub*set* of X has an R-minimal element, then R is well-founded on X.

Exercise 19.24. Show that if X and Y are transitive classes and $f\colon X \to Y$ is a bijective functional relation such that $\forall x_1, x_2 \in X\, (x_1 \in x_2 \Leftrightarrow f(x_1) \in f(x_2))$, then $f = \mathrm{id} \upharpoonright X$ and $X = Y$. Conclude that the classes $\boldsymbol{\pi}_{R,X}$ and $\overline{X}$ in part (a) of Proposition 19.8 are unique.

Exercise 19.25. Check that if R is a well-order on X then $\operatorname{ran}(\boldsymbol{\varrho}_{R,X}) = \operatorname{ot}(X, R)$ and $\boldsymbol{\varrho}_{R,X}\colon X \to \operatorname{ot}(X, R)$ is the inverse of the enumerating function (see page 389).

Exercise 19.26. Suppose $X \subseteq Y$ are classes. Show that:

(i) $\mathrm{TC}(X) \subseteq \mathrm{TC}(Y)$.

(ii) If Y is transitive, then $\mathrm{TC}(X) \subseteq Y$.

Exercise 19.27. Suppose X is a transitive class, and let $\Omega = \mathrm{rank}``X$. Show that $\Omega \in \mathrm{Ord}$ if X is a set, and $\Omega = \mathrm{Ord}$ if X is a proper class.

Exercise 19.28. Prove the properties of ordinal addition, multiplication, and exponentiation listed in Table 2.

Exercise 19.29. Show that $f \colon \langle \{0\} \times \alpha \cup \{1\} \times \beta, <_{\mathrm{lex}} \rangle \to \langle \alpha \dotplus \beta, < \rangle$ and $g \colon \langle \beta \times \alpha, <_{\mathrm{lex}} \rangle \to \langle \alpha \cdot \beta, < \rangle$ are order isomorphisms,[7] where $f(0, \nu) = \nu$ and $f(1, \nu) = \alpha \dotplus \nu$, and $g(\gamma, \delta) = \alpha \cdot \gamma \dotplus \delta$. Conclude that:

- $|\alpha \dotplus \beta| = |\alpha| + |\beta|$ and $|\alpha \cdot \beta| = |\alpha||\beta|$, where on the right-hand-side we use the *cardinal* operations. In particular, $n \dotplus m = n + m$ and $n \cdot m = nm$ for all $n, m \in \omega$;
- if $\kappa \geq \omega$ is a cardinal and $\alpha, \beta < \kappa$ then $\alpha \dotplus \beta, \alpha \cdot \beta < \kappa$.

Exercise 19.30. Show that

(i) ${}^{m}n$ is finite and $|{}^{m}n| = n^{\cdot m}$ for all $n, m \in \omega$.

(ii) there are ordinals such that $\alpha \dotplus \beta \neq \beta \dotplus \alpha$; such that $\alpha \cdot \beta \neq \beta \cdot \alpha$; such that $(\alpha \dotplus \beta) \cdot \gamma \neq (\alpha \cdot \gamma) \dotplus (\beta \cdot \gamma)$.

Exercise 19.31. Show that

(i) all axioms of MK except the axiom of infinity hold in $\mathrm{V}_{\mathbf{S}(\omega)}$,

(ii) if $\lambda > \omega$ is limit, then all axioms of MK with the possible exception of replacement hold in $\mathrm{V}_{\mathbf{S}(\lambda)}$, and if we assume choice, also AC holds.

Exercise 19.32. Show that if $\alpha < \beta$ then $\omega^{\cdot\alpha} \cdot n \dotplus \omega^{\cdot\beta} = \omega^{\cdot\beta}$ for all $n \in \omega$; if $\alpha < \omega^{\cdot\beta}$ then $\alpha \dotplus \omega^{\cdot\beta} = \omega^{\cdot\beta}$.

Exercise 19.33. If $F \colon \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ is a binary operation on the ordinals, an ordinal α is F-indecomposable[8] if and only if $\forall \beta, \gamma < \alpha\, (F(\beta, \gamma) < \alpha)$. The ordinals $0, \omega$ are additively, multiplicatively, and exponentially indecomposable, 1 is additively and multiplicatively indecomposable, and 2 is multiplicatively indecomposable.

Show that for $\alpha, \lambda \in \mathrm{Ord}$ and λ limit:

(i) If $\alpha \geq 2$ then $\alpha < \alpha \dotplus \alpha \leq \alpha \cdot \alpha \leq \alpha^{\cdot\alpha}$, and if $\alpha > 2$ then all the inequalities are strict.

[7] This shows the correctness of the definitions of addition and multiplication of ordinals seen in Section 13.A.

[8] When F is the addition, multiplication, or exponential operation we will speak of additively, multiplicatively, or exponentially indecomposable ordinals defined on page 407.

(ii) If λ is exponentially indecomposable, then it is multiplicatively indecomposable; if λ is multiplicatively indecomposable, then it is additively indecomposable.

(iii) If $\nu \mapsto F(\alpha, \nu)$ is increasing and continuous, for all α, then λ is F-indecomposable if and only if $F(\alpha, \lambda) = \lambda$, for all $\alpha < \lambda$. (Therefore $\forall \alpha, \beta < \lambda\, (\alpha \dotplus \beta < \lambda) \Leftrightarrow \forall \alpha < \lambda\, (\alpha \dotplus \lambda = \lambda)$, and similarly for multiplication and exponentiation.)

(iv) λ is additively indecomposable if and only if $\exists \alpha\, (\lambda = \omega^{\cdot \alpha})$ and α is multiplicatively indecomposable $\exists \alpha (\lambda = \omega^{\cdot \omega^{\cdot \alpha}})$.

(v) If λ is additively decomposable, then there are $0 < \beta < \alpha < \lambda$ such that $\lambda = \alpha \dotplus \beta$; if λ is multiplicatively decomposable, then there are $0 < \beta < \alpha < \lambda$ such that $\lambda = \alpha \cdot \beta$.

Exercise 19.34. Define by recursion $E(0, \alpha) = \alpha$ and $E(n \dotplus 1, \alpha) = \alpha^{\cdot E(n, \alpha)}$. Show that for $\alpha \geq 2$:

(i) if $n \leq m$ then $E(n, \alpha) \leq E(m, \alpha)$ and $E(n, \alpha) \dotplus E(m, \alpha) \leq E(m \dotplus 1, \alpha)$;

(ii) $\sup_n E(n, \alpha)$ is the smallest exponentially indecomposable ordinal $> \alpha$, and $\sup_n E(n, \alpha) = \sup_n E'(n, \alpha)$ where $E'(n \dotplus 1, \alpha) = E'(n, \alpha)^{\cdot E'(n, \alpha)}$ and $E'(0, \alpha) = \alpha$.

Exercise 19.35. Order the ordinals $\alpha_0, \ldots, \alpha_5$:

$$\begin{array}{lll}
\alpha_0 = \omega^{\cdot \omega} \cdot (\omega \dotplus \omega) & \alpha_1 = (\omega \dotplus \omega) \cdot \omega^{\cdot \omega} & \alpha_2 = (\omega^{\cdot \omega} \dotplus \omega) \cdot \omega \dotplus \omega^{\cdot \omega} \\
\alpha_3 = \omega \cdot \omega^{\cdot \omega} \dotplus \omega^{\cdot \omega} \cdot \omega & \alpha_4 = \omega^{\cdot \omega} \cdot \omega \dotplus \omega \cdot \omega^{\cdot \omega} \cdot \omega & \alpha_5 = (\omega \cdot 3)^{\omega \dotplus 1}
\end{array}$$

Exercise 19.36. Let $F \colon \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ be the unique isomorphism between $\langle \mathrm{Ord} \times \mathrm{Ord}, <_{\mathrm{G}} \rangle$ and $\langle \mathrm{Ord}, < \rangle$. Show that:

(i) The anti-lexicographic ordering and $<_{\mathrm{G}}$ agree on $\alpha \times [\alpha; \alpha \dotplus \beta)$, for all $\alpha, \beta \in \mathrm{Ord}$. Therefore $\operatorname{ot} \langle \alpha \times [\alpha; \alpha \dotplus \beta), <_{\mathrm{G}} \rangle = \alpha \cdot \beta$.

(ii) If $\operatorname{ot} \langle \lambda \times \lambda, <_{\mathrm{G}} \rangle = \lambda$, then λ is multiplicatively indecomposable. [Hint: argue that λ is additively indecomposable.]

(iii) If $\gamma \geq \omega$ is additively indecomposable and $\nu < \gamma$, then $\operatorname{ot} \langle \nu \times \nu, <_{\mathrm{G}} \rangle < \gamma^2$. Conclude that if λ is multiplicatively indecomposable, then $\lambda = \operatorname{ot} \langle \lambda \times \lambda, <_{\mathrm{G}} \rangle$.

Exercise 19.37. Let $\beta > 1$.

(i) Consider the equation

$$(*) \qquad \begin{array}{l} \nu = \beta^{\cdot \gamma_0} \cdot \delta_0 \dotplus \beta^{\cdot \gamma_1} \cdot \delta_1 \dotplus \cdots \dotplus \beta^{\cdot \gamma_{m-1}} \cdot \delta_{m-1}, \text{ with } m \in \omega, \\ \gamma_0 > \gamma_1 > \cdots > \gamma_{m-1} \text{ and } 0 < \delta_i < \beta \text{ for all } i < m, \end{array}$$

where $\nu = 0$ if and only if $m = 0$. Show that

- if ν is as in $(*)$ then $\nu < \beta^{\cdot \gamma_0 \dotplus 1}$,

- for every $\nu \in \mathrm{Ord}$ there exist and are unique $m \in \omega$ and γ_i, δ_i for $i < m$ such that $(*)$ holds.

The expression $(*)$ is the normal form of ν in base β, and when $\beta = \omega$ it is called **Cantor's normal form**.

(ii) Let $E(\alpha, \beta) = \{f \in {}^{\alpha}\beta \mid \{\gamma \in \alpha \mid f(\gamma) \neq 0\} \text{ is finite}\}$. If $f, g \in E(\alpha, \beta)$ are distinct, there is a largest $\gamma \in \alpha$ such that $f(\gamma) \neq g(\gamma)$ and set $f \prec g \Leftrightarrow f(\gamma) < g(\gamma)$. For each $\nu \in \beta^{\cdot\alpha}$ let $\Phi(\nu) \in E(\alpha, \beta)$ be defined by using the equation $(*)$ above:

$$\Phi(\nu)(\gamma) = \begin{cases} \delta_i & \text{if } \gamma = \gamma_i, \\ 0 & \text{otherwise.} \end{cases}$$

Show that $\Phi \colon \langle \beta^{\cdot\alpha}, < \rangle \to \langle E(\alpha, \beta), \prec \rangle$ is an order isomorphism.

(iii) Show that if $\kappa \geq \omega$ is a cardinal, then $\alpha, \beta < \kappa \Rightarrow \beta^{\cdot\alpha} < \kappa$.

Exercise 19.38. The ordinal sum of a sequence of ordinals $\langle \alpha_i \mid i < \nu \rangle$ is $\dot{\sum}_{i<\nu} \alpha_i \overset{\text{def}}{=} \mathrm{ot}\langle \biguplus_{i<\nu} \alpha_i, \leq_{\text{lex}} \rangle$. Show that:

(i) If $\nu = \xi \dotplus 1$, then $\dot{\sum}_{i<\nu} \alpha_i = \dot{\sum}_{i<\xi} \alpha_i \dotplus \alpha_\xi$. In particular if $\nu = 2$, $\dot{\sum}_{i<\nu} \alpha_i = \alpha_0 \dotplus \alpha_1$.

(ii) If $\xi < \nu$, then $\dot{\sum}_{i<\xi} \alpha_i \leq \dot{\sum}_{i<\nu} \alpha_i$ and the inequality is strict if and only if $\alpha_j \neq 0$ for some $\xi \leq j < \nu$.

(iii) If ν is limit, then $\dot{\sum}_{i<\nu} \alpha_i = \sup_{\xi<\nu} \dot{\sum}_{i<\xi} \alpha_i$.

Exercise 19.39. If f and g are real valued function of a real variable, set

$$f \prec g \Leftrightarrow \exists M \forall x > M \left(f(x) < g(x) \right).$$

(See Exercise 13.69.) Let $\mathcal{F}$ be the smallest set of functions containing $\mathbb{N}[X]$ and closed under addition and the operation $f \mapsto X^f$. (Thus $X^{(X^{3X+2} + 5X^X)} + 2X + 4$ is in $\mathcal{F}$, but $(X+1)^X$ is not.) Show that the ordering $\prec$ on $\mathcal{F}$ is a well-order of type $\boldsymbol{\epsilon}_0$.

Exercise 19.40. Consider the first-order language $\mathcal{L}$ with only $<$ as nonlogical symbol. A statement σ **characterizes** an ordinal $\alpha \neq 0$ if α is the unique non-zero ordinal satisfying σ, that is if $\beta \neq 0$ and $\langle \beta, < \rangle \vDash \sigma$ then $\alpha = \beta$.

Show that:

(i) every $0 < \alpha < \omega^{\cdot\omega}$ can be characterized by a sentence σ of $\mathcal{L}$,

(ii) if $0 < \alpha < \beta < \omega^{\cdot\omega}$ then $\langle \alpha, < \rangle$ and $\langle \beta, < \rangle$ are not elementarily equivalent.

(We will prove in **??** that this is optimal: the only characterizable ordinals are those $< \omega^{\omega}$.)

Exercise 19.41. Let b be a natural number > 1. The expression of n in **pure base** b is computed as follows:

- write n in base b, that is $n = b^{k_0} h_0 + \cdots + b^{k_{m-1}} h_{m-1}$;
- every k_i is written in base b, that is $k_i = b^{\bar{k}_0} \bar{h}_0 + \cdots + b^{\bar{k}_{m-1}} \bar{h}_{m-1}$;
- every $\bar{k}_i$ is written in base b, and so on…

until in the expression we have digits $\leq b$. For example the expression of $n = 1931$ in pure base $b = 2, 3, 4$ is

$$\begin{aligned} 1931 &= 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2+1} + 2 + 1 \\ &= 3^{3 \cdot 2} \cdot 2 + 3^{3+2} + 3^{3+1} \cdot 2 + 3^3 \cdot 2 + 3^2 + 3 + 2 \\ &= 4^{4+1} + 4^4 \cdot 3 + 4^3 \cdot 2 + 4 \cdot 2 + 3. \end{aligned}$$

Per each $n \in \mathbb{N}$, the **Goodstein sequence** of n is computed as follows: $G_n(0) = n$, $G_n(k+1)$ is obtained from $G_n(k)$ written in pure base $k+2$, replacing every $k+2$ with $k+3$, and then subtracting 1. Thus $G_n(1)$ is obtained by replacing every 2 in the expression in pure base 2 with 3 and then subtracting 1, $G_n(2)$ is obtained from $G_n(1)$ written in pure base 3, replacing 3 with 4 and then subtracting 1, and so on. The first few elements of the Goodstein sequence $n = 1931$ are

$$\begin{aligned} G_0(1931) &= 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2+1} + 2 + 1 \\ G_1(1931) &= 3^{3^{3+1}+3} + 3^{3^{3+1}+1} + 3^{3^{3+1}} + 3^{3^3+3+1} + 3^{3+1} + 3 \\ G_2(1931) &= 4^{4^{4+1}+4} + 4^{4^{4+1}+1} + 4^{4^{4+1}} + 4^{4^4+4+1} + 4^{4+1} + 3 \\ G_3(1931) &= 5^{5^{5+1}+5} + 5^{5^{5+1}+1} + 5^{5^{5+1}} + 5^{5^5+5+1} + 5^{5+1} + 2 \\ &\;\;\vdots \end{aligned}$$

Show that every Goodstein sequence ends with a 0, that is $\forall n \exists k\, G_n(k) = 0$.

Exercise 19.42. By Cantor's Theorem 13.22 there is no injection F from the powerset $\mathscr{P}(X)$ into X. In this exercise we will explicitly construct sets W and Z of X such that $F(W) = F(Z)$.

Let $F\colon \mathscr{P}(X) \to X$. Show that there is a unique $W \subseteq X$ and a unique well-order $\lhd$ on W such that

(a) $F(\{z \in W \mid z \lhd w\}) = w$, for all $w \in W$ and

(b) $F(W) \in W$.

Conclude that F is not injective, even if restricted to $\mathscr{P}_{\mathrm{WO}}(X) = \{Y \subseteq X \mid Y \text{ is well-orderable}\}$.

Exercise 19.43. Let $\mathfrak{a}\colon \mathrm{V}_\omega \to \omega$ be the map defined by $\mathfrak{a}(\emptyset) = 0$ and $\mathfrak{a}(x) = \sum_{i\leq k} 2^{\mathfrak{a}(x_i)}$ if $x = \{x_0, \dots, x_k\}$ has size $k+1$. Show that $\mathfrak{a}$ is a bijection.

[Hint: see Exercise 8.58.]

20. Cardinality and the axiom of choice

Recall that the axiom of choice is equivalent both to Zorn's Lemma and to the well-ordering principle, that is the statement that every set is well-orderable (Theorem 14.3). In particular **cardinal exponentiation** is defined by

$$\lambda^\kappa = |{}^\kappa\lambda| .$$

This definition subsumes that the set ${}^\kappa\lambda$ is well-orderable, so *the operation of cardinal exponentiation is defined under* AC. By Lemma 13.24 we have that for cardinals $\kappa, \lambda, \mu, \nu$

$$\kappa \leq \nu \wedge \lambda \leq \mu \Rightarrow \kappa^\lambda \leq \nu^\mu \qquad \left(\kappa^\lambda\right)^\mu = \kappa^{\lambda\cdot\mu}$$
$$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu \qquad (\kappa\cdot\lambda)^\mu = \kappa^\mu \cdot \lambda^\mu .$$

Definition 20.1. If X is a set and κ is a cardinal

$$\mathscr{P}_\kappa(X) = \{Y \subseteq X \mid |Y| < \kappa\}$$

is the collection of all well-orderable subsets of X of size less than κ.

Note that $\mathscr{P}_\kappa(\lambda) = [\lambda]^{<\kappa}$, as in Definition 18.32. By Exercise 20.19, $\mathscr{P}_\kappa(\lambda)$ has size $\lambda^{<\kappa} \leq \lambda^\kappa$, where

$$\lambda^{<\kappa} \overset{\text{def}}{=} \sup\{\lambda^\nu \mid \nu \in \mathrm{Card} \wedge \nu < \kappa\} .$$

The class-function $\beth\colon \mathrm{Ord} \to \mathrm{Card}$, where $\beth$ (to be read: beth) is the second letter of the Hebrew alphabet, is defined by recursion by

$$\beth_0 = \omega, \qquad \beth_{\alpha+1} = 2^{\beth_\alpha}, \qquad \beth_\lambda = \sup\nolimits_{\alpha<\lambda} 2^{\beth_\alpha}, \text{ for } \lambda \text{ limit.}$$

Cardinal exponentiation will be presented in detail in Section 21. For the time being we just look at some elementary facts.

20.A. The continuum hypothesis. Cantor's Theorem 13.22 can be restated as $\forall I \left(|I| < 2^{|I|}\right)$. The **Continuum Hypothesis** CH is the statement that

$$2^{\aleph_0} = \aleph_1,$$

or, equivalently, $\forall X \subseteq \mathbb{R}\,(|X| \leq \aleph_0 \vee |X| = |\mathbb{R}|)$. The **Generalized Continuum Hypothesis** GCH is its generalization to all infinite cardinals

$$\forall\alpha \in \mathrm{Ord}\big(2^{\aleph_\alpha} = \aleph_{\alpha+1}\big),$$

or, equivalently, $\forall X \subseteq \mathscr{P}(\aleph_\alpha)\,(|X| \leq \aleph_\alpha \vee |X| = |\mathscr{P}(\aleph_\alpha)|)$. Both CH and GCH are independent from the usual axiomatizations of set theory, like

$\mathsf{MK}+\mathsf{AC}$, $\mathsf{NGB}+\mathsf{AC}$, or ZFC. In particular it may happen that $2^{\aleph_n}=\aleph_{f(n)}$ for any monotone function $f\colon\omega\to\omega$ such that $f(n)\geq n+1$. Thus if $2^{\aleph_0}=2^{\aleph_1}=\aleph_k$ for some $k\geq 2$, then $|\mathscr{P}(\omega)|=|\mathscr{P}(\omega_1)|$, so that the implication $X\precsim Y\Rightarrow\mathscr{P}(X)\precsim\mathscr{P}(Y)$ cannot be reversed. Similarly, the implication $\kappa_1<\kappa_2\Rightarrow\mathscr{P}_{\kappa_1}(\lambda)\precsim\mathscr{P}_{\kappa_2}(\lambda)$ cannot be reversed.

The continuum hypothesis asserts that two very different uncountable sets, $\mathbb{R}$ and ω_1, are in bijection. One might ask if one of the two sets surjects onto or injects into the other. The only result that one can prove without choice is that $\mathbb{R}\twoheadrightarrow\omega_1$, as it follows from (18.3). All other possibilities (that is $\omega_1\precsim\mathbb{R}$, $\mathbb{R}\precsim\omega_1$, and $\omega_1\twoheadrightarrow\mathbb{R}$) either follow from AC or else are equivalent to CH. More to the point:

- Assuming AC then $\mathbb{R}$ is well-orderable, so $\omega_1\precsim\mathbb{R}$. But $\omega_1\precsim\mathbb{R}$ does not imply that $\mathbb{R}$ is well-orderable. From $\omega_1\precsim\mathbb{R}$ it is possible to construct certain "pathological" subsets of $\mathbb{R}$ (sets that are non-Lebesgue measurable, that do not have the property of Baire,...), see Section 28.B.
- If $\omega_1\twoheadrightarrow\mathbb{R}$ then $\mathbb{R}\precsim\omega_1$, so $\mathbb{R}$ is well-orderable, and since ω_1 is the least uncountable ordinal, it follows that $\omega_1\asymp\mathbb{R}$.

Remark 20.2. As we shall see in Section 20.C below, it is possible to develop the notion of cardinality in a choice-less world. In this context, the continuum hypothesis can be restated as: $\forall\mathcal{A}\subseteq\mathscr{P}(\omega)\bigl(\mathcal{A}\precsim\omega\vee\mathcal{A}\asymp\mathscr{P}(\omega)\bigr)$. This sentence does not to imply that $\mathscr{P}(\omega)$ is well-orderable, so it is weaker than CH. The generalized continuum hypothesis becomes $\forall X\,\forall\mathcal{A}\subseteq\mathscr{P}(X)\,\bigl(X\text{ infinite}\Rightarrow\mathcal{A}\precsim X\vee\mathcal{A}\asymp\mathscr{P}(X)\bigr)$. The statement implies the axiom of choice, and hence it is fully equivalent to GCH (Exercise 20.28).

20.B. Which sets are well-orderable? The axiom of choice says that given a non-empty family of non-empty sets $\mathcal{A}$ there is a function $f\colon\mathcal{A}\to\bigcup\mathcal{A}$ such that $\forall A\in\mathcal{A}\,(f(A)\in A)$. The family $\mathcal{A}$ can be written as $\{A_i\mid i\in I\}$ with $A_i\subseteq X$, for suitable sets I and X. By fixing one or both parameters I and X interesting weak forms of AC are obtained.

Focusing on the set of indexes I we obtain AC_I

(AC_I) given $\langle A_i\mid i\in I\rangle$ such that $A_i\neq\emptyset$ for all $i\in I$, there is $\langle a_i\mid i\in I\rangle$ such that $a_i\in A_i$, for all $i\in I$.

When I is finite, AC_I is provable in both MK and ZF, but when I is infinite a statement strictly weaker than AC, but still independent of the other axioms of set theory, is obtained. When $I=\omega$ we obtain the **Axiom of Countable Choices** AC_ω which we talked about in Section **??**.

Focusing on the set X we obtain the principle $\mathsf{AC}(X)$

($\mathsf{AC}(X)$) if X is a non-empty set, then there is a choice function on X.

Lastly, $\mathsf{AC}_I(X)$ is the statement

($\mathsf{AC}_I(X)$) if X is a non-empty set and $I \to \mathscr{P}(X) \setminus \{\emptyset\}$, $i \mapsto A_i$, then there is a function $I \to X$, $i \mapsto a_i \in A_i$.

Therefore $\mathsf{AC}_I \Leftrightarrow \forall X\, \mathsf{AC}_I(X)$, $\mathsf{AC}(X) \Leftrightarrow \forall I\, \mathsf{AC}_I(X)$ and $\mathsf{AC} \Leftrightarrow \forall I\, \forall X\, \mathsf{AC}_I(X)$. If $X \twoheadrightarrow Y$ and $J \rightarrowtail I$, then $\mathsf{AC}_I(X) \Rightarrow \mathsf{AC}_J(Y)$ (Exercise 20.16). Exercise **??** shows a few statements equivalent to AC:

- every partition of a non-empty set has a selector,
- the cartesian product of non-empty sets is non-empty,
- every surjection has a left inverse,
- for every relation R there is a function f such that $\forall x \in \mathrm{dom}(R)\, [x\ R\ f(x)]$,

and more examples, from various parts of mathematics, will be seen in Section 28.

By Theorem 14.3 the axiom of choice, that is $\forall X\, \mathsf{AC}(X)$, is equivalent to "every set X is well-orderable". In fact the equivalence holds for every set X, that is $\mathsf{AC}(X)$ if and only if X is well-orderable: the reverse implication is Theorem 18.3 and the forward implication is the next result.

Theorem 20.3. $\mathsf{AC}(X)$ *implies that* X *is well-orderable.*

Proof. If $X = \emptyset$ then, trivially, X is well-orderable, hence we may assume that X is non-empty and fix a choice function C for X. Let $x_0 = C(X)$ and suppose we have constructed $x_0, x_1, \dots, x_\beta, \dots$ distinct elements of X, with $\beta < \alpha$. If $X = \{x_\beta \mid \beta < \alpha\}$ then $\alpha \to X$, $\beta \mapsto x_\beta$ is the required bijection. Otherwise choose an element $x_\alpha \in X$ distinct from the preceding ones, for example $x_\alpha = C(X \setminus \{x_\beta \mid \beta < \alpha\})$. If the function $\alpha \mapsto x_\alpha$ were defined for all $\alpha < \mathrm{Hrtg}(X)$, we would have an injection $\mathrm{Hrtg}(X) \rightarrowtail X$, against the definition of Hartogs' number (pag. 392). Therefore there is $\bar{\alpha} < \mathrm{Hrtg}(X)$ such that $X = \{x_\beta \mid \beta < \bar{\alpha}\}$. □

The preceding results can be extended to proper classes if we convene that a choice function for a proper class X is a class-function F with domain $\{y \mid \emptyset \neq y \subseteq X\}$ and such that $F(y) \in y$, for all $y \in \mathrm{dom}(F)$.

Theorem 20.4. *A class X is well-orderable if and only if there is a choice function on X. In particular,* V *is well-orderable if and only if* AGC*, the global axiom of choice (pag. 378), holds.*

We proved in Chapter **??** that the axiom of choice is equivalent to Zorn's Lemma (Theorem 14.3), which says $\forall X\, \textsc{Zorn}(X)$, where

$\textsc{Zorn}(X)$: if $\leq$ is an ordering on X such that every chain has an upper bound, then there is a maximal element $x \in X$.

If the assumption is strengthened by replacing "chain" with "upward directed set" we obtain the weaker principle:

$\textsc{wZorn}(X)$: if $\leq$ is an ordering on X such that every upward directed set has an upper bound, then there is a maximal $x \in X$

and $\forall X\, \textsc{wZorn}(X)$ is known as the **weak Zorn's Lemma**. The **Hausdorff's maximality principle** says that every ordered set contains a maximal chain, $\forall X\, \textsc{MaxHaus}(X)$, where

$\textsc{MaxHaus}(X)$: if $\leq$ is an ordering on X, then $\exists C \subseteq X\, (C$ maximal chain).

Proposition 20.5. *Fix a non-empty set X,*

$$X \text{ is well-orderable} \Rightarrow \textsc{MaxHaus}(X) \Rightarrow \textsc{Zorn}(X) \Rightarrow \textsc{wZorn}(X)$$

and

$$\textsc{wZorn}(\mathscr{P}(X \times X)) \Rightarrow X \text{ is well-orderable.}$$

Proof. Suppose X is well-orderable, and towards a contradiction, let $\leq$ be an ordering on X without maximal chains. If $C \subseteq X$ is a chain, the set

$$K(C) = \{x \in X \setminus C \mid C \cup \{x\} \text{ is a chain}\}$$

is non-empty. Fix a choice function $F \colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. Then

$$g \colon \mathrm{Hrtg}(X) \to X, \quad \alpha \mapsto F\left(K\left(\{g(\beta) \mid \beta < \alpha\}\right)\right).$$

is injective, against Theorem 18.23.

Suppose now $\textsc{MaxHaus}(X)$, and let $\leq$ be an order on X such that each chain has an upper bound. If $C \subseteq X$ is a maximal chain, then the upper bound of C must belong to C hence it is a maximal element of X.

The implication $\textsc{Zorn}(X) \Rightarrow \textsc{wZorn}(X)$ is immediate.

Finally notice that in part (a)⇒(b) of the proof of Theorem 14.3, i.e. that Zorn's Lemma implies the well-ordering principle, we actually used $\textsc{wZorn}(\mathscr{P}(X \times X))$. □

Theorem 20.6. AC *is equivalent to* $\forall \alpha \in \mathrm{Ord}\, (\mathscr{P}(\alpha)$ *is well-orderable*).

Proof. By Corollary 19.13 it is enough to show that V_α is well-orderable for all α. Proceed by induction on α.

Clearly $\mathrm{V}_0 = \emptyset$ is well-orderable, and if V_α is well-orderable and $f \colon \mathrm{V}_\alpha \to \gamma$ is a bijection, then by hypothesis there is a well-order $\prec$ on $\mathscr{P}(\gamma)$ that induces via f a well-order on $\mathrm{V}_{\alpha+1} = \mathscr{P}(\mathrm{V}_\alpha)$.

We now consider the more complex case when λ is limit. Suppose V_α is well-orderable for every $\alpha < \lambda$: if we can construct (without appealing to AC!) well-orders $\lhd_\alpha$ on V_α, for all $\alpha < \lambda$, then for $x, y \in \mathrm{V}_\lambda$

$$x \lhd_\lambda y \Leftrightarrow \exists \alpha < \lambda \left[(x \in \mathrm{V}_\alpha \wedge y \notin \mathrm{V}_\alpha) \vee (x, y \in \mathrm{V}_{\alpha+1} \setminus \mathrm{V}_\alpha \wedge x \lhd_{\alpha+1} y)\right] \tag{20.1}$$

is a well-order of V_λ (Exercise 18.46) as required. Let $\gamma = \sup_{\alpha<\lambda} \gamma_\alpha^+$ where $\gamma_\alpha = |\mathscr{P}(\alpha)|$, so that every well-order of V_α has order-type $< \gamma$. Let $\prec$ be a well-order on $\mathscr{P}(\gamma)$. It is enough to construct by induction on $\alpha < \lambda$ a well-order $\lhd_\alpha$ on V_α. Set $\lhd_0 = \emptyset$; if $\lhd_\alpha$ is a well-order on V_α and $f_\alpha \colon \mathrm{V}_\alpha \to \gamma^+$ is its enumerating function, then define $\lhd_{\alpha+1}$ on $\mathrm{V}_{\alpha+1}$ using f_α and $\prec$; if $\nu < \lambda$ is a limit ordinal, apply construction (20.1) with ν in place of λ. □

The next result summarizes some equivalents of the axiom of choice. Recall from page 42 that a subset Q of an preordered set $\langle P, \leq \rangle$ is **independent** if $x \nleq y$ and $y \nleq x$ for all distinct $x, y \in Q$.[9]

Theorem 20.7. *The following are equivalent:*

(a) AC.

(b) *Hausdorff's maximality principle.*

(c) *Zorn's Lemma.*

(d) *The weak form of Zorn's Lemma.*

(e) *The* **Teichmüller-Tukey Lemma:** *Let $\emptyset \neq \mathcal{F} \subseteq \mathscr{P}(X)$ be a family of* ***finite character****, that is*

$$\forall Y \subseteq X\ (Y \in \mathcal{F} \Leftrightarrow \forall Z \subseteq Y\ (Z \text{ finite} \Rightarrow Z \in \mathcal{F}))\,.$$

Then every $Y \in \mathcal{F}$ is included in a maximal $Z \in \mathcal{F}$.

(f) *The* **Axiom of Multiple Choices (AMC):** *For every set $X \neq \emptyset$ there is a function $F \colon \mathscr{P}(X) \setminus \{\emptyset\} \to \mathscr{P}(X) \setminus \{\emptyset\}$ such that $F(A) \subseteq A$ is finite, for each $\emptyset \neq A \subseteq X$.*

(g) *Every pre-order contains a maximal independent subset.*

(h) **Kurepa's maximality principle:** *Every order contains a maximal independent subset.*

(i) *Every linear order is well-orderable.*

Proof. The implications (g) ⇒ (h) and (a) ⇒ (f) are immediate, while (a) ⇔ (b) ⇔ (c) ⇔ (d) follow from Proposition 20.5.

(d) ⇒ (e). Let $\mathcal{F} \subseteq \mathscr{P}(X)$ be of finite character, and let $Y \in \mathcal{F}$. If $\mathcal{D} \subseteq \mathcal{F}$ is an upward directed collection of sets containing Y, then $\bigcup \mathcal{D} \in \mathcal{F}$ by the finite character of $\mathcal{F}$, so $\mathcal{D}$ has an upper bound in $\mathcal{F}$. Therefore there is a $Z \in \mathcal{F}$ which is maximal and contains Y.

(e) ⇒ (g). Let $\langle X, \leq \rangle$ be a preordered set. The collection $\mathcal{F}$ of all indpendent subsets of X has finite character, and $\emptyset \in \mathcal{F}$, hence it contains a maximal set.

[9] In combinatorics independent subsets of orders are also known as **antichains**, but in this book we eschew this terminology since for Boolean algebras, which are particular kind of ordered sets, the word 'antichain' has a different meaning.

(f) ⇒ (i) and (h) ⇒ (i). Let $\langle X, \leq\rangle$ be a linear order: we will show that there is a choice function for X hence the result follows from Theorem 20.3.

Suppose (f) holds: by assumption there is $G\colon \mathscr{P}(X)\setminus\{\emptyset\} \to \mathscr{P}(X)\setminus\{\emptyset\}$ such that $G(A) \subseteq A$ is finite, for each $\emptyset \neq A \subseteq X$. Let $g(A)$ be the last element of $G(A)$. Then g is a choice function on X.

Suppose (h) holds: let $\preceq$ be the order on $\mathcal{P} = \{(A, a) \mid A \subseteq X \wedge a \in A\}$ defined by

$$(A, a) \preceq (B, b) \Leftrightarrow A = B \wedge a \leq b.$$

By assumption there is a maximal independent $\mathcal{A} \subseteq \mathcal{P}$: it is clear that $\mathcal{A}$ is a choice function for X.

(i) ⇒ (a). ${}^{\alpha}2$ is linearly ordered by the lexicographic $<_{\text{lex}}$, hence ${}^{\alpha}2$ is well-orderable. Since ${}^{\alpha}2 \asymp \mathscr{P}(\alpha)$ the result follows from Theorem 20.6. □

20.C. Cardinality without choice*. Assuming the axiom of choice, every set is in bijection with an ordinal, hence the notion of cardinality (Definition 18.20) is defined by

$$|X| = \min\{\alpha \mid \alpha \asymp X\}$$

where $\asymp$ is the equipotence relation between sets. But how do we define this notion in the absence of AC? In naïve set theory (Section 13) the cardinality of a set X is defined as

$$\operatorname{card}(X) = [X]_{\asymp},$$

and comparison between cardinalities is

$$\operatorname{card}(X) \leq \operatorname{card}(Y) \Leftrightarrow X \precsim Y. \tag{20.2}$$

By the Cantor-Schröder-Bernstein Theorem 13.11 $\leq$ is antisymmetric, hence it is an order on cardinalities. The drawback of this approach is that $\operatorname{card}(X)$ is a proper class when X is non-empty (Exercise 18.41). A similar problem occurs when dealing with an equivalence relation E on a proper class $\mathcal{A}$ such that E is not left-narrow, that is the equivalence classes are proper classes—this is the typical case when one studies structures up to isomorphism. Given a class $\mathcal{A}$ and an equivalence relation E as above, we would like a class function $\boldsymbol{C}\colon \mathcal{A} \to \mathcal{A}$ such that

$$\forall x \in \mathcal{A}\,(\boldsymbol{C}(x) \in [x]_E) \qquad \text{and} \qquad \forall x, y \in \mathcal{A}\,(x \mathrel{E} y \Rightarrow \boldsymbol{C}(x) = \boldsymbol{C}(y)).$$

The existence of such a $\boldsymbol{C}$ is equivalent to the existence of a **transversal** T **for the relation** E, that is a class $T \subseteq \mathcal{A}$ such that $T \cap [x]_E$ is a singleton, for each $x \in \mathcal{A}$.

In some situations the function $\boldsymbol{C}$ can be explicitly defined, even when E is not left-narrow on $\mathcal{A}$:

- If $\mathcal{A}$ is the class of well-ordered sets and E is the isomorphism relation, then every equivalence class contains exactly one ordinal, hence we can set $\boldsymbol{C}(A,<) = \operatorname{ot}(A,<)$;
- If $\mathcal{A}$ is the class of countable compact spaces and E is the homeomorphism relation, then we can set $\boldsymbol{C}(K)$ to be the unique ordinal of the form $\omega^{\cdot\gamma} \cdot n + 1$, with $\gamma < \omega_1$ (Theorem 27.2);
- If $\mathcal{A}$ is the class of all finitely generated abelian groups and E is the isomorphism relation, then set $\boldsymbol{C}(G) = \mathbb{Z}^n \times \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}$ for suitable $n \geq 0$, primes $p_1 \leq p_2 \leq \cdots \leq p_k$, and $k \geq 0$.

If some form of choice is assumed, the above list can be extended:

- Assuming AC and letting $\mathcal{A}$ be the class V and E the relation $\asymp$, then we can define $\boldsymbol{C}(A)$ as the unique cardinal κ in bijection with A.
- If the axiom of *global* choice is assumed, then V is well-orderable (Theorem 20.4) hence a class-function $\boldsymbol{C}$ can be defined for each $\mathcal{A}$ and E.

Conversely, in absence of choice it is not possible, in general, to select a canonical representative in each equivalence class of E. Using the V_α hierarchy of Section 19.E, it is possible to define (without choice!) a function $[\![\cdot]\!]_E \colon \mathcal{A} \to \mathrm{V}$ such that

$$\emptyset \neq [\![x]\!]_E \subseteq [x]_E \qquad \text{and} \qquad x \mathrel{E} y \Leftrightarrow [\![x]\!]_E = [\![y]\!]_E.$$

The set $[\![x]\!]_E$ is called the Scott's E-equivalence class,

$$\begin{aligned} [\![x]\!]_E &= \{y \mid y \mathrel{E} x \wedge \forall z\,(z \mathrel{E} x \Rightarrow \operatorname{rank}(y) \leq \operatorname{rank}(z))\} \\ &= [x]_E \cap \mathrm{V}_{\bar{\alpha}}, \end{aligned}$$

where $\bar{\alpha} = \min\{\alpha \mid \mathrm{V}_\alpha \cap [x]_E \neq \emptyset\}$. Note that x need not to belong to $[\![x]\!]_E$. If $[\![x]\!]_E$ is a singleton for each x, then we can define a choice function for the E-equivalence classes by setting $\boldsymbol{C}(x) = \bigcup [\![x]\!]_E$.

Example 20.8. The **order type** of an ordered set $\langle A,<\rangle$ is defined by

$$\operatorname{type}\langle A,<\rangle = \begin{cases} \operatorname{ot}\langle A,<\rangle & \text{if } \langle A,<\rangle \text{ is a well-order,} \\ [\![\langle A,<\rangle]\!]_{\cong} & \text{otherwise,} \end{cases}$$

where $\cong$ is the isomorphism relation for ordered sets.

Order types can be added and multiplied—see Section 13.A.

20.C.1. *Cardinalities in the absence of choice.* In the absence of AC the **cardinality** of a set X is defined as

$$\operatorname{card}(X) = \begin{cases} |X| & \text{if } X \text{ is well-orderable,} \\ [\![X]\!]_{\asymp} & \text{otherwise.} \end{cases} \tag{20.3}$$

Cardinalities are usually denoted by lower case german letters, with $\mathfrak{c}$ denoting the cardinality of the continuum. The ordering on cardinalities is given by (20.2), that is

$$\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow A \precsim B \text{ for some/every } A \in \mathfrak{a} \text{ and } B \in \mathfrak{b}.$$

Remark 20.9. Using this definition every cardinal is a cardinality—the converse (that is every cardinality is a cardinal) is equivalent to the axiom of choice by the arguments in Section 20.B.

Assuming AC two cardinalities are always comparable, as they are ordinals. In fact comparability between cardinalities is equivalent to the axiom of choice.

Theorem 20.10. AC *is equivalent to the statement:*

$$\forall \mathfrak{a}, \mathfrak{b}\ (\mathfrak{a} \leq \mathfrak{b} \vee \mathfrak{b} \leq \mathfrak{a}),$$

or equivalently: $A \precsim B \vee B \precsim A$*, for every set* A, B.

Proof. By Theorem 18.3 and by the argument above, it is enough to show that comparability of cardinalities implies that every set is well-orderable. Fix a set A: as $\mathrm{Hrtg}(A) \precsim A$ is impossible by Theorem 18.23, then $A \precsim \mathrm{Hrtg}(A) \subseteq \mathrm{Ord}$. □

The operations on cardinalities are defined by

$$\begin{aligned} \operatorname{card}(A) + \operatorname{card}(B) &= \operatorname{card}(A \uplus B), \\ \operatorname{card}(A) \cdot \operatorname{card}(B) &= \operatorname{card}(A \times B), \\ \operatorname{card}(A)^{\operatorname{card}(B)} &= \operatorname{card}({}^{B}A). \end{aligned}$$

Note that this definition of addition and multiplication agrees with Definition 18.27 whenever A and B are well-orderable. The proof on page 314 shows that if $2 \leq \mathfrak{a}, \mathfrak{b}$, then $\mathfrak{a} + \mathfrak{b} \leq \mathfrak{a} \cdot \mathfrak{b}$. By definition $\mathfrak{a}$ is infinite if and only if $\mathfrak{a} \not< \omega$, so Theorem 18.28 says that AC implies

$$\mathfrak{a} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{a} = \mathfrak{a}, \tag{20.4}$$

that is to say: if A is infinite, then $A \asymp A \times A$. Assuming (20.4), if $A \in \mathfrak{a}$ and $B \in \mathfrak{b}$ are infinite disjoint sets then

$$A \cup B \asymp (A \cup B) \times (A \cup B) \asymp A \cup (A \times B) \cup (B \times A) \cup B,$$

hence $A \times B \rightarrowtail A \cup B$, and therefore $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} + \mathfrak{b}$. The next result shows that this last equality implies AC.

Theorem 20.11. *The following are equivalent:*

(a) AC,

(b) $\forall \mathfrak{a} (\mathfrak{a} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{a} = \mathfrak{a})$,

(c) $\forall \mathfrak{a} \forall \mathfrak{b} (\mathfrak{a}, \mathfrak{b} \not< \omega \Rightarrow \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} + \mathfrak{b})$.

Proof. It is enough to show that (c) implies that every set A is well-orderable. First of all we may assume that A is disjoint from $B = \mathrm{Hrtg}(A)$. By assumption there is a bijection $F\colon A \times \mathrm{Hrtg}(A) \to A \cup \mathrm{Hrtg}(A)$. Since $\mathrm{Hrtg}(A) \precsim A$ is impossible,

$$\forall x \in A \, \exists \alpha \in \mathrm{Hrtg}(A) \, (F(x,\alpha) \notin A).$$

If $\alpha(x)$ is the least witness, then $A \to \mathrm{Hrtg}(A)$, $x \mapsto F(x, \alpha(x))$, is injective hence A is well-orderable. □

Part (b) of Theorem 20.11 should be contrasted with Corollary 18.35.

20.D. Countable and dependent choices. The axiom of countable choices AC_ω, first introduced in Section 14.E, implies that the countable union of countable sets is countable (Theorem 14.31). In particular: ω_1 is not countable union of countable sets. To prove this it is enough to tap a particular instance of AC_ω.

Theorem 20.12. *Assume* $\mathsf{AC}_\omega(\mathbb{R})$. *Then ω_1 is not countable union of countable sets. In particular: if $\alpha_n < \omega_1$ for all $n < \omega$, then $\sup_n \alpha_n < \omega_1$.*

Proof. Let $X_n \subseteq \omega_1$ be countable sets, for $n < \omega$. Without loss of generality, we may assume that each X_n is infinite, and let

$$A_n = \{R \subseteq \omega \times \omega \mid R \text{ is a well-order of } \omega \text{ and } \operatorname{ot}\langle \omega, R\rangle = \operatorname{ot}\langle X_n, \leq\rangle\} .$$

As $\mathscr{P}(\omega \times \omega) \asymp \mathbb{R}$ we may choose $R_n \in A_n$ for all $n \in \omega$, and let $f_n\colon \langle \omega, R_n\rangle \to \langle X_n, \leq\rangle$ be the unique isomorphism. Then

$$\omega \times \omega \to \textstyle\bigcup_{n\in\omega} X_n, \quad (n,m) \mapsto f_n(m)$$

is surjective, thus $\bigcup_{n\in\omega} X_n$ is countable. □

By Hartogs' result $\mathbb{R} \twoheadrightarrow \omega_1$ (see (18.3) on page 393), so we have:

Corollary 20.13. $\mathsf{AC}_\omega(\mathbb{R})$ *implies that $\mathbb{R}$ is not countable union of countable sets.*

Another weak form of the axiom of choice is DC, the **axiom of dependent choices**:

$$(\mathsf{DC}) \qquad \forall X \in \mathrm{V} \setminus \{\emptyset\} \;\; \mathsf{DC}(X)$$

where $\mathsf{DC}(X)$ says: *If $R \subseteq X \times X$ and $\forall x \exists y \, (x \mathrel{R} y)$, then for all $\bar{x} \in X$ there is an $f\colon \omega \to X$ such that $f(0) = \bar{x}$ and $\forall n \, (f(n) \mathrel{R} f(n+1))$.*

As for the axiom of countable choices, $\mathsf{DC}(X)$ is outright provable when X is well-orderable, and if $X \twoheadrightarrow Y$ then $\mathsf{DC}(X) \Rightarrow \mathsf{DC}(Y)$ (Exercise 20.16).

Proposition 20.14. *For every non-empty set X,* $\mathsf{AC}(X) \Rightarrow \mathsf{DC}(X)$ *and* $\mathsf{DC}(X \times \omega) \Rightarrow \mathsf{AC}_\omega(X)$. *In particular:* $\mathsf{AC} \Rightarrow \mathsf{DC} \Rightarrow \mathsf{AC}_\omega$.

Proof. Assume $\mathsf{AC}(X)$ towards proving $\mathsf{DC}(X)$. Let $X \neq \emptyset$ and let $R \subseteq X \times X$ be such that $\forall x \exists y\, (x\, R\, y)$. Pick $x_0 \in X$ and a choice function $C\colon \mathscr{P}(X) \setminus \{\emptyset\} \to X$. Recursively define $f\colon \omega \to X$ by $f(0) = x_0$ and $f(n+1) = C\,(\{y \in X \mid f(n)\ R\ y\})$. It is immediate to check that f witnesses $\mathsf{DC}(X)$ for R and x_0.

Assume $\mathsf{DC}(X \times \omega)$ towards proving $\mathsf{AC}_\omega(X)$. Given $\{A_n \mid n \in \omega\} \subseteq \mathscr{P}(X) \setminus \{\emptyset\}$ let R be the relation on $X \times \omega$ defined by

$$(a, n)\ R\ (b, m) \Leftrightarrow m = n + 1 \wedge (a \in A_n \Rightarrow b \in A_m).$$

For every $(a, n) \in X \times \omega$ there is some $b \in X$ such that $(a, n)\ R\ (b, n+1)$: if $a \in A_n$ pick $b \in A_{n+1}$, if $a \notin A_n$ let $b = a$. Fix an element $a_0 \in A_0$: by $\mathsf{DC}(X \times \omega)$ there is a function $f\colon \omega \to X \times \omega$ such that $f(0) = (a_0, 0)$ and $f(n)\ R\ f(n+1)$ for all n. The function $g\colon \omega \to X$

$$g(n) = \text{the first component of the ordered pair } f(n)$$

is the required function. □

Neither AC_ω nor DC is provable without choice, and the implications in Proposition 20.14 cannot be reversed. Both AC_ω and DC are used throughout mathematics, and Section 28.C collects some of these applications. For the time being, let us point out a few results. As already observed on page 353, AC_ω is used to prove that the equivalence between continuity and sequential continuity, and to construct the Lebesgue measure (Section 26.D); the stronger DC is even more useful, since it implies pivotal results such as the Baire category Theorem 26.8.

Exercises

Exercise 20.15. Show that GCH is equivalent to $\forall \alpha\, (\aleph_\alpha = \beth_\alpha)$.

Exercise 20.16. Suppose $X \twoheadrightarrow Y$. Show that

(i) $\mathsf{DC}(X) \Rightarrow \mathsf{DC}(Y)$;

(ii) if $I \precsim J$, then $\mathsf{AC}_J(X) \Rightarrow \mathsf{AC}_I(Y)$

Exercise 20.17. Show that the following are equivalent to AC.

(i) For every family of sets $\mathcal{A}$ there is a maximal subfamily $\mathcal{B} \subseteq \mathcal{A}$ of pairwise disjoint sets.

(ii) For every $\langle A_i \mid i \in I \rangle$ there is $\langle B_i \mid i \in I \rangle$ such that $\emptyset \subseteq B_i \subseteq A_i$, $\bigcup_{i \in I} B_i = \bigcup_{i \in I} A_i$ and $B_i \cap B_j = \emptyset$ for $i \neq j$.

(iii) An ordered set in which every chain has the least upper bound, has a maximal element.[10]

(iv) An ordered set in which every well-ordered chain has an upper bound, has a maximal element.

Exercise 20.18. Show that $\mathbb{R} \precsim \mathscr{P}_{\omega_1}(\mathbb{R})$ and $\mathbb{R} \twoheadrightarrow \mathscr{P}_{\omega_1}(\mathbb{R})$.

Exercise 20.19. Suppose $\lambda \leq \kappa$ are infinite cardinals. Show that:

(i) $[\kappa]^\lambda \precsim {}^\lambda\kappa \precsim \mathscr{P}_{\lambda^+}(\kappa)$ and $\mathscr{P}_{\kappa^+}(\kappa) = \mathscr{P}(\kappa) \asymp [\kappa]^\kappa = \{x \subseteq \kappa \mid |x| = \kappa\}$.

(ii) Assuming AC, then $|\mathscr{P}_{\lambda^+}(\kappa)| = \kappa^\lambda$, and hence $|\mathscr{P}_\lambda(\kappa)| = \kappa^{<\lambda}$.

(iii) Assuming AC, then $|[\kappa]^\kappa| = \kappa^\kappa$.[11]

Exercise 20.20. Assume DC. Show that an irreflexive relation R on a set X is well-founded if and only if there are no sequences $\langle x_n \mid n < \omega\rangle$ such that $x_{n+1} \mathrel{R} x_n$, for all n.

Exercise 20.21. Assume AC and let κ be an infinite cardinal. A graph $\langle V, E\rangle$ is **κ-random** if for every pair of disjoint sets $X, Y \in \mathscr{P}_\kappa(V)$ there is a $v \in V$ such that $\forall x \in X\,(x \mathrel{E} v)$ and $\neg\exists y \in Y\,(y \mathrel{E} v)$.[12] Show that:

(i) any isomorphism between two induced subgraphs of size $< \kappa$ of a κ-random graph can be extended to an automorphism of the κ-random graph;

(ii) the κ-random graph is isomorphic up to isomorphism;

(iii) every graph of size $\leq \kappa$ is (isomorphic to) an induced subgraph of the κ-random graph;

(iv) if $\kappa^{<\kappa} = \kappa$ then there is a κ-random graph.

Exercise 20.22. Show that if $\mathbb{R}$ is well-orderable then

(i) $\mathscr{P}_{\omega_1}(\mathbb{R})$ is also well-orderable and $|\mathbb{R}| = |\mathscr{P}_{\omega_1}(\mathbb{R})|$,

(ii) $|\mathcal{M}| = 2^{\aleph_0}$, where $\mathcal{M} = \{f \in \mathbb{R}^\mathbb{R} \mid f \text{ is monotone}\}$.

Exercise 20.23. Show that

(i) DC implies that its version for classes: For each class $X \neq \emptyset$ (proper or otherwise), for each $\bar{x} \in X$ and each relation R on X such that $\forall x \exists y\,(x \mathrel{R} y)$, there is a sequence $s\colon \omega \to X$ such that $s(0) = \bar{x}$ and $\forall n\,(s(n) \mathrel{R} s(n+1))$;

(ii) $\mathsf{DC}(X)$ is equivalent to the seemingly weaker statement, where the first element of the sequence f is not given in advance: If R is a binary relation on X such that $\forall x \exists y\,(x \mathrel{R} y)$, then there is a sequence $s\colon \omega \to X$ such that $\forall n\,(s(n) \mathrel{R} s(n+1))$.

[10] This is the statement of Zorn's Lemma with *least upper bound* instead of *upper bound.*

[11] See also Exercise 21.49.

[12] Thus a random graph in the sense of Section **??** is an ω-random graph.

Exercise 20.24. Suppose V is a non-trivial vector space on a field $\Bbbk$, that is V is not just the null vector. Show that if V is well-orderable, then so is $\Bbbk$, and V has a **basis**, that is a maximal linearly independent set.

Exercise 20.25. Without assuming AC show that $\mathrm{V}_\alpha \asymp \mathrm{V}_\alpha \times \mathrm{V}_\alpha$ for all $\alpha \geq \omega$.

Exercise 20.26. Show that:

(i) $\mathrm{Hrtg}(X) \asymp \mathscr{P}(X)$ if and only if $X, \mathscr{P}(X)$ are well-orderable, and $|X|^+ = 2^{|X|}$. In particular GCH is equivalent to $\forall X(X \text{ infinite} \Rightarrow \mathrm{Hrtg}(X) \asymp \mathscr{P}(X))$;

(ii) if $X \precsim Y$ then $\mathrm{Hrtg}(X) \not\asymp \mathscr{P}(\mathscr{P}(Y))$.

Exercise 20.27. Suppose A, B are disjoint. Show that:

(i) if $C \times C \asymp C$, and there is no surjection $A \twoheadrightarrow C$, then $A \cup B \asymp C$ implies that $B \asymp C$;

(ii) if $2 \times A \asymp A$ and $A \cup B \asymp \mathscr{P}(A)$, then $B \asymp \mathscr{P}(A)$.

Exercise 20.28. For X an infinite set, let $\Phi(X)$ be the formula

$$\forall \mathcal{A} \subseteq \mathscr{P}(X) \left(\mathcal{A} \precsim X \vee \mathcal{A} \asymp \mathscr{P}(X)\right).$$

Let $\mathscr{P}^0(X) = X$ and $\mathscr{P}^{i+1}(X) = \mathscr{P}(\mathscr{P}^i(X))$.

(i) Assume that $X \asymp 2 \times X$ and that $\Phi(\mathscr{P}^i(X))$ holds for $i \leq 2$. Use Exercises 18.47, 20.26, and 20.27 to show that:
   (1) $\mathscr{P}^i(X) \asymp \mathscr{P}^i(X) \times \mathscr{P}^i(X)$ and hence $\mathscr{P}^i(X) \asymp 2 \times \mathscr{P}^i(X)$ for $1 \leq i \leq \omega$,
   (2) $\mathscr{P}^2(X) \precsim \mathrm{Hrtg}(X) \uplus \mathscr{P}^2(X) \precsim \mathscr{P}^3(X)$, and conclude that $\mathrm{Hrtg}(X) \precsim \mathrm{Hrtg}(X) \uplus \mathscr{P}^2(X) \asymp \mathscr{P}^2(X)$,
   (3) $\mathscr{P}(X) \precsim \mathrm{Hrtg}(X) \uplus \mathscr{P}(X) \precsim \mathscr{P}^2(X)$, so $\mathscr{P}(X) \asymp \mathrm{Hrtg}(X)$.
   Conclude that X is well-orderable.

(ii) Use that $X \precsim \omega \times X$ to prove that the assumption that $X \asymp 2 \times X$ in part (i) can be omitted, and conclude that $\forall X(X \text{ infinite} \Rightarrow \Phi(X))$ implies AC.

Exercise 20.29. Assume AC and show that:

(i) For any set X and any infinite cardinal κ, $|X| \leq \kappa$ if and only if there is $\mathcal{C} \subseteq \mathscr{P}_\kappa(X)$ such that $\bigcup \mathcal{C} = X$ and $\mathcal{C}$ is linearly ordered under inclusion, that is: $\forall A, B \in \mathcal{C}\, (A \subseteq B \vee B \subseteq A)$.

(ii) CH is equivalent to each of the following:
   - there is a preorder $\trianglelefteq$ on X such that $\{x \in X \mid x \trianglelefteq y\}$ is countable, for any $y \in X$, where X is any set in bijection with $\mathbb{R}$;

- there are countable fields $F_i \subseteq \mathbb{R}$ $(i \in I)$ such that $\mathbb{R} = \bigcup_{i\in I} F_i$ and $F_i \subseteq F_j \vee F_j \subseteq F_i$, for all $i, j \in I$. (It is possible to swap $\mathbb{R}$ with any algebraic structure which is in bijection with $\mathbb{R}$ and "field" with any suitable notion of substructure.)

Notes and remarks

The literature on the axiom of choice is very vast. Besides the classical books [**Jec73, RR85**] and the monumental [**HR98**] let us single out the book by [**Her06**]. The proofs of the relative consistency of the axiom of choice the (generalized) continuum hypothesis, and their negation were obtained, respectively, by Gödel in 1937 and by Cohen in 1963. Theorem 20.6 is due to Sierpiński. The continuum problem is to determine the cardinality of $\mathbb{R}$ or, equivalently, of $\mathscr{P}(\omega)$. Cantor in 1878, conjectured that the size of $\mathbb{R}$ were the least uncountable cardinality; using modern notation, we can say that Cantor conjectured wCH or even CH, as the statement "every set is well-orderable" was considered by Cantor as a valid principle. The generalized continuum hypothesis GCH is due to Hausdorff in 1914. Proposition 20.11 is due to Tarski. The statement '$\mathrm{card}(X) + \mathrm{card}(X) = \mathrm{card}(X)$ for every infinite set X' does not imply AC [**Sag75**].

21. Cardinal exponentiation

21.A. Generalized sums and products.

Definition 21.1 (AC). Let $\langle \kappa_i \mid i \in I\rangle$ be a sequence of cardinals.

(i) The **generalized sum** of the κ_is is $\sum_{i\in I} \kappa_i = |\bigcup_{i\in I}\{i\} \times \kappa_i|$;

(ii) The **generalized product** of the κ_is is $\prod_{i\in I} \kappa_i = |\bigtimes_{i\in I}\kappa_i|$.

The definition of generalized cardinal sum does not require the axiom of choice, if I is well-orderable. The case of generalized product is different: if $I = \omega$ and $\kappa_i = 2$, in order to find a well-order on $\bigtimes_{i\in I}\kappa_i = {}^{\omega}2 \asymp \mathbb{R}$ we must tap choice. It follows at once that

- $\kappa = \sum_{i\in\kappa} 1 = \sum_{i\in\kappa} \kappa_i$, with $\kappa_i = 1$,
- $2^\kappa = \prod_{i\in\kappa} 2 = \prod_{i\in\kappa} \kappa_i$, with $\kappa_i = 2$,
- the operations of generalized sum and product are monotone, that is if $\kappa_i \leq \lambda_i$, then $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i$.

Proposition 21.2. *If I is a well-orderable set and $1 \leq \kappa_i$ for every $i \in I$, then*

$$\textstyle\sum_{i\in I} \kappa_i \leq |I| \cdot \sup_{i\in I} \kappa_i,$$

and if $\max(|I|, \sup_{i\in I} \kappa_i) \geq \omega$, *then equality holds.*

Proof. The inclusion $\bigcup_{i\in I}\{i\} \times \kappa_i \subseteq I \times \sup_{i\in I} \kappa_i$ proves the inequality. For every $\alpha \in \sup_{i\in I} \kappa_i$ pick $i(\alpha) \in I$ such that $\alpha \in \kappa_{i(\alpha)}$: the function $\sup_{i\in I} \kappa_i \to \bigcup_{i\in I}\{i\} \times \kappa_i$, $\alpha \mapsto (i(\alpha), \alpha)$ is injective and proves that

$\sup_{i\in I}\kappa_i \leq \sum_{i\in I}\kappa_i$. By monotonicity $|I| = \sum_{i\in I} 1 \leq \sum_{i\in I}\kappa_i$. Therefore $\max(|I|, \sup_{i\in I}\kappa_i) \leq \sum_{i\in I}\kappa_i$. The conclusion follows from Corollary 18.29. □

Therefore if κ is an infinite cardinal, $2^{<\kappa} = \sum_{\lambda\in\mathrm{Card}\cap\kappa} 2^\lambda$.

Theorem 21.3 (AC). *If I and $\{X_i \mid i \in I\}$ are sets, then*

$$|\bigcup_{i\in I} X_i| \leq |I| \cdot \sup_{i\in I}|X_i|.$$

Proof. For each $i \in I$ choose a bijection $f_i \colon X_i \to |X_i|$ and for each $x \in \bigcup_{i\in I} X_i$ choose $i(x) \in I$ such that $x \in X_{i(x)}$. The function

$$\bigcup_{i\in I} X_i \to \bigcup_{i\in I}\{i\} \times |X_i| \quad x \mapsto (i(x), f_{i(x)}(x))$$

is injective hence $|\bigcup_{i\in I} X_i| \leq \sum_{i\in I}|X_i|$. The result follows immediately from Proposition 21.2. □

By formula (18.4) and Exercise 21.56 we get that if $I \neq \emptyset$ and $\kappa_i \leq \lambda_i \geq 2$ then $\sum_{i\in I}\kappa_i \leq \prod_{i\in I}\lambda_i$.

Theorem 21.4 (J. König). *Assume* AC. *If $\kappa_i < \lambda_i$ for all $i \in I$, then*

$$\sum_{i\in I}\kappa_i < \prod_{i\in I}\lambda_i.$$

Proof. It is enough to show that $\sum_{i\in I}\kappa_i \not\geq \prod_{i\in I}\lambda_i$, that is no $F \colon \bigcup_i\{i\} \times \kappa_i \to \mathsf{X}_{i\in I}\lambda_i$ can be surjective. Fix an F as above: for every $i \in I$, the set $\{F(i,\alpha)(i) \mid \alpha \in \kappa_i\}$ has cardinality $< \lambda_i$, so we can define a function $f \in \mathsf{X}_{i\in I}\lambda_i$:

$$f(i) = \min\left(\lambda_i \setminus \{F(i,\alpha)(i) \mid \alpha \in \kappa_i\}\right).$$

Let us check that $f \notin \mathrm{ran}(F)$: if, towards a contradiction, $f = F(i_0, \alpha_0)$ for some i_0, α_0, then $f(i_0) \notin \{F(i_0,\alpha)(i_0) \mid \alpha \in \kappa_{i_0}\}$ by definition of f, a contradiction. □

In particular, taking $\kappa_i = 1$ and $\lambda_i = 2$ we obtain again Cantor's theorem, $|I| < 2^{|I|}$.

21.B. Regular and singular cardinals.

Definition 21.5. A function $f \colon \beta \to \alpha$ is **cofinal (in α)** if $\mathrm{ran}(f)$ is unbounded in α, that is $\forall\alpha' < \alpha\,\exists\beta' < \beta\,(\alpha' \leq f(\beta'))$. The **cofinality** of an ordinal α is the least β such that there is a cofinal $f \colon \beta \to \alpha$. This β is denoted by $\mathrm{cof}(\alpha)$.

Let us see some examples.

- As $\mathrm{id} \restriction \alpha$ is cofinal, $\mathrm{cof}(\alpha) \leq \alpha$, for each α. In particular $\mathrm{cof}(0) = 0$.
- The cofinality of a successor ordinal $\gamma + 1$ is 1, as witnessed by the function $0 \mapsto \gamma$. Conversely, if λ is limit, $\mathrm{cof}(\lambda)$ is limit.

- $\operatorname{cof}(\omega) = \omega$ and if we assume a bit of choice, by Theorem 20.12 $\operatorname{cof}(\omega_1) = \omega_1$. On the other hand, $\operatorname{cof}(\aleph_\omega) = \omega$, since $n \mapsto \aleph_n$ is cofinal.

A cofinal map $\operatorname{cof}(\alpha) \to \alpha$ need not be monotone, but by the next result we can always assume that this is the case. (Actually, we could even assume the map be increasing and continuous—see Exercise 21.47.)

Lemma 21.6. *There is a cofinal monotone function $f \colon \operatorname{cof}(\alpha) \to \alpha$.*

Proof. Let $g \colon \operatorname{cof}(\alpha) \to \alpha$ be cofinal, and to avoid trivialities we may assume that α is limit. For $\beta < \operatorname{cof}(\alpha)$ let $f(\beta) = \max\bigl(g(\beta), \sup_{\gamma<\beta} f(\gamma)\bigr)$. By construction f is monotone and cofinal. If there is a least $\bar\beta < \operatorname{cof}(\alpha)$ such that $\sup_{\gamma<\beta} f(\gamma) = \alpha$, then $f \colon \bar\beta \to \alpha$ would be cofinal: a contradiction. Therefore $f \colon \operatorname{cof}(\alpha) \to \alpha$ is as required. □

Lemma 21.7. *If $f \colon \beta \to \alpha$ and $g \colon \gamma \to \beta$ are cofinal and f is also monotone, then $f \circ g \colon \gamma \to \alpha$ is cofinal.*

Proof. If $\alpha' < \alpha$ let $\beta' < \beta$ be such that $f(\beta') \geq \alpha'$ and let $\gamma' < \gamma$ be such that $g(\gamma') \geq \beta'$. Then $f(g(\gamma')) \geq \alpha'$. □

Corollary 21.8. $\operatorname{cof}(\operatorname{cof}(\alpha)) = \operatorname{cof}(\alpha)$.

Definition 21.9. A limit ordinal λ is **regular** if $\operatorname{cof}(\lambda) = \lambda$. Otherwise it is **singular**. If λ is an infinite cardinal, we will speak of **regular** or **singular cardinal**.

If $f \colon |\lambda| \to \lambda$ is a bijection, then f is cofinal, hence a regular ordinal is a cardinal. Conversely, limit ordinals that are not cardinals are singular. Note that although not an ordinal, Ord can be thought to be regular, since by the axiom of replacement, no $f \colon \alpha \to \mathrm{Ord}$ can be cofinal.

Theorem 21.10 (AC)**.** *If $\kappa \geq \omega$ then κ^+ is regular.*

Proof. Towards a contradiction suppose $\operatorname{cof}(\kappa^+) \leq \kappa$. Let $f \colon \operatorname{cof}(\kappa^+) \to \kappa^+$ be cofinal. Then $\kappa^+ = \bigcup_{i<\operatorname{cof}(\kappa^+)} f(i)$ hence by Theorem 21.3

$$\kappa^+ \leq \textstyle\sum_{i<\operatorname{cof}(\kappa^+)} |f(i)| \leq \operatorname{cof}(\kappa^+) \cdot \sup_{i<\operatorname{cof}(\kappa^+)} |f(i)| \leq \kappa,$$

a contradiction. □

Theorem 21.11 (AC)**.** *If κ is a singular cardinal, then there is an increasing sequence $\langle \kappa_i \mid i < \operatorname{cof}(\kappa) \rangle$ of regular cardinals such that*

$$\kappa = \textstyle\sup_{i<\operatorname{cof}(\kappa)} \kappa_i = \sum_{i<\operatorname{cof}(\kappa)} \kappa_i.$$

Proof. Let $f \colon \operatorname{cof}(\kappa) \to \kappa$ be increasing and cofinal. The function

$$g(\alpha) = \min\{\lambda \in \kappa \mid \lambda \text{ is regular, } \lambda \geq f(\alpha) \text{ and } \forall \beta < \alpha\, (g(\beta) < \lambda)\}$$

is defined for all $\alpha < \operatorname{cof}(\kappa)$ since the regular cardinals are unbounded below κ hence if $\bar{\alpha} < \operatorname{cof}(\kappa)$ were the least ordinal such that $g(\bar{\alpha})$ is not defined, then it would mean that $\kappa = \sup_{\beta<\bar{\alpha}} g(\beta)$, that is $g\colon \bar{\alpha} \to \kappa$ would be cofinal, against $\bar{\alpha} < \operatorname{cof}(\kappa)$. Letting $\kappa_i = g(i)$, it follows that

$$\kappa = \sup_{i<\operatorname{cof}(\kappa)} \kappa_i \leq \textstyle\sum_{i<\operatorname{cof}(\kappa)} \kappa_i \leq \kappa \cdot \operatorname{cof}(\kappa) = \kappa$$

as required. □

Theorem 21.12 (AC). *$\kappa^{\operatorname{cof}(\kappa)} > \kappa$ when κ is an infinite cardinal.*

Proof. If κ is regular, the statement becomes $\kappa^\kappa = 2^\kappa > \kappa$, which is true by Cantor's Theorem 13.22. We may therefore suppose that $\operatorname{cof}(\kappa) < \kappa$. By Theorem 21.11 there are cardinals κ_i such that $\kappa = \sup_{i<\operatorname{cof}(\kappa)} \kappa_i$ and hence by König's Theorem 21.4

$$\kappa = \textstyle\sum_{i<\operatorname{cof}(\kappa)} \kappa_i < \prod_{i<\operatorname{cof}(\kappa)} \kappa = \kappa^{\operatorname{cof}(\kappa)}. \qquad \square$$

Corollary 21.13 (AC). *$\operatorname{cof}(2^\kappa) > \kappa$ when κ is an infinite cardinal.*

Proof. If $\lambda = \operatorname{cof}(2^\kappa) \leq \kappa$, then $2^\kappa < (2^\kappa)^\lambda = 2^{\kappa\cdot\lambda} = 2^\kappa$, a contradiction. □

In particular, $\operatorname{cof}(2^{\aleph_0}) > \aleph_0$ hence $2^{\aleph_0}$ can neither be $\aleph_\omega$, $\aleph_{\omega+\omega}$ (or, more generally, $\aleph_\lambda$ with $\lambda < \omega_1$ limit) nor can be the least fixed point of the $\aleph$ function (see pag. 405). The next result is known as **Hausdorff's formula**.

Theorem 21.14 (AC). $\aleph_{\alpha+1}^{\aleph_\beta} = \max\left(\aleph_{\alpha+1}, \aleph_\alpha^{\aleph_\beta}\right)$.

Proof. If $\aleph_{\alpha+1} \leq \aleph_\beta$ then by Proposition 18.30 $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}^{\aleph_\beta} > \aleph_\beta \geq \aleph_{\alpha+1}$ hence the result is proved.

Suppose instead that $\aleph_\beta < \aleph_{\alpha+1}$. If $f\colon \aleph_\beta \to \aleph_{\alpha+1}$, then by regularity $\aleph_{\alpha+1}$ (Theorem 21.10) there is a $\gamma < \aleph_{\alpha+1}$ such that $\operatorname{ran} f \subseteq \gamma$. Thus ${}^{\aleph_\beta}\aleph_{\alpha+1} = \bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma$ and by Theorem 21.3

$$\aleph_{\alpha+1}^{\aleph_\beta} = |\textstyle\bigcup_{\gamma<\aleph_{\alpha+1}} {}^{\aleph_\beta}\gamma| \leq \aleph_{\alpha+1} \cdot \aleph_\alpha^{\aleph_\beta}.$$

The other inequality is immediate. □

Theorem 21.15 (Bukovsky–Hechler). *Assume* AC. *If* $\operatorname{cof}(2^{<\kappa}) > \kappa > \operatorname{cof}(\kappa)$ *then* $2^\kappa = 2^{<\kappa}$.

Proof. Let $\langle \kappa_\alpha \mid \alpha < \operatorname{cof}(\kappa)\rangle$ be increasing and $\sup_{\alpha\in\operatorname{cof}(\kappa)} \kappa_\alpha = \kappa$. If $\forall\alpha \in \operatorname{cof}(\kappa)\, \exists\beta \in \operatorname{cof}(\kappa)\, (2^{\kappa_\alpha} < 2^{\kappa_\beta})$, then $\operatorname{cof}(2^{<\kappa}) = \operatorname{cof}(\kappa) < \kappa$, against our assumption. Therefore there is γ such that $2^{\kappa_\beta} = 2^{\kappa_\gamma}$ for all $\beta \geq \gamma$. We may assume that $\kappa_\gamma \geq \operatorname{cof}(\kappa)$. Then by Exercise 21.44(iii)

$$2^\kappa = 2^{\sum_{\alpha\in\operatorname{cof}(\kappa)} \kappa_\alpha} = \textstyle\prod_{\alpha\in\operatorname{cof}(\kappa)} 2^{\kappa_\alpha} \leq (2^{\kappa_\gamma})^{\operatorname{cof}(\kappa)} = 2^{\kappa_\gamma} = 2^{<\kappa}. \qquad \square$$

21.C. Applications. Recall that an operation on a set X is a function $f\colon {}^nX \to X$ for some $n < \omega$, and that if $\mathcal{F}$ is a collection of operations on X and $Y \subseteq X$, then $\mathrm{Cl}_{\mathcal{F}} Y$, the closure of Y under $\mathcal{F}$, is the smallest subset of X containing Y and closed under each $f \in \mathcal{F}$. By Section 7.A.1, $\mathrm{Cl}_{\mathcal{F}} Y = \bigcup_n Y_n$, where $Y_0 = Y$ and $Y_{n+1} = Y_n \cup \{f(\vec{a}) \mid \vec{a} \in Y_n^{<\omega} \wedge f \in \mathcal{F}\}$.

Definition 21.16. A **generalized operation** on X is a $f\colon {}^\alpha X \to X$ where $\alpha \in \mathrm{Ord}$ is the **arity of** f, written $\mathrm{ar}\, f$; when $\alpha \geq \omega$ we will speak of **infinitary operations**, while ordinary operations, i.e. when $\alpha < \omega$, are often called **finitary operations**.

If $\mathcal{F}$ is a collection of generalized operations on X and $Y \subseteq X$, then

$$\mathrm{Cl}_{\mathcal{F}} Y = \bigcap \{Z \subseteq X \mid Y \subseteq Z \wedge \forall f \in \mathcal{F} \forall \vec{a} \in {}^{\mathrm{ar}(f)}Z \; (f(\vec{a}) \in Z)\}$$

is the smallest subset of X containing Y and closed under each $f \in \mathcal{F}$.

Theorem 21.17. *Let $\mathcal{F}$ be a family of generalized operations on a set X and let $Y \subseteq X$. Suppose λ is a regular cardinal such that $\lambda > \mathrm{ar}(f)$ for all $f \in \mathcal{F}$.*

(a) *Then $\mathrm{Cl}_{\mathcal{F}} Y = \bigcup_{\beta<\lambda} Y_\beta$ where $Y_0 = Y$, $Y_\gamma = \bigcup_{\beta<\gamma} Y_\beta$ when γ is limit, and $Y_{\beta+1} = Y_\beta \cup \{f(\vec{a}) \mid f \in \mathcal{F} \wedge \vec{a} \in {}^{\mathrm{ar}(f)}Y_\beta\}$.*

(b) *Assume AC and suppose $\kappa \geq \max(\lambda, |\mathcal{F}|, |Y|)$ and $\forall f \in \mathcal{F} \left(\kappa^{|\mathrm{ar}(f)|} = \kappa\right)$. Then $|\mathrm{Cl}_{\mathcal{F}} Y| \leq \kappa$.*

Proof. (a) It is clear that $\overline{Y} = \bigcup_{\alpha<\lambda} Y_\alpha$ is contained in $\mathrm{Cl}_{\mathcal{F}} Y$. To prove the other inclusion note that if $f \in \mathcal{F}$ and $\alpha = \mathrm{ar}\, f$, then by regularity of λ every $\vec{a} \in {}^\alpha\overline{Y}$ belongs to some Y_β, so $f(\vec{a}) \in Y_{\beta+1} \subseteq \overline{Y}$.

(b) By Theorem 21.3 it is enough to show that $\forall \beta < \lambda \, (|Y_\beta| \leq \kappa)$. This is true if $\beta = 0$ or β limit. Suppose this holds for some β, so that $|Y_\beta| \leq \kappa$ and $|{}^{\mathrm{ar}(f)}Y_\beta| \leq \kappa$ for all $f \in \mathcal{F}$. As $\{f(\vec{a}) \mid f \in \mathcal{F} \wedge \vec{a} \in {}^{\mathrm{ar}(f)}Y_\beta\}$ is the surjective image of $\bigcup_{f\in\mathcal{F}} \{f\} \times {}^{\mathrm{ar}(f)}Y_\beta$, which has size $\leq |\mathcal{F}| \cdot \kappa$, then $|Y_{\beta+1}| \leq \kappa$. □

Theorem 21.18 (AC). *Let $\mathcal{F}$ is a family of generalized operations on a set X and let $Y \subseteq X$.*

(a) *If $\mathrm{ar}(f) < \omega$ for all $f \in \mathcal{F}$, i.e. $\mathcal{F}$ is a family of finitary operations, then $|\mathrm{Cl}_{\mathcal{F}} Y| \leq \max(\omega, |\mathcal{F}|, |Y|)$.*

(b) *If $\mathrm{ar}(f) < \omega_1$ for all $f \in \mathcal{F}$, and $|\mathcal{F}| \leq |Y|^\omega$, then $|\mathrm{Cl}_{\mathcal{F}} Y| \leq |Y|^\omega$.*

Proof. (a) It is enough to check that $\lambda = \omega$ and $\kappa = \max(\omega, |\mathcal{F}|, |Y|)$ satisfy the hypotheses of Theorem 21.17, namely that $\kappa^n = \kappa$. This follows from Theorem 18.31.

(b) It is enough to observe that $\lambda = \omega_1$ and $\kappa = |Y|^\omega$ satisfy the hypotheses of Theorem 21.17, namely $\kappa^\omega = \kappa$. □

Example 21.19. If $\mathcal{M} = \langle M, \dots \rangle$ is an $\mathcal{L}$-structure, then the substructure generated by $Y \subseteq M$ has size $\leq \max(\omega, \lambda, |Y|)$, where λ is the cardinality of the set of non-logical symbols of $\mathcal{L}$.

Example 21.20. A Boolean algebra B is **countably complete** if it is closed under countable joins or, equivalently, countable meets. The smallest countably complete subalgebra of B containing $Y \subseteq B$ has size $\leq |Y|^{\omega}$.

A **σ-algebra** is an algebra of sets which is closed under countable unions or, equivalently, countable intersections; thus a σ-algebra is an example of a countably complete Boolean algebra. If X is a topological space, the σ-algebra generated by the open sets is the family $\textsc{Bor}(X)$ of **Borel subsets** of X. By Section 13.G.4 when X is infinite, second countable, and T_1, then $|\textsc{Bor}(X)| = 2^{\aleph_0}$.

21.D. The topology on the ordinals. Every ordinal, being a linear order, is a topological space, and since α is a subspace of β when $\alpha < \beta$, it is natural to consider the topology on an ordinal as the one induced by the topology of the intervals on $\langle \mathrm{Ord}, \leq \rangle$. The problem is that, strictly speaking, it makes no sense to talk of a topology on a proper class such as Ord. On the other hand one can give the following:

Definition 21.21. Let $\Omega \leq \mathrm{Ord}$. A class $A \subseteq \Omega$ is **open** in Ω if for every $\alpha \in A$ there is are $\beta < \alpha < \gamma$ such that $(\beta; \gamma) \subseteq A$, with the proviso that if $\alpha = 0$ then we require $[0; \gamma) \subseteq A$ for some $\gamma > 0$. A class $C \subseteq \Omega$ is **closed** in Ω if $\Omega \setminus C$ is open in Ω; equivalently:

$$\forall \lambda \bigl(0 < \bigcup (C \cap \lambda) = \lambda \Rightarrow \lambda \in C\bigr).$$

Thus 0 and all successor ordinals are isolated points of Ω. The spaces $\omega \dotplus 1$ and $\omega \dotplus n$ are homeomorphic for all $1 \leq n < \omega$ (Exercise 21.50), while the spaces $\omega \dotplus 1$ and $\omega \dotplus \omega \dotplus 1$ are not homeomorphic, since the former has one non-isolated point, namely ω, while the latter has two non-isolated points, ω and $\omega \dotplus \omega$.

Proposition 21.22. *An ordinal is a compact space if and only if it is either zero or else a successor ordinal.*

Proof. We will prove by induction on α that every open covering $\mathcal{U}$ of $\alpha \dotplus 1$ has a finite subcovering. If $\alpha = 0$ the result follows at once, thus we may assume that $\alpha > 0$ and that $\beta \dotplus 1$ be compact, for all $\beta < \alpha$. Let $\mathcal{U}$ be an open cover of $\alpha \dotplus 1$ and let $U \in \mathcal{U}$ be such that $\alpha \in U$. Choose $\beta < \alpha$ such that $[\beta \dotplus 1, \alpha] \subseteq U$: by inductive assumption there is a finite $\mathcal{U}_0 \subseteq \mathcal{U}$ covering $\beta \dotplus 1 \leq \alpha$, hence $\mathcal{U}_0 \cup \{U\}$ is a finite open cover of $\alpha \dotplus 1$.

Conversely, suppose λ is a limit ordinal: then $\{[0; \alpha) \mid \alpha < \lambda\}$ is an open covering of λ that has no finite subcovering. □

Definition 21.23. A Hausdorff topological space is **totally disconnected** or **zero-dimensional** if every point has a neighborhood base made of clopen sets.

A topological space X is **completely regular**, if given a closed set C and a point $x \notin C$ there is a continuous $f\colon X \to [0;1]$ such that $f(x) = 1$ and $\forall y \in C\,(f(y) = 0)$.

By Tietze's theorem, every metric space is completely regular, and a completely regular space is Hausdorff. An ordinal is a totally disconnected, completely regular space.

Proposition 21.24. *Let X be a completely regular topological space that does not surject onto $\mathbb{R}$. Then X is totally disconnected.*

Proof. Fix $x \in X$ and V an open neighborhood, and let f be a continuous function such that $f(x) = 0$ and $f(y) = 1$ for all $y \in X \setminus V$. By assumption there is $r \in (0;1)\backslash\operatorname{ran}(f)$. Then $f^{-1}[0;r] = f^{-1}[0;r)$ is a clopen neighborhood of x contained in V. □

Corollary 21.25. *A countable metric space is totally disconnected.*

By Exercise 13.74, every countable ordinal is homeomorphic to a countable closed subset of $\mathbb{R}$, hence by Proposition 21.22 every countable successor ordinal is homeomorphic to a countable compact subset of $\mathbb{R}$. In Section 27 the converse will be proved: every countable compact space is homeomorphic to a countable ordinal, hence to a compact subset of $\mathbb{R}$.

Which conditions must $f\colon \Omega \to \mathrm{Ord}$ satisfy in order to be continuous? Continuity is never a problem on the successor ordinals, as they are isolated points. If $\gamma < \Omega$ is limit and $f(\gamma)$ is a successor, then by continuity of f, there is an interval $[\beta;\gamma]$ which is mapped by f in the singleton $\{f(\gamma)\}$; in other words: f is eventually constant below γ. If $\gamma < \Omega$ is limit and $f(\gamma)$ is limit, then for every $\delta < f(\gamma)$ there is $\beta < \gamma$ such that the interval $[\beta;\gamma]$ is mapped by f into the interval $[\delta; f(\gamma)]$. Therefore we have the proved the following:

Lemma 21.26. *Suppose $f\colon \Omega \to \mathrm{Ord}$ is monotone. Then f is continuous if and only if for every limit ordinal $\lambda < \Omega$*

$$f(\lambda) = \sup\nolimits_{\beta<\lambda} f(\beta) \quad \textit{and} \quad \forall X \subseteq \lambda\,(\sup X = \lambda \Rightarrow f(\lambda) = \sup\nolimits_{\nu \in X} f(\nu)).$$

Thus if $f\colon \Omega \to \mathrm{Ord}$ is increasing and continuous, then $f(\lambda)$ is limit for all limit ordinals λ.

Proposition 21.27. *Suppose Ω is either a regular cardinal or* Ord. *If $f\colon \Omega \to \Omega$ is increasing and continuous then* $\operatorname{ran} f$ *is closed and unbounded in Ω. Conversely, if C is closed and unbounded in Ω, then its enumerating function $f\colon \Omega \to C \subseteq \Omega$ is increasing and continuous.*

Proof. Suppose $f\colon \Omega \to \Omega$ is increasing and continuous. Then $f(\alpha) \geq \alpha$, as f is increasing, so $\operatorname{ran} f$ is unbounded in Ω. Suppose λ is limit and $\lambda \cap \operatorname{ran} f$ is unbounded in λ, and let $\nu = \{\alpha < \Omega \mid f(\alpha) < \lambda\}$; then ν must be limit, and by continuity $\lambda = f(\nu) \in \operatorname{ran} f$. Therefore $\operatorname{ran} f$ is closed in Ω.

Conversely, suppose C is closed and unbounded in Ω, and let f be its enumerating function. Then f is increasing and $\operatorname{dom} f = \Omega$ by our assumption on Ω. If $\lambda \in \Omega$ is limit, then $\nu \overset{\text{def}}{=} \sup_{\gamma<\lambda} f(\gamma)$ is limit and $C = \operatorname{ran} f$ is unbounded in ν, so $\nu \in C$ and hence $f(\lambda) = \nu = \sup_{\gamma<\lambda} f(\gamma)$. Therefore f is continuous. □

21.E. Stationary and club sets. In this section, unless otherwise stated

κ is an uncountable regular cardinal.

The next result shows that

$$\mathrm{Club}(\kappa) = \{X \subseteq \kappa \mid \exists C \subseteq X\,(C \text{ is closed and unbounded in } \kappa)\}$$

is a proper filter on κ. (Properness follows from the fact that $\emptyset$ is not unbounded, so if $X \in \mathrm{Club}(\kappa)$ then $\kappa \setminus X \notin \mathrm{Club}(\kappa)$.)

Theorem 21.28. *If $C, D \subseteq \kappa$ are closed and unbounded in κ, then $C \cap D$ is closed and unbounded in κ.*

Proof. Clearly $C \cap D$ is closed, so it is enough to show that it is unbounded in κ. Given $\alpha < \kappa$ let us find a $\beta \in C \cap D$ with $\alpha < \beta$. Using that C and D are unbounded, let us construct inductively an increasing sequence of ordinals $\alpha < \gamma_0 < \delta_0 < \gamma_1 < \delta_1 < \dots$ such that $\gamma_i \in C$ and $\delta_i \in D$. Let $\beta = \sup_i \gamma_i = \sup_i \delta_i$. Since κ is regular then $\beta \in \kappa$ and since C and D are closed, $\beta = \sup_i \gamma_i \in C$ and $\beta = \sup_i \delta_i \in D$, that is $\beta \in C \cap D$ as required. □

The assumption that κ be regular and uncountable cannot be removed—the sets $\{2n \mid n \in \omega\}$ and $\{2n+1 \mid n \in \omega\}$ are closed and unbounded in ω but their intersection $\emptyset$ is not unbounded in ω.

Theorem 21.29. *If $\gamma < \kappa$ and the $\langle C_\alpha \mid \alpha < \gamma\rangle$ are closed unbounded in κ, then $\bigcap_{\alpha<\gamma} C_\alpha$ is closed unbounded in κ.*

Proof. Clearly $\bigcap_{\alpha<\gamma} C_\alpha$ is a closed subset of κ, so it is enough to show that it is unbounded. We argue by induction on γ. If $\gamma = 0$ or $\gamma = 1$ there is nothing to prove. The case of γ a successor ordinal follows from Theorem 21.28, so we may assume that γ is limit. Replacing C_α with $\bigcap_{\beta\leq\alpha} C_\beta$, we may assume that

$$\alpha < \beta < \gamma \Rightarrow C_\alpha \supseteq C_\beta.$$

Given a $\nu < \kappa$, construct an increasing sequence $\langle \xi_\alpha \mid \alpha < \gamma \rangle$ with $\nu < \xi_0$ and $\xi_\alpha \in C_\alpha$. Then $\xi = \sup_{\alpha<\gamma} \xi_\alpha \in \kappa$ as κ is regular, and since the C_αs are closed and $\{\xi_\beta \mid \beta \geq \alpha\} \subseteq C_\alpha$, then $\xi \in C_\alpha$ for each $\alpha < \gamma$. □

An ordinal $\alpha < \kappa$ is closed under $f \colon {}^n\kappa \to \kappa$ if $f(\beta_1, \dots, \beta_n) \in \alpha$ for all $\beta_1, \dots, \beta_n \in \alpha$. The set of all ordinals closed under f is $\mathbf{C}(f)$.

Theorem 21.30. (a) $\mathbf{C}(f)$ *is closed and unbounded, for all* $f \colon {}^n\kappa \to \kappa$.

(b) *If* $C \subseteq \kappa$ *is closed and unbounded, then* $C \supseteq \mathbf{C}(f)$ *for some* $f \colon \kappa \to \kappa$.

Proof. (a) As $\alpha < \kappa$ we must find $\gamma \geq \alpha$ which is closed under f. Let

$$\gamma_{i+1} = \sup \{f(\beta_1, \dots, \beta_n) \mid \beta_1, \dots, \beta_n \in \gamma_i\}$$

where $\gamma_0 = \alpha$. By our assumption on κ, we have that

$$|\{f(\beta_1, \dots, \beta_n) \mid \beta_1, \dots, \beta_n \in \gamma_i\}| \leq |\gamma_i|^n < \kappa,$$

hence $\gamma = \sup_i \gamma_i < \kappa$ is the ordinal we are looking for.

Closure of $\mathbf{C}(f)$ in κ is immediate.

(b) Let $C \subseteq \kappa$ be a closed unbounded, let g be its enumerating function, and let $f(\alpha) = g(\alpha + 1)$: as $\alpha \leq g(\alpha) < f(\alpha)$, if γ is closed under f, then γ is limit and $C \cap \gamma$ is unbounded in γ. Therefore $\mathbf{C}(f) \subseteq C$. □

Corollary 21.31. *If* $\mathcal{F}$ *is a collection of operations on a regular cardinal* κ *and* $|\mathcal{F}| < \kappa$, *then* $\bigcap_{f\in\mathcal{F}} \mathbf{C}(f)$, *the set of all* $\alpha < \kappa$ *which are closed under all* $f \in \mathcal{F}$, *is closed and unbounded in* κ.

Therefore if A is an algebraic structure of size κ a regular cardinal with $< \kappa$ many operations and constants (e.g. a group, a ring, a lattice, ...) and $\langle a_\alpha \mid \alpha < \kappa \rangle$ is an enumeration of A, then the set of all $\nu < \kappa$ such that $\{a_\alpha \mid \alpha < \nu\}$ is a substructure of A is closed and unbounded in κ.

21.E.1. *Diagonal intersections and Fodor's lemma.* Theorem 21.29 says that the intersection of $\gamma < \kappa$ sets that are closed and unbounded is closed and unbounded. We cannot hope to replace γ with κ since $D_\alpha = \kappa \setminus \alpha$ is closed and unbounded but $\emptyset = \bigcap_{\alpha<\kappa} D_\alpha$. As we shall see, this is, in some sense, the only obstruction.

Definition 21.32. The **diagonal intersection** of a sequence $\langle X_\alpha \mid \alpha < \kappa \rangle$ of subsets of κ is $\triangle_{\alpha<\kappa} X_\alpha = \{\beta < \kappa \mid \beta \in \bigcap_{\alpha<\beta} X_\alpha\}$.

Let us derive a couple of easy facts from Definition 21.32. The first is that if $Y_\alpha = \bigcap_{\beta\leq\alpha} X_\beta$, then $\bigcap_{\alpha<\beta} X_\alpha = \bigcap_{\alpha<\beta} Y_\alpha$ so that $\triangle_{\alpha<\kappa} X_\alpha = \triangle_{\alpha<\kappa} Y_\alpha$. The second is that $\beta \in \bigcap_{\alpha<\beta} X_\alpha$ is equivalent to $\forall \alpha < \beta\, (\beta \in X_\alpha)$, which is equivalent to $\forall \alpha < \kappa\, (\beta \in \alpha \dotplus 1 \vee \beta \in X_\alpha)$, and hence

$$\triangle_{\alpha<\kappa} X_\alpha = \bigcap_{\alpha<\kappa} (X_\alpha \cup \alpha \dotplus 1). \tag{21.1}$$

Proposition 21.33. *If $\kappa > \omega$ and C_α is closed and unbounded in κ for each $\alpha < \kappa$, then $\triangle_{\alpha<\kappa} C_\alpha$ is closed and unbounded in κ.*

Proof. First of all, we may assume that $\alpha < \beta \Rightarrow C_\alpha \supseteq C_\beta$. Closure of $C = \triangle_{\alpha<\kappa} C_\alpha$ is immediate by (21.1), so it is enough to check that C is unbounded. Fix $\beta_0 < \kappa$. As $\bigcap_{\nu \leq \gamma} C_\nu$ is unbounded in κ for all $\gamma < \kappa$ (Theorem 21.29), one defines an increasing sequence

$$\beta_0 < \beta_1 < \beta_2 < \cdots < \beta = \sup_n \beta_n$$

such that $\beta_{n+1} \in \bigcap_{\nu \leq \beta_n} C_\nu$. As $n < m \Rightarrow \beta_m \in C_{\beta n}$, the fact that C_{β_n} is closed implies that $\beta = \sup_{m>n} \beta_m \in C_{\beta_n}$, hence $\beta \in \bigcap_n C_{\beta_n} = \bigcap_{\nu<\beta} C_\nu$, that is $\beta_0 < \beta \in C$ as required. □

Definition 21.34. $A \subseteq \kappa$ is **stationary in** κ if $A \cap C \neq \emptyset$ for all closed unbounded $C \subseteq \kappa$.

By Theorem 21.29, a set in $\mathrm{Club}(\kappa)$ is stationary, but not conversely—Exercise 21.58. As observed in Section 7.H a filter on X is a notion of "largeness" for subsets of X, so sets in $\mathrm{Club}(\kappa)$ are large, their complements are small and are non-stationary, while stationary sets are not small. A stationary subset of κ is unbounded in κ since it must intersect every closed set of the form $(\alpha; \kappa)$ for $\alpha < \kappa$. Thus regularity of κ implies that the stationary sets have size κ.

Theorem 21.35 (Fodor). *Let $S \subseteq \kappa$ be stationary and let $F \colon S \to \kappa$ be such that $\forall \alpha \in S\ (\alpha \neq 0 \Rightarrow F(\alpha) < \alpha)$. Then F is constant on a stationary subset of κ.*

Proof. Towards a contradiction, suppose that $F^{-1}\{\alpha\}$ is non-stationary for all $\alpha < \kappa$, that is

$$\forall \alpha \in \kappa\, \exists C_\alpha \subseteq \kappa\ \left(C_\alpha \text{ closed and unbounded in } \kappa \text{ and } C_\alpha \cap F^{-1}\{\alpha\} = \emptyset\right).$$

By Proposition 21.33, $\triangle_{\alpha<\kappa} C_\alpha$ is closed and unbounded, and since $(0; \kappa)$ is also closed and unbounded, the same is true of $C = (\triangle_{\alpha<\kappa} C_\alpha) \setminus \{0\}$ by Theorem 21.29. Let $\alpha \in S \cap C$: then $\beta \overset{\text{def}}{=} F(\alpha) < \alpha$ by definition of F, and $\alpha \in C_\beta$ by definition of diagonal intersection, hence $\alpha \notin F^{-1}\{\beta\}$ that is $F(\alpha) \neq \beta$: a contradiction. □

Remark 21.36. The assumption 'κ is an uncountable regular cardinal' posited at the beginning of this section was meant to streamline the presentation, but can be relaxed to 'κ is a limit ordinal of uncountable cofinality', and under this weaker assumption $\mathrm{Club}(\kappa)$ becomes a proper filter closed under intersections of size $< \mathrm{cof}(\kappa)$. Thus by Corollary 21.13 $\mathrm{Club}(2^{\aleph_0})$ is a proper filter closed under countable intersections. Replacing κ with Ord the arguments go through, but the members of Club(Ord) are proper classes, and

Club(Ord) is closed under set-size intersections. As Club(Ord) is a collection of proper classes, it is *not* a legitimate object in MK or NGB, nor *a fortiori* in ZF; note that Club(Ord) is construed in MK or in NGB as a formula $\varphi(X)$ saying that $\exists C \subseteq X$ (C is a closed and unbounded proper class of ordinals).

21.E.2. *The exponential function.* The study of the class-function $\kappa \mapsto 2^\kappa$ is a central topic in set theory. We have proved a few general rules, namely

Rule 1: $\kappa < \lambda \Rightarrow 2^\kappa \leq 2^\lambda$,

Rule 2: $\kappa < \operatorname{cof}(2^\kappa)$, and hence $\kappa^+ \leq 2^\kappa$.

The GCH strengthens Rule 2 by requiring that $2^\kappa = \kappa^+$, and therefore $\operatorname{cof}(2^\kappa) = \kappa^+ > \kappa$, for all infinite cardinals κ. By work of Gödel in 1937 GCH cannot be refuted from ZFC, and by work of Cohen in 1963, it cannot be proved in ZFC.[13] Extending Cohen's work, Easton showed in 1964 that Rule 1 and Rule 2 are the only restrictions for the exponential function $\kappa \mapsto 2^\kappa$ whenever κ is *regular.* For example, it is consistent that $2^\kappa = \kappa^{++}$ for every regular κ, or that $2^\kappa > \kappa^+$ and that $\forall \lambda < \kappa \left(2^\lambda = \lambda^+\right)$, with κ regular cardinal. The situation for *singular cardinals* is much deeper and interesting. Silver proved in 1974 that GCH cannot fail first at a singular cardinal of *uncountable cofinality.*

Rule 3: If λ is a limit ordinal of uncountable cofinality and $\{\alpha < \operatorname{cof}(\lambda) \mid 2^{\aleph_\alpha} = \aleph_{\alpha+1}\}$ is stationary in $\operatorname{cof}(\lambda)$, then $2^{\aleph_\lambda} = \aleph_{\lambda+1}$.

In particular, GCH *cannot fail* first at $\aleph_{\omega_1}$. The assumption $\omega < \operatorname{cof}(\lambda)$ in Rule 3 cannot be removed since Magidor proved in 1978 that GCH *can fail* first at $\aleph_\omega$, that is that $\forall n < \omega \left(2^{\aleph_n} = \aleph_{n+1}\right)$ and $2^{\aleph_\omega} > \aleph_{\omega+1}$. The value $2^{\aleph_\omega}$ cannot be arbitrarily large: in 1989 Shelah proved that:

Rule 4: if $\forall n \left(2^{\aleph_n} < \aleph_\omega\right)$, then $2^{\aleph_\omega} < \aleph_{\min(\omega_4,(2^{\aleph_0})^+)}$.

For an exposition of these results see [**Kun83, Jec03**].

21.F. Universes.

Definition 21.37. A cardinal κ is **strong limit** if $2^\lambda < \kappa$ for all $\lambda < \kappa$. A regular cardinal $\kappa > \omega$ is **weakly inaccessible** if it is limit; it is **strongly inaccessible** if it is strong limit.

If κ is weakly inaccessible then $\kappa = \aleph_\kappa$, but the least fixed point of the $\aleph$ function is of cofinality ω and hence not regular. A strongly inaccessible cardinal is necessarily weakly inaccessible, and GCH guarantees the converse. In the absence of some cardinal arithmetic assumption, the two notions can be quite different; it is possible that $2^{\aleph_0}$ is weakly inaccessible, while if κ is strongly inaccessible then $2^{\aleph_0} < \kappa$.

[13] Similar results hold when ZFC is replaced by NGB + AC or MK + AC.

Lemma 21.38. *Assume* AC *and suppose κ is strongly inaccessible. Then $|\mathrm{V}_\alpha| < \kappa$ for all $\alpha < \kappa$. In particular $|x| < \kappa$ for all $x \in \mathrm{V}_\kappa$.*

Proof. Proceed by induction on α. If $|\mathrm{V}_\alpha| < \kappa$ then $|\mathrm{V}_{\alpha+1}| = 2^{|\mathrm{V}_\alpha|} < \kappa$, as κ is strong limit. If α is limit, then $|\mathrm{V}_\alpha| = |\alpha| \cdot \sup_{\beta<\alpha}|\mathrm{V}_\beta| < \kappa$ by regularity. □

Theorem 21.39. *Assume* AC. *If κ is strongly inaccessible, then* $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$.

Proof. Suppose κ is strongly inaccessible. In order to prove that $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$, by Theorem 19.15 it is enough to show that V_κ satisfies replacement. By part (g) of Theorem 19.22 it is enough to show that if $f\colon a \to \mathrm{V}_\kappa$ with $a \in \mathrm{V}_\kappa$, then there is $b \in \mathrm{V}_\kappa$ such that $\operatorname{ran} f \subseteq b$. Let $g\colon a \to \kappa$, $g(x) =$ the least $\alpha < \kappa$ such that $f(x) \in \mathrm{V}_\alpha$. By Lemma 21.38 $|a| < \kappa$, so $\operatorname{ran} g \subseteq \gamma$ for some $\gamma < \kappa$, and hence $\operatorname{ran} f \subseteq \mathrm{V}_\gamma \in \mathrm{V}_\kappa$. □

The converse of Theorem 21.39 fails since if κ is inaccessible there are many $\alpha < \kappa$ such that $\mathrm{V}_\alpha \vDash \mathsf{ZFC}$ (Theorem 31.22). See Exercise 21.63 for a sort of converse with MK instead of ZF.

Definition 21.40. A **universe** is a transitive set U closed under the operation $x \mapsto \mathscr{P}(x)$, such that $\omega \in U$, and $\forall I \in U\, \forall f\colon I \to U\ \bigl(\bigcup_{i\in I} f(i) \in U\bigr)$.

Theorem 21.41 (AC)**.** *U is a universe if and only if $U = \mathrm{V}_\kappa$ for some strongly inaccessible cardinal κ.*

The proof of Theorem 21.41 is based on the following:

Lemma 21.42. *If U is a universe then*

(a) *$x \subseteq y \in U \Rightarrow x \in U$,*

(b) *$x, y \in U \Rightarrow x \cup y \in U$,*

(c) *if $x, y \in U$ then $\{x, y\} \in U$ and hence $(x, y) \in U$,*

(d) *if $x, y \in U$ then $x \times y \in U$ and ${}^{x}y \in U$,*

(e) *if $f\colon I \to U$ and $I \in U$ then $\operatorname{ran} f \in U$ and $f \in U$.*

Proof. (a) $x \in \mathscr{P}(y) \in U$ so $x \in U$ by transitivity.

(b) $2 \in \omega \in U$, so $2 \in U$ by transitivity. Then $x \cup y = \bigcup_{i\in 2} f(i)$ where $f\colon 2 \to U$ is defined by $f(0) = x$ and $f(1) = y$.

(c) If $x \in U$ then $\{x\} \in \mathscr{P}\mathscr{P}(x) \in U$, so $\{x\} \in U$. Thus if $x, y \in U$ then $\{x\}, \{y\} \in U$, so $\{x, y\} \in U$, and therefore $(x, y) \in U$.

(d) The result follows from $x \times y \subseteq \mathscr{P}\mathscr{P}(x \cup y)$ and ${}^{x}y \subseteq \mathscr{P}(x \times y)$.

(e) Letting $g\colon I \to U$ be $i \mapsto \{f(i)\}$, then $\operatorname{ran} f = \bigcup_{i\in I} g(i) \in U$. Moreover $f \subseteq I \times \operatorname{ran} f \in U$, whence $f \in U$. □

Proof of Theorem 21.41. Suppose U is a universe and let $\kappa = U \cap \mathrm{Ord}$.

By Lemma 21.42(c) κ must be a limit ordinal and $\kappa \notin U$. If $\gamma < \kappa$ and $f\colon \gamma \to \kappa$, then $\sup \operatorname{ran} f = \bigcup_{\alpha<\gamma} f(\alpha) \in U$ and hence f cannot be cofinal in κ. It follows that κ is a regular cardinal. If $2^\lambda \geq \kappa$ for some infinite cardinal $\lambda < \kappa$ there would exist a surjection $f\colon \mathscr{P}(\lambda) \twoheadrightarrow \kappa \subseteq U$. But $\mathscr{P}(\lambda) \in U$ and by Lemma 21.42(e) $\kappa \in U$, a contradiction. It follows that κ is a strongly inaccessible cardinal.

Let us check that $\mathrm{V}_\alpha \in U$ for all $\alpha < \kappa$, so that $\mathrm{V}_\kappa \subseteq U$. As U is closed under the $\mathscr{P}$ operation, then $\bar{\kappa} = \{\alpha < \kappa \mid \mathrm{V}_\alpha \in U\}$ is a limit ordinal: if $\bar{\kappa} < \kappa$ then using the function $\bar{\kappa} \to U$, $\alpha \mapsto \mathrm{V}_\alpha$, we would have that $\mathrm{V}_{\bar{\kappa}} = \bigcup_{\alpha<\bar{\kappa}} \mathrm{V}_\alpha \in U$, so that $\bar{\kappa} \in \bar{\kappa}$, a contradiction. Having shown that $\mathrm{V}_\kappa \subseteq U$, we must prove the converse inclusion, so that $\mathrm{V}_\kappa = U$. Towards a contradiction, let $x \in U \setminus \mathrm{V}_\kappa$ be of least rank: then $\operatorname{rank}(x) = \kappa$ so that the map $x \to \kappa$, $y \mapsto \operatorname{rank}(y)$, is cofinal so that $\kappa = \sup_{y\in x} \operatorname{rank}(y) \in U$, a contradiction.

Suppose now κ is a strongly inaccessible cardinal, and let us check that V_κ is a universe. Suppose $f\colon I \to \mathrm{V}_\kappa$ with $I \in \mathrm{V}_\kappa$. Then the function $I \to \kappa$, $i \mapsto \operatorname{rank}(f(i))$, is bounded in κ, since $|I| < \kappa$, so $\operatorname{ran} f \subseteq \mathrm{V}_\alpha$ for some $\alpha < \kappa$. Therefore $\bigcup_{i\in I} f(i) \subseteq \mathrm{V}_\alpha$, and hence $\bigcup_{i\in I} f(i) \in \mathrm{V}_{\alpha+1} \subseteq \mathrm{V}_\kappa$. The other clauses in the definition of universe are immediate. □

Exercises

Exercise 21.43. Show that a non-zero ordinal is a compact topological space if and only if it is a successor ordinal.

Exercise 21.44. Assume AC, and suppose that λ and all κs below are cardinals. Show that:

(i) $\sum_{i\in I} \kappa_i = \sum_{i\in I} \kappa_{\varphi(i)}$ and $\prod_{i\in I} \kappa_i = \prod_{i\in I} \kappa_{\varphi(i)}$, for all bijections $\varphi\colon I \to I$ (commutativity of generalized addition and multiplication of cardinals).

(ii) $\sum_{i\in I} \kappa_i = \sum_{j\in J} \sum_{i\in A_j} \kappa_i$ and $\prod_{i\in I} \kappa_i = \prod_{j\in J} \prod_{i\in A_j} \kappa_i$, for any partition $\langle A_j \mid j \in J\rangle$ of I (associativity of generalized addition and multiplication of cardinals).

(iii) $\lambda^{\sum_{i\in I} \kappa_i} = \prod_{i\in I} \lambda^{\kappa_i}$.

(iv) If $\langle \kappa_n \mid n < \omega\rangle$ is increasing and $\kappa_0 > 0$, then $\sum_n \kappa_n < \prod_n \kappa_n$.

(v) If κ is a limit cardinal and $\lambda < \operatorname{cof}(\kappa)$, then $\kappa^\lambda = \sum_{\delta\in\mathrm{Card}\cap\kappa} \delta^\lambda$.

Exercise 21.45. Assume AC and suppose κ, λ are infinite cardinals, and that $\kappa = \sup_{\alpha<\lambda} \kappa_\alpha$ where $\langle \kappa_\alpha \mid \alpha < \lambda \rangle$ is a monotone sequence of cardinals. Show that:

(i) If $A \subseteq \lambda$ has size λ then $\kappa = \sup_{\alpha \in A} \kappa_\alpha \leq \prod_{\alpha \in A} \kappa_\alpha$.

(ii) There is a partition $\langle A_i \mid i < \lambda \rangle$ of λ such that $|A_i| = \lambda$ for all $i \in \lambda$.

(iii) $\kappa^\lambda = \prod_{\alpha \in \lambda} \kappa_\alpha$. In particular $\aleph_\omega^{\aleph_0} = \prod_{n \in \omega} \aleph_n$.

Exercise 21.46. Show that for any infinite cardinal κ the classes $\{\lambda \in \mathrm{Card} \mid \lambda^\kappa = \lambda\}$ and $\{\lambda \in \mathrm{Card} \mid \lambda^\kappa > \lambda\}$ are proper.

Exercise 21.47. Show that if λ is limit, then there is a cofinal $f\colon \mathrm{cof}(\lambda) \to \lambda$ which is increasing and continuous.

Exercise 21.48. Show that:

(i) If $f_i\colon \kappa_i \to \alpha$ is increasing and cofinal and κ_i is regular ($i = 0, 1$), then $\kappa_0 = \kappa_1$;

(ii) If $f\colon \kappa \to \gamma$ is increasing and cofinal then $\kappa = \mathrm{cof}(\gamma)$;

(iii) If λ is limit, then $\mathrm{cof}(\aleph_\lambda) = \mathrm{cof}(\lambda)$.

Exercise 21.49. Suppose $\kappa \leq \lambda$ are infinite cardinals, and show that:

(i) If $\lambda \leq \mathrm{cof}(\kappa)$ then $[\kappa]^\lambda \asymp {}^\lambda\kappa$.

(ii) Assuming AC, $\mathrm{cof}(\lambda) > \mathrm{cof}(\kappa)$, and $\sup\left\{\nu^\lambda \mid \nu \in \mathrm{Card} \cap \kappa\right\} \leq \kappa$, then $|[\kappa]^\lambda| < \kappa^\lambda$.

Exercise 21.50. Show that:

(i) An ordinal is a totally disconnected, completely regular space.

(ii) If λ is a limit ordinal, then $\lambda \dotplus 1$ and $\lambda \dotplus n$ are homeomorphic, for $1 \leq n < \omega$.

(iii) If ξ and λ are limit ordinals, $f\colon \xi \to \lambda$ is increasing and continuous, and $\bigcup \mathrm{ran}(f) = \lambda$, then $\mathrm{ran}(f)$ is a closed subset of λ.

(iv) Every function $f\colon \omega \to \omega$ is continuous.

(v) The class-function $\mathrm{Ord} \to \mathrm{Ord}$, $\alpha \mapsto \alpha \dotplus 1$, is discontinuous on all limit ordinals.

Exercise 21.51. Suppose λ is a limit ordinal with $\mathrm{cof}(\lambda) > \omega$, and let $f\colon \lambda \to \lambda$ be increasing and continuous. Show that $\{\alpha < \lambda \mid f(\alpha) = \alpha\}$ is closed and unbounded.

Exercise 21.52. Show that $|\mathrm{V}_n| < \omega$ for all n, and that $|\mathrm{V}_{\omega \dotplus \alpha}| = \beth_\alpha$, for all $\alpha \in \mathrm{Ord}$.

Exercise 21.53. Following Remark 21.36, generalize the results and definitions in Section 21.E to the case when κ is either an ordinal of uncountable cofinality, or else when κ is Ord.

Exercise 21.54. Let Ω be either a regular, uncountable cardinal, or else $\Omega = \mathrm{Ord}$. Let $X \subseteq \Omega$ be unbounded in Ω. Show that:

(i) X is closed if and only if its enumerating class-function $F_X \colon \Omega \to X \subseteq \Omega$ is continuous.

(ii) Letting $X' = \{F_X(\lambda) \mid \lambda < \Omega \text{ is limit}\}$, if X is closed then so is X', and $X' \subseteq X$.

(iii) If X is closed, then so are the classes $X^{(\alpha)}$ for $\alpha < \Omega$ defined inductively by $X^{(0)} = X$, $X^{(\alpha+1)} = (X^{(\alpha)})'$ and $X^{(\lambda)} = \bigcap_{\alpha<\lambda} X^{(\alpha)}$ when λ is limit. Therefore also $\triangle_{\alpha<\Omega} X^{(\alpha)} \overset{\text{def}}{=} \{\nu \in \Omega \mid \forall \alpha < \nu\, (\nu \in X^{(\alpha)})\}$ is closed and unbounded in Ω.

(iv) If $X = \Omega$ then $X' = \{\gamma \in \Omega \mid \gamma \text{ is limit}\} = \{\omega \cdot \alpha \mid \alpha \in \Omega \setminus \{0\}\}$, and $X'' = \{\gamma \in \Omega \mid \gamma \text{ is limit of limits}\} = \{\omega^2 \cdot \alpha \mid \alpha \in \Omega \setminus \{0\}\}$.

Exercise 21.55. Show that if $f \colon {}^n\kappa \to \kappa$ is a surjection, then $\{\alpha < \kappa \mid f \restriction {}^n\alpha \colon {}^n\alpha \to \alpha \text{ is a surjection}\}$ is closed and unbounded. Repeat with "bijection" in place of "surjection".

Exercise 21.56. Suppose $\langle \kappa_i \mid i \in I\rangle$ and $\langle \lambda_i \mid i \in I\rangle$ are (finite or infinite) cardinals and that $\kappa_i \leq \lambda_i$ and $2 \leq \lambda_i$ for all $i \in I$. Show that if I has at least three elements, then $F \colon \bigcup_{i\in I}\{i\} \times \kappa_i \to \bigtimes_{i\in I}\lambda_i$

$$F(i,\alpha)(j) = \begin{cases} \alpha & \text{if } i = j, \\ 0 & \text{if } i \neq j \text{ and } \alpha \neq 0, \\ 1 & \text{if } i \neq j \text{ and } \alpha = 0, \end{cases}$$

is injective. Conclude that $\bigcup_{i\in I}\{i\} \times \kappa_i \precsim \bigtimes_{i\in I}\lambda_i$, for every I.

Exercise 21.57. For κ an infinite cardinal, $\mathrm{cof}(\kappa)$ is the least λ such that there is $\langle A_\alpha \mid \alpha < \lambda\rangle$ such that $\bigcup_{\alpha<\lambda} A_\alpha = \kappa$ and $|A_\alpha| < \kappa$ for all $\alpha < \lambda$.

Exercise 21.58. For $\lambda < \kappa$ regular cardinals, let $E^\kappa_\lambda = \{\alpha < \kappa \mid \mathrm{cof}(\alpha) = \lambda\}$. Show that E^κ_λ is stationary in κ. Conclude that $E^{\omega_2}_{\omega}, E^{\omega_2}_{\omega_1} \notin \mathrm{Club}(\omega_2)$.

Exercise 21.59. Suppose κ and λ are infinite cardinals and $X_\alpha \subseteq \lambda$ for each $\alpha \in \kappa$. Show, without assuming AC, that $\bigcup_{\alpha<\kappa} X_\alpha \precsim \kappa \times \sup_{\alpha\in\kappa} \mathrm{ot}(X_\alpha)$, and hence $|\bigcup_{\alpha<\kappa} X_\alpha| \leq \kappa \cdot \sup_{\alpha\in\kappa}|X_\alpha|^+$. In particular, ω_2 is not a countable union of countable sets.

Exercise 21.60. Let $\langle P, \leq\rangle$ be an ordered set without maximum. We say that $X \subseteq P$ is

- **unbounded** if there is no $p \in P$ such that $\forall q \in X\, (q \leq p)$; equivalently if $X^{\blacktriangledown} = \emptyset$ with the notation of Section 7.A;
- **dominating** if $\forall p \in P\, \exists q \in X\, (p \leq q)$.

Whenever P is well-orderable let

$$\mathfrak{b}(P) = \min\{|X| \mid X \text{ is unbounded in } P\}$$
$$\mathfrak{d}(P) = \min\{|X| \mid X \text{ is dominating in } P\}$$

Show that

(i) a dominating set is unbounded, and if $\langle P, \leq \rangle$ is linear then the converse holds;

(ii) if $\mathfrak{b}(P)$ is infinite, then it is regular, and if $\langle P, \leq \rangle$ is a well-order, then $\mathfrak{b}(P) = \operatorname{cof}(\operatorname{ot}(P))$;

(iii) assuming AC, there is an ordered set with $\mathfrak{d}(P)$ singular;

(iv) for each $n > 1$ construct P such that $\mathfrak{b}(P) = n$.

Exercise 21.61. Show that GCH implies that for all infinite cardinals κ, λ

$$\kappa^\lambda = \begin{cases} \kappa & \text{if } \lambda < \operatorname{cof} \kappa, \\ \kappa^+ & \text{if } \operatorname{cof} \kappa \leq \lambda \leq \kappa, \\ \lambda^+ & \text{if } \kappa < \lambda. \end{cases}$$

Exercise 21.62. Suppose ν is an ordinal such that $2^{\aleph_\alpha} = \aleph_{\alpha + \nu}$, for all $\alpha \in \mathrm{Ord}$. Show that if $\nu \geq \omega$, then ν is a successor, and if γ is least such that $\gamma \dotplus \nu > \nu$ then $\gamma < \nu$ is limit. Use the Bukovsky–Hechler Theorem 21.15 to derive a contradiction, and conclude that $\nu < \omega$.

Exercise 21.63. Assume AC. Show that:

(i) $\gamma < \kappa$ is a limit cardinal if and only if $\mathrm{V}_\kappa \vDash$"γ is a limit cardinal".

Repeat the argument with "strong limit" and "regular" in place of "limit".

(ii) If $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$ then κ is a strong limit cardinal, $|\mathrm{V}_\kappa| = \kappa$ and hence $\kappa = \aleph_\kappa$.

(iii) κ is strongly inaccessible if and only if $\mathrm{V}_{\kappa+1} \vDash \mathsf{MK} + \mathsf{AC}$.

(iv) The existence of a weakly/strongly inaccessible cardinal cannot be proved in ZFC or MK + AC.

Exercise 21.64. A train runs along the countable ordinals, leaving station 0 with destination ω_1. At every station α a passenger steps-down, if the train is non-empty, and then ω new passengers get on the train. How many passengers are on the train when it arrives at station ω_1?

22. Categories

In this Section we present the bare minimum of category theory, in order to provide a useful language for many parts of mathematics.

A **category** $\mathfrak{C}$ consists of

- two non-empty classes $\mathbf{Obj}^{\mathfrak{C}}$ and $\mathbf{Arw}^{\mathfrak{C}}$, whose elements are called, respectively, **objects** and **arrows** (or **morphisms**)
- two functional relations assigning to each arrow f two objects $\mathbf{dom}^{\mathfrak{C}}(f)$ and $\mathbf{cod}^{\mathfrak{C}}(f)$ called, respectively, **domain** and **codomain** of the arrow f,
- a functional relation assigning to each object a an arrow $\mathbf{1}_a^{\mathfrak{C}}$ with domain and codomain a,
- a partial binary operation $\circ^{\mathfrak{C}}$ on arrows $(f, g) \mapsto f \circ^{\mathfrak{C}} g \in \mathbf{Arw}^{\mathfrak{C}}$, called **composition** with domain $\{(g, f) \in \mathbf{Arw}^{\mathfrak{C}} \times \mathbf{Arw}^{\mathfrak{C}} \mid \mathbf{cod}^{\mathfrak{C}} f = \mathbf{dom}^{\mathfrak{C}} g\}$,

satisfying the following:

(i) if $f, g \in \mathbf{Arw}$ and $g \circ f$ is defined, then $\mathbf{dom}\, g \circ f = \mathbf{dom}\, f$ and $\mathbf{cod}\, g \circ f = \mathbf{cod}\, g$,

(ii) if $\mathbf{cod}\, f = \mathbf{dom}\, g$ and $\mathbf{cod}\, g = \mathbf{dom}\, h$, then $h \circ (g \circ f) = (h \circ g) \circ f$,

(iii) $\mathbf{dom}\, \mathbf{1}_a = a = \mathbf{cod}\, \mathbf{1}_a$,

(iv) $\mathbf{cod}\, f = \mathbf{dom}\, g = b \Rightarrow f = \mathbf{1}_b \circ f \wedge g = g \circ \mathbf{1}_b$.

We write $f \colon a \to b$ or $a \xrightarrow{f} b$ or $a \underset{f}{\to} b$ to say that f is an arrow from a to b, that is an element of

$$\hom(a, b) = \{f \in \mathbf{Arw} \mid \mathbf{dom}(f) = a \wedge \mathbf{cod}(f) = b\}.$$

A category is:

- **locally small** if $\hom(a, b)$ is a set for all $a, b \in \mathbf{Obj}$; if moreover $\mathbf{Obj}$ is a set then the category is **small**;
- **concrete** if $\hom(a, b) \subseteq {}^{a}b$ that is arrows are functions, $\circ$ is the usual composition, and $\mathbf{1}_a = \mathrm{id}_a$, for all $a, b \in \mathbf{Obj}$.

We say that $\mathfrak{D}$ is a subcategory of $\mathfrak{C}$ if $\mathbf{Obj}^{\mathfrak{D}} \subseteq \mathbf{Obj}^{\mathfrak{C}}$ and $\hom^{\mathfrak{D}}(a, b) \subseteq \hom^{\mathfrak{C}}(a, b)$ for all $a, b \in \mathbf{Obj}^{\mathfrak{D}}$.

Examples 22.1. (a) The prototypical example of a category is Sets: the class of objects is V and an arrow from a to b is a triple (a, f, b) with $f \colon a \to b$, $\circ$ is the usual composition, and $\mathbf{1}_a = \mathrm{id}_a$.

(b) The category $\mathrm{Str}(\mathcal{L})$ has $\mathcal{L}$-structures as objects and the arrows are $f \colon M \to N$ morphisms of structures. If we require that the structures satisfy some theory T, a subcategory is obtained. In particular we obtain the category of ordered sets with monotone functions, the category of groups with homomorphisms, ...

Similarly one can consider collections of sets endowed with additional structure, and functions preserving such structure, such as topological spaces with continuous functions, ...

$$\begin{tikzcd}
\bullet \arrow[r] & \bullet \\
\bullet \arrow[u] \arrow[r] & \bullet \arrow[u]
\end{tikzcd}$$

$\langle I, E\rangle$

$$\begin{tikzcd}
b \arrow[r, "g"] & d \\
a \arrow[u, "f"] \arrow[r, "h"'] & c \arrow[u, "k"']
\end{tikzcd}$$

$\mathfrak{C}$

$$\begin{tikzcd}
M \arrow[r, "n"] & M \\
M \arrow[u, "m"] \arrow[r, "n"'] & M \arrow[u, "m"']
\end{tikzcd}$$

M

Figure 22. Diagrams indexed by a directed graph $\langle I, E\rangle$ in a category $\mathfrak{C}$, and in a monoid M

(c) Every preorder set $\langle P, \leq\rangle$ can be described as a category letting $\mathbf{Obj} = P$ and stipulating that there is exactly one arrow between p and q if and only if $p \leq q$.

(d) Every monoid M can be seen as a category with just one object, whose arrows are the elements of M, composition is the operation and $\mathbf{1}_M$ is the identity of M.

(e) Any directed multigraph (Section 9.C.3) (V, E, s, t) gives rise to a category: the objects are the elements of V, and the arrows are finite compositions of edges in E and the $\mathbf{1}_v$ for $v \in V$.

(f) The set of all matrices over a ring can be construed as a category, where $\mathbf{Obj} = \mathbb{N} \setminus \{0\}$, the arrows $m \to n$ are the $m \times n$ matrices, and the composition is row-by-column multiplication.

The categories of examples (a) and (b) are concrete categories, while those of examples (c)–(f) are not.

Definition 22.2. Let $\mathfrak{C}$ be a category, and let $\langle I, E\rangle$ be a directed graph such that $(i, i) \notin E$ for all $i \in I$. A **diagram with shape** I is a map assigning to each vertex $i \in I$ an object a_i, and to each oriented edge $(i, j) \in E$ an arrow $a_i \to a_j$. For the ease of notation we denote such diagram by $\{a_i, f_{i,j} \mid i, j \in I\}$, and say that I is the index set of the diagram. A diagram **commutes** if $h = g \circ f$ for all arrows f, g, h in the diagram such that $\mathbf{cod}(f) = \mathbf{dom}(g)$ and $\mathbf{cod}(g) = \mathbf{dom}(h)$.

In Figure 22 we have a directed graph and a commutative diagram in $\mathfrak{C}$ and in a monoid M (Example (d)): in the first case it says that $g \circ f = k \circ h$, in the second case it says that $mn = nm$. In particular, properties (ii) and (iv) can be stated by saying that the following diagrams commute.

$$\begin{tikzcd}
& b \arrow[rr, "h\circ g"] \arrow[dr, "g"] & & d \\
a \arrow[ur, "f"] \arrow[rr, "g\circ f"] \arrow[urrr, bend left, "(h\circ g)\circ f"] \arrow[urrr, bend right, "h\circ(g\circ f)"'] & & c \arrow[ur, "h"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
a \arrow[r, "f"] \arrow[dr, "f"'] & b \arrow[d, "\mathbf{1}_b"] \arrow[dr, "g"] & \\
& b \arrow[r, "g"'] & c
\end{tikzcd}$$

22.A. Functors.

Definition 22.3. A **functor** $\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}$ is a pair of functional relations $\mathbf{Obj}^{\mathfrak{C}} \to \mathbf{Obj}^{\mathfrak{D}}$ and $\mathbf{Arw}^{\mathfrak{C}} \to \mathbf{Arw}^{\mathfrak{D}}$, such that

(1) $\mathbf{F}(\mathbf{1}^{\mathfrak{C}}_a) = \mathbf{1}^{\mathfrak{D}}_{\mathbf{F}(a)}$,

(2) if $f\colon a \to b$ then $\mathbf{F}(f)\colon \mathbf{F}(a) \to \mathbf{F}(b)$ and

(3) $\mathbf{F}(g \circ^{\mathfrak{C}} f) = \mathbf{F}(g) \circ^{\mathfrak{D}} \mathbf{F}(f)$.

Examples 22.4. (a) The functional relation associating to each $\mathcal{L}$-structure $\mathcal{M}$ its universe M is a functor $\mathrm{Str}_{\mathcal{L}} \to$ SETS. Similarly the functional relation associating to any rng the underlying abelian group defines a functor from the category of rngs to the one of abelian groups. Functors as above are called **forgetful** since they forget in part or completely the structure of the starting object.

(b) A function between preordered sets (considered as categories) is monotone if and only if it is a functor. Similarly a map between monoids is a homomorphism if and only if it is a functor.

(c) The category of all small categories CAT has for objects all small categories with functors between them as arrows. It is locally small, but not small.

(d) As every directed graph can be seen as a category (Example 22.1(e)), the assignment from $\langle I, E\rangle$ to $\mathfrak{C}$ in Definition 22.2 is a functor.

Definition 22.5. Let $\mathbf{F}, \mathbf{G}\colon \mathfrak{C} \to \mathfrak{D}$ be functors. A **natural transformation** $\boldsymbol{\eta}\colon \mathbf{F} \to \mathbf{G}$ is a system of $\mathfrak{D}$-arrows $\boldsymbol{\eta}_a\colon \mathbf{F}(a) \to \mathbf{G}(a)$ for $a \in \mathbf{Obj}^{\mathfrak{C}}$ such that for any $\mathfrak{C}$-arrow $f\colon a \to b$ the diagram

$$\begin{tikzcd}
\mathbf{F}(a) \arrow[r, "\eta_a"] \arrow[d, "\mathbf{F}(f)"'] & \mathbf{G}(a) \arrow[d, "\mathbf{G}(f)"] \\
\mathbf{F}(b) \arrow[r, "\eta_b"'] & \mathbf{G}(b)
\end{tikzcd}$$

commutes. If each $\boldsymbol{\eta}_a$ is an isomorphism, then $\boldsymbol{\eta}$ is called a **natural isomorphism** between $\mathbf{F}$ and $\mathbf{G}$.

Definition 22.6. Suppose $\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}$ and $\mathbf{G}\colon \mathfrak{D} \to \mathfrak{C}$ are functors. If there is a natural bijection between $\hom(\mathbf{F}(a), b)$ and $\hom(a, \mathbf{G}(b))$ then $\mathbf{F}, \mathbf{G}$ is an **adjoint pair** of functors, with $\mathbf{F}$ the **left adjoint** and $\mathbf{G}$ the **right adjoint**.

Examples 22.7. (a)

(b)

22.B. Duality. The definition of category can be cast in first-order logic, using a language $\mathcal{L}$ with two unary predicates $\mathbf{Obj}$ and $\mathbf{Arw}$, two binary predicates $\mathbf{dom}$ and $\mathbf{cod}$, and a ternary predicate $\circ$. Of the following four axioms, the first says that anything is either an object or else it is an arrow, the second and the third say that $\mathbf{dom}$ and $\mathbf{cod}$ are functions on the arrows, and the fourth says that $\circ$ is an associative binary operation on arrows:

$$\forall x\,(\mathbf{Obj}(x) \Leftrightarrow \neg\mathbf{Arw}(x)) \tag{22.1a}$$

$$\begin{aligned}&\forall f, a\,(\mathbf{dom}(f,a) \Rightarrow \mathbf{Arw}(f) \wedge \mathbf{Obj}(a))\\ &\qquad\qquad \wedge \forall f\,(\mathbf{Arw}(f) \Rightarrow \exists! a(\mathbf{Obj}(a) \wedge \mathbf{dom}(f,a)))\end{aligned} \tag{22.1b}$$

$$\begin{aligned}&\forall f, b\,(\mathbf{cod}(f,b) \Rightarrow \mathbf{Arw}(f) \wedge \mathbf{Obj}(b))\\ &\qquad\qquad \wedge \forall f\,(\mathbf{Arw}(f) \Rightarrow \exists! b(\mathbf{Obj}(b) \wedge \mathbf{cod}(f,b)))\end{aligned} \tag{22.1c}$$

$$\begin{aligned}&\forall f, g, a, b, c\,\big(\mathbf{dom}(f,a) \wedge \mathbf{cod}(f,b) \wedge \mathbf{dom}(g,b) \wedge \mathbf{cod}(g,c)\\ &\qquad \Rightarrow \exists! h(\mathbf{Arw}(h) \wedge \mathbf{dom}(h,a) \wedge \mathbf{cod}(h,c) \wedge \circ(f,g,h))\big)\end{aligned} \tag{22.1d}$$

(For the sake of readability we have used a, b, c for variables that range over objects, and f, g, h for variables that range over arrows—in fact using a two sorted language as in Section 9.C with $\mathbf{dom}$ and $\mathbf{cod}$ unary partial functions, and $\circ$ as a binary partial operation would have ensured a less baroque presentation.) The class of models of these axioms is the class of all small categories. (The restriction to small categories is due to our insistence to consider only structures whose universe is a set.)

The dual of an $\mathcal{L}$-formula φ is obtained by

- swapping $\mathbf{dom}$ and $\mathbf{cod}$, while leaving the other predicates unchanged
- replace any instance of $\circ(x, y, z)$ with $\circ(y, x, z)$.

The axioms (22.1b) and (22.1c) are dual to each other, and (22.1a) and (22.1d) are (logically equivalent to) their dual. Therefore the axiom system (22.1a)–(22.1d) exhibit a duality similar to the one for Boolean algebras. The analogue of the dual of a Boolean algebra is the following notion.

Definition 22.8. Given a category $\mathfrak{C}$, the **opposite category** $\mathfrak{C}^{\mathrm{op}}$ has the same objects and arrows as $\mathfrak{C}$, but the operations $\mathbf{dom}$ and $\mathbf{cod}$ are swapped and the composition is performed backwards: $\mathbf{Obj}^{\mathrm{op}} = \mathbf{Obj}$, $\mathbf{Arw}^{\mathrm{op}} = \mathbf{Arw}$, $\mathbf{dom}^{\mathrm{op}}(f) = \mathbf{cod}(f)$ and $\mathbf{cod}^{\mathrm{op}}(f) = \mathbf{dom}(f)$, and $f \circ^{\mathrm{op}} g = g \circ f$.

Many concepts in category theory can be "dualized" by inverting the arrows in a commutative diagram, or considering the opposite category. For example, an arrow from a to b is **mono** or a **monomorphism**, $f\colon a \rightarrowtail b$, if $f \circ g = f \circ h \Rightarrow g = h$ for every object c and every pair of arrows g, h from c to a. The dual notion is that of being **epi** or an **epimorphism**, $f\colon a \twoheadrightarrow b$, if $g \circ f = h \circ f \Rightarrow g = h$ for every object c and every pair of arrows g, h from b to c. Note that in the category of sets, a function is mono if it is injective, and it is epi if it is surjective, thus "being a subset" and "being a quotient" are dual notions.

An arrow from a to b is **iso** or an **isomorphism**, $f\colon a \xrightarrow{\sim} b$, if there is a $g\colon b \to a$ such that $g \circ f = \mathbf{1}_a$ and $f \circ g = \mathbf{1}_b$. Moreover g is unique, and it is called the inverse of f, denoted by f^{-1}: if g_1 and g_2 are inverses of f, then

$$g_1 = \mathbf{1}_a \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \mathbf{1}_b = g_2.$$

Two objects a and b are **isomorphic**, $a \cong b$, if there is an isomorphism between them.

Definition 22.9. An object a of a category $\mathfrak{C}$ is

- **injective** if for every arrow $f\colon b \to a$ and every mono arrow $h\colon b \to c$ there is an arrow $g\colon c \to a$ such that $g \circ h = f$;
- **projective** if for every arrow $f\colon a \to b$ and every epi arrow $h\colon c \to b$ there is an arrow $g\colon a \to c$ such that $g \circ h = f$.

Definition 22.10. An **initial object** of $\mathfrak{C}$ is an object $\mathbf{0}$ such that for all $a \in \mathbf{Obj}^{\mathfrak{C}}$ there is a unique arrow $\mathbf{0} \to a$. A **terminal object** in $\mathfrak{C}$ is an initial object in $\mathfrak{C}^{\mathrm{op}}$, i.e. it is a $\mathbf{1} \in \mathbf{Obj}^{\mathfrak{C}}$ such that for all $a \in \mathbf{Obj}^{\mathfrak{C}}$ there is a unique arrow $a \to \mathbf{1}$.

Proposition 22.11. *Two initial (terminal) objects (if they exist) are isomorphic, and moreover the isomorphism is unique.*

Proof. Suppose $\mathbf{0}, \mathbf{0}'$ are initial objects in a category $\mathfrak{C}$. Then there are $f\colon \mathbf{0} \to \mathbf{0}'$ and $f'\colon \mathbf{0}' \to \mathbf{0}$, so that $f' \circ f\colon \mathbf{0} \to \mathbf{0}$. As $\mathbf{0}$ is an initial object the arrow $\mathbf{1}_{\mathbf{0}}\colon \mathbf{0} \to \mathbf{0}$ is unique, so $f' \circ f = \mathbf{1}_{\mathbf{0}}$. Similarly $f \circ f' = \mathbf{1}_{\mathbf{0}'}$ so $f\colon \mathbf{0} \to \mathbf{0}'$ is the unique isomorphism between $\mathbf{0}$ and $\mathbf{0}'$. The argument for terminal objects is analogous. □

Examples 22.12. (a) In the category Sets the empty set is the unique initial object, and any singleton is a final object.

(b) In an ordered set the minimum is the initial object, and the maximum is the terminal object. Therefore not every category has an initial or a terminal object.

(c) In the category of groups the trivial group with one element is both the initial and the terminal object.

A **controvariant functor** $\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}$ is a functor $\mathbf{F}\colon \mathfrak{C}^{\mathrm{op}} \to \mathfrak{D}$ or equivalently a functor $\mathbf{F}\colon \mathfrak{C} \to \mathfrak{D}^{\mathrm{op}}$. In order to distinguish the two concepts, sometimes the notion of Definition 22.3 is called a **covariant functor**.

Example 22.13. Let $\mathfrak{C}$ be the category of vector spaces over a field $\Bbbk$ with linear maps as arrows. Then $\mathfrak{C} \to \mathfrak{C}$, $W \mapsto W^*$ sending each vector space to its dual and each linear map $f\colon W \to Z$ to $f^*\colon Z^* \to W^*$, $f^*(z^*) = z^* \circ f$ is a controvariant functor.

Definition 22.14. Let $\mathcal{D} = \{a_i, f_{i,j} \mid i, j \in I\}$ be a diagram in $\mathfrak{C}$ indexed by a directed graph I (Definition 22.2).

- A **cone** for $\mathcal{D}$ is an object b together with arrows $g\colon b \to a_i$ $(i \in I)$ such that $f_{i,j} \circ g_i = g_j$ for all arrows $f_{i,j}\colon a_i \to a_j$ of $\mathcal{D}$, and such that if $b' \in \mathbf{Obj}^{\mathfrak{C}}$ and $g'_i\colon b' \to a_i$ are such that $f_{i,j} \circ g'_i = g'_j$ for all $f_{i,j}\colon a_i \to a_j$, then there is a unique $h\colon b' \to b$ such that $g_i \circ h = g'_i$ for all $i \in I$.
- Dually, a **cocone** for $\mathcal{D}$ is a $b \in \mathbf{Obj}^{\mathfrak{C}}$ and $g_i\colon a_i \to b$ that commute with the $f_{i,j}$s, and such that for all $b' \in \mathbf{Obj}^{\mathfrak{C}}$ and $g'_i\colon a_i \to b$ commuting with the $f_{i,j}$s, there is a unique $h\colon b \to b'$.

The existence of cones or cocones even for finite diagrams is an important property for a category to have. Arguing as in Proposition 22.11 a cone and a cocone for a diagram are unique up to isomorphism, and the isomorphism is unique.

22.B.1. *Products and coproducts.* Consider the diagram given by objects $\{a_i \mid i \in I\}$ and no arrows between them—in other words, the indexing directed graph has no edges. A cone for $\{a_i \mid i \in I\}$ is called a **product** of the a_is, $\boldsymbol{p}_j\colon \prod_{i\in I} a_i \to a_j$, while a cocone for this diagram is called a **coproduct** of the a_is, $\boldsymbol{i}_j\colon a_j \to \coprod_{i\in I} a_i$. In case the diagram is just a two element set $\{a, b\}$ the product and coproduct are denoted by $a \times b$ and $a + b$. A category admits (finite) products just in case every (finite) family of objects has a product.

Examples 22.15. (a) In the category SETS a product is the usual cartesian product $\bigtimes_{i\in I} A_i$ with $\boldsymbol{p}_j(f) = f(j)$, and the coproduct is the disjoint union $\biguplus_{i\in I} A_i$ with $\boldsymbol{i}_j(x) = (j, x)$. In the category of topological spaces where arrows are continuous functions, the product is given by the set-theoretic cartesian product endowed with the product topology, and the coproduct is the disjoint union with the topology defined as follow:s $X \subseteq \bigcup_{i\in I}\{i\} \times A_i$ is open if and only if $\{a \in A_i \mid (i, a) \in X\}$ is open in A_i, for all $i \in I$.

(b) If $\langle P, \leq\rangle$ is an ordered set and $X \subseteq P$, then $\prod X = \inf X$ and $\coprod X = \sup X$. Therefore not every category has product or coproducts, not even finite ones.

$$\begin{tikzcd}
a_i \arrow[dr, "\pi_{i,k}"'] \arrow[drr, "\pi_{i,\infty}"] \arrow[drrr, bend left, "\rho_i"] & & & \\
 & a_k \arrow[r, "\pi_{k,\infty}"] \arrow[rr, bend left, "\rho_k"] & a_\infty \arrow[r, "\sigma"'] & b \\
a_j \arrow[ur, "\pi_{j,k}"] \arrow[urr, "\pi_{ij,\infty}"] \arrow[urrr, bend right, "\rho_j"'] & & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & a_i \\
b \arrow[urrr, bend left, "\rho_i"] \arrow[rr, bend left, "\rho_k"] \arrow[r, "\sigma"'] \arrow[drrr, bend right, "\rho_j"'] & a_\infty \arrow[urr, "\pi_{\infty,j}"] \arrow[r, "\pi_{\infty,k}"] \arrow[drr, "\pi_{\infty,j}"'] & a_k \arrow[ur, "\pi_{k,i}"'] \arrow[dr, "\pi_{k,j}"] & \\
 & & & a_j
\end{tikzcd}$$

Figure 23. Direct and inverse limits

(c) In the category of groups $\prod_{i\in I} G_i$ is the set $\times_{i\in I} G_i$ with the operation of pointwise multiplication, while $\coprod_{i\in I} G_i$ is

$$\bigoplus_{i\in I} G_i = \{f \in \times_{i\in I} G_i \mid \{i \in I \mid f(i) \neq e_i\} \text{ is finite}\}$$

where e_i is the identity of G_i. (It is easy to check that the resulting structures are groups.) Note that in the finite case, the product and coproduct of groups coincide, that is $G \times H$ is the product and the coproduct of G and H.

22.C. Limits. A **directed system in $\mathfrak{C}$** is a covariant functor from an upward directed order set $\langle I, \leq\rangle$ (considered as a category) to $\mathfrak{C}$. In other words it consists of objects a_i and arrows $\pi_{i,j}\colon a_i \to a_j$ for $i \leq j$ such that $\pi_{i,i} = \mathbf{1}_{a_i}$ and $\pi_{i,h} = \pi_{j,h} \circ \pi_{i,j}$ for $i \leq j \leq h$, and it is denoted by $\langle a_i, \pi_{i,j} \mid i \leq j \in I\rangle$. A **limit for a directed system** is an object a_∞ together with arrows $\pi_{i,\infty}\colon a_i \to a_\infty$ such that $\pi_{j,\infty} \circ \pi_{i,j} = \pi_{i,\infty}$ with the property that for all $b \in \mathbf{Obj}$ and all arrows $\rho_i\colon a_i \to b$ that commute with the πs, that is $\rho_j \circ \pi_{i,j} = \rho_i$ for $i \leq j$, there is a unique $\sigma\colon a_\infty \to b$ such that $\sigma \circ \pi_{i,\infty} = \rho_i$ for all $i \in I$. By universality the direct limit $\langle a_i, \pi_{i,j} \mid i \leq j \in I\rangle$ is unique up to isomorphism and it is denoted by $\varinjlim \langle a_i, \pi_{i,j} \mid i \leq j \in I\rangle$ or $\varinjlim a_i$. A category $\mathfrak{C}$ has direct limits if every directed system has a limit.

Theorem 22.16. *The category of sets has direct limits, that is if $\langle A_i, \pi_{i,j} \mid i \leq j \in I\rangle$ is a directed system of sets and functions then $\varinjlim A_i$ exists. If moreover the $\pi_{i,j}$s are injective, so are the $\pi_{i,\infty}$, and for any set B and injective maps $\rho_i\colon A_i \to B$, the unique map $\sigma\colon \varinjlim A_i \to B$ is injective as well.*

Proof. Let $\langle I, \leq\rangle$ be upward directed and fix sets A_i and functions $\pi_{i,j}\colon A_i \to A_j$ for $i \leq j \in I$. Let $A_\infty = \bigcup_{i\in I}\{i\} \times A_i/{\sim}$ where $\sim$ is the equivalence relation defined by

$$(i, a) \sim (j, b) \Leftrightarrow \exists k \in I\,(i \leq k \wedge j \leq k \wedge \pi_{i,k}(a) = \pi_{j,k}(b)).$$

(Transitivity follows from upward directedness.) Let $\pi_{i,\infty}(a) = [(i, a)]_\sim$. If $i \leq j$ and $a \in A_i$ then $(i, a) \sim (j, \pi_{i,j}(a))$ and hence $\pi_{i,\infty} = \pi_{j,\infty} \circ \pi_{i,j}$. Given a set B and functions $\rho_i\colon A_i \to B$ such that $\rho_i = \rho_j \circ \pi_{i,j}$ for $i \leq j$, we must show that there is a unique $\sigma\colon A_\infty \to B$ satisfying $\rho_i = \sigma \circ \pi_{i,\infty}$ for all $i \in I$. Let $\sigma\colon A_\infty \to B$ be defined by $\sigma([(i, a)]_\sim) = \rho_i(a)$. It is easy to check that the definition of σ does not depend on the representative, and that it is the unique function that works.

Suppose now the $\pi_{i,j}$s are injective. If $\pi_{i,\infty}(a) = \pi_{i,\infty}(b)$ then $(i, a) \sim (i, b)$, that is $\exists j \geq i\ (\pi_{i.j}(a) = \pi_{i,j}(b))$. By case assuoption $a = b$, so $\pi_{i,\infty}$ is injective. Finally, suppose that the $\rho_i\colon A_i \to B$ are injective towards proving that $\sigma\colon A_\infty \to B$ is injective as well. If $\sigma([(i, a)]_\sim) = \sigma([(j, b)]_\sim)$ then $\rho_i(a) = \rho_j(b)$ so $\rho_k(\pi_{i,k}(a)) = \rho_k(\pi_{j,k}(b))$ for any $k \geq i, j$, and hence $\pi_{i,k}(a) = \pi_{j,k}(b)$ so that $(i, a) \sim (j, b)$, that is $[(i, a)]_\sim = [(j, b)]_\sim$. □

Fix a directed system $\langle A_i, \pi_{i,j} \mid i \leq j \in I\rangle$ a directed system of sets and functions. Suppose that R_i is an n-ary relation on A_i and that $\pi_{i,j}\colon \langle A_i, R_i\rangle \to \langle A_j, R_j\rangle$ is a morphism, that is

$$\langle a_1, \ldots, a_n\rangle \in R_i \Rightarrow \langle \pi_{i,j}(a_1), \ldots, \pi_{i,j}(a_n)\rangle \in R_j.$$

Let R_∞ be the n-ary relation on A_∞ defined by

$$\langle [(i_1, a_1)]_\sim, \ldots, [(i_n, a_n)]_\sim\rangle \in R_\infty \Leftrightarrow \\ \exists k \geq i_1, \ldots, i_n\ (\langle \pi_{i_1,k}(a_1), \ldots, \pi_{i_n,k}(a_n)\rangle \in R_k)\,.$$

We leave it to the reader to check that the definition of R_∞ does not depend on the representatives, that

$$\pi_{i,\infty}\colon \langle A_i, R_i\rangle \to\langle A_\infty, R_\infty\rangle \qquad\qquad a \mapsto [(i, a)]_\sim$$

is a morphism, and that for any set B with n-ary relation S, and morphisms $\rho_i\colon \langle A_i, R_i\rangle \to \langle B, S\rangle$ that commute with the $\pi_{i,j}$s, there is a unique morphism $\sigma\colon \langle A_\infty, R_\infty\rangle \to \langle B, S\rangle$.

Suppose now that f_i is a binary operation on A_i, and that $\pi_{i,j}\colon \langle A_i, f_i\rangle \to \langle A_j, f_j\rangle$ is a morphism. Let

$$\begin{aligned} &f_\infty\colon A_\infty \times A_\infty \to A_\infty \\ &([(i, a)]_\sim, [(j, b)]_\sim) \mapsto [(k, f_k(\pi_{i,k}(a), \pi_{j,k}(b)))]_\sim \quad \text{for some/any } k \geq i, j. \end{aligned}$$

We leave it to the reader to check that f_∞ is a well-defined operation, that $\pi_{i,\infty}\colon \langle A_i, f_i\rangle \to \langle A_\infty, f_\infty\rangle$ is a morphism, and that for any set B with a binary operation g, and morphisms $\rho_i \colon \langle A_i, f_i \rangle \to \langle B, g \rangle$ that commute with the $\pi_{i,j}$s, there is a unique morphism $\sigma \colon \langle A_\infty, f_\infty \rangle \to \langle B, g \rangle$.

Theorem 22.17. *The category of $\mathcal{L}$-structures has direct limits.*

The notion of **inverse system** and **inverse limit** are obtained by "dualizing" the definitions of direct system and limit. An inverse system for $\mathfrak{C}$ is a controvariant functor from an upper directed order, or equivalently it is a functor $I \to \mathfrak{C}$ with $\langle I, \leq \rangle$ a lower directed order: in other words, we are given objects a_i and commuting arrows $\pi_{i,j} \colon a_i \to a_j$ for $i \leq j$. An **inverse limit** of $\langle a_i, \pi_{i,j} \mid i \leq j \in I \rangle$ is an object a_∞ together with a system of arrows $\pi_{\infty,i} \colon a_\infty \to a_i$ that commute with the $\pi_{i,j}$, that is

$$\pi_{\infty,j} = \pi_{i,j} \circ \pi_{\infty,i} \qquad (i \leq j)$$

and such that for every object b and arrows $\rho_i \colon b \to a_i$ that commute with the $\pi_{i,j}$s, there is a unique arrow $\sigma \colon b \to a_\infty$ such that

The inverse limit of $\langle a_i, \pi_{i,j} \mid i \leq j \in I \rangle$ is obtained by dualizing the direct limit construction: instead of taking a quotient of a coproduct, we take a subset of a product

$$\begin{aligned} &\varprojlim_i a_i = \{ f \in \times_{i \in I} a_i \mid \forall i, j \in I \, (i \leq j \Rightarrow \pi_{i,j}(f(i)) = f(j)) \} , \\ &\pi_{j,\infty} \colon \varprojlim_i M_i \to M_j, \quad f \mapsto f(j). \end{aligned}$$

22.D. The Cantor-Lawvere Theorem*. The kind of categories used in this book are quite close to set theory, in the sense that the arrows are functions satisfying some properties. For these categories it is possible to generalize Cantor's Theorem 13.22.

Theorem 22.18 (Lawvere)**.** *Let $\mathfrak{C}$ be a concrete category, let a, b be objects and suppose $F \colon a \to \hom(a, b)$ is a surjection such that*

$$a \to b \qquad x \mapsto F(x)(x)$$

is an arrow of $\mathfrak{C}$. Then b has the fixed point property, that is for each arrow $f \colon b \to b$ there is $x \in b$ such that $f(x) = x$.

Proof. Let $f \colon b \to b$ be an arrow and let $g \colon a \to b$

$$g(x) = f(F(x)(x)). \tag{22.2}$$

By assumption of F, the arrow g is a morphism of $\mathfrak{C}$ and there is an $\bar{x} \in a$ such that $F(\bar{x}) = g$. Let $\bar{y} = g(\bar{x}) \in b$. Then

$$\begin{aligned} f(\bar{y}) &= f(g(\bar{x})) \\ &= f\big(F(\bar{x})(\bar{x})\big) && \text{(since } g = F(\bar{x})) \\ &= g(\bar{x}) && \text{(by (22.2))} \\ &= \bar{y} \end{aligned}$$

that is: $\bar{y}$ is the fixed point of the morphism g. □

As corollary we obtain a new proof of Cantor's Theorem 13.22.

Corollary 22.19. *If X and Y are sets and Y has at least two elements, then there is no surjection $X \twoheadrightarrow Y^X$.*

Here is an interesting application to topology.

Corollary 22.20. *Suppose that X and Y are topological spaces and let $f \colon Y \to Y$ be a function without fixed points. Then there is no continuous surjection*

$$F \colon X \twoheadrightarrow \mathcal{C}(X,Y) \overset{\text{def}}{=} \{f \colon X \to Y \mid f \textit{ is continuous}\}$$

such that the map $X \to Y$, $x \mapsto F(x)(x)$, is continuous.

Exercises

Exercise 22.21. (i) Show in the category of sets, the arrows mono, epi and iso are the injective, surjective, and bijective functions, respectively.

(ii) Show that in the category of topological spaces, mono arrows are injective functions; in the category of T_2 topological spaces, a continuous function $f \colon X \to Y$ is epi if and only if $\operatorname{ran}(f)$ is dense in Y.

(iii) Consider the monoid $\langle \mathbb{N}, +, 0\rangle$ as a category. Show that all arrows are mono and epi, but only 0 is iso.

Exercise 22.22. Show that the product of two objects (if it exists) is unique up to isomorphism.

Exercise 22.23. Consider an ordered set $\langle P, \leq\rangle$ as a category: the objects are the elements of P and add an arrow $p \to q$ if and only if $p \leq q$. Show that this category has products if and only if $\langle P, \leq\rangle$ is lower semi-lattice and $p \times q = \inf\{p, q\}$.

Exercise 22.24. Show that the category of topological spaces TOP has direct and inverse limits.

Exercise 22.25. Show that an iso arrow is mono and epi and that if $f\colon a \to b$ is iso, then so is $f^{-1}\colon b \to a$.

Exercise 22.26. Verify that the categories of sets, of groups, and of topological spaces admit products.

Notes and remarks

Category theory was invented in 1942 by Samuel Eilenberg (1913–1998) and Saunders Mac Lane (1909–2005) while working in algebraic topology. Our exposition is very short—the interested reader is referred to [**ML98**] and [**Gol84**].

Chapter VI

Elementary mathematics from an advanced perspective

In this Chapter we embark on a thorough study of several important objects in mathematics. Some of these notions were introduced in Chapters I–**??**, and the infusion of set-theoretic techniques from Chapter V will allow us to obtain new insight on these matters.

23. Finite sequences

Recall that ${}^{<\omega}X$ the set of all finite sequences of elements of X with the concatenation operation is the free monoid on X. We say that $u, v \in {}^{<\omega}X$ are **compatible** $u \subseteq v \vee v \subseteq u$. Then

$$u^\frown v \text{ and } u'^\frown v' \text{ compatible} \Rightarrow u \text{ and } u' \text{ compatible} \tag{23.1a}$$

$$u^\frown v \text{ and } u^\frown v' \text{ compatible} \Rightarrow v \text{ and } v' \text{ compatible.} \tag{23.1b}$$

23.A. Expressions. Given a set of symbols and a function assigning an arity to each symbol, we can form the set of all expressions. More formally:

Definition 23.1. The set $\mathrm{Expr} = \mathrm{Expr}(S, a)$ of all **expressions** on $\langle S, a\rangle$, where $a\colon S \to \omega$ and $S \neq \emptyset$, is the smallest $W \subseteq {}^{<\omega}S$ containing

$$\{\langle s\rangle \mid s \in S \wedge a(s) = 0\} \tag{23.2}$$

and closed under the operation

$$s \in S \wedge w_1, \dots, w_m \in W \wedge a(s) = m \Rightarrow \langle s\rangle^\frown w_1{}^\frown \dots {}^\frown w_m \in W.$$

Definition 23.1 can cause a small, yet annoying, notational problem. Suppose that $*, s, t \in S$ with $a(s) = a(t) = 0$ and $a(*) = 2$, and suppose that $s = \langle x \rangle$ and $t = \langle y \rangle$. Then $s * t$ is the string $\langle *, \langle x \rangle, \langle y \rangle \rangle$, even if it would be more natural to write it as $\langle *, x, y \rangle$. For this reason we stipulate the following

Convention 23.2. If $a\colon S \to \omega$ and every $s \in S$ with $a(s) = 0$ is a sequence of length 1, then in the definition of $\operatorname{Expr}(S, a)$ we replace (23.2) with $\{s \mid s \in S \wedge a(s) = 0\}$.

In other words: if $X = \{x \mid \exists s \in S\, (a(s) = 0 \wedge s = \langle x \rangle)\}$, then letting

$$\overline{S} = (S \setminus \{s \in S \mid a(s) = 0\}) \cup X$$

and letting $\overline{a}\colon \overline{S} \to \omega$ be defined as $\overline{a}(x) = a(\langle x \rangle)$ if $x \in X$ and $\overline{a}(s) = a(s)$ for all other $s \in \overline{S}$, then $\operatorname{Expr}(S, a)$ computed according to our convention is exactly $\operatorname{Expr}(\overline{S}, \overline{a})$ according to Definition 23.1.

The proof of the following result is left to the reader.

Lemma 23.3. *Let $\langle S, a \rangle$ be as above. Then*

(a) $\operatorname{Expr}(S, a) = \bigcup_{S' \in [S]^{<\omega}} \operatorname{Expr}(S', a \restriction S')$.

(b) $\operatorname{Expr}(S, a) = \bigcup_n \operatorname{Expr}_n(S, a)$ *where* $\operatorname{Expr}_0(S, a) = \{\langle s \rangle \mid s \in S \wedge a(s) = 0\}$ *and*

$$\operatorname{Expr}_{n+1}(S, a) = \operatorname{Expr}_n(S, a) \cup \\ \{\langle s \rangle ^\frown w_1 ^\frown \cdots ^\frown w_m \mid s \in S \wedge a(s) = m \wedge \} w_1, \ldots, w_m \in \operatorname{Expr}_n(S, a).$$

Definition 23.4. The **height** of $w \in \operatorname{Expr}(S, a)$ is the least n such that $w \in \operatorname{Expr}_n(S, a)$. The height function is $\operatorname{ht}\colon \operatorname{Expr}(S, a) \to \omega$.

Example 23.5. Given an inductive system $(A, \mathcal{F}, X)$ (Section 7.A.1) set $S = \mathcal{F} \uplus X$ and $a\colon S \to \omega$ where

$$a(s) = \begin{cases} 0 & \text{if } s \in X, \\ \operatorname{ar}(s) & \text{if } s \in \mathcal{F}. \end{cases}$$

With the notation of Lemma 23.3 and the Convention stipulated on page 458, then $\operatorname{Expr}_0 = \{s \mid s \in X \cup C\}$ where $C = \{s \in \mathcal{F} \mid a(s) = 0\}$ and for all $w \in \operatorname{Expr}_{n+1}$ there exist unique $f \in \mathcal{F}$ and $w_1, \ldots, w_m \in \operatorname{Expr}_n$ such that $w = \langle f \rangle ^\frown w_1 ^\frown \ldots ^\frown w_m$. By unique readability for expressions, it is possible to define a map

$$\Phi\colon \operatorname{Expr} \to X$$

$\Phi \restriction \operatorname{Expr}_0 = \operatorname{id} \restriction \operatorname{Expr}_0$ and $\Phi(\langle f \rangle ^\frown w_1 ^\frown \ldots ^\frown w_m) = f(\Phi(w_1), \ldots, \Phi(w_m))$. Let $X_n = \Phi[\operatorname{Expr}_n]$. It is easy to check that $(X_n)_{n \in \omega}$ is the canonical sequence associated to the inductive system $(A, \mathcal{F}, X)$. Thus the closure of $(A, \mathcal{F}, X)$ is the surjective image of a set of expressions. Conversely, any $\operatorname{Expr}(S, a)$ can be seen as the closure under the inductive system $(A, \mathcal{F}, S)$ where $A = S^{<\omega}$, $\mathcal{F} = \{f_s \mid s \in S\}$ and

$$f_s \colon X^{a(s)} \to S, \qquad \big\langle w_1, \ldots, w_{a(s)} \big\rangle \mapsto \langle s \rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_{a(s)}.$$

Lemma 23.6. *If $u_1{}^\frown \ldots {}^\frown u_n$ and $v_1{}^\frown \ldots {}^\frown v_n$ are compatible, where $u_1, \ldots, u_n$, $v_1, \ldots, v_n \in \operatorname{Expr}(S, a)$, then $u_i = v_i$ per $1 \le i \le n$.*

Proof. By induction on $N = \operatorname{lh}(u_1{}^\frown \ldots {}^\frown u_n)$. Let $s \in S$ be the first element of u_1 so that $u_1 = \langle s \rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_k$, where $k = a(s)$ and $w_1, \ldots, w_k \in \operatorname{Expr}(S, a)$. Then s is the first element of the string $v_1{}^\frown \ldots {}^\frown v_n$ hence $v_1 = \langle s \rangle {}^\frown z_1{}^\frown \ldots {}^\frown z_k$, where $z_1, \ldots, z_k \in \operatorname{Expr}(S, a)$. By (23.1a) u_1 and v_1 are compatible, and so are $w_1{}^\frown \ldots {}^\frown w_k$ and $z_1{}^\frown \ldots {}^\frown z_k$. As $\operatorname{lh}(w_1{}^\frown \ldots {}^\frown w_k) < \operatorname{lh}(u_1) \le N$, by inductive assumption $w_i = z_i$ for $1 \le i \le k$, and therefore

$$u_1 = \langle s \rangle {}^\frown w_1{}^\frown \ldots {}^\frown w_k = \langle s \rangle {}^\frown z_1{}^\frown \ldots {}^\frown z_k = v_1.$$

From our assumption and (23.1b) it follows that $u_2{}^\frown \ldots {}^\frown u_n$ and $v_2{}^\frown \ldots {}^\frown v_n$ are compatible, so by inductive assumption $u_i = v_i$ for $2 \le i \le n$. □

Applying Lemma 23.6 with $n = 1$ we get:

Corollary 23.7. $\forall w, v \in \operatorname{Expr}(S, a) \, (w \subseteq v \Rightarrow w = v)$.

These results guarantee that the expressions on a set S can be read in a unique way: given $u \in \operatorname{Expr}(S, a)$ let $s = u(0)$ and $n = a(s)$: if $\operatorname{lh}(u) = 1$ then $n = 0$ and if $\operatorname{lh}(u) > 1$ there are unique $u_1, \ldots, u_n \in \operatorname{Expr}(S, a)$ such that $u = \langle s \rangle {}^\frown u_1{}^\frown \ldots {}^\frown u_n$.

23.B. Occurrences. Recall that for $v, w \in S^{<\omega}$ we say that v occurs in w if there are $u_0, u_1 \in S^{<\omega}$ such that $w = u_0{}^\frown v{}^\frown u_1$. We say that $s \in S$ occurs in $w \in S^{<\omega}$ if $\langle s \rangle$ occurs in w, that is $s \in \operatorname{ran}(w)$.

Definition 23.8. If $v, w \in \operatorname{Expr}(S, a)$ and $v \sqsubseteq w$ we say that v is a **sub-expression of** w. By Corollary 23.7 if $w = u_0{}^\frown v{}^\frown u_1$ and $u_0 = \emptyset$ then $u_1 = \emptyset$. If $v \sqsubseteq w$ and $v \neq w$ then v is a proper sub-expression of w, in symbols $v \sqsubset w$. An **occurrence** of $s \in S$ in $w \in \operatorname{Expr}(S, a)$ is an $n \in \operatorname{dom}(w)$ such that $w(n) = s$. If $s = w(0)$ we say that s occurs in first position of w.

Lemma 23.9. *If $s \in S$ occurs in $w \in \operatorname{Expr}(S, a)$, then every occurrence of s in w is an occurrence in first position of some sub-expression v of w,*

$$w(n) = s \Rightarrow \exists v \in \operatorname{Expr}(S, a) \, \exists u_0, u_1 \in S^{<\omega} \, \big(w = u_0{}^\frown v{}^\frown u_1 \wedge \operatorname{lh}(u_0) = n\big).$$

Proof. By induction on $\operatorname{lh}(w)$. Let n be the occurrence of s in w. If $n = 0$, the result is proved, hence we may assume that $n > 0$. Then $\operatorname{lh}(w) > 1$

and thus $w = \langle s' \rangle ^\frown w_1 {}^\frown \dots {}^\frown w_m$ for some $s' \in S$ with $a(s') = m > 0$ and $w_1, \dots, w_m \in \mathrm{Expr}$. Then the occurrence of s is inside some w_i, so

$$1 + \mathrm{lh}(w_1) + \cdots + \mathrm{lh}(w_{i-1}) \leq n < 1 + \mathrm{lh}(w_1) + \cdots + \mathrm{lh}(w_i).$$

By inductive assumption, the occurrence of s is in the first position of some sub-expression v of w_i and since $v \sqsubseteq w$ the result follows. □

The definition of occurrence can be suitably generalized.

Definition 23.10. If $v, w \in S^{<\omega}$, an **occurrence** of v in w is an *interval of natural numbers*

$$\{k, k+1, \dots, k+n-1\} \subseteq \mathrm{lh}(w)$$

where $n = \mathrm{lh}(v)$ and such that $\forall i < n\, (w(k+i) = v(i))$. If $w = u ^\frown w' {}^\frown z$ we say that the occurrence $\{k, k+1, \dots, k+n-1\}$ is contained in w' if $\mathrm{lh}(u) \leq k$ and $k + n - 1 < \mathrm{lh}(u) + \mathrm{lh}(w')$.

For example the occurrences of $v = \langle s, s \rangle$ in $w = \langle s, s, s \rangle$ are $\{0, 1\}$ and $\{1, 2\}$, showing that occurrences need not be disjoint intervals. The result guarantees that this problem disappear for expressions.

Theorem 23.11. *Suppose that $v \sqsubset w$ where $v, w \in \mathrm{Expr}(S, a)$.*

(a) *If $w = \langle s \rangle ^\frown w_1 {}^\frown \dots {}^\frown w_n$, where $w_1, \dots, w_n \in \mathrm{Expr}(S, a)$, then $v \sqsubseteq w_i$ for some $1 \leq i \leq n$.*

(b) *The occurrences of v in w are pairwise disjoint. Therefore there exist unique $u_0, \dots, u_k \in S^{<\omega}$ such that*

$$w = u_0 {}^\frown v ^\frown u_1 {}^\frown \dots {}^\frown v ^\frown u_k \quad \text{and} \quad \forall i \leq k\ (v \not\sqsubseteq u_i)\,.$$

Proof. (a) Fix u_0, u_1 such that $w = u_0 {}^\frown v ^\frown u_1$. By Corollary 23.7 $u_0 \neq \emptyset$. Thus the occurrence $v(0)$ is inside some w_i hence by Lemma 23.9 is in the first position of some sub-expression $\tilde{v} \sqsubseteq w_i$. As v and $\tilde{v}$ are compatible, by Corollary 23.7 $v = \tilde{v}$.

(b) By induction on $\mathrm{lh}(w)$. Let I, J be two occurrences of v in w. By part (a) there are $1 \leq i, j \leq n$ such that the occurrence I is in w_i and the occurrence J is in w_j: if $i \neq j$ then I and J are disjoint, if $i = j$ we apply the inductive hypothesis. □

We now introduce an auxiliary notion: if $w = \langle s \rangle ^\frown v_1 {}^\frown \dots {}^\frown v_m$ and $v = v_j$ for some $1 \leq j \leq m$, write $v \prec w$. Clearly if $v \prec w$ then $v \sqsubset w$, but not conversely. The next result shows that $\sqsubset$ is the transitive closure (see page 43) of $\prec$.

Proposition 23.12. *For each $v, w \in \mathrm{Expr}$*

$$v \sqsubset w \Leftrightarrow \exists k > 0\, \exists z_0, \dots, z_k \in \mathrm{Expr}\ (v = z_0 \prec z_1 \prec \cdots \prec z_k = w)\,.$$

Proof. As $\sqsubset$ extends $\prec$, it is enough to show the $\Rightarrow$ direction. We show by induction on n that if $w \in \mathrm{Expr}_n$

$$\forall v \in \mathrm{Expr}\,\bigl(v \sqsubset w \Rightarrow \exists k > 0\,\exists z_0, \dots, z_k \in \mathrm{Expr}\,(v = z_0 \prec \cdots \prec z_k = w)\bigr).$$

When $n = 0$ there is nothing to prove, so we may assume that the result holds for some n and that $w \in \mathrm{Expr}_{n+1}$ and $v \sqsubset w$. Then

$$w = \langle s\rangle^\frown w_1{}^\frown \dots {}^\frown w_m = u_0{}^\frown v^\frown u_1.$$

If $u_0 = \emptyset$ then $v \subseteq w$ hence by Corollary 23.7 $v = w$, against our assumption. Therefore the first occurrence $v(0)$ in v is not the s at the first position of w and by Lemma 23.9 it is the first occurrence of an expression $\tilde{v}$ with $\tilde{v} \sqsubseteq w_i$, for some $1 \le i \le m$. But then v and $\tilde{v}$ are compatible, and again by Corollary 23.7 they coincide, and hence $v \sqsubseteq w_i$. If $v = w_i$ the result follows at once, so we may assume that $v \sqsubset w_i$. By inductive hypothesis there are $z_0, \dots, z_k$ such that $v = z_0 \prec \cdots \prec z_k = w_i$ and since $w_i \prec w$, the result is proved. □

23.C. Substitution. Suppose $\langle S, a\rangle$ are as above. If $s_1, \dots, s_n \in S$ are distinct and $w \in S^{<\omega}$, then

$$w = u_0{}^\frown \langle s_{i_1}\rangle^\frown u_1{}^\frown \langle s_{i_2}\rangle^\frown u_2{}^\frown \dots {}^\frown \langle s_{i_m}\rangle^\frown u_m$$

where $\{i_1, \dots, i_m\} \subseteq \{1, \dots, n\}$, $u_0, \dots, u_m \in S^{<\omega}$ and s_{i_j} does not occur in u_k. Let $w, v_1, \dots, v_n \in \mathrm{Expr}(S, a)$ with $v_1, \dots, v_n$ distinct and such that $v_i \not\sqsubseteq v_j$ for $1 \le i, j \le n$ and $i \ne j$. Then there exist (and are unique by Theorem 23.11) $u_0, \dots, u_m \in S^{<\omega}$ such that

$$w = u_0{}^\frown v_{i_1}{}^\frown u_1{}^\frown v_{i_2}{}^\frown u_2{}^\frown \dots {}^\frown v_{i_m}{}^\frown u_m$$

with $\{i_1, \dots, i_m\} \subseteq \{1, \dots, n\}$ and $v_i \not\sqsubseteq u_j$ for all $1 \le i \le n$ and $j \le m$. If $z_1, \dots, z_n$ are expressions (not necessarily distinct), then the **expression obtained by substituting** $v_1, \dots, v_n$ **in** w **with** $z_1, \dots, z_n$ is

$$w[z_1/v_1, \dots, z_n/v_n] = u_0{}^\frown z_{i_1}{}^\frown u_1{}^\frown z_{i_2}{}^\frown u_2{}^\frown \dots {}^\frown z_{i_m}{}^\frown u_m.$$

In particular, $w[z_1/v_1, \dots, z_n/v_n] = w[z_{j_1}/v_{j_1}, \dots, z_{j_k}/v_{j_k}]$ where $\{j_1, \dots, j_k\}$ is the set of all indices $1 \le j \le n$ such that $v_j \sqsubseteq w$.

Note that the substitutions must be performed simultaneously for all expressions $v_1, \dots, v_n$—in general $w[z_1/v_1, z_2/v_2] \ne (w[z_1/v_1])[z_2/v_2]$.

23.D. Trees.

Definition 23.13. A **tree** is an ordered set $\langle T, \trianglelefteq\rangle$, whose elements are called **nodes**, such that $\mathrm{pred}(x, T; \triangleleft) = \{y \in T \mid y \triangleleft x\}$ is well-ordered, for each $x \in T$. Equivalently: $\trianglelefteq$ is well-founded on T and $\mathrm{pred}(x)$ is linearly ordered, for every node x. A node is **terminal** if it has no immediate successors; it is **splitting** if it has more than one immediate successors. If every node has a finite number of immediate successors, we will say that T is **finitely branching**. A **branch** is a maximal chain of T. The **height** $\mathrm{ht}_T \colon T \to \mathrm{Ord}$ is the rank function for $\langle T, \trianglelefteq \rangle$, that is $\mathrm{ht}_T(x) = \mathrm{ot}(\mathrm{pred}(x))$. The ordinal $\mathrm{ht}(T) \overset{\text{def}}{=} \mathrm{ran}(\mathrm{ht}_T)$ is called **height of** T. The α-th **level** of T is

$$\mathrm{Lev}_\alpha(T) = \{x \in T \mid \mathrm{ht}_T(x) = \alpha\} .$$

A node of $\mathrm{Lev}_0(T)$ is a **root** of T.

The next result is known as **König's Lemma**.

Lemma 23.14. *Let $\langle T, \trianglelefteq \rangle$ be a finitely branching tree with finitely many roots. Suppose there is an order $\leq$ on T which is total on every $\mathrm{Lev}_n(T)$, for $n \in \omega$. Then T is infinite if and only if T has an infinite chain.*

Proof. It is enough to show that if T is infinite, then it contains an infinite chain. For $t \in T$ the set $T_{[t]} \overset{\text{def}}{=} \{u \in T \mid t \trianglelefteq u\}$ is a tree with the induced ordering. By recursion on n construct $t_n \in \mathrm{Lev}_n(T)$ so that

(A) $t_n \triangleleft t_{n+1}$ and

(B) $T_{[t_n]}$ is infinite.

Since $T = \bigcup \bigl\{T_{[t]} \mid t \in \mathrm{Lev}_0(T)\bigr\}$ is infinite and $\mathrm{Lev}_0(T)$, the set of all roots of T, is finite, there is a $t_0 \in \mathrm{Lev}_0(T)$ such that $T_{[t_0]}$ is infinite. Suppose we have constructed t_i for $i \leq n$ and that (A) and (B) are fulfilled: since $T_{[t_n]} = \{t_n\} \cup \bigcup_{s \in S_n} T_{[s]}$, where $S_n = \{s \in T \mid s \text{ is an immediate successor of } t_n\}$, and since S_n is finite by assumption, then by (B) there is $t_{n+1} \in S_n$ such that $T_{[t_{n+1}]}$ is infinite. Therefore (A) and (B) are witnessed by t_{n+1}.

The choice of the t_ns does not require AC. In fact $\mathrm{Lev}_0(T)$ and the S_ns are finite hence well-ordered by $<$, therefore we can choose t_n as the $<$-least node satisfying the requirements. □

Corollary 23.15. *Assume T is a well-orderable finitely branching tree of height ω, with finitely many roots. Then T has an infinite chain.*

23.D.1. *Descriptive trees.*

Definition 23.16. A **descriptive tree on a set** $X \neq \emptyset$ is a $T \subseteq X^{<\omega}$ such that $\forall t \in T \, \forall n \in \omega \, (t \restriction n \in T)$. A **branch** of T is a function $b \colon \omega \to X$ such that $\forall n \in \omega \, (b \restriction n \in T)$.

A descriptive tree T ordered by inclusion is tree in the sense of Definition 23.13, with $\langle\rangle$ the unique root of T. Theorem 18.31 shows that $X^{<\omega}$ is well-orderable when X so is. Therefore Corollary 23.15 for descriptive trees is:

Corollary 23.17. *If T is a finitely branching descriptive tree on a well-orderable set X, then T is infinite if and only if T has a branch.*

Suppose $T \neq \emptyset$ is a descriptive tree on some set $X \neq \emptyset$ without terminal nodes, that is to say: for every $t \in T \subseteq X^{<\omega}$ there is $u \in T$ such that $t \subset u$. Thus starting with the empty sequence one can construct a branch step-by-step, but this procedure requires the axiom of dependent choices.

Theorem 23.18. *Let X be a non-empty set. Then $\mathsf{DC}(X^{<\omega})$ implies that "every descriptive tree on X without terminal nodes has a branch" which in turn implies $\mathsf{DC}(X)$. Therefore DC is equivalent to the fact that every descriptive tree without terminal nodes has a branch.*

Proof. Assume $\mathsf{DC}(X^{<\omega})$ and suppose T is a descriptive tree on X without terminal nodes. Let R be the relation on T defined by

$$u \mathrel{R} t \Leftrightarrow s \subseteq t \wedge \mathrm{lh}(s) + 1 = \mathrm{lh}(t).$$

As $T \subseteq X^{<\omega}$ we can apply $\mathsf{DC}(X^{<\omega})$ and obtain $f\colon \omega \to T$ such that $f(0) = \langle\rangle$ and $f(n) \mathrel{R} f(n+1)$ for all n. Thus $\bigcup_{n\in\omega} f(n)$ is a branch of T.

Assume that every descriptive tree on X without terminal nodes has a branch, and let $R \subseteq X \times X$ be such that $\forall x \in X \, \exists y \in X \, (x \mathrel{R} y)$. Fix an element $x_0 \in X$ and let T be the descriptive tree of attempts to build a sequence $\langle x_n \mid n \in \omega\rangle$ such that $x_n \mathrel{R} x_{n+1}$, that is

$$T = \{u \in X^{<\omega} \mid u(0) = x_0 \wedge \forall i + 1 < \mathrm{lh}\, u \, (u(i) \mathrel{R} u(i+1))\}.$$

Clearly T is a descriptive tree on X, and it has no terminal nodes by our assumption on R. Any branch of T witnesses $\mathsf{DC}(X)$ for R and x_0. □

23.D.2. *Labelled trees.* A descriptive tree T on some ordinal γ is **gapless** if

$$\forall \alpha, \beta \in \gamma \, \forall s \in {}^{<\omega}\gamma \, (\alpha < \beta \wedge s^\frown\langle\beta\rangle \in T \Rightarrow s^\frown\langle\alpha\rangle \in T).$$

Every finite tree with one root is isomorphic to a unique gapless tree on some $n \in \omega$ (Exercise 23.21)—for example the tree of Figure 2 on page 24 is isomorphic to the tree on $3 = \{0, 1, 2\}$ of Figure 24. A **labelled tree** on a set $S \neq \emptyset$ is a tree finite gapless T on ω, together with a function $L\colon T \to S$, the **labelling of** T. A labelled tree on $\langle S, a\rangle$ where $a\colon S \to \omega$ is a labelled tree on S such that for all $t \in T$

$$a(L(t)) = |\{s \mid s \text{ is an immediate successor of } t\}|\,.$$

For example the tree of Figure 3 on page 28 can be seen as a labelled tree by taking a tree on 3 described above, labelled as follows: $L(\langle\rangle) = h$, $L(\langle 0\rangle) = f$, $L(\langle 1\rangle) = g$, $L(\langle 2\rangle) = f$, etc. Thus labelled trees can be used to capture the notion of syntactic tree seen in Section 3. The set of all labelled trees on $\langle S, a\rangle$ is $\mathrm{LTr}(S, a)$.

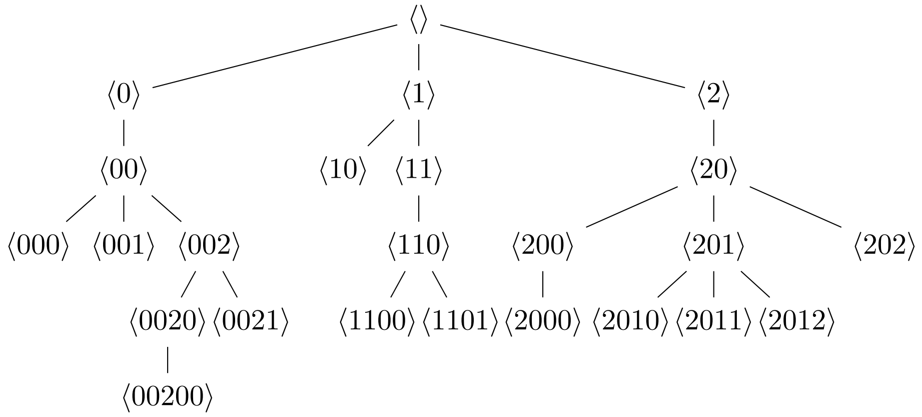


Figure 24. A gapless tree on the ordinal 3

Exercises

Exercise 23.19. Suppose $w \in \mathrm{Expr}(S, a)$. Show that

(i) $w[z_1/v_1, \ldots, z_n/v_n] \in \mathrm{Expr}(S, a)$ if $z_1, \ldots, z_n, v_1, \ldots, v_n \in \mathrm{Expr}(S, a)$ and the $v_1, \ldots, v_n$ are distinct;

(ii) $\mathrm{ht}(w) = \max\{\mathrm{ht}(z) \mid z \sqsubset w\} + 1$.

Exercise 23.20. Given $a\colon S \to \omega$ let $\hat{a}\colon S^{<\omega} \to \mathbb{Z}$ be defined by $\hat{a}(\emptyset) = 0$ and $\hat{a}(\langle s_0, \ldots, s_n\rangle) = \sum_{i \le n} (a(s_i) - 1)$. Show that $\forall u \in S^{<\omega} \, [u \in \mathrm{Expr}(S, a) \Leftrightarrow \hat{a}(u) = -1 \wedge \forall v \subset u \, (\hat{a}(v) \geq 0)]$.

Exercise 23.21. Show that every finite tree with a single root is isomorphic to a gapless tree on some $n \in \omega$.

Exercise 23.22. Show that

(i) $\mathrm{LTr}(S, a) = \bigcup_n \mathrm{LTr}_n(S, a)$ where $\mathrm{LTr}_0(S, a) = \{\langle s\rangle \mid s \in S \wedge a(s) = 0\}$ and

$$\begin{aligned} \mathrm{LTr}_{n+1}(S, a) = {} & \mathrm{LTr}_n(S, a) \cup \\ & \{\langle s, t_1, \ldots, t_m\rangle \mid s \in S \wedge a(s) = m \wedge t_1, \ldots, t_m \in \mathrm{LTr}_n(S, a)\}; \end{aligned}$$

(ii) there is a height-preserving bijection $\mathrm{Expr}(S, a) \to \mathrm{LTr}(S, a)$, where $\mathrm{ht}\colon \mathrm{LTr}(S, a) \to \omega$ is defined by $\mathrm{ht}(t) = \min\{n \in \omega \mid t \in \mathrm{LTr}_n\}$.

Exercise 23.23. Show that:

(i) There is a **universal** $f \in {}^{\omega}2$ that is $\forall s \in {}^{<\omega}2 \, \exists u \in {}^{<\omega}2 \, \big(u^\frown s \subseteq f\big)$.

(ii) If $f \in {}^{\omega}2$ is universal, then every finite sequence occurs infinitely often, that is $\forall n \in \omega \, \forall s \in {}^{<\omega}2 \, \exists u \in {}^{<\omega}2 \, \bigl(\mathrm{lh}\, u \geq n \wedge u^\frown s \subseteq f\bigr)$.

(iii) If $f \in {}^{\omega}2$ is universal, then $\langle \mathbb{Z}, E \rangle$ is a random graph, where $n \mathrel{E} m \Leftrightarrow f(|n - m|) = 1$;

(iv) $\mathrm{Aut}(\mathrm{R}_\omega)$ has elements of order 2 and elements of infinite order.

Exercise 23.24. Show that

(i) if $\langle T, \trianglelefteq \rangle$ is a tree, then $\mathrm{ht}(T) = \min \{\alpha \mid \mathrm{Lev}_\alpha(T) = \emptyset\}$,

(ii) every branch b of a tree $\langle T, \triangleleft \rangle$ is well-ordered by $\triangleleft$ and $\mathrm{ot}(b)$ coincides with its height $\mathrm{ht}(b)$. The ordinal $\mathrm{ot}(b)$ is the **length** of the branch.

Exercise 23.25. Show that a tree T on some ordinal α is gapless if and only if for every $t \in T$ the set $\bigl\{\nu \in \alpha \mid t^\frown \langle \nu \rangle \in T\bigr\}$ is an ordinal.

Exercise 23.26. The Four Colors Theorem asserts that every finite planar graph is 4-colourable (see Section 10). Use König's Lemma to generalize this to countable graphs.

24. Computable functions

24.A. Relativization.

Definition 24.1. Let $f \colon \mathbb{N}^n \to \mathbb{N}$ be arbitrary with $n \geq 1$. The set of all operations **computable-in-f** is the smallest set $\mathfrak{C}(f)$ of operations on $\mathbb{N}$ containing f, $+$, $\cdot$, $\chi_{\leq}$, and closed under composition and minimization.

By Exercise 24.35 the function f in Definition 24.1 can be taken to be unary. The set $\mathfrak{C}(f)$ consists of all functions which can be computed using f as an oracle. Note that $\mathfrak{C} \subseteq \mathfrak{C}(f)$, and equality holds if and only if $f \in \mathfrak{C}$.

Definition 24.2. Given two operations f and g on $\mathbb{N}$, we say that f **is computable from** g, in symbols $f \leq_{\mathrm{T}} g$, if $\mathfrak{C}(f) \subseteq \mathfrak{C}(g)$.

The relation $f \leq_{\mathrm{T}} g$ is often read "f **is Turing reducible to** g". The naming is in honor of Alan Turing, one of the founders of computability theory, and the attribute *reducible* suggests that the problem of computing f is reduced to the (possibly much harder) problem of computing g. If $A \subseteq \mathbb{N}^n$ and $B \subseteq \mathbb{N}^m$ we say that A **is computable from** f if $\chi_A \colon \mathbb{N}^n \to \{0, 1\}$ is in $\mathfrak{C}(f)$, and A **is computable from** B if A is computable from χ_B, in symbols $A \leq_{\mathrm{T}} B$. By Exercise 24.35 the notion of Turing reduciblity on operations agrees with the one on sets, and $\leq_{\mathrm{T}}$ can be seen as a pre-order either on the set of all operations on $\mathbb{N}$, or else on $\mathscr{P}(\mathbb{N})$. In either case the induced equivalence relation, called **Turing equivalence**, is denoted by $=_{\mathrm{T}}$.

The notions and the results of Section 8 can be extended to this context. A set $A \subseteq \mathbb{N}^k$ is **semi-computable-in-f** if either $A = \emptyset$ or else $A =$

$\{\langle h_1(i), \dots, h_k(i)\rangle \mid i \in \mathbb{N}\}$ for some $h_1, \dots, h_k \in \mathfrak{C}(f)$; equivalently if it is the projection of a computable-in-f subset of $\mathbb{N}^{k+1}$. Every computable-in-f set is semi-computable-in-f, but not conversely; if A and $\mathbb{N} \setminus A$ are semi-computable-in-f, they are computable-in-f.

24.B. Computability in V_ω. The main result (Theorem 24.17) of this section is a characterization of computability in terms of definability over the structure $\langle \mathrm{V}_\omega, \in\rangle$. By Exercise 8.58, every $n \in \mathbb{N} \setminus \{0\}$ can be written in a unique way as $n = 2^{e_0} + \dots + 2^{e_{k(n)}}$ with distinct e_is, and the predicate $\mathfrak{E} \subseteq \mathbb{N} \times \mathbb{N}$,

$$\mathfrak{E}(e, n) \Leftrightarrow n > 0 \land \exists i \leq k(n)\, (e = e_i) \tag{24.1}$$

is elementary computable. By Exercise 19.43

$$\mathfrak{a} \colon \mathrm{V}_\omega \to \omega,$$

$\mathfrak{a}(\emptyset) = 0$ and $\mathfrak{a}(\{x_0, \dots, x_k\}) = \sum_{i<k} 2^{\mathfrak{a}(x_i)}$ is a bijection. Observe that if $\mathfrak{E}(e, n)$ then $e < n$ and if $x \in y$ then $\mathfrak{a}(x) < \mathfrak{a}(y)$.

An n**-ary predicate of** V_ω, where $n \geq 1$, is a subset of ${}^n\mathrm{V}_\omega$; as ${}^n\mathrm{V}_\omega \subseteq \mathrm{V}_\omega$ it is simply a subset of V_ω whose elements are functions with domain n. As usual, a unary predicate is identified with a subset of V_ω. Recall from the notion of Δ_0 and Σ_1 formula (Definitions 19.17 and 19.18).

Definition 24.3. An n-ary predicate A of V_ω is Γ**-definable**, where Γ is Δ_0, Σ_1 or Π_1, if

$$A = \{\langle a_1, \dots, a_n\rangle \in \mathrm{V}_\omega \mid \mathrm{V}_\omega \vDash \varphi[a_1, \dots, a_n]\}$$

with $\varphi(x_1, \dots, x_n)$ a Γ-formula. If A is both Σ_1-definable and Π_1-definable then we say it is Δ_1**-definable**.

A function $f \colon A \to \mathrm{V}_\omega$ with A an n-ary predicate of V_ω is Γ-definable (with Γ one of Δ_0, Σ_1, Π_1, Δ_1) if the $n+1$-ary predicate $\{\langle a_1, \dots, a_n, b\rangle \mid f(a_1, \dots, a_n) = b\}$ is Γ-definable.

Lemma 24.4. *If $\varphi(x_1, \dots, x_n, y_1, y_2)$ is Δ_0 then*

$$\{\langle a_1, \dots, a_n\rangle \in \mathrm{V}_\omega \mid \mathrm{V}_\omega \vDash \exists y_1, y_2\, \varphi[a_1, \dots, a_n]\}$$

is Σ_1-definable.

Proof. As V_ω is closed under unions and pairing,

$$\mathrm{V}_\omega \vDash \exists y_1, y_2\, \varphi[a_1, \dots, a_n] \Leftrightarrow \mathrm{V}_\omega \vDash \exists u \exists y_1, y_2 \in u\, \varphi[a_1, \dots, a_n]$$

and $\exists y_1, y_2 \in u\, \varphi$ is Δ_0. □

Corollary 24.5. *The collection of all Σ_1-definable predicates is closed under intersections, unions, and projections, i.e. if $A \subseteq \mathrm{V}_\omega$ is a Σ_1-definable $(n+1)$-ary predicate, then $\{\langle a_1, \dots, a_n\rangle \in \mathrm{V}_\omega \mid \exists a_0 \in \mathrm{V}_\omega\, \langle a_0, a_1, \dots, a_n\rangle \in A\}$ is Σ_1-definable.*

Proof. By the prenex normal form algorithm (Section 3.C.4) the conjunction/disjunction of two Σ_1-formulæ $\exists y_1\, \varphi_1$ and $\exists y_2\, \varphi_2$ is of the form $\exists y_1, y_2\, (\varphi_1 \odot \varphi_2)$ where $\odot$ is either $\wedge$ or $\vee$, so the result follows from the Lemma 24.4. □

Proposition 24.6. (a) *For each $a \in \mathrm{V}_\omega$ there is a Δ_0-formula $\delta_a(x)$ that defines a in V_ω.*

(b) *Let Γ be either Σ_1 or Π_1. If $A \subseteq \mathrm{V}_\omega$ is Γ-definable with parameters, then it is Γ-definable without parameters.*

Proof. (a) Set

$$\begin{aligned} \delta_\emptyset(x) : &\quad \forall y \in x\, (y \neq y) \\ \delta_a(x) : &\quad \bigl(\exists y_1 \in x \ldots \exists y_n \in x \bigwedge_{1 \le i \le n} \delta_{b_i}(y_i)\bigr) \wedge \forall y \in x \bigvee_{1 \le i \le n} \delta_{b_i}(y), \end{aligned}$$

if $a = \{b_1, \ldots, b_n\} \neq \emptyset$.

(b) Suppose A is defined using the Γ-formula $\varphi(x, y_1, \ldots, y_n)$ together with parameters $p_1, \ldots, p_n \in \mathrm{V}_\omega$. Then

$$\begin{cases} \exists y_1, \ldots, y_n [\bigwedge_{1 \le i \le n} \delta_{p_i}(y_i) \wedge \varphi(x, \vec{y})] & \text{if } \Gamma \text{ is } \Sigma_1, \\ \forall y_1, \ldots, y_n [\bigwedge_{1 \le i \le n} \delta_{p_i}(y_i) \Rightarrow \varphi(x, \vec{y})] & \text{if } \Gamma \text{ is } \Pi_1, \end{cases}$$

is a Γ-formula that defines A in V_ω. □

Therefore the notions of definability in V_ω with or without parameters (Section 4.H) agree.

Lemma 24.7. *If $\varphi(x, y, z_1, \ldots, z_n)$ is a Σ_1 formula then there is a Σ_1 formula $\psi(x, z_1, \ldots, z_n)$ such that*

$$\langle \mathrm{V}_\omega, \in \rangle \vDash \forall x, z_1, \ldots, z_n (\forall y \in x\, \varphi \Leftrightarrow \psi).$$

Proof. Without loss of generality we may assume that φ is $\exists w \bar{\varphi}$ with $\bar{\varphi}$ a Δ_0 formula, and let ψ be $\exists u\, \forall y \in x\, \exists w \in u\, \bar{\varphi}$. We must check that $\forall y \in x\, \exists w\, \bar{\varphi} \Leftrightarrow \exists u\, \forall y \in x\, \exists w \in u\, \bar{\varphi}$ is true in V_ω. Fix $x, z_1, \ldots, z_n \in \mathrm{V}_\omega$ and assume that $\langle \mathrm{V}_\omega, \in \rangle \vDash \forall y \in x\, \exists w\, \bar{\varphi}$. As V_ω is well-ordered via the bijection $\mathfrak{a}$, for each $y \in x$ pick the least w such that $\bar{\varphi}$ holds, and let u be the set of all these ws. Then $u \subseteq \mathrm{V}_\omega$, and since x is finite, then so is u, and hence $u \in \mathrm{V}_\omega$. Therefore $\langle \mathrm{V}_\omega, \in \rangle \vDash \exists u\, \forall y \in x\, \exists w \in u\, \bar{\varphi}$ as required. The reverse implication $\exists u\, \forall y \in x\, \exists w \in u\, \bar{\varphi} \Rightarrow \forall y \in x\, \exists w\, \bar{\varphi}$ is trivial. □

Proposition 24.8. *Suppose $f, g \subseteq \mathrm{V}_\omega$ are Σ_1-definable functions.*

(a) $\operatorname{dom} f$ *and* $\operatorname{ran} f$ *are Σ_1-definable.*

(b) $g \circ f$ *is Σ_1-definable.*

(c) *If* $\operatorname{dom} f$ *is* Δ_1*-definable, then* f *is* Δ_1*-definable; if moreover* $\operatorname{ran} g \subseteq \operatorname{dom} f$ *then* $g \circ f$ *is* Δ_1*-definable.*

Proof. Suppose $\varphi(x, y)$ and $\varphi'(y, z)$ are Σ_1-formulæ with exactly two free variables defining f and g, respectively.

(a) $\operatorname{dom} f$ is defined by $\exists y \varphi(x, y)$, while $\operatorname{ran} f$ is defined by $\exists x \varphi(x, y)$.

(b) $g \circ f$ defined by the formula $\chi(x, z)$ given by $\exists y(\varphi(x, y) \wedge \varphi'(y, z))$.

(c) Suppose $\psi(x)$ is a Π_1-formula defining $\operatorname{dom} f$, and let $\gamma(x, z)$ be the formula $\neg\psi(x) \vee \exists y\, (\varphi(x, y) \wedge y \neq z)$. Then $\gamma(x, z)$ is a Σ_1-formula defining ${}^2\mathrm{V}_\omega \setminus f$, so f is Δ_1-definable.

By part (b) $g \circ f$ is Σ_1-definable, and if $\operatorname{ran} f \subseteq \operatorname{dom} g$ then $\operatorname{dom}(g \circ f) = \operatorname{dom}(f)$ is Δ_1-definable, and so is $g \circ f$. □

Corollary 24.9. *If* $f\colon A \to \mathrm{V}_\omega$ *is* Δ_1*-definable, with* A *an* n*-ary predicate, and the functions* $g_i\colon {}^k\mathrm{V}_\omega \to \mathrm{V}_\omega$ *for* $1 \leq i \leq n$ *are* Σ_1*-definable, then their composition* $A \to \mathrm{V}_\omega$*,* $\langle a_1, \ldots, a_k\rangle \mapsto f(g_1(\vec{a}), \ldots, g_n(\vec{a}))$ *is* Δ_1*-definable.*

Lemma 24.10. *If* A *is* Δ_1*-definable* n*-ary predicate and* $f_1, \ldots, f_n\colon {}^k\mathrm{V}_\omega \to \mathrm{V}_\omega$ *are* Δ_1*-definable, then* $B = \{\langle b_1, \ldots, b_k\rangle \in \mathrm{V}_\omega \mid \langle f_1(\vec{b}), \ldots, f_n(\vec{b})\rangle \in A\}$ *is* Δ_1*-definable.*

Proof. Note that

$$\begin{aligned}
&\langle b_1, \ldots, b_k\rangle \in B\\
&\qquad \Leftrightarrow \exists a_1, \ldots, a_n[f_1(\vec{b}) = a_1 \wedge \cdots \wedge f_n(\vec{b}) = a_n \wedge \langle a_1, \ldots, a_n\rangle \in A]\\
&\qquad \Leftrightarrow \forall a_1, \ldots, a_n[f_1(\vec{b}) = a_1 \wedge \cdots \wedge f_n(\vec{b}) = a_n \Rightarrow \langle a_1, \ldots, a_n\rangle \in A]. \quad \square
\end{aligned}$$

For $\varphi(x_1, \ldots, x_n)$ a formula of $\mathcal{L}_\in$, set

$$D_{\varphi(x_1,\ldots,x_n)} = \{\langle k_1, \ldots, k_n\rangle \in \mathbb{N}^n \mid \mathrm{V}_\omega \vDash \varphi[\mathfrak{a}(k_1), \ldots, \mathfrak{a}(k_n)]\}.$$

Proposition 24.11. (a) *Every* $f \in \mathfrak{C}$ *is* Δ_1*-definable in* V_ω*.*

(b) *If* $A \subseteq \mathbb{N}^n$ *is semi-computable then it is* Σ_1*-definable; if it is computable then it is* Δ_1*-definable.*

Proof. (a) We must show that $\mathfrak{C} \subseteq \mathcal{F}$, where $\mathcal{F}$ is the collection of all $f\colon \mathbb{N}^k \to \mathbb{N}$ that are Δ_1-definable in V_ω. Since $\mathcal{F}$ is closed under composition and $I^n_k, +, \cdot, \boldsymbol{\chi}_\leq$ belong to it, it is enough to show that $\mathcal{F}$ is closed under minimization. Suppose $g\colon \mathbb{N}^{k+1} \to \mathbb{N}$ is in $\mathcal{F}$ and that for all $\vec{a} \in \mathbb{N}^k$ there is $b \in \mathbb{N}$ such that $g(\vec{a}, b) = 0$; we must show that $f\colon \mathbb{N}^k \to \mathbb{N}$, $\vec{a} \mapsto \boldsymbol{\mu} b\, (g(\vec{a}, b) = 0)$, is in $\mathcal{F}$. Choose formulæ $\varphi_i(\vec{x}, y, z)$ $(i = 0, 1)$ that define f, with φ_0 in Σ_1 and φ_1 in Π_1. Assigning 0 to the variable z, the formula

$$\chi_i(\vec{x}, y, z) \;:\quad \varphi_i \wedge \forall y' \in y\, \neg\varphi_{1-i}(\!|y'/y|\!)$$

defines f in V_ω, so it is enough to show that χ_0 is Σ_1 and χ_1 is Π_1. By Lemma 24.7 $\forall y' \in y \neg\varphi_1(\!|y'/y|\!)$ is Σ_1, so χ_0 is the conjunction of two Σ_1 formulæ, and hence Σ_1. The formula $\forall y' \in y \neg\varphi_0(\!|y'/y|\!)$ is Π_1, so χ_1 is Π_1.

(b) For notational simplicity set $n = 1$. If $A = \emptyset$ then it is defined by the Δ_0-formula $x \neq x$, so we may assume that $A = \operatorname{ran} f$ with $f \colon \mathbb{N} \to \mathbb{N}$ computable. If $\varphi(x, y)$ is a Σ_1-formula defining f, then $\exists x \varphi$ defines A. □

Lemma 24.12. *If $\varphi(x_1, \dots, x_n)$ is Δ_0 then $D_{\varphi(x_1,\dots,x_n)}$ is computable; in fact it is in $\mathcal{E}$.*

Proof. By Exercise 19.43 the set $\mathfrak{E} = D_{x\in y}$ in (??) is elementary, and so is $D_{x=y}$. If $D_{\varphi(y,x_1,\dots,x_n)}$ is elementary, then

$$D_{\exists y \in x_1 \varphi} = \bigl\{\langle k_1, \dots, k_n\rangle \in \mathbb{N}^n \mid \exists m < k_1 \, [\langle m, k_1\rangle \in \mathfrak{E} \\ \wedge \langle m, k_1, \dots, k_n\rangle \in D_{\varphi(y,x_1,\dots,x_n)}]\bigr\}$$

is elementary. Since elementary predicates are closed under Boolean combinations, the result follows. □

Theorem 24.13. *If $\varphi(x_1, \dots, x_n)$ is Σ_1, then $D_{\varphi(x_1,\dots,x_n)}$ is semi-computable.*

Proof. Let Γ be the set of all $\varphi(x_1, \dots, x_n)$ such that $D_{\varphi(x_1,\dots,x_n)}$ is semi-computable. By Lemma 24.12 and the fact that every computable set is semi-computable, every Δ_0-formula is in Γ. The set Γ is closed under conjunctions and disjunctions since the collection of all semi-computable sets is closed under intersections and unions. Moreover if $\psi(y, x_1, \dots, x_n)$ is in Γ, then $\exists y \psi(y, x_1, \dots, x_n)$ is in Γ since

$$D_{\exists y\psi(y,x_1,\dots,x_n)} = \{\langle m_1, \dots, m_n\rangle \in \mathbb{N}^n \mid \exists k \, \bigl(\langle k, m_1, \dots, m_n\rangle \in D_{\psi(y,x_1,\dots,x_n)}\bigr)\}$$

and the projection of a semi-computable set is semi-computable (Theorem **??**). Therefore every Σ_1-formula is in Γ. □

Corollary 24.14. *Let A be an n-ary predicate of V_ω and let*

$$B = \{\langle k_1, \dots, k_n\rangle \mid \langle \mathfrak{a}(k_1), \dots, \mathfrak{a}(k_n)\rangle \in A\}.$$

If A is Σ_1-definable then B is semi-computable; if A is Δ_1-definable then B is computable.

Theorem 24.15. *The function $\mathfrak{a} \colon \omega \to \mathrm{V}_\omega$ is Δ_1-definable.*

Proof. As $\omega = \operatorname{dom} \mathfrak{a}$ is Δ_1-definable in V_ω, by Proposition 24.8(c) it is enough to check Σ_1-definability of $\mathfrak{a}$ in V_ω. We have that $\mathfrak{a}(n) = x$ if and only if

$$\begin{aligned}\exists s \in \mathrm{V}_\omega \big[&s \text{ is a function with } n+1 \subseteq \mathrm{dom}(s) \text{ such that}\\ &s(0)=\emptyset,\ s(n)=x \text{ and } \forall i \leq n\,(\forall y \in s(i)\,\exists j \in i\,(E(i,j)=1\\ &\qquad\wedge s(j)=y)\ \wedge\ \forall j \in i\,(E(i,j)=1 \Rightarrow s(j) \in s(i)))\big]\end{aligned}$$

where E is the function of (24.1). As E is computable, there are Δ_0-formulæ $\varphi(t,x,y,z)$ and $\varphi'(t,x,y,z)$ such that $\exists t\,\varphi$ and $\forall t\,\varphi'$ define E in V_ω, so the following Σ_1-formula defines '$\mathfrak{a}(n)=x$' in V_ω:

$$\begin{aligned}\exists s,t_1,t_2,m\Big[&\mathsf{Fn}(s)\wedge \mathsf{Ord}(m)\wedge m=\mathbf{S}(n)\wedge m\subseteq \mathrm{dom}\,s\\ &\wedge(\emptyset,\emptyset)\in s\wedge(n,x)\in s\wedge\forall i\in m\,\big(\forall y\in s(i)\,\exists j\in i\,(\varphi(t_1,i,j,1)\\ &\qquad\wedge(j,y)\in s)\wedge\forall j\in i\,(\varphi'(t_2,i,j,1)\Rightarrow s(j)\in s(i))\big)\Big].\quad\square\end{aligned}$$

Proposition 24.16. (a) *Let $A \subseteq \mathbb{N}^n$: if A is Σ_1-definable, then A is semi-computable, if it is Δ_1-definable, then A is computable.*

(b) *If $f\colon \mathbb{N}^n \to \mathbb{N}$ is Δ_1-definable, then $f \in \mathfrak{C}$.*

Proof. (a) Suppose $A \subseteq \mathbb{N}^n$ is Σ_1-definable. By Theorem 24.13 $\tilde{A} = \{s \in \tilde{\mathbb{N}}^n \mid \langle \mathfrak{a}(s_0),\dots,\mathfrak{a}(s_{n-1})\rangle \in A\}$ is a semi-computable subset of $\mathbb{N}^n$, and therefore $A = \{s \in \mathbb{N}^n \mid \langle j(s_0),\dots,j(s_{n-1})\rangle \in \tilde{A}\}$ is a semi-computable subset of $\mathbb{N}^n$ (Exercise **??**). The case when A is Δ_1-definable follows now from Theorem **??**.

(b) Suppose $f\colon \mathbb{N}^n \to \mathbb{N}$ is Δ_1-definable. By part (a) f is a computable subset of $\mathbb{N}^{n+1}$, thus $f \in \mathfrak{C}$ by Lemma 8.26. □

If $A \subseteq \mathrm{V}_\omega$ is infinite, then let $e_A\colon \omega \to \mathfrak{a}^{-1}[A]$ be the enumerating function. Let $f\colon A^k \to A$ be an n-ary operation on A. The **copy of** f **on** $\mathbb{N}$ **via** $\mathfrak{a}$ is the operation $g\colon \mathbb{N}^k \to \mathbb{N}$ defined by

$$g(n_1,\dots,n_k) = (\mathfrak{a}\circ e_A)^{-1}\Big(f\big(\mathfrak{a}\circ e_A(n_1),\dots,\mathfrak{a}\circ e_A(n_k)\big)\Big).$$

Similarly, the copy of $f\colon A \to B$ on $\mathbb{N}$ via $\mathfrak{a}$ is $(\mathfrak{a}\circ e_B)^{-1}\circ f\circ\mathfrak{a}\circ e_A$. The next theorem summarizes the results proved so far.

Theorem 24.17. (a) *Let $f\colon \mathbb{N}^k \to \mathbb{N}$ and let $A \subseteq \mathbb{N}^k$. Then $f \in \mathfrak{C}$ iff f is Δ_1-definable; A is semi-computable if and only if A is Σ_1-definable, and therefore A is recursive if and only if A is Δ_1-definable.*

(b) *Suppose $A, B \subseteq \mathrm{V}_\omega$ are infinite. If $f\colon A \to B$ is Δ_1-definable, then its copy on $\mathbb{N}$ via $\mathfrak{a}$ is in $\mathfrak{C}$; if the operation $f\colon A^k \to A$ is Δ_1-definable, then its copy on $\mathbb{N}$ via $\mathfrak{a}$ is in $\mathfrak{C}$.*

In view of all this, we say that any set or function contained in V_ω is **computable** if it is Δ_1-definable.

Proposition 24.18. *Let $\boldsymbol{E}\colon \omega \to \omega$ be the iterated exponential defined by $\boldsymbol{E}(0) = 0$ and $\boldsymbol{E}(n+1) = 2^{\boldsymbol{E}(n)}$. Then*

$$\forall n \in \omega \ (\mathfrak{a}(\boldsymbol{E}(n+1)-1) = \{\mathfrak{a}(i) \mid i < \boldsymbol{E}(n)\} = \mathrm{V}_n)\,.$$

Proof. The result is immediate when $n = 0$. Assume the result holds for some n towards proving it for $n+1$. If $x \subseteq \mathrm{V}_n$ then $x = \{\mathfrak{a}(j) \mid j \in J\}$ for some $J \subseteq \boldsymbol{E}(n)$, and hence $\mathfrak{a}^{-1}(x) = \sum_{j\in J} 2^j \leq \sum_{j<\boldsymbol{E}(n)} 2^j = 2^{\boldsymbol{E}(n)} - 1 = \boldsymbol{E}(n+1) - 1$. Therefore $\mathrm{V}_{n+1} \subseteq \{\mathfrak{a}(j) \mid j < \boldsymbol{E}(n+1)\}$, and the inclusion can be replaced by equality, as $|\mathrm{V}_{n+1}| = \boldsymbol{E}(n+1)$. For the other equality note that

$$\mathfrak{a}^{-1}(\mathrm{V}_{n+1}) = \sum_{x\in \mathrm{V}_{n+1}} 2^{\mathfrak{a}^{-1}(x)} = \sum_{j<\boldsymbol{E}(n+1)} 2^j = 2^{\boldsymbol{E}(n+1)} - 1. \qquad \square$$

Corollary 24.19. *The maps $n \mapsto \mathrm{V}_n$, $x \mapsto \mathscr{P}(x)$, and $(x,y) \mapsto {}^x y$ are Δ_1-definable in V_ω.*

Proof. The function $n \mapsto \boldsymbol{E}(n) - 1$ is computable, and hence Δ_1-definable. Therefore $n \mapsto \mathrm{V}_n$ is composition of Δ_1-definable functions.

Note that $y = \mathscr{P}(x)$ just in case $\forall z \in y\, (z \subseteq x) \wedge \exists n\, \varphi(n, \mathrm{V}_n, y)$ where $\varphi(n, z, y)$ is $\mathsf{Ord}(n) \wedge \forall w \in z\, (w \subseteq x \Rightarrow w \in y)$. Similarly ${}^x y = z$ if and only if $\exists n \left[x, y \in \mathrm{V}_n \wedge \forall f \in z\, (f\colon x \to y) \wedge \forall f \in \mathrm{V}_{n+3}\, (f\colon x \to y \Rightarrow f \in z)\right]$. $\square$

Remark 24.20. We can define the notion of being Δ_1-definable in the structure $\langle \mathrm{V}_\omega, \in, X\rangle$, where $X \subseteq \mathrm{V}_\omega$. It turns out that $g \in \mathfrak{C}(f)$ if and only if g is Δ_1-definable in $\langle \mathrm{V}_\omega, \in, X\rangle$ where X is (the graph of) f.

24.C. Computable operations on strings*. Using the techniques developed in Section 24.B, it is easy to show that many constructions in finite combinatorics are indeed computable.

Proposition 24.21. (a) *If $X \subseteq \mathrm{V}_\omega$ is Δ_1-definable, then so is ${}^{<\omega}X$.*

(b) *The binary operation on ${}^{<\omega}\mathrm{V}_\omega$, $(u,v) \mapsto u^\frown v$, is Δ_1-definable.*

(c) *If $X \subseteq \mathrm{V}_\omega$ is Δ_1-definable, then the ordering $\sqsubseteq$ on ${}^{<\omega}X$ is Δ_1-definable.*

(d) *Suppose $Z \subseteq \mathrm{V}_\omega$ is Δ_1-definable, and let $f\colon Z \to \mathrm{V}_\omega$ and $F\colon \omega \times Z \times \mathrm{V}_\omega \to \mathrm{V}_\omega$ be Σ_1-definable. Then $G\colon \omega \times Z \to \mathrm{V}_\omega$, defined by $G(0,z) = f(z)$ and $G(n+1,z) = F(n,z,G(n,z))$ is Δ_1-definable.*

(e) *The concatenating function*

$$\mathrm{Cnc}\colon {}^{<\omega}({}^{<\omega}\mathrm{V}_\omega) \to {}^{<\omega}\mathrm{V}_\omega, \quad \mathrm{Cnc}(\langle u_0, \ldots, u_{n-1}\rangle) = u_0{}^\frown \cdots {}^\frown u_{n-1},$$

is Δ_1-definable.

(f) *If $S \in \mathrm{V}_\omega$ and $a\colon S \to \omega$, then $\mathrm{Expr}(S,a)$ is Δ_1-definable. In fact the result holds uniformly: $\{\langle S, a, w\rangle \mid w \in \mathrm{Expr}(S,a)\}$ is Δ_1-definable.*

Proof. (a) $u \in {}^{<\omega}X \Leftrightarrow \mathsf{Fn}(u) \wedge \mathrm{dom}(u) \in \omega \wedge \forall i \in \mathrm{dom}(u)\,(u(i) \in X)$.

(b) $u^\frown v = w$ iff

$$\begin{aligned} u, v, w \in {}^{<\omega}\mathrm{V}_\omega \wedge \mathrm{dom}(w) &= \mathrm{dom}(u) + \mathrm{dom}(v) \\ &\wedge \forall i \in \mathrm{dom}(w)\,[(i \in \mathrm{dom}(u) \Rightarrow u(i) = w(i)) \\ &\wedge (i \notin \mathrm{dom}(u) \Rightarrow \exists j \in i\,(i = \mathrm{dom}(u) + j \wedge v(j) = w(i)))]. \end{aligned}$$

Since ${}^{<\omega}\mathrm{V}_\omega$ is Δ_1-definable by part (a), then the operation of concatenation is Δ_1-definable.

(c) $u \sqsubseteq v$ if and only if $\exists n \in \mathrm{dom}(v)\ \big[(v \restriction n)^\frown u \subseteq v\big]$.

(d) $G(n, z) = x$ iff

$$\begin{aligned} \exists p\big[&\mathsf{Fn}(p) \wedge \mathrm{dom}(p) \subseteq \omega \times Z \wedge ((n, z), x) \in p \wedge \\ &\forall (k, z) \in \mathrm{dom}(p)\,\forall k' \in k\,((k', z) \in \mathrm{dom}(p)) \wedge \\ &\forall (m, z) \in \mathrm{dom}(p)\,\big((m = 0 \Rightarrow p(m, z) = f(z)) \\ &\wedge \forall k \in m\,(m = \mathbf{S}(k) \Rightarrow p(m, z) = F(k, z, p(k, z)))\big)\big]. \end{aligned}$$

Thus G is Σ_1-definable, and since $\mathrm{dom}\, G = \omega \times Z$ is Δ_1-definable, then G is Δ_1-definable.

(e) Note that ${}^{<\omega}({}^{<\omega}\mathrm{V}_\omega)$ is Δ_1-definable by part (a). Let

$$C' \colon \omega \times {}^{<\omega}({}^{<\omega}\mathrm{V}_\omega) \to {}^{<\omega}\mathrm{V}_\omega$$

be defined by $C'(n, u) = u_0{}^\frown \cdots {}^\frown u_{n-1}$ if $n \leq \mathrm{lh}\, u$, and $\emptyset$ otherwise. Then $\mathrm{Cnc}(u) = C'(\mathrm{dom}\, u, u)$, so it is enough to show that C' is Δ_1-definable. But C' is defined inductively by $C'(0, u) = \emptyset$ and $C'(n+1, u) = F(n, u, C'(n, u))$, where $F \colon \omega \times {}^{<\omega}\mathrm{V}_\omega \times \mathrm{V}_\omega \to {}^{<\omega}\mathrm{V}_\omega$

$$F(n, u, y) = \begin{cases} y^\frown u(n) & \text{if } y \in {}^{<\omega}\mathrm{V}_\omega \wedge u \in {}^{<\omega}({}^{<\omega}\mathrm{V}_\omega) \wedge n \in \mathrm{dom}\, u, \\ \emptyset & \text{otherwise,} \end{cases}$$

is Δ_1-definable, so we are done by part (d).

(f) By Lemma 23.3 $\mathrm{Expr}(S, a) = \bigcup_{n\in\omega} \mathrm{Expr}_n(S, a)$, and since S and a are finite, then so are the $\mathrm{Expr}_n(S, a)$. Moreover strings in $\mathrm{Expr}_{n+1}(S, a) \setminus \mathrm{Expr}_n(S, a)$ are strictly longer than those in $\mathrm{Expr}_n(S, a)$, so that

$$w \in \mathrm{Expr}(S, a) \Leftrightarrow w \in \mathrm{Expr}_{\mathrm{dom}\, w}(S, a).$$

Therefore it is enough to show that $E_{S,a} \colon \omega \to \mathrm{V}_\omega$, $n \mapsto \mathrm{Expr}_n(S, a)$ is Δ_1-definable.

Let $S' = \{s \in S \mid a(s) = 0\}$ and $S'' = S \setminus S'$. Then $E_{S,a}(0) = \{\langle s \rangle \mid s \in S'\}$ and $E_{S,a}(n+1) = F_{S,a}(E_{S,a}(n))$, where $F = F_{S,a} \colon \mathrm{V}_\omega \to \mathrm{V}_\omega$ is defined by

$$v \in F(y) \Leftrightarrow v \in {}^{<\omega}\mathrm{V}_\omega \wedge \Big[v \in y \vee \exists u \in {}^{<\omega}y\, \exists s \in S''\, (v(0) = s$$
$$\wedge \operatorname{dom} u = \mathbf{S}(a(s))) \wedge v = \langle s\rangle^\frown \mathrm{Cnc}(u)\Big].$$

Since $F_{S,a}$ is Δ_1-definable, then so is $E_{S,a}$ by part (d).

The same proof shows that the result holds uniformly. □

Theorem 24.22. *Suppose* $S \subseteq \mathrm{V}_\omega$ *and* $a\colon S \to \omega$ *are* Δ_1*-definable. Then*

(a) $\mathrm{Expr}(S, a)$ *is* Δ_1*-definable,*

(b) *the function* $\mathrm{Subs}\colon {}^{<\omega}\mathrm{Expr}(S, a) \to \mathrm{Expr}(S, a)$ *defined by*

$$\mathrm{Subs}(u) = \begin{cases} w[z_1/v_1, \dots, z_n/v_n] & \textit{if } u = \langle w, v_1, \dots, v_n, z_1, \dots, z_n\rangle \\ & \textit{and } v_1, \dots, v_n \textit{ are distinct,} \\ \emptyset & \textit{otherwise,} \end{cases}$$

is Δ_1*-definable.*

Proof. (a) By Lemma 23.3(a)

$$w \in \mathrm{Expr}(S, a) \Leftrightarrow \mathrm{ran}(w) \subseteq S \wedge w \in \mathrm{Expr}(\mathrm{ran}(w), a \restriction \mathrm{ran}(w))$$

and since $w \in \mathrm{Expr}(\mathrm{ran}(w), a \restriction \mathrm{ran}(w))$ is Δ-definable by Proposition 24.21(f) the result is proved.

(b) The set U of all $u \in (\mathrm{Expr}(S, a))^{<\omega}$ such that

$$\exists n < \mathrm{dom}(u)\, [\mathrm{dom}(u) = 2n + 1 \wedge \forall i, j < n\, (i < j \Rightarrow u(i + 1) \neq u(j + 1))]$$

is Δ_1-definable, and it is the set where the definition of Subst is non-trivial. Thus if $u \in U$ then $\mathrm{Subst}(u) = v$ if and only if there is $t = \langle t_0, \dots, t_{2n}\rangle$ such that $u(0) = w = t_0{}^\frown t_1{}^\frown \dots {}^\frown t_{2n-1}{}^\frown t_{2n}$ and $t_1 = z_1$, $t_3 = z_2$, …, $t_{2n-1} = z_n$, and $v = t_0{}^\frown v_1{}^\frown t_2{}^\frown \dots {}^\frown t_{2n-2}{}^\frown v_n{}^\frown t_{2n}$. Therefore $\mathrm{Subst}(u) = v$ iff

$$\Big[u \notin U \wedge v = \emptyset\Big] \vee \Big[u \in U \wedge \exists n\, \exists t, t' \in (S^{<\omega})^{<\omega} \big(\operatorname{dom} t = \operatorname{dom} t' =$$
$$= \operatorname{dom} u = 2n + 1 \wedge u(0) = \mathrm{Cnc}(t) \wedge v = \mathrm{Cnc}(t') \wedge$$
$$\forall i \in n\, (t(2i + 1) = u(i + 1) \wedge t'(2i + 1) = u(n + i + 1)) \wedge$$
$$\forall i \in n + 1\, (t(2i) = t'(2i)) \wedge \forall i \in n\, \forall j \in n + 1\, (u(i + 1) \not\subseteq t(2j))\big)\Big]. \quad \square$$

24.D. Computable functions and representability. Next we show that every computable function is representable in Peano arithmetic, a fact that was already mentioned at the very end of Section 12.D. In fact, computable functions are representable in systems much weaker than PA.

Definition 24.23. Let $\mathcal{L}$ be a language extending $\mathcal{L}_{\mathsf{D}}$ of Section 11.A, so that numerals (Definition 11.5) are available. An $\mathcal{L}$-theory T

- **represents the function** $F\colon D \to \mathbb{N}$ **with** $D \subseteq \mathbb{N}^k$ **by** $\varphi(x_1, \dots, x_k, y)$ if for all $\langle a_1, \dots, a_k\rangle \in \operatorname{dom} F$
$$T \vdash \forall y \big(\varphi(\!|\overline{a_1}/x_1, \dots \overline{a_k}/x_k|\!) \Leftrightarrow y = \overline{F(a_1, \dots, a_k)}\big).$$
- **represents the predicate** $A \subseteq \mathbb{N}^k$ **by** $\varphi(x_1, \dots, x_k)$ if the following two conditions hold:
  - if $\langle a_1, \dots, a_k\rangle \in A$, then $T \vdash \varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!)$
  - if $\langle a_1, \dots, a_k\rangle \notin A$, then $T \vdash \neg\varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!)$.

Suppose T proves $\forall x \ \big(\mathsf{S}(x) \neq \overline{0}\big)$ (that is $\mathsf{PA1}$), $\forall x, y \ (x \neq y \Rightarrow \mathsf{S}(x) \neq \mathsf{S}(y))$ (that is $\mathsf{PA2}$) and that T proves

$$\forall x \ \big((x = \overline{0} \vee x = \overline{1} \vee \dots \vee x = \overline{n}) \Leftrightarrow \varphi_{\leq}(x, \overline{n})\big) \tag{24.2}$$

for every $n \in \mathbb{N}$. Then T is **order adequate** via some $\varphi_{\leq}(x, y)$ if this formula represents $\{(n, m) \mid n \leq m\}$ in T.

If T is order adequate, and if there is no danger of confusion, we write[1] $x \leq y$ for $\varphi_{\leq}(x, y)$, and $x < y$ for $x \leq y \wedge x \neq y$. As $\forall x \ \big(x = \overline{0} \Leftrightarrow x \leq \overline{0}\big)$, that is the formula (24.2) when $n = 0$, is provable from T, then $T \vdash \neg\exists x(x < \overline{0})$.

Remarks 24.24. (a) The notion of representability requires to verify case-by-case that certain facts about natural numbers are logical consequences of T. If $\varphi(x_1, \dots, x_k, y)$ represents a k-ary function F, then it defines a $k + 1$-ary predicate F^M in any $M \vDash T$. If $\mathbb{N} \subseteq M$ then $F^M \cap (\mathbb{N}^k \times \mathbb{N})$ is the graph of F, but it is not required that F^M be the graph of a function on the whole M.

(b) If $\mathcal{L}$ has a symbol $+$ for a binary operation, and if T represents addition via $x + y = z$, then for all $n, m \in \mathbb{N}$
$$T \vdash \overline{n} + \overline{m} = \overline{n + m} \quad \text{and} \quad T \vdash \overline{m} + \overline{n} = \overline{m + n},$$
and since $\overline{n + m}$ is the same as $\overline{m + n}$, it follows that $\overline{n} + \overline{m} = \overline{m} + \overline{n}$ is provable from T. This is much weaker than requiring that commutativity be provable in T, that is $T \vdash \forall x, y(x + y = y + x)$.

If T is order adequate, we do not require that T proves that $\leq$ is an order—see Exercise 24.39.

(c) If $A, B \subseteq \mathbb{N}^k$ are represented in T by formulæ $\varphi(\vec{x})$ and $\psi(\vec{x})$, then $\mathbb{N}^k \setminus A$, $A \cap B$, $A \cup B$ are represented in T by $\neg\varphi(\vec{x})$, $\varphi(\vec{x}) \wedge \psi(\vec{x})$, and $\varphi(\vec{x}) \vee \psi(\vec{x})$. Thus the collection of all subsets of $\mathbb{N}^k$ that are representable in T is a Boolean algebra.

[1] Clearly this encompasses the case when $\leq$ is a binary relation symbol of $\mathcal{L}$.

(d) The projection functions I^n_k are representable by $x_k \mathrel{=} y \wedge \bigwedge_{i<n} x_i \mathrel{=} x_i$ in any theory in a language extending $\mathcal{L}_{\mathsf{D}}$.

Lemma 24.25. *Let T be a theory such that $T \vdash \overline{1} \neq \overline{0}$. A predicate $A \subseteq \mathbb{N}^k$ is representable in T if and only if its characteristic function $\boldsymbol{\chi}_A \colon \mathbb{N}^k \to \{0, 1\}$ is representable in T.*

Proof. If $\varphi(\vec{x})$ represents A, then

$$\psi(\vec{x}, y): \qquad \big(\varphi(\vec{x}) \wedge y \mathrel{=} \overline{1}\big) \vee \big(\neg\varphi(\vec{x}) \wedge y \mathrel{=} \overline{0}\big)$$

represents $\boldsymbol{\chi}_A$. In fact for all $a_1, \dots, a_k \in \mathbb{N}$

$$\begin{aligned} \langle a_1, \dots, a_k\rangle \in A &\Rightarrow T \vdash \varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \\ &\Rightarrow T \vdash \psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k, \overline{1}/y|\!) \\ &\Rightarrow T \vdash \forall y(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{1}) \end{aligned}$$

and

$$\begin{aligned} \langle a_1, \dots, a_k\rangle \notin A &\Rightarrow T \vdash \neg\varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \\ &\Rightarrow T \vdash \psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k, \overline{0}/y|\!) \\ &\Rightarrow T \vdash \forall y(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{0}) \end{aligned}$$

so that $T \vdash \forall y(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{\boldsymbol{\chi}_A(a_1, \dots, a_k)})$.

Conversely, if $\psi(\vec{x}, y)$ represents $\boldsymbol{\chi}_A$, then $\varphi(\vec{x})$ defined as $\psi(\!|\overline{1}/y|\!)$ represents A:

$$\begin{aligned} \langle a_1, \dots, a_k\rangle \in A &\Rightarrow \boldsymbol{\chi}_A(a_1, \dots, a_k) = 1 \\ &\Rightarrow T \vdash \forall y \left(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{1}\right) \\ &\Rightarrow T \vdash \left(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{1}\right)(\!|\overline{1}/y|\!) \\ &\Rightarrow T \vdash \varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \end{aligned}$$

and

$$\begin{aligned} \langle a_1, \dots, a_k\rangle \notin A &\Rightarrow \boldsymbol{\chi}_A(a_1, \dots, a_k) = 0 \\ &\Rightarrow T \vdash \forall y \left(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{0}\right) \\ &\Rightarrow T \vdash \left(\psi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \Leftrightarrow y \mathrel{=} \overline{0}\right)(\!|\overline{1}/y|\!) \\ &\Rightarrow T \vdash \neg\varphi(\!|\overline{a_1}/x_1, \dots, \overline{a_k}/x_k|\!) \end{aligned}$$

where for the last implication we have used that $T \vdash \overline{1} \neq \overline{0}$. □

Lemma 24.26. *Suppose that the language of T has the symbols $\overline{0}$ and S. If $\mathsf{PA1}$ and $\mathsf{PA2}$ are provable from T then $\{(n, m) \mid n = m\}$ is representable in T via $x_1 \mathrel{=} x_2$.*

Proof. One implication is immediate: if $n = m$ then the two terms $\overline{n}$ and $\overline{m}$ coincide, so $T \vdash \overline{n} \doteq \overline{m}$. Suppose now $n \neq m$ towards proving that $T \vdash \overline{n} \neq \overline{m}$. For definiteness assume $n < m$ so that there is k such that $n + k + 1 = m$. If, towards a contradiction, $T \vdash \overline{n} \doteq \overline{m}$, then applying n-times our assumption we have that $T \vdash \overline{0} \doteq \overline{k+1}$ and since $\overline{k+1}$ is $\mathtt{S}(\overline{k})$, a contradiction follows from PA1. □

As any model of M of PA1 and PA2 contains a copy on $\mathbb{N}$, namely $\{\overline{n}^M \mid n \in \mathbb{N}\}$, we can assume that $\mathbb{N}$ is a subset of any such M.

Lemma 24.27. *Suppose that $\mathcal{L}$, the language of T, has the symbols $\overline{0}, \mathtt{S}, +$.*

(a) *If* PA*i is provable from T for $1 \leq i \leq 4$, then addition is representable in T.*

(b) *If moreover $\mathcal{L}$ has $\cdot$ and* PA*i is provable from T for $1 \leq i \leq 6$, then multiplication is representable in T.*

Proof. (a) One shows by induction on m that $T \vdash \overline{n} + \overline{m} \doteq \overline{n+m}$, for all $n \in \mathbb{N}$.

(b) Using part (a) one shows by induction on m that $T \vdash \overline{n} \cdot \overline{m} \doteq \overline{nm}$, for all $n \in \mathbb{N}$. □

Lemma 24.28. *If T is order adequate, x is the unique free variable of φ, and $T \vdash \bigwedge_{k \leq n} \varphi(\!|\overline{k}/x|\!)$ then $T \vdash \forall x(x \leq \overline{n} \Rightarrow \varphi(x))$.*

Proof. Fix an x. If $x \leq \overline{n}$ then $x \doteq \overline{0} \vee \cdots \vee x \doteq \overline{n}$ by order adequacy, and since $\varphi(\!|\overline{0}/x|\!) \wedge \cdots \wedge \varphi(\!|\overline{n}/x|\!)$ we have that $\varphi(x)$. As x is arbitrary the result follows. □

Theorem 24.29. *If T is order adequate and $T \vdash$* PA*i for $i \leq 6$, then every $f \in \mathfrak{C}$ is representable in T.*

Proof. Let us prove that the set of all partial functions that are representable in T is closed under composition.

Suppose f is k-ary and $g_0, \ldots, g_{k-1}$ are n-ary, and that they are represented in T by $\varphi(y_0, \ldots, y_{k-1}, z)$ and $\psi_i(x_0, \ldots, x_{n-1}, y_i)$ for $i < k$. Let $h(\vec{x}) = f(g_0(\vec{x}), \ldots, g_{k-1}(\vec{x}))$. Then h is represented by $\tilde{\varphi}(x_0, \ldots, x_{n-1}, z)$

$$\exists y_0, \ldots, y_{k-1} \left(\bigwedge_{i<k} \psi_i(x_0, \ldots, x_{n-1}, y_i) \wedge \varphi(y_0, \ldots, y_{k-1}, z)\right).$$

To see this suppose $\vec{a} = \langle a_0, \ldots, a_{n-1} \rangle \in \operatorname{dom} h$ and let us check that

$$T \vdash \forall z \left(\tilde{\varphi}(\!|\overline{a_0}/x_0, \ldots, \overline{a_{n-1}}/x_{n-1}, z|\!) \Leftrightarrow z \doteq \overline{h(a_0, \ldots, a_{n-1})}\right). \tag{24.3}$$

For each $i < k$, $\vec{a} \in \operatorname{dom} g_i$ and $\langle g_0(\vec{a}), \dots, g_{k-1}(\vec{a})\rangle \in \operatorname{dom} f$, so by assumption T proves

$$\forall y_i\, (\psi_i \llparenthesis \overline{a_0}/x_0, \dots, \overline{a_{n-1}}/x_{n-1}, y_i \rrparenthesis \Leftrightarrow y_i = \overline{g_i(\vec{a})}) \quad \text{for all } i < k, \tag{24.4}$$

$$\forall z\, (\varphi \llparenthesis \overline{g_0(\vec{a})}/y_0, \dots, \overline{g_{n-1}(\vec{a})}/y_{k-1}, z \rrparenthesis \Leftrightarrow z = \overline{f(g_0(\vec{a}), \dots, g_{k-1}(\vec{a}))}) \tag{24.5}$$

If z is $\overline{f(g_0(\vec{a}), \dots, g_{k-1}(\vec{a}))} = \overline{h(a_0, \dots, a_{n-1})}$, then (24.5) yields that

$$\varphi \llparenthesis \overline{g_0(\vec{a})}/y_0, \dots, \overline{g_{n-1}(\vec{a})}/y_{k-1}, z \rrparenthesis,$$

and letting y_i be $\overline{g_i(\vec{a})}$ we have by (24.4) that $\psi_i \llparenthesis \overline{a_0}/x_0, \dots, \overline{a_{n-1}}/x_{n-1}, y_i \rrparenthesis$ for all $i < k$, and hence $\tilde{\varphi} \llparenthesis \overline{a_0}/x_0, \dots, \overline{a_{n-1}}/x_{n-1}, z \rrparenthesis$.

Conversely, suppose $\tilde{\varphi} \llparenthesis \overline{a_0}/x_0, \dots, \overline{a_{n-1}}/x_{n-1}, z \rrparenthesis$. Then there are y_0, $\dots$, y_{k-1} such that $\psi_i \llparenthesis \overline{a_0}/x_0, \dots, \overline{a_{n-1}}/x_{n-1}, y_i \rrparenthesis$ and $\varphi(y_0, \dots, y_{k-1}, z)$ hold. By (24.4) y_i is $\overline{g_i(\vec{a})}$ and by (24.5) z is $\overline{h(a_0, \dots, a_{n-1})}$.

Therefore (24.3) is proved, and hence the collection of representable functions is closed under composition.

The projections are representable, the operations $+$ and $\cdot$ are representable by Lemma 24.27. By order adequacy, the ordering is represented by $\exists z\, (z + x = y)$, so $\boldsymbol{\chi}_{\leq}$ is representable by Lemma 24.25.

Therefore it is enough to show that the collection of functions that are representable in T is closed under minimization.

Suppose $g\colon \mathbb{N}^{n+1} \to \mathbb{N}$ is represented by $\psi(x_1, \dots, x_n, y, z)$. We must show that the n-ary function $f(\vec{a}) = \boldsymbol{\mu} y\, [g(\vec{a}, y) = 0]$ is representable. We claim that f is represented by $\varphi(x_1, \dots, x_n, y)$

$$\psi \llparenthesis \overline{0}/z \rrparenthesis \wedge \forall w < y\, \exists z\, (z \neq \overline{0} \wedge \psi \llparenthesis w/y \rrparenthesis)$$

where $\psi \llparenthesis \overline{0}/z \rrparenthesis$ is $\psi(x_1, \dots, x_n, y, \overline{0})$, that is the formula ψ in which z is replaced by $\overline{0}$ and $\psi \llparenthesis w/y \rrparenthesis$ is $\psi(x_1, \dots, x_n, w, z)$, that is the formula ψ in which y is replaced by w. To prove this, given $\langle a_1, \dots, a_n\rangle \in \operatorname{dom} f$ we must show that

$$T \vdash \forall y \left(\varphi \llparenthesis \overline{a_1}/x_1, \dots, \overline{a_n}/x_n \rrparenthesis \Leftrightarrow y = \overline{f(a_1, \dots, a_n)} \right). \tag{24.6}$$

Suppose $f(\vec{a}) = b$ so that $g(\vec{a}, b) = 0$ and $g(\vec{a}, k)$ is defined, and it is different from 0, for every $k < b$. As ψ represents g

$$T \vdash \bigwedge_{k<b} \exists z\, (z \neq \overline{0} \wedge \psi \llparenthesis \overline{a}_1/x_1, \dots, \overline{a}_n/x_n, \overline{k}/y \rrparenthesis) \wedge \psi \llparenthesis \overline{a}_1/x_1, \dots, \overline{a}_n/x_n, \overline{b}/y, \overline{0}/z \rrparenthesis$$

and by order adequacy $T \vdash \forall z (z < \overline{b} \Leftrightarrow z = \overline{0} \vee \dots \vee z = \overline{b-1})$, so $T \vdash \forall w < \overline{b}\, \exists z\, \psi \llparenthesis \overline{a}_1/x_1, \dots, \overline{a}_n/x_n, w/y \rrparenthesis$ and hence

$$\begin{aligned} T \vdash \forall y \bigl(& \psi \llparenthesis \overline{a}_1/x_1, \dots, \overline{a}_n/x_n, \overline{0}/z \rrparenthesis \wedge \\ & \qquad \forall w < y\, \exists z\, (z \neq \overline{0} \wedge \psi \llparenthesis \overline{a}_1/x_1, \dots, \overline{a}_n/x_n, w/y \rrparenthesis) \Leftrightarrow y = \overline{b} \bigr) \end{aligned}$$

which is the same as (24.6). Therefore f is representable, and this concludes the proof of the theorem. □

By Lemma 24.25 if T is order adequate, then every computable predicate is representable in T.

Definition 24.30. The theory Q is formulated in the language containing symbols $+, \cdot, \mathtt{S}, \bar{0}$ and has the following axioms:

(Q1) $\forall x(\mathtt{S}(x) \neq \bar{0})$,

(Q2) $\forall x, y\, (x \neq y \Rightarrow \mathtt{S}(x) \neq \mathtt{S}(y))$,

(Q3) $\forall x(x + \bar{0} = x)$,

(Q4) $\forall x, y(x + \mathtt{S}(y) = \mathtt{S}(x + y))$

(Q5) $\forall x(x \cdot \bar{0} = \bar{0})$,

(Q6) $\forall x, y(x \cdot \mathtt{S}(y) = (x \cdot y) + x)$,

(Q7) $\forall x\, \big(x \neq \bar{0} \Rightarrow \exists y(x = \mathtt{S}(y))\big)$.

The axiom $\mathsf{Q}n$ is $\mathsf{PA}n$ for $1 \leq n \leq 6$, and by Lemma 12.13 Q7 follows from PA^-, and therefore every theorem of Q is provable in PA^-. Thus a model of PA is a model of Q; in particular a non-standard model of Q (i.e. a model not isomorphic to ω) can be of the form $\mathbb{N} \uplus \mathbb{Z} \times Q$ where Q is a dense linear order without endpoints, but there are other non-standard models of Q (Exercise 24.39). Note that Q1 implies that $\bar{1} \neq \bar{0}$, so Q satisfies the hypothesis of Lemma 24.25.

Define

$$x \leq y \Leftrightarrow \exists z(z + x = y). \tag{24.7}$$

For all natural numbers $n \leq m$ if and only if $\exists k \in \mathbb{N}(k + n = m)$, so by Lemma 24.27 $\{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \leq m\}$ is represented in Q by the formula $x_1 \leq x_2$.

Theorem 24.31. *The theory* Q *is order adequate, and hence every computable function is representable in it.*

Proof. It is enough to show that $\mathsf{Q} \vdash \forall x(x \leq \bar{n} \Leftrightarrow x = \bar{0} \vee \cdots \vee x = \overline{n})$ for every $n \in \mathbb{N}$. If x is $\overline{m}$ for some $m \leq k$, then $x \leq \overline{n}$, so it is enough to prove by induction on n that $\mathsf{Q} \vdash \forall x(x \leq \bar{n} \Rightarrow x = \bar{0} \vee \cdots \vee x = \overline{n})$. If $n = 0$ then $x \leq \bar{0}$ implies that $x = \bar{0}$, so we are done. Assuming the result for some n, we prove it for $n + 1$. Suppose $x \leq \overline{n+1}$, that is $\exists z(z + x = \mathtt{S}(\overline{n}))$. If $x = \bar{0}$ we are done, otherwise by Q7 $x = \mathtt{S}(y)$ for some y, so $\exists z(\mathtt{S}(z + y) = z + \mathtt{S}(y) = \mathtt{S}(\overline{n}))$. By Q2 $\exists z(z + y = \overline{n})$, i.e. $y \leq \overline{n}$, and hence $y = \bar{0} \vee \cdots \vee y = \overline{n}$. Therefore $x = \bar{1} \vee \cdots \vee y = \overline{n+1}$. □

There is another version of Robinson's arithmetic used in the literature.

Definition 24.32. The $\mathcal{L}_{\mathsf{PA}}$-theory $\bar{\mathsf{Q}}$ has the same axioms as Q except that the last axiom Q7 is replaced by the following two axioms:

($\bar{\mathsf{Q}}$7) $\forall x \neg \left(x < \bar{0}\right)$,

($\bar{\mathsf{Q}}$8) $\forall x, y (x < \mathtt{S}(y) \Leftrightarrow (x < y \vee x = y))$.

For uniformity of notation, when dealing with $\bar{\mathsf{Q}}$ we write $\bar{\mathsf{Q}}1, \dots, \bar{\mathsf{Q}}6$ rather than $\mathsf{Q}1, \dots, \mathsf{Q}6$ or $\mathsf{PA}1, \dots, \mathsf{PA}6$.

As $\bar{\mathsf{Q}}$ is PA minus induction, every theorem of $\bar{\mathsf{Q}}$ is a theorem of PA. Just like for Q, every computable function is representable in $\bar{\mathsf{Q}}$ (Exercise 24.41). The advantage of Q over $\bar{\mathsf{Q}}$ is that its language does not contain the symbol for the order relation; conversely, there are models of $\bar{\mathsf{Q}}$ that are not models of Q.

Theorem 24.31 has useful consequences for PA.

24.D.1. *Formalization in* PA. Many mathematical statements can be shown to be *formalizable* in the language of PA. One such example is Ramsey's Theorem 10.8. Another, even more striking example is given by the **Riemann Hypothesis**, the statement that the non-trivial zeroes of the ζ function lie on the line $\Re(s) = \frac{1}{2}$. (The function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is defined on the half-plane $\Re(s) > 1$, and then extended to a meromorphic function on $\mathbb{C}$.) This is one of the most important conjecture in mathematics, and it is equivalent to the following statement:

$$\forall k \, \exists x \, \forall y > x \, \left[\left| \sum_{n=1}^{y} \mu(n) \right| < y^{\frac{1}{2} + 2^{-k}} \right]$$

where μ is the Möbius function (Example 2.6), which can be easily formalized in $\mathcal{L}_{\mathsf{PA}}$.

24.D.2. *Primitive recursive and elementary arithmetic.*

24.D.3. *Long induction.*

24.E. Representability in set theory. Since computable functions are Δ_1-definable in V_ω, it is natural to seek for an analogue of Robinson's arithmetic in set theory.

Definition 24.33. Elementary set theory (EST) has the following four axioms:

- the axiom of extensionality: $\forall x, y \, (\forall z \, (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$,
- existence of the empty set: $\exists x \forall y (y \notin x)$,
- existence of singletons: $\forall x \exists y \forall z (z \in y \Leftrightarrow z = x)$,
- existence of unions: $\forall x, y \exists z \forall w (w \in z \Leftrightarrow w \in x \vee w \in y)$.

By extensionality, one can write $\exists!$ in place of the existential quantifiers in the axioms of EST. In particular, if $\mathcal{M} = \langle M, E \rangle$ is an arbitrary model of EST then

- $\emptyset^{\mathcal{M}}$ is the unique $a \in M$ such that $(b, a) \notin E$, for all $b \in M$;

- for $a \in M$, then $\{a\}^{\mathcal{M}}$ is the unique $b \in M$ such that $(a,b) \in E$ and $(a',b) \notin E$ for all $a' \neq a$,
- if $a,b \in M$ then $a \cup^{\mathcal{M}} b$ is the unique $c \in M$ such that $\forall x \in M\,((x,c) \in E \Leftrightarrow (x,a) \in E \vee (x,b) \in E)$.

Define $\pi\colon \mathrm{V}_\omega \to M$ as follows: $\pi(\emptyset) = \emptyset^{\mathcal{M}}$, $\pi(\{a\}) = \{\pi(a)\}^{\mathcal{M}}$, and for $n \geq 1$

$$\pi(\{a_1,\dots,a_n,a_{n+1}\}) = \pi(\{a_1,\dots,a_n\}) \cup^{\mathcal{M}} \{\pi(a_{n+1})\}^{\mathcal{M}}.$$

Therefore $\pi\colon \langle \mathrm{V}_\omega, \in\rangle \to \langle M, E\rangle$ is an embedding and

$$\forall a \in \mathrm{V}_\omega \forall m \in M (m \mathrel{E} \pi(a) \Rightarrow \exists b \in a(\pi(b) = m)).$$

An n-ary predicate $A \subseteq \mathrm{V}_\omega$ is representable in EST if there is $\varphi(x_1,\dots,x_n)$ such that for every $a_1,\dots,a_n \in \mathrm{V}_\omega$

$$\langle a_1,\dots,a_n\rangle \in A \Rightarrow \mathsf{EST} \vdash \forall x_1,\dots,x_n[\bigwedge_{1\leq i\leq n} \delta_{a_i}(x_i) \Rightarrow \varphi(\vec{x})]$$

$$\langle a_1,\dots,a_n\rangle \notin A \Rightarrow \mathsf{EST} \vdash \forall x_1,\dots,x_n[\bigwedge_{1\leq i\leq n} \delta_{a_i}(x_i) \Rightarrow \neg\varphi(\vec{x})]$$

Note that in the formulæ above we could have asked the EST proves that $\exists x_1,\dots,x_n[\bigwedge_{1\leq i\leq n} \delta_{a_i}(x_i) \wedge \dots]$.

Theorem 24.34. *If $A \subseteq \mathrm{V}_\omega$ is an n-ary predicate, then*

(a) *if A is Σ_1-definable via $\varphi(\vec{x})$, then*

$$\langle a_1,\dots,a_n\rangle \in A \Rightarrow \mathsf{EST} \vdash \forall x_1,\dots,x_n[\bigwedge_{1\leq i\leq n} \delta_{a_i}(x_i) \Rightarrow \varphi(\vec{x})]$$

(b) *if A is Δ_1-definable, then it is representable in* EST.

Exercises

Exercise 24.35. Show that

(i) if $f\colon \mathbb{N}^n \to \mathbb{N}$ and $n \geq 1$, then $\mathfrak{C}(f) = \mathfrak{C}(f \circ J_n)$ where $J_n\colon \mathbb{N} \to \mathbb{N}^n$ is a recursive bijection;

(ii) if $f\colon \mathbb{N}^n \to \mathbb{N}$ and $A = \mathrm{Gr}(f) \subseteq \mathbb{N}^{n+1}$, then $\mathfrak{C}(f) = \mathfrak{C}(\boldsymbol{\chi}_A)$.

Exercise 24.36. Show that the formulæ in Table 3 are indeed Δ_0.

Exercise 24.37. Let $S \subseteq \mathrm{V}_\omega$ and $a\colon S \to \omega$. Show that:

(i) if S is computable, then so is the set ${}^{<\omega}S$ and the operation $(s,t) \mapsto s^\frown t$;

(ii) if a is also computable, then so are $\mathrm{Expr}(S,a)$ and $\mathrm{ht}\colon \mathrm{Expr}(S,a) \to \omega$;

(iii) if $v_1, \dots, v_n, z_1, \dots, z_n \in \mathrm{Expr}(S, a)$ and $v_1, \dots, v_n$ are distinct, then the operation on $\mathrm{Expr}(S, a)$, $w \mapsto w[z_1/v_1, \dots, z_n/v_n]$, is computable.

Exercise 24.38. Show that the following are provable in Q, with $\leq$ as in (24.7).

(1) $\forall x(\overline{0} \leq x)$;

(2) $\forall x(x \leq \overline{n} \Rightarrow x \leq \overline{n+1})$;

(3) $\forall x(\overline{n} \leq x \Rightarrow \overline{n} \eqcirc x \vee \overline{n+1} \leq x)$;

(4) $\forall x\,(x \leq \overline{n} \vee \overline{n} \leq x)$.

Exercise 24.39. Show that the following are models of Q.

(1) The set $M_1 = \omega \uplus \{a_0, a_1\}$ with $a_0 \neq a_1$, where $S, +, \cdot, 0$ have the usual meaning on ω, and
- $S(a_i) = a_i$ for $i = 0, 1$,
- $a_i + n = a_i$ for all $n \in \omega$, and $x + a_i = a_{1-i}$ for all $x \in M_1$,
- $x \cdot 0 = 0$ and $x \cdot (n + 1) = (x \cdot n) + x$ for any $x \in M_1$ and $n \in \omega$; $n \cdot a_i = a_i$ for all $n \in \omega$; and $a_i \cdot a_j = a_{1-i}$.

(2) The set $M_2 = \kappa \cap \mathrm{Card}$ with $\omega < \kappa \in \mathrm{Card}$ and $+, \cdot, 0$ have the usual meaning as in cardinal arithmetic, and $S(x) = 1 \dot{+} x$ for all $x \in M_2$.

(3) The set M_3 of all polynomials of $\mathbb{Z}[X]$ with non-negative leading coefficient, with 0 the zero polynomial, the usual addition and multiplication, and $S(p) = p + 1$.

Conclude that none of the following is provable in Q, with $\leq$ defined as in (24.7):

- $\forall x(\overline{0} + x \eqcirc x)$;
- $\forall x(\mathtt{S}(x) \neq x)$;
- $\forall x, y, z((x + y) + z \eqcirc x + (y + z))$;
- $\forall x, y(x + y \eqcirc y + x)$;
- $\forall x(\overline{0} \cdot x = \overline{0})$;
- $\forall x, y, z((x \cdot y) \cdot z \eqcirc x \cdot (y \cdot z))$;
- $\forall x, y(x \cdot y \eqcirc y \cdot x)$;
- $\forall x(x \leq x)$;
- $\forall x, y(x \leq y \wedge y \leq x \Rightarrow x \eqcirc y)$;
- $\forall x, y, z(x \leq y \wedge y \leq z \Rightarrow x \leq z)$.

Exercise 24.40. Let Q' be the theory Q with $\mathsf{Q}7$ replaced by

$$\forall x, y\,(\exists z(x + z \eqcirc y) \Leftrightarrow (\exists z(x + \mathtt{S}(z) \eqcirc y) \vee x \eqcirc y))\,.$$

Define $x < y$ as $\exists z(x + \mathtt{S}(z) \eqcirc y)$. Show that $\bar{\mathsf{Q}}7$–$\bar{\mathsf{Q}}8$ follow from Q', so any model of Q' can be expanded to a model of $\bar{\mathsf{Q}}$.

Exercise 24.41. Show that $\bar{\mathsf{Q}}$ is order adequate and hence every recursive function is representable in it.

Exercise 24.42. Show that the following are models of $\bar{\mathsf{Q}}$.

(1) Any infinite multiplicatively indecomposable ordinal, with ordinal addition and multiplication, the successor function $\mathbf{S}$, and the usual order.

(2) The set $2 \times \omega$ with the order $(i,n) < (j,m) \Leftrightarrow (i = j \wedge n < m)$ and the operations $S(i,n) = (i, n+1)$, $(i,n) + (j,m) = (\max(i,j), n+m)$ and where $(i,n) \cdot (j,m)$ is set to be $(\max(i,j), nm)$ if $(i,n), (j,m) \neq (0,0)$ and $(0,0)$ otherwise.

Conclude that neither $\mathsf{Q7}$ nor $\forall x, y (x < y \vee x \mathbin{\dot{=}} y \vee y < x)$ are provable in $\bar{\mathsf{Q}}$.

Exercise 24.43. Show that

(i) if M is a countable transitive set, closed under the operations $x \mapsto \{x\}$ and $(x,y) \mapsto x \cup y$, then (M, E) is a countable random graph, where $x \mathrel{E} y \Leftrightarrow (x \in y \vee y \in x)$;

(ii) $(\mathbb{N}, F)$ is a countable random graph, where $n \mathrel{F} m \Leftrightarrow$ (the n-th digit in the binary expansion of m is $1 \vee$ the m-th digit in the binary expansion of n is 1).

Exercise 24.44. Show that the following functions are recursive:

(i) the function $f \colon \mathbb{N} \to \mathbb{N}$ defined by $f(0) = 0$ and for $n > 0$, $f(n) = \mu(n)$ if $\mu(n) \geq 0$, and $f(n) = 2$ if $\mu(n) = -1$ and the function $n \mapsto |\sum_{k=1}^{n} \mu(k)|$, where μ is the Möbius function (see page 11);

(ii) Ramsey's function $R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by: $R(n,k)$ is the least m such that for every coloring of K_m with $k+1$ colors has a monochromatic complete subgraph with n vertexes.

Exercise 24.45. By Remark 19.14 $\mathbb{Q}$ can be taken to be a subset of V_ω. Check that $\langle \mathbb{Q}, +, \cdot, < \rangle$ is computable by showing that the operations and the ordering are Δ_1-definable.

Exercise 24.46. Let LO be the set of all $R \subseteq \mathbb{N} \times \mathbb{N}$ which are reflexive, antisymmetric, transitive and total on $\mathrm{fld}(R) = \{n \in \mathbb{N} \mid (n,n) \in R\}$, and let WO be the set of all $R \in \mathrm{LO}$ which are well-orders on their own fields. A **recursive well-order** is a recursive $R \in \mathrm{WO}$; a **recursive ordinal** α is an ordinal isomorphic to $\langle \mathrm{fld}(R), R \rangle$ with $R \in \mathrm{WO}$. The **Church-Kleene ordinal** ω_1^{CK} is the supremum of all recursive ordinals.

(i) Show that if $R \in \mathrm{WO}$ and $\bar{n} \in \mathrm{fld}(R)$, then $R_{\leq \bar{n}} = \{(n,m) \in R \mid (n, \bar{n}) \in R\}$ and $R_{< \bar{n}} = R_{\leq \bar{n}} \setminus \{(\bar{n}, \bar{n})\}$ are recursive. Conclude that if β is recursive and $\alpha < \beta$ then α is recursive.

(ii) Show that ω_1^{CK} is a countable limit ordinal bigger than ω, and it is exponentially (and hence multiplicatively and additively) indecomposable.

Notes and remarks

The theories Q and $\bar{\mathsf{Q}}$ were introduced by R. Robinson in the early 50s and presented in detail in the book [**Tar68**]. Unfortunately there seems to be no general consensus on how these and related theories should be named, and all of them are denoted by the letters $\bar{\mathsf{Q}}$ or Q. So the reader should be warned that what we call Q some authors call $\bar{\mathsf{Q}}$, and conversely.

25. Boolean algebras

Recall that a lattice is an ordered set L such that $x \curlyvee y$ and $x \curlywedge y$ exist for all $x, y \in L$; if $\bigcurlyvee X$ and $\bigcurlywedge X$ exist for all $X \subseteq L$ we will speak of a complete lattice. A Boolean algebra is a complemented distributive lattice; it is complete if it is complete as a lattice. A Boolean algebra B is a commutative ring, thus it makes sense to speak of ideals. An ideal is a non-empty set $I \subseteq B$ which is an initial segment with respect to $\leq$ and closed under $\curlyvee$; we say that I is proper if $I \neq B$. The dual of an ideal is a filter, that is a non-empty set $F \subseteq B$ which is a final segment with respect to $\leq$ and closed under $\curlywedge$.

25.A. Ideals and filters.

Definition 25.1. An **ideal in a lattice** L is an initial segment $\emptyset \neq I \subseteq L$ closed under $\curlyvee$. When $I \neq L$ we say that I is **proper**. For all $a \in L$ the set ${\downarrow}a = \{x \in L \mid x \leq a\}$ is the **principal ideal** generated by a. A **prime ideal** is a proper ideal I such that

$$\forall x, y\, (x \curlywedge y \in I \Rightarrow x \in I \vee y \in I).$$

A **maximal ideal** is a proper ideal that is not contained in any other proper ideal.

The concept dual to ‘ideal’ is that of ‘filter’: a **filter in a lattice** L is a final segment $\emptyset \neq F \subseteq L$ closed under $\curlywedge$. The notions of proper, principal, prime, maximal filter are defined by duality: a filter F in a lattice L is **proper** if $F \neq L$, **principal** if $F = {\uparrow}a$ for some $a \in L$, **prime** if $a \curlyvee b \in F$ implies that $a \in F$ or $b \in F$, **maximal** if it is proper, and not contained in any other proper filter. If L has minimum $\mathbf{0}$, then a filter $F \subseteq L$ is proper if and only if $\mathbf{0} \notin F$; dually if L has maximum $\mathbf{1}$, then an ideal $I \subseteq L$ proper if and only if $\mathbf{1} \notin I$.

Theorem 25.2. *Let L be a well-orderable lattice. If L has minimum, then every proper filter can be extended to a maximal filter. Dually, if L has maximum, then every proper ideal can be extended to a maximal ideal.*

Proof. Suppose F is a proper filter of a well-orderable lattice L with minimum $\mathbf{0}$. Enumerate $L \setminus F$ as $\{x_\alpha \mid \alpha < \kappa\}$ and construct $\langle F_\alpha \mid \alpha \leq \kappa \rangle$ by setting $F_0 = F$, $F_\lambda = \bigcup_{\alpha<\lambda} F_\alpha$ when λ is limit, and

$$F_{\alpha+1} = \begin{cases} \uparrow\{x_\alpha \curlywedge y \mid y \in F_\alpha\} & \text{if this is a proper filter,} \\ F_\alpha & \text{otherwise.} \end{cases}$$

Note that the F_αs are filters and that $\alpha < \beta \Rightarrow F_\alpha \subseteq F_\beta$. Moreover the F_αs are proper filters. In fact if $\alpha \leq \kappa$ were the least ordinal such that $F_\alpha = L$, then α would be limit, hence $\mathbf{0} \in F_\beta$ for some $\beta < \alpha$, and thus $F_\beta = L$, against the minimality of α. The proof will be done if we show that F_κ is maximal. If, towards a contradiction, $G \supset F_\kappa$ were a proper filter, choose $x_\alpha \in G \setminus F_\kappa$: but then $x_\alpha \in F_{\alpha+1} \subseteq F_\kappa$, a contradiction. □

Corollary 25.3. *If B is a well-orderable Boolean algebra, then every proper filter can be extended to an ultrafilter and every proper ideal can be extended to a prime ideal.*

A **filter-base** in a bounded lattice L is an $X \subseteq L$ closed under $\curlywedge$ and such that $\mathbf{0} \notin X$; a **filter-subbase** is an $X \subseteq L$ such that $X^{\curlywedge}$ is a filter-base.[2] If X is a filter-base, then $\uparrow X$ is a proper filter, and it is called the filter generated by X. A lattice L is **κ-complete** if $\bigcurlyvee X$ and $\bigcurlywedge X$ exist, for all $X \subseteq L$ of size $< \kappa$. Thus a lattice is complete if and only if it is κ-complete for any cardinal κ. A **κ-complete ideal** I of a κ-complete lattice L is an ideal such that $\bigcurlyvee X \in I$ for all $X \subseteq I$ of size $\leq \kappa$. The dual of a κ-complete ideal is a κ-complete filter. Finally an ω_1-complete lattice/ideal/filter is said to be **σ-complete**.

Remark 25.4. The equivalence between the notions *prime ideal* and *maximal ideal* (and dually: *prime filter* and *ultrafilter*) for Boolean algebras (Proposition 7.41(b)), cannot be generalized to the case of lattices. In a distributive lattice, every maximal ideal is prime, but the converse might fail, and in a modular lattice a maximal ideal might not be prime (Exercise 25.11).

Theorem 25.5 (Ulam). *Assume* AC*, and let $\kappa = \lambda^+$, with λ an infinite cardinal, and let S be a set of cardinality κ. Suppose $\mathcal{I} \subseteq \mathscr{P}(S)$ is a κ-complete proper ideal such that $X \in \mathcal{I}$ for all $X \subseteq S$ of size $< \kappa$—equivalently: $\{x\} \in \mathcal{I}$ for all $x \in S$. Then there are κ pairwise disjoint sets not in $\mathcal{I}$.*

Proof. Without loss of generality, we may assume that $S = \kappa$. For each $\alpha \in \kappa$ pick $f_\alpha \colon \alpha \to \lambda$ injective, and for $\nu \in \lambda$ let[3]

$$A^\nu_\alpha = \{\beta \in \kappa \mid f_\beta(\alpha) = \nu\}.$$

[2] The set $X^{\curlywedge}$ was defined in Section 7.K on page 184.

[3] The family $\langle A^\nu_\alpha \mid \nu \in \lambda \wedge \alpha \in \kappa \rangle$ is called a Ulam matrix.

For fixed $\nu \in \lambda$, if α, β are distinct, then $A^\nu_\alpha \cap A^\nu_\beta = \emptyset$ as the functions f_γ are injective. For fixed $\alpha \in \kappa$, by hypothesis $\alpha\dot{+}1 \in \mathcal{I}$ so $\bigcup_{\nu\in\lambda} A^\nu_\alpha = \kappa\setminus(\alpha\dot{+}1) \notin \mathcal{I}$. Therefore by κ-additivity there is a function $f\colon \kappa \to \lambda$ such that $A^{f(\alpha)}_\alpha \notin \mathcal{I}$. Let $\nu \in \lambda$ be such that $I = \{\alpha \in \kappa \mid f(\alpha) = \nu\}$ has size κ. Then $\{A^\nu_\alpha \mid \alpha \in I\}$ is the required family. □

25.B. Stone duality. The Boolean prime ideal principle BPI of Definition 14.6 can be parametrized:

($\mathsf{BPI}(B)$) Any proper ideal of B is contained in a prime ideal.

Equivalently, $\mathsf{BPI}(B)$ says that every proper filter of B is contained in an ultrafilter. Thus BPI is $\mathsf{BPI}(B)$ for all Boolean algebras B.

Remarks 25.6. (a) The axiom of choice implies BPI, but the converse implication does not hold; moreover BPI is independent from AC_ω and DC, meaning that it does not imply AC_ω, nor it is implied by DC—see [**Her06**]. The principle BPI has important consequences in mathematics—see Section 28.C.

(b) The first part of Corollary 25.3 can be stated as: if B is well-orderable then $\mathsf{BPI}(B)$.

In Section 14.C the Boolean prime ideal principle was used to prove Stone's representation Theorem 14.19: if B is a Boolean algebra and $\mathsf{BPI}(B)$ is assumed, then $\mathrm{St}(B)$, the set of all ultrafilters of B, is non-empty and

$$\mathfrak{U}\colon B \to \mathscr{P}(\mathrm{St}(B)), \qquad \mathfrak{U}(b) = \{D \in \mathrm{St}(B) \mid b \in D\},$$

is an injective homomorphism. The **Stone space of** B is $\mathrm{St}(B)$ with the topology generated by the sets $\mathfrak{U}(b)$.

Theorem 25.7. *Assume* $\mathsf{BPI}(B)$. *The space* $\mathrm{St}(B)$ *is compact, Hausdorff, zero dimensional, and* B *is isomorphic to* $\mathbf{CLOP}\,(\mathrm{St}(B))$.

First we need a preliminary result.

Lemma 25.8. *If* $\mathcal{B}$ *is an algebra of sets, and it is a basis for a compact space* X, *then* $\mathcal{B} = \mathbf{CLOP}(X)$.

Proof. Since $\mathcal{B}$ is closed under complements, then each set in $\mathcal{B}$ is clopen, so $\mathcal{B} \subseteq \mathbf{CLOP}(X)$. Conversely, if $C \in \mathbf{CLOP}(X)$, then C is compact, so any cover $C = \bigcup_{i\in I} U_i$ with $U_i \in \mathcal{B}$ admits a finite subcover $C = U_{i_1} \cup \cdots \cup U_{i_n}$. As $\mathcal{B}$ is closed under finite unions, $C \in \mathcal{B}$. □

Proof of Theorem 25.7. Since $\mathfrak{U}(b^*) = \mathrm{St}(B) \setminus \mathfrak{U}(b)$, then

$$\{\mathfrak{U}(b) \mid b \in B\} \text{ is a base of clopen sets.} \tag{25.1}$$

If $\mathcal{U}, \mathbf{D} \in \mathrm{St}(B)$ are distinct, let $b \in \mathcal{U} \setminus \mathcal{D}$: then $b^* \in \mathcal{D} \setminus \mathcal{U}$ and $\mathfrak{U}(b)$ and $\mathfrak{U}(b^*)$ are disjoint open neighborhoods of $\mathcal{U}$ and $\mathcal{D}$. This proves that $\mathrm{St}(B)$ is zero-dimensional and T_2.

For compactness it is enough to show that any open cover of the form $\{\mathfrak{U}(b_i) \mid i \in I\}$ admits a finite subcover. Towards a contradiction, suppose that $\mathrm{St}(B) \neq \bigcup_{i\in J} \mathfrak{U}(b_i)$ for any finite $J \subseteq I$, so that

$$\mathfrak{U}\big(\textstyle\bigwedge_{i\in J} b_i^*\big) = \bigcap_{i\in J} \mathfrak{U}(b_i^*) = \mathrm{St}(B) \setminus \bigcup_{i\in J} \mathfrak{U}(b_i) \neq \emptyset = \mathfrak{U}(\mathbf{0}_B).$$

Since $\mathfrak{U}$ is an injective homomorphism, this implies that $\bigwedge_{i\in J} b_i^* \neq \mathbf{0}_B$ for all finite $J \subseteq I$. The set $\{b_i^* \mid i \in I\}$ generates a proper filter that by $\mathsf{BPI}(B)$ can be extended to an ultrafilter $\mathcal{U}$. By case assumption $\mathcal{U} \in \mathfrak{U}(b_{i_0})$ for some $i_0 \in I$, and $b_{i_0}^* \in \mathcal{U}$ by construction: a contradiction.

Finally, $B \cong \mathbf{CLOP}\,(\mathrm{St}(B))$ follows from (25.1), Lemma 25.8 and Theorem 14.18. □

Theorem 25.9. *Let X be compact, Hausdorff, zero-dimensional, and assume* $\mathsf{BPI}(\mathbf{CLOP}(X))$. *Then X is homeomorphic to* $\mathrm{St}(\mathbf{CLOP}(X))$.

Proof. Let $\mathcal{U} \in \mathrm{St}(\mathbf{CLOP}(X))$. Then $\mathcal{U}$ is a collection of non-empty clopen subsets of X, and by definition of filter, $C_1 \cap \cdots \cap C_n \neq \emptyset$ for all $C_1, \ldots, C_n \in \mathcal{U}$. By compactness of X, the set $K = \bigcap \mathcal{U}$ is non-empty. If $x, y \in K$ were distinct, pick $D \in \mathbf{CLOP}(X)$ such that $x \in D$ and $y \notin D$. Any finite subset of $\mathcal{F} = \{C \cap D \mid C \in \mathcal{U}\}$ has non-empty intersection, as x belongs to such intersection, hence $\uparrow\mathcal{F}$ is a proper filter. As $\mathcal{F} \subseteq \mathcal{U}$ then $\uparrow\mathcal{F} \subseteq \mathcal{U}$ so $K = \bigcap \mathcal{U} \subseteq \bigcap \mathcal{F} \subseteq D$ and therefore $y \in D$: a contradiction. Therefore $\bigcap \mathcal{U}$ is a singleton, for all $\mathcal{U} \in \mathrm{St}(\mathbf{CLOP}(X))$. Let

$$h\colon \mathrm{St}(\mathbf{CLOP}(X)) \to X, \qquad h(\mathcal{U}) = \text{the unique element of } \bigcap \mathcal{U}.$$

Claim 25.9.1. $\forall \mathcal{U} \in \mathrm{St}(\mathbf{CLOP}(X))\, \forall C \in \mathbf{CLOP}(X)\, [h(\mathcal{U}) \in C \Leftrightarrow C \in \mathcal{U}]$.

Proof. If $h(\mathcal{U}) \in C$ and $C \notin \mathcal{U}$ then $X \setminus C \in \mathcal{U}$ so $h(\mathcal{U}) \in X \setminus C$, a contradiction. Conversely, if $C \in \mathcal{U}$ then $h(\mathcal{U}) \in C$ by construction. □

Claim 25.9.2. *h is injective.*

Proof. Suppose $\mathcal{U}, \mathcal{U}' \in \mathrm{St}(\mathbf{CLOP}(X))$ are distinct. Then there is $C \in \mathbf{CLOP}(X)$ such that $C \in \mathcal{U}$ and $C \notin \mathcal{U}'$, hence $h(\mathcal{U}) \in C$ and $h(\mathcal{U}') \notin C$ by Claim 25.9.1. □

Claim 25.9.3. *h is surjective.*

Proof. Fix $x \in X$. Let $\mathcal{F} = \{C \in \mathbf{CLOP}(X) \mid x \in C\}$ and let $\mathcal{U}$ be an ultrafilter extending $\mathcal{F}$. As X is T_2 and zero-dimensional, for all $x \in X$ we have that $\{x\} = \bigcap \mathcal{F} \supseteq \bigcap \mathcal{U}$, so $h(\mathcal{U}) = x$. □

For $C \in \mathbf{CLOP}(X)$ and using Claim 25.9.1,

$$h^{-1}(C) = \{\mathcal{U} \mid h(\mathcal{U}) \in C\} = \{\mathcal{U} \in \mathrm{St}(\mathbf{CLOP}(X)) \mid C \in \mathcal{U}\} = \mathfrak{U}(C).$$

Thus the preimage of a clopen subset of X is clopen in $\mathrm{St}(\mathbf{CLOP}(X))$, hence h is a continuous bijection. Since we are dealing with compact spaces, this shows that h is a homeomorphism. □

In view of this, the study of Boolean algebras is equivalent to the study of zero dimensional compact Hausdorff spaces, so results in one area can be recast in the other area: for example, a Boolean algebra is countable and atomless if and only if its Stone space is second countable and perfect (Exercise 25.24). Theorem 13.38 shows that any two countable atomless Boolean algebras are isomorphic, hence two compact, second countable, zero dimensional, perfect Hausdorff spaces are homeomorphic. In particular

Theorem 25.10 ($\mathsf{BPI} + \mathsf{AC}_\omega$). *The Cantor space is, up to homeomorphism, the unique compact, separable, zero dimensional Hausdorff space without isolated points.*

Proof. We need to show that in the statement of the theorem, “separable” can be replaced by “second countable”. By AC_ω a second countable topological space is separable. For the other direction, note that a Hausdorff, compact, separable space is metrizable, and any separable metric space is second countable. □

25.C. Filters on a set. A filter (ideal) is **κ-complete** if it is closed under intersections (unions) of size $< \kappa$; thus every filter (ideal) is ω-complete. When $\kappa = \omega_1$ it is customary to speak of countably complete filters and ideals; in the latter case one speak of **σ-ideals**. For example $\mathrm{Club}(\kappa)$ is a κ-complete filter, while the collection of null sets, and the collection of meager sets are σ-ideals.

Exercises

Exercise 25.11. Show that:

(i) in a distributive lattice, a maximal ideal is prime;

(ii) the lattice $\mathcal{M}_3$ of Figure 7 on page 78 has three maximal ideals, none of which is prime;

(iii) in the lattice $\mathcal{O}$ of open subsets of $\mathbb{R}$, the family $\mathcal{F}_r = \{U \in \mathcal{O} \mid r \in U\}$ is a prime, non-maximal, filter, for every $r \in \mathbb{R}$.

(iv) Give an example of a lattice L with minimum, without maximum, and with no maximal ideals, so that L^{Δ} is a lattice with maximum, without minimum, and with no maximal filters.

(v) If L is a lattice, then $\mathcal{I}(L) = \{I \subseteq L \mid I \text{ is an ideal of } L\}$ ordered under inclusion is a lattice.

(vi) If $\emptyset \neq \mathcal{I}$ is a family of ideals of a lattice L, then $\bigcap \mathcal{I}$ is an ideal of L. Similarly for $\mathcal{F}$ a non-empty family of filters on L.

Exercise 25.12. A **finitely additive measure** on a Boolean algebra B with values in $\{0,1\}$ is a function $\mu \colon B \to \{0,1\}$ such that $\mu(\mathbf{0}_B) = 0$ and $\mu(a \curlyvee b) = \mu(a) + \mu(b)$ if $a \curlywedge b = \mathbf{0}_B$. If B is ω_1-complete and if the additivity assumption is strengthened to: $\mu(\bigcurlyvee_{n\in\omega} a_n) = \sum_{n=0}^{\infty} \mu(a_n)$ when $a_n \curlywedge a_m = \mathbf{0}_B$ and distinct n, m, we say that μ is a σ-additive measure.

Show that :

(i) If I is a maximal ideal of B, then $\mu_I \colon B \to \{0,1\}$

$$\mu_I(a) = \begin{cases} 0 & \text{if } a \in I, \\ 1 & \text{otherwise,} \end{cases}$$

is a measure on B. Conversely, every measure on B is of the form μ_I for some maximal ideal I.

(ii) If B and I are ω_1-complete, then μ_I is a σ-additive measure.

Exercise 25.13. Show that if $\lambda \leq \kappa$ are infinite cardinals, then $\{X \subseteq \kappa \mid |X| < \lambda \vee |\kappa \setminus X| < \lambda\}$ is a $\operatorname{cof}(\kappa)$-complete subalgebra of $\mathscr{P}(\kappa)$, and that $[\kappa]^{<\lambda}$ is a $\operatorname{cof}(\kappa)$-complete ideal.

Exercise 25.14. Let B be a Boolean algebra and let $b \in B \setminus \{\mathbf{0}\}$ be an element below which there are no atoms.

(i) Assume $\mathsf{DC}(B)$ and construct a function $\langle b_s \mid s \in {}^{<\omega}2\rangle$ such that $b_\emptyset = b$, $\mathbf{0} < b_{s^\frown\langle i\rangle} < b_s$ and $b_{s^\frown\langle 0\rangle} \curlywedge b_{s^\frown\langle 1\rangle} = \mathbf{0}$ for all $s \in {}^{<\omega}2$.

(ii) Assume $\mathsf{DC}(B)$ and show that ${}^{\omega}2 \precsim \{F \mid F \text{ is a filter of } B \text{ and } b \in F\}$.

(iii) Conclude that if B is countable and atomless, then $\operatorname{St}(B) \asymp \mathbb{R}$.

Exercise 25.15. Assume AC. Let U be a non-principal ultrafilter on ω and let A_n be a finite non-empty sets. Show that ${}^{\omega}2 \precsim \prod_U A_n$ if one of the following conditions hold:

(i) $2^n \leq |A_n|$ for all n.

(ii) $n \leq |A_n|$ for all n.

(iii) There is $I = \{i_n \mid n \in \omega\} \in U$ such that $n \leq |A_{i_n}|$.

[Hint: start with (i) and then escalate it to (ii) and (iii).]

Exercise 25.16. Let $\mathscr{C}(X, 2)$ be the set of all continuous maps from X to 2, where 2 is given the discrete topology. Show that:

(i) If X is discrete and finite, then $X \to \mathscr{P}(\mathscr{C}(X, 2))$, $x \mapsto \{f \mid f(x) = 1\}$ is continuous and closed,[4] where $\mathscr{P}(\mathscr{C}(X, 2))$ is identified with ${}^{\mathscr{C}(X,2)}2$.

(ii) If ${}^{Y}2$ is compact, for any set Y, then the product of finite, discrete spaces is compact.

Exercise 25.17. Show that the following are equivalent:

(i) Stone's representation Theorem 14.18.

(ii) Every Boolean algebra has a prime ideal.

(iii) BPI.

(iv) $\mathsf{BPI}(\mathscr{P}(X))$ for all non-empty set X. In other words: every proper filter on X can be extended to an ultrafilter.

(v) Tychonoff's theorem of Hausdorff's spaces.

(vi) ${}^{I}2$ is compact, for all I.

Exercise 25.18. Let Boole be the category of Boolean algebras and ZdCmp be the category of zero-dimensional compact Hausdorff spaces. Assume BPI and show that $\mathrm{St}\colon \textsc{Boole} \to \textsc{ZdCmp}$,

$$f\colon B \to C \quad \rightsquigarrow \quad f_{\mathrm{St}}\colon \mathrm{St}(C) \to \mathrm{St}(B)$$

$f_{\mathrm{St}}(U) = f^{-1}[U]$, and $\mathbf{CLOP}\colon \textsc{ZdCmp} \to \textsc{Boole}$,

$$f\colon X \to Y \quad \rightsquigarrow \quad f_{\mathbf{CLOP}}\colon \mathbf{CLOP}(Y) \to \mathbf{CLOP}(X)$$

$f_{\mathbf{CLOP}}(C) = f^{-1}[C]$, are controvariant functors, and they are inverse of each other.

Exercise 25.19. Let $\langle P, \leq\rangle$ be a non-empty pre-order.

(i) Show that $\sim$ is indeed an equivalence relation, that $\lesssim$ is an ordering, that $\langle P/{\sim}, \lesssim\rangle$ is separative, and that the map

$$\langle P, \leq, \perp\rangle \to \langle P/{\sim}, \lesssim, \perp^*\rangle\,, \qquad p \mapsto [p]$$

is a morphism of structures, where $\perp^*$ is the incompatibility relation for $\lesssim$.

(ii) A **node below** p is a $q \leq p$ which is comparable with every element below p, that is

$$\forall r \leq p\ (q \leq r \ \vee\ r \leq q)\,.$$

Show that if q is a node below p then $q \sim p$. Conclude that if either every element in P is comparable, or else if P has a minimum, then the separable quotient has just one element.

[4] A function between topological spaces is *closed* if it maps closed sets to closed sets.

Exercise 25.20. Show that if D is a dense subset of a complete Boolean algebra B, then

$$\forall X \subseteq B\, \exists Y \subseteq D\, [\bigvee Y = \bigvee X].$$

Exercise 25.21. Let $j\colon P \to Q$ be a map between orders, and assume that j is a dense embedding, or else that P and Q are Boolean algebras, and that j is an embedding of Boolean algebras. Show that j is an embedding of structures $\langle P, \leq_P, \perp_P\rangle \to \langle Q, \leq_Q, \perp_Q\rangle$.

Exercise 25.22. Suppose L is a complete separative lattice. Show that

(i) L is complemented,

(ii) L is a complete Boolean algebra.

Exercise 25.23. Let P be an ordered set. Show that:

(i) if P is separative, then also $\mathbf{DM}(P)$ is separative, hence $\mathbf{DM}(P) \cong \mathbf{RO}(P)$;

(ii) if P is a dense linear order, then $\mathbf{DM}(P) \cong \mathbf{D}(P)$.

Exercise 25.24. Let B be a Boolean algebra. Show that:

(i) B is complete if and only if $\mathrm{St}(B)$ is extremely disconnected, i.e. the closure of any open set is clopen;

(ii) $D \in \mathrm{St}(B)$ is principal if and only if it is an isolated point, so that B is atomless if and only if $\mathrm{St}(B)$ is perfect;

(iii) B is countable if and only if $\mathrm{St}(B)$ is second countable.

Exercise 25.25. Show that:

(i) If A is a countable Boolean algebra and B is an atomless Boolean algebra, then every partial isomorphism $p\colon A' \to B'$ extends to a monomorphism $f\colon A \to B$.

(ii) Every countable atomless Boolean algebra B is **ultrahomogeneous** that is any partial isomorphism $p\colon B' \to B''$ with $B', B'' \subseteq B$ extends to an automorphism $f\colon B \to B$.

Exercise 25.26. Show that there is a $\mathbf{G}_\delta$ set $X \subseteq \mathbb{R}$ which is comeager and of Lebesgue measure zero.

Exercise 25.27. Suppose B be a Boolean algebra, $a \in B^+$ and that $a_n = \inf A_n$, with $A_n \subseteq B$. Show that:

(i) $\{D \in \mathrm{St}(B) \mid A_n \nsubseteq D \vee a_n \in D\}$ is open and dense in $\mathrm{St}(B)$.

(ii) There is $D \in \mathrm{St}(B)$ such that $a \in D$ and $A_n \subseteq D \Rightarrow a_n \in D$ for all $n \in \omega$.

(iii) There is a homomorphism $h\colon B \to \mathbf{2}$ such that $h(a) = \mathbf{1}$ and $h(a_n) = \inf h``A_n$.

Notes and remarks

Theorem 14.18 was proved in 1936 by Stone. The Boolean completion construction was defined by MacNeille in 1937. Exercise 25.27 is due to Tarski.

26. Topology, category, and measure

26.A. Completion of metric spaces. A map $j\colon \langle X_1, d_1\rangle \to \langle X_2, d_2\rangle$ between metric spaces is an **isometric embedding** if $d_1(a,b) = d_2(j(a), j(b))$ for all $a, b \in X_1$. An isometric embedding is always injective; when it is also surjective, then it is called an **isometry** or an **isomorphism of metric spaces**. A **completion** of a metric space $\langle X, d\rangle$ is a complete metric space $\langle \hat{X}, \hat{d}\rangle$ together with an isometric embedding $j\colon X \to \hat{X}$ such that $\operatorname{ran} j$ dense in $\hat{X}$. One way to construct such completion is to take $\hat{X}$ to be the quotient

$$\{s \in {}^{\omega}X \mid s \text{ is a Cauchy sequence in } \langle X, d\rangle\}/{\sim}$$

where $s \sim t \Leftrightarrow \forall \varepsilon > 0\, \exists N\, \forall n, m > N\, d(s(n), t(m)) < \varepsilon$. Then

$$\hat{d}([s],[t]) = \lim_{n\to\infty} d(s(n), t(n))$$

is a metric on $\hat{X}$, the map $j\colon X \to \hat{X}$ sending a point $x \in X$ to the constant sequence $\langle x, x, x, \ldots\rangle$, is an isometric embedding, and $\operatorname{ran} j$ is dense in $\langle \hat{X}, \hat{d}\rangle$. If $j_1\colon \langle X, d\rangle \to \langle \hat{X}_1, \hat{d}_1\rangle$ and $j_2\colon \langle X, d\rangle \to \langle \hat{X}_2, \hat{d}_2\rangle$ are completions, then define $f\colon \hat{X}_1 \to \hat{X}_2$ as follows: given $\hat{x} \in \hat{X}_1$ pick a sequence $s\colon \omega \to X$ such that $j_1(s(n)) \to \hat{x}$, so that $n \mapsto j_1(s(n))$ is a Cauchy sequence in $\hat{X}_1$, and hence s is a Cauchy sequence in X, so that $n \mapsto j_2(s(n))$ is a Cauchy sequence in $\hat{X}_2$, and therefore it converges to a point $f(\hat{x}) \in \hat{X}_2$. Thus $f\colon \langle \hat{X}_1, \hat{d}_1\rangle \to \langle \hat{X}_2, \hat{d}_2\rangle$ is an isometry. Therefore we have shown

Theorem 26.1. *Assume* AC_ω. *The completion of a metric space exists and it is unique up to isomorphism.*

We will always identify the metric space X with its isomorphic copy $j[X] \subseteq \hat{X}$. Note that if $\langle X, d\rangle$ contains a dense subset D of size κ, then D is also dense in $\hat{X}$; in particular, the completion of a separable metric space is separable. The metric space $\mathbb{R}$ can be obtained as the completion of $\mathbb{Q}$ with the Euclidean distance $d(r,s) = |r - s|$.

Definition 26.2. A **Polish space** is a separable topological space which is completely metrizable, i.e. the topology is induced by some complete metric.

Examples of Polish spaces are $\mathbb{R}^n$, separable Banach spaces, countable sets with the discrete topology; an open interval is also Polish, since it is homeomorphic to $\mathbb{R}$. If X is Polish then $Y \subseteq X$ is Polish if and only if Y is $\mathbf{G}_\delta$ in X, that is $Y = \bigcap_n U_n$ with U_n open in X [**Kec95**, Theorem 3.11].

Proposition 26.3 (AC_ω). *Suppose X_i $(i \in \omega)$ are topological spaces.*

(a) *If the X_is are separable, then so is $\prod_{i\in\omega} X_i$.*

(b) *If the X_is are completely metrizable, then so is $\prod_{i\in\omega} X_i$.*

(c) *If the X_is are Polish, then so is $\prod_{i\in\omega} X_i$.*

Proof. (a) To avoid trivialities, suppose $X_i \neq \emptyset$ for all $i \in \omega$, and choose $D_i = \{d_{i,n} \mid n \in \omega\}$ dense in X_i. Let S be the set of all functions s such that $\operatorname{dom} s \subseteq \omega$ is finite and $s(i) \in D_i$ for all $i \in \operatorname{dom} s$. Then S is countable, and so is

$$D = \{f \in \bigtimes_{n\in\omega} X_n \mid \exists s \in S\, (s \subset f \wedge \forall i \in \omega \setminus \operatorname{dom} s\, (f(i) = d_{i,0}))\}.$$

Given a non-empty basic open set $V = \prod_{m\in M} U_m$ where $M \in [\omega]^{<\omega}$ and U_m is open in X_m, pick $s \in S$ with $\operatorname{dom} s = M$, so that any $f \in \bigtimes_{n\in\omega} X_n$ extending s belongs to $V \cap D$. This proves that D is dense in $\prod_{i\in\omega} X_i$.

(b) Let d_i be a complete distance on X_i. Replacing d_i with $\frac{d_i}{1+d_i}$ if needed, we may assume that $d_i \leq 1$ for all $i \in \omega$. We claim that the metric on $\prod_{i\in\omega} X_i$

$$d(f, g) = \sum_{i=0}^{\infty} \frac{d_i(f(i), g(i))}{2^i}$$

is compatible with the product topology, and it is complete.

finish!

(c) follows from (a) and (b). □

Any discrete space X is completely metrizable via the distance $d(x, y) = 1$ if and only if $x \neq y$, and $d(x, x) = 0$. Therefore any set of the form ${}^\omega X$ can be seen as a complete metric space; if moreover X is countable, then ${}^\omega X$ is separable, and hence Polish. In particular the **Cantor space** ${}^\omega 2$ and the **Baire space** ${}^\omega\omega$ are Polish. Recall from Section 13.F that the lexicographic order $\leq_{\text{lex}}$ on ${}^\omega 2$ is a total order, and ${}^\omega 2$ with the order topology is homeomorphic to Cantor's ternary set $E_{1/3} \subseteq [0; 1]$ defined in (13.10) on page 323. By Exercise 26.20 the order topology on ${}^\omega 2$ is the same as the product topology, so the Cantor space can be identified with $E_{1/3}$. On the other hand the order topology is not the same as the product topology on ${}^\omega\omega$. The Baire space is homeomorphic to $\mathbb{R} \setminus D$ where D is countable and dense in $\mathbb{R}$; in particular it is homeomorphic to the irrationals (Exercise 26.21).

The **body** of a descriptive tree T on X (Definition 23.16) is the set of all infinite branches of T

$$[T] = \{f \in {}^\omega X \mid \forall n \in \omega\, (f \restriction n \in T)\}$$

with the topology induced by the basic open sets

$$\boldsymbol{N}_s([T]) = \boldsymbol{N}_s = \{f \in [T] \mid s \subset f\}, \qquad (s \in T).$$

So an open set of $[T]$ is of the form $\bigcup_{s\in\mathcal{A}} \boldsymbol{N}_s$ for some $\mathcal{A} \subseteq T$. In particular, if $T = {}^{<\omega}X$, then $[T] = {}^{\omega}X$ and its topology is the product topology when X is given the discrete topology.

Corollary 26.4. *If T is a descriptive tree on some countable set X, then $[T]$ is Polish.*

The closed subsets of $[T]$ can be identified with pruned subtrees of T.

Proposition 26.5. *Suppose T is a descriptive tree on $X \neq \emptyset$.*

(a) *If $S \subseteq T$ is a descriptive tree on X then $[S]$ is a closed subset of $[T]$.*

(b) *Every non-empty closed subset of $[T]$ of the form $[S]$ for some pruned descriptive tree $S \subseteq T$.*

Proof. (a) If $f \in [T] \setminus [S]$ then $f \restriction n \notin S$ for some $n \in \omega$, and therefore $\boldsymbol{N}_{f\restriction n}$ is an open neighborhood of f disjoint from $[S]$.

(b) Let $C \subseteq [T]$ be closed. The set $S = \{s \in T \mid \boldsymbol{N}_s \cap C \neq \emptyset\}$ is a pruned descriptive tree on X, and $C \subseteq [S]$ by construction. Suppose $f \in [S]$ and pick $f_n \in \boldsymbol{N}_{f\restriction n} \cap C$ which is possible since $f \restriction n \in S$ for all n. Then $f_n \to f$ and therefore $f \in C$ by closure. Therefore $[S] \subseteq C$. □

26.B. Cantor schemes. The construction of Cantor's set $E_{1/3}$ in Section 13.F.1 can be generalized. A **Cantor scheme** in a complete metric space $\langle X, d\rangle$ is a function $\langle (x_s, r_s) \mid s \in {}^{<\omega}2\rangle$ with the following properties: for every $s \in {}^{<\omega}2$

- $x_s \in X$ and $r_s \in \mathbb{R}_+$,
- $\operatorname{Cl} \mathrm{B}(x_{s^\frown\langle i\rangle}; r_{s^\frown\langle i\rangle}) \subseteq \mathrm{B}(x_s; r_s)$, for all $i \in 2$,
- $\mathrm{B}(x_{s^\frown\langle 0\rangle}; r_{s^\frown\langle 0\rangle}) \cap \mathrm{B}(x_{s^\frown\langle 1\rangle}; r_{s^\frown\langle 1\rangle}) = \emptyset$,

and such that $\lim_{n\to\infty} r_{z\restriction n} = 0$ for all $z \in {}^{\omega}2$. It is immediate to check that

$$s \subset t \Rightarrow \mathrm{B}(x_s; r_s) \supset \mathrm{B}(x_t; r_t). \tag{26.1}$$

Suppose instead that $s, t \in {}^{<\omega}2$ are incomparable, that is $s \not\subseteq t$ and $s \not\supseteq t$. Let $\bar{n}$ be such that $s \restriction \bar{n} = t \restriction \bar{n}$, but $s(\bar{n}) \neq t(\bar{n})$. Then $\mathrm{B}(x_{s\restriction\bar{n}+1}; r_{s\restriction\bar{n}+1}) \cap \mathrm{B}(x_{t\restriction\bar{n}+1}; r_{t\restriction\bar{n}+1}) = \emptyset$ hence $\mathrm{B}(x_s; r_s) \cap \mathrm{B}(x_t; r_t) = \emptyset$ by (26.1).

We can thus construct a continuous function $f\colon {}^{\omega}2 \to X$, $\{f(z)\} = \bigcap_n \mathrm{B}(x_{z\restriction n}; r_{z\restriction n})$.

Theorem 26.6. *Let $\langle X, d\rangle$ be a separable metric space, non-empty and without isolated points. Then there is a continuous injective function $f\colon {}^{\omega}2 \rightarrowtail X$. In particular: X contains a homeomorphic copy of Cantor's set.*

Proof. Let $E = \{e_n \mid n \in \omega\}$ be dense in X. Inductively construct real numbers r_s and points $x_s \in X$ ($s \in {}^{<\omega}2$), such that

(i) $0 < r_s \leq 2^{-\operatorname{lh}(s)}$,

(ii) $\operatorname{Cl}(\mathrm{B}(x_{s^\frown\langle i\rangle}; r_{s^\frown\langle i\rangle})) \subseteq \mathrm{B}(x_s, r_s)$, for $i = 0, 1$,

(iii) $\operatorname{Cl}\bigl(\mathrm{B}(x_{s^\frown\langle 0\rangle}; r_{s^\frown\langle 0\rangle})\bigr) \cap \operatorname{Cl}\Bigl(\mathrm{B}(x_{s^\frown\langle 1\rangle}; r_{s^\frown\langle 1\rangle})\Bigr) = \emptyset$.

Set $x_\emptyset \in X$ and $r_\emptyset = 1$. Given x_s and r_s it is easy to check that $E \cap \mathrm{B}(x_s, r_s)$ is infinite, hence it is possible to choose two distinct points $x_{s^\frown\langle 0\rangle}$ and $x_{s^\frown\langle 1\rangle}$ in this set. (For example, take e_k and e_h, where k and h are the first two indexes i such that $e_i \in E \cap \mathrm{B}(x_s, r_s)$.) Choose sufficiently small $r_{s^\frown\langle i\rangle}$ ($i = 0, 1$) so that (i)–(iii) hold.

For every $y \in {}^\omega 2$ consider the sequence $\langle x_{y\restriction n} \mid n\rangle$. As $\mathrm{B}(x_{y\restriction n}, r_{y\restriction n}) \supseteq \mathrm{B}(x_{y\restriction n+1}, r_{y\restriction n+1})$ by (ii),

$$\forall k \geq n\, (x_{y\restriction k} \in \mathrm{B}(x_{y\restriction n}, r_{y\restriction n}))\,. \tag{26.2}$$

Therefore $\langle x_{y\restriction n} \mid n\rangle$ is a Cauchy sequence, and let $f(y) = \lim_n x_{y\restriction n}$. By (26.2) $f(y) \in \operatorname{Cl}\bigl(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n})\bigr)$ for every n and hence

$$f(y) \in \textstyle\bigcap_n \operatorname{Cl}\bigl(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n})\bigr) = \bigcap_n \mathrm{B}(x_{y\restriction n}, r_{y\restriction n}),$$

where the second equality follows from (ii). If $y, z \in {}^\omega 2$ are distinct, let n be such that $y \restriction n = z \restriction n$ and $y(n) \neq z(n)$. Then $f(y) \in \operatorname{Cl}\bigl(\mathrm{B}(x_{y\restriction n}, r_{y\restriction n})\bigr)$ and $f(z) \in \operatorname{Cl}\bigl(\mathrm{B}(x_{z\restriction n}, r_{z\restriction n})\bigr)$, hence $f(y) \neq f(z)$ by (iii). In other words, the function $f\colon {}^\omega 2 \to X$ is injective. We are left to show that it is continuous. Given $y \in {}^\omega 2$ and n, it is enough to find k such that if $z \restriction k = y \restriction k$, then $d(x_{z\restriction k}, x_{y\restriction k}) < 2^{-n}$. It is easy to check that $k = n$ works. □

26.C. The property of Baire. Recall from Section 7.A in Chapter **??** the **downward topology** on a preordered set $\langle P, \leq\rangle$. Thus $D \subseteq P$ is **dense** (with respect to the downward topology) if and only if $\forall p \in P \exists q \in D\, (q \leq p)$.

Theorem 26.7. *Let $\langle P, \leq\rangle$ be a preordered set, and assume $\mathsf{DC}(\omega \times P)$. Let $D_n \subseteq P$ ($n \in \omega$) be dense sets in the downward topology. Then for every $\bar{p} \in P$ there is a sequence $\bar{p} \geq p_0 \geq p_1 \geq \dots$ of elements of P such that $\forall n \in \omega\, (p_n \in D_n)$.*

Proof. Fix $\bar{p} \in P$ and consider the relation R on $X = \bigcup_{n\in\omega} \{n\} \times D_n$,

$$(n, q)\ R\ (m, r) \quad \Leftrightarrow \quad m = n + 1 \wedge q \geq r.$$

By density there is $p_0 \in D_0$ such that $\bar{p} \geq p_0$, so by $\mathsf{DC}(X)$ (which follows from $\mathsf{DC}(\omega \times P)$ as $\omega \times P \twoheadrightarrow X$) a sequence $(0, p_0)\ R\ (1, p_1)\ R\ (2, p_2)\ R \dots$ is obtained, hence the sequence $\bar{p} \geq p_0 \geq p_1 \geq \dots$ is the object we were looking for. □

The next result, known as the **Baire Category Theorem**, states that in many topological spaces the countable intersection of open dense sets is non-empty. Recall that a topological space X is locally compact if it is T_2 and every point has a neighborhood with compact closure. it follows that for all $x \in U$ there is $V \subseteq U$ compact neighborhood of x.

Theorem 26.8. *Assume* DC. *Let $X \neq \emptyset$ be a locally compact space, or a complete metric space. If the U_ns are open and dense then $\bigcap_{n\in\omega} U_n$ is dense.*

Proof. Let $U \neq \emptyset$ be open.

Suppose first that X is a complete metric space. Let

$$P = \{p \subseteq X \mid p \text{ is an open ball}\}$$

with $p \leq q \Leftrightarrow p \subseteq q$, and let $D_n = \{p \mid \operatorname{diam}(p) \leq 2^{-n} \wedge \operatorname{Cl}(p) \subseteq U_n\}$. By Exercise 26.18 D_n is dense in P with respect to the downward topology. Let $\bar{p} \in P$ be such that $\bar{p} \subseteq U$. Construct a sequence $\langle p_n \mid n \in \omega\rangle$ as in Theorem 26.7. Let $x_n \in X$ be the center of p_n. By construction, $x_i, x_j \in p_N$ hence $d(x_i, x_j) < 2^{-N}$, for all $i, j \geq N$ hence $\langle x_n \mid n \in \omega\rangle$ is a Cauchy sequence with respect to the complete metric d, and let $\bar{x} \in X$ be its limit. For each $n \in \omega$, $d(\bar{x}, x_n) \leq 2^{-n}$ hence $\bar{x} \in \operatorname{Cl}(p_n) \subseteq U_n$. In other words: $\bar{x} \in \bigcap_n U_n$. Since $\bar{x} \in p_0 \subseteq U$, we have proved that $\bigcap_{n\in\omega} U_n \cap U \neq \emptyset$, as required.

Suppose now that X is locally compact: the preorder is

$$P = \{p \subseteq X \mid p \neq \emptyset \text{ is an open set with compact closure}\}$$

with the ordering $p \leq q \Leftrightarrow \operatorname{Cl}(p) = \operatorname{Cl}(q)$ and let $D_n = \{p \in P \mid p \subseteq U_n\}$. Let $\bar{p} \in P$ be such that $\bar{p} \subseteq U$. Fix $(p_n)_n$ as in Theorem 26.7, and note that $\{\operatorname{Cl}(p_n) \mid n \in \omega\}$ is a decreasing family of non-empty compact sets, hence by the finite intersection property $\bigcap_n \operatorname{Cl}(p_n)$ contains an element $\bar{x}$. Therefore $\bar{x} \in \bigcap_n U_n$ and since $\bar{x} \in p_0 \subseteq \bar{p} \subseteq U$ the result is proved. □

Remarks 26.9. (a) If X is *separable* complete metric, or *second countable* locally compact, then the order P can be taken to be countable, hence DC can be avoided. (In the case of metric spaces, take the open balls with centers in the countable dense sets and rational radius; in the case of locally compact spaces take the basic open sets with compact closure.) In particular, Theorem 26.8 for $\mathbb{R}^n$ or for a separable Banach space is provable without choice.

(b) Theorem 26.8 for arbitrary complete metric implies DC.

expand

(c) If X satisfies the hypotheses of Theorem 26.8 and has no isolated points, then $X \setminus \{x\}$ is an open dense subset of X, hence X is not countable.

A subset M of a topological space X is **meager** or of **first category** if there are closed sets C_n with empty interior such that $M \subseteq \bigcup_n C_n$. Thus the

Baire category theorem says that in a locally compact space, or in a complete metric space, no non-empty open set is meager.

The Baire category theorem is often used to prove *existence* results: in order to prove the existence of some $x \in X$ satisfying property P (assuming X is a complete metric space or a locally compact space) it is enough to show that $\{x \in X \mid P(x)\}$ is non-meager, hence non-empty. (In many cases one shows that this set is comeager, and hence non-meager.) For example the set

$$\mathscr{D} = \{\mathscr{C}([0;1]) \mid \exists x \in [0;1]\ f \text{ is differentiable in } x\}$$

is meager, hence $\mathscr{C}([0;1]) \setminus \mathscr{D}$ is comeager [**Fol99**, pag.??]. In particular, the generic continuous function on $[0;1]$ is not differentiable at any point.

26.D. Measure.

26.D.1. *Basic notions.* A **measure space** is a triple $\langle X, \mathcal{S}, \mu\rangle$ such that $\mathcal{S}$ is a σ-algebra on X and $\mu\colon \mathcal{S} \to [0;+\infty]$ is a **measure** that is a function such that $\mu(\emptyset) = 0$ and $\mu\big(\bigcup_n A_n\big) = \sum_{n=0}^{\infty} \mu(A_n)$, if the $A_n \in \mathcal{S}$ are pairwise disjoint—this last property is called **σ-additivity**.[5] The sets in $\mathcal{S}$ are said to be **$\mathcal{S}$-measurable** and $\textsc{Null}(X, \mathcal{S}, \mu) = \{A \in \mathcal{S} \mid \mu(A) = 0\}$ is the family of **null sets**. A measure space is

- **complete** if $A \in \textsc{Null}(\mu)$ and $B \subseteq A$ implies that $B \in \mathcal{S}$ and hence $\mu(B) = 0$;
- **singular** if there are $x \in X$ such that $\{x\} \in \mathcal{S}$ and $\mu(\{x\}) > 0$;
- **atomless** if there are no **atoms**, that is sets $A \in \mathcal{S} \setminus \textsc{Null}(\mu)$ such that $\forall B \in \mathscr{P}(A) \cap \mathcal{S}\, (\mu(B) = \mu(A) \vee \mu(B) = 0)$;
- **non-zero** if $\textsc{Null}(\mu) \neq \mathcal{S}$;
- **finite** if $\mu(X) < +\infty$, **σ-finite** if there are $X_n \in \mathcal{S}$ such that $X = \bigcup_n X_n$ and $\mu(X_n) < +\infty$, and **probability** if $\mu(X) = 1$.

Remark 26.10. The definition of measure space is redundant, as everything can be retrieved from the measure: $\mathcal{S} = \operatorname{dom}(\mu)$ and $X = \bigcup \mathcal{S}$. For this reason it is customary ascribe the above attributes (complete, singular, ...) to the measure μ rather than to the measure space. On the other hand one often does not distinguish μ from its restriction to a sub-σ-algebra, so this redundancy comes handy.

The property of being atomless is a strengthening of being non-singular. It implies that inside any set of positive finite measure there are sets of any prescribed smaller measure (Exercise 26.31). Thus the range of an atomless measure is an initial segment of $[0 : +\infty]$.

[5] It is understood that if one or more summands is infinite, then so is the sum of the series.

Given a measure space $\langle X, \mathcal{S}, \mu \rangle$ the family

$$\mathcal{N} = \{N \subseteq X \mid \exists A \in \textsc{Null}(\mu)\, (N \subseteq A)\}$$

is a σ-ideal of $\mathscr{P}(X)$, and by Exercise **??** $\bar{\mathcal{S}} = \{A \triangle N \mid A \in \mathcal{S} \wedge N \in \mathcal{N}\}$ is the smallest σ-algebra containing $\mathcal{S} \cup \mathcal{N}$. The function $\bar{\mu} \colon \bar{\mathcal{S}} \to [0; +\infty]$, $\bar{\mu}(A \triangle N) = \mu(A)$ is well-defined, and it is a complete measure extending μ, and such that $\textsc{Null}(\bar{\mu}) = \mathcal{N}$. The measure space $\langle X, \bar{\mathcal{S}}, \bar{\mu} \rangle$ is the **completion** of $\langle X, \mathcal{S}, \mu \rangle$—clearly a complete measure coincides with its completion.

If X is a topological space, then $\mu \colon \textsc{Bor}(X) \to [0; +\infty]$ is called a **Borel measure**. If X is metrizable then any finite Borel measure μ satisfies

$$\begin{aligned} \mu(A) &= \sup\{\mu(F) \mid F \subseteq A \text{ is closed}\} \\ &= \inf\{\mu(U) \mid U \supseteq A \text{ is open}\}. \end{aligned}$$

Moreover if X is Polish, then $\mu(A) = \sup\{\mu(K) \mid K \subseteq A \text{ is compact}\}$—see [**Kec95**, Theorems 17.1 and 17.11].

If $\langle G, + \rangle$ is an abelian group, then $\langle G, \mathcal{S}, \mu \rangle$ is **translation invariant** if $\mu(A) = \mu(g + A)$ for all $g \in G$ and $A \in \mathcal{S}$, where it is required that $A \in \mathcal{S} \Rightarrow g + A = \{g + a \mid a \in A\} \in \mathcal{S}$. If G is locally compact, then there is a non-zero, σ-finite, translation invariant Borel measure on G called a **Haar measure**, and if μ_1 and μ_2 are two such measures, there is $r > 0$ such that $\mu_1(A) = r \cdot \mu_2(A)$ for all Borel A. If G is compact then the Haar measure μ is finite, and for any $r > 0$ there is a unique Haar measure such that $\mu(G) = r$. In view of this if G is a compact group it is customary to assume that the Haar measure is a probability one.

26.D.2. *Outer measures.* An **outer measure** on X is a function $F \colon \mathscr{P}(X) \to [0; +\infty]$ such that $F(\emptyset) = 0$, $A \subseteq B \Rightarrow F(A) \leq F(B)$, and it is σ-subadditive, namely: $F(\bigcup_{n \in \omega} X_n) \leq \sum_{n=0}^{\infty} F(X_n)$, for all choices of $X_n \subseteq X$. Despite its name, an outer measure need not be a measure, but it induces one. If F is an outer measure on X, then

$$\mathcal{S} = \{A \subseteq X \mid \forall B \subseteq X\, (F(B \cap A) + F(B \setminus A) \leq F(B))\}$$

is a σ-algebra, $\mu = F \restriction \mathcal{S}$ is a measure, and $\langle X, \mathcal{S}, \mu \rangle$ is a complete measure space [**Fre04a**, Carathéodory's Theorem 113C].

Proposition 26.11. *Let $\mathcal{B} \subseteq \mathscr{P}(X)$ be a family covering X, and let $\nu \colon \mathcal{B} \to [0; +\infty)$ be monotone. Then $\mathsf{AC}_\omega(\mathcal{B})$ implies that $F \colon \mathscr{P}(X) \to [0; +\infty]$*

$$F(A) = \inf\{\textstyle\sum_{n=0}^{\infty} \nu(B_n) \mid B_n \in \mathcal{B} \wedge A \subseteq \bigcup_{n \in \omega} B_n\}$$

is an outer measure.

Proof. Monotonicity is clear. Towards showing σ-subadditivity, we fix an $\varepsilon > 0$ and prove that $F(\bigcup_n X_n) \leq \sum_{n=0}^{\infty} F(X_n) + \varepsilon$. For every n, using

$\mathsf{AC}_\omega(\mathcal{B})$ choose $B^i_n \in \mathcal{B}$ such that

$$X_n \subseteq \bigcup_{i\in\omega} B^i_n \quad\text{and}\quad \sum_{i=0}^{\infty} \nu(B^i_n) < F(X_n) + \varepsilon/2^{n+1}. \tag{26.3}$$

Once the B^i_n are chosen, the result follows by noting that $\bigcup_{n\in\omega} X_n \subseteq \bigcup_{n\in\omega}\bigcup_{i\in\omega} B^i_n$ and

$$\sum_{n=0}^{\infty}\sum_{i=0}^{\infty} \nu(B^i_n) \leq \sum_{n=0}^{\infty}(F(X_n) + \varepsilon/2^{n+1}) = \sum_{n=0}^{\infty} F(X_n) + \varepsilon. \qquad \square$$

26.D.3. *The Lebesgue measure on the reals.* Let $\mathcal{B} = \{[a;b) \mid a < b\} \subseteq \mathscr{P}(\mathbb{R})$ be the family of all half-open intervals, and let $\nu([a;b)) = b - a$. Observe that $\mathcal{B} \asymp \mathbb{R}$, so $\mathsf{AC}_\omega(\mathbb{R})$ implies that

$$F(A) = \inf\{\textstyle\sum_{n=0}^{\infty}(b_n - a_n) \mid A \subseteq \bigcup_{n<\omega}[a_n; b_n)\},$$

is an outer measure. The measure induced by F is the **Lebesgue measure** on $\mathbb{R}$ and it is denoted with λ, the σ-algebra from Carathéodory's theorem is the collection of the **Lebesgue measurable sets** and it is denoted with $\textsc{Meas}(\mathbb{R}, \lambda)$ or simply $\textsc{Meas}(\lambda)$. The Lebesgue measure λ is complete, non-singular, atomless, σ-finite, and translation invariant, that is it is the completion of a Haar measure for $\langle \mathbb{R}, + \rangle$.

Remark 26.12. The appeal to $\mathsf{AC}_\omega(\mathbb{R})$ cannot be avoided, since the existence of any non-singular measure on $\mathbb{R}$ (or on ${}^{\omega}2$, or ${}^{\omega}\omega$) implies that $\mathbb{R}$ is not countable union of countable sets, a fact that cannot be proved without choice.

The construction of the Lebesgue measure can be repeated for $\mathbb{R}^n$, using the sets

$$[\boldsymbol{a}; \boldsymbol{b}) \overset{\text{def}}{=} \{\boldsymbol{c} \in \mathbb{R}^n \mid a_i \leq c_i < b_i\}$$

in place of the intervals $[a;b)$, where we have followed the convention that the n-tuple $(x_1, \ldots, x_n) \in \mathbb{R}^n$ is denoted by $\boldsymbol{x}$. Similarly, the volume $\prod_{i=1}^{n}(b_i - a_i)$ is used in place of the length $(b-a)$. The corresponding measure and σ-algebra are denoted with λ^n and $\textsc{Meas}(\mathbb{R}^n, \lambda^n)$ or $\textsc{Meas}(\lambda^n)$.

If I is an (open, closed, semi-open) interval with endpoints $a < b$, then $\lambda(I) = b - a$. Recall that the Cantor set $E_{1/3}$ (see page 323) is obtained by removing a countable family of open sets from the interval $[0;1]$. The measure of its complement in $[0;1]$ is $\sum_{n=1}^{\infty} \frac{1}{3^n} = 1$ and hence $\lambda(E_{1/3}) = 0$. Therefore $E_{1/3}$ is an example of a closed, uncountable set without interior and of measure 0.

26.D.4. *The measure on the Cantor and Baire spaces.* Let T be a pruned descriptive tree on ω, and let $m\colon T \to [0;1]$ be a function such that $m(\langle\rangle) = 1$ and for all $t \in T$

$$m(t) = \sum_{t^\frown\langle n\rangle \in T} m(t^\frown\langle n\rangle).$$

Then $F\colon \mathscr{P}([T]) \to [0;1]$, $F(A) = \inf\{\sum_{t\in\mathcal{A}} m(t) \mid \mathcal{A} \subseteq T \wedge A \subseteq \bigcup_{t\in\mathcal{A}} \boldsymbol{N}_t\}$ is an outer-measure, yielding a probability measure such that $\mu(\boldsymbol{N}_t) = m(t)$ for all $t \in T$.

Suppose $T = {}^{<\omega}2$ so that $[T] = {}^{\omega}2$ is the Cantor space, and let m be such that $m(s^\frown\langle i\rangle) = m(s)/2$ for all $s \in {}^{<\omega}2$ and $i \in 2$. The resulting measure μ_{C} is called the **Cantor measure** or **coin-tossing measure** and $\mu_{\mathrm{C}}(\boldsymbol{N}_s) = 2^{-\operatorname{lh} s}$.

Suppose $T = {}^{<\omega}\omega$ so that $[T] = {}^{\omega}\omega$ is the Baire space, and let m be such that $m(s^\frown\langle i\rangle) = m(s)/2^{i+1}$ for all $s \in {}^{<\omega}2$ and $i \in \omega$. The resulting measure μ_{B} is called the **Baire measure**.

μ_{C} is called the **Cantor measure** or **Lebesgue measure on Cantor's set**. Calling μ_{C} the Lebesgue measure may seem a bit peculiar, since ${}^{\omega}2$ is usually identified with $E_{1/3}$ and $\mu_{\mathrm{C}}({}^{\omega}2) = 1$, while $\lambda(E_{1/3}) = 0$. On the other hand ${}^{\omega}2$ can be identified with (i.e. is homeomorphic to) a subset of $[0;2]$ of λ-measure equal to 1 (Exercise 26.27). Subsets of $\mathbb{R}$ homeomorphic to ${}^{\omega}2$ are obtained by generalizing in several directions the construction of $E_{1/3}$. For example we can replace the interval $[0;1]$ with an arbitrary closed interval J and choose a coefficient $r_n \in (0;1)$ to be used at stage n of the construction, that is we define

expand

$$\operatorname{Cantor}(J;(r_m)_m) = \bigcap_n \operatorname{Cantor}^{(n)}(J;(r_m)_m) \tag{26.4}$$

where $\operatorname{Cantor}^{(0)}(J;(r_m)_m) = J$, $\operatorname{Cantor}^{(n)}(J;(r_m)_m)$ is union of 2^n closed pairwise disjoint intervals and $\operatorname{Cantor}^{(n+1)}(J;(r_m)_m)$ is obtained by replacing each interval I of $\operatorname{Cantor}^{(n)}(J;(r_m)_m)$ with $I_{(0;r_n)}$ and $I_{(1;r_n)}$, defined in (13.9). The sets $\operatorname{Cantor}(J;(r_m)_m)$ are called **generalized Cantor sets**. When the sequence $(r_n)_n$ is constantly equal to r we will write $\operatorname{Cantor}(J,r)$. Thus $E^{(n)}_{1/3} = \operatorname{Cantor}^{(n)}([0;1],1/3)$ and

$$E_{1/3} = \operatorname{Cantor}([0;1],1/3).$$

26.D.5. *Extensions of the Lebesgue measure.* By Vitali's construction there aren't any non-zero, non-singular, translation invariant measures on $\mathscr{P}(\mathbb{R})$ or, equivalently, on $\mathscr{P}([0;1])$. The requirements that the measure be non-zero and non-singular are put forth to avoid trivialities, so the culprit must be translation invariance.

Question 26.13 (Banach)**.** Is there a non-zero, non-singular measure μ with domain $\mathscr{P}([0;1])$? Is it possible to have such μ extending the Lebesgue measure?

More generally one could ask whether there is a non-singular probability measure on some set X, that is a measure with domain $\mathscr{P}(X)$. A measure on a set is **κ-additive** if the union of $< \kappa$ null sets null—thus ω_1-additivity is just σ-additivity. Observe that if μ is κ-additive, $\gamma < \kappa$, and the sets $\{A_\alpha \mid \alpha < \gamma\}$ are pairwise disjoint, then

$$\mu(\textstyle\bigcup_{\alpha<\gamma} A_\alpha) = \sum_{\alpha<\gamma} \mu(A_\alpha) = \sup\{\sum_{\alpha \in F} \mu(A_\alpha) \mid F \in [\gamma]^{<\omega}\}$$

as by Exercise 26.30 all but countably many A_αs are null.

Theorem 26.14. *Assume* AC *and suppose $\langle X, \mathcal{S}, \mu\rangle$ is a non-zero, finite, atomless measure space. Then μ is not $(2^{\aleph_0})^+$-complete, and if $\mathcal{S} = \mathscr{P}(X)$ then there is a probability measure $\nu \colon \mathscr{P}({}^{\omega}2) \to [0;1]$ extending μ_{C}.*

Proof. Using Exercise 26.31 we can construct $X_s \in \mathcal{S}$, for $s \in {}^{<\omega}2$. Set $X_{\langle\rangle} = X$ and given X_s pick disjoint $X_{s^\frown\langle 0\rangle}, X_{s^\frown\langle 1\rangle}$ of measure $\mu(X_s)/2$ such that $X_s = X_{s^\frown\langle 0\rangle} \cup X_{s^\frown\langle 1\rangle}$. For all $f \in {}^{\omega}2$ the set $X_f = \bigcap_{n\in\omega} X_{f\restriction n} \in \mathcal{S}$ is null, and since $X = \bigcup_{f\in{}^{\omega}2} X_f$ is non-null, this means that $\textsc{Null}(\mu)$ is not closed under unions of size $2^{\aleph_0}$.

Suppose now $\mathcal{S} = \mathscr{P}(X)$. Replacing μ with $\mu/\mu(X)$ if needed, we may assume that μ is a probability measure. For $A \subseteq {}^{\omega}2$ set $\nu(A) = \mu(\bigcup_{f\in A} X_f)$. As $\nu(\boldsymbol{N}_s) = \mu(X_s) = \mu_{\mathrm{C}}(\boldsymbol{N}_s)$ for all $s \in {}^{<\omega}2$, the measure ν extends μ_{C}. □

The proof above can be modified with ${}^{\omega}2$ replaced by $[0;1]$. Therefore the answer to Banach's question 26.13 is positive if we assume the existence of a non-zero, atomless measure on some $\mathscr{P}(X)$. As the nature of X is irrelevant, we may replace it with its cardinality κ, which must be uncountable by σ-additivity.

Lemma 26.15. *Suppose κ is the least cardinal for which there is a non-singular, probability measure μ with domain $\mathscr{P}(\kappa)$. Then μ is κ-additive.*

Proof. Towards a contradiction there is $\lambda < \kappa$ and there are null sets $A_\alpha \subseteq \kappa$ for $\alpha < \lambda$, such that $\mu(\bigcup_{\alpha<\lambda} A_\alpha) > 0$. Then

$$\nu \colon \mathscr{P}(\lambda) \to [0;1], \quad \nu(X) = \frac{\mu(\bigcup_{\alpha\in X} A_\alpha)}{\mu(\bigcup_{\alpha<\lambda} A_\alpha)}$$

is a non-singular probability measure, against the minimality of κ. □

Definition 26.16. A cardinal $\kappa > \omega$ is **real-valued measurable** if there is a κ-additive, non-singular, probability measure with domain $\mathscr{P}(\kappa)$.

Theorem 26.17. *A real-valued measurable cardinal κ is regular, and if* AC *is assumed, then κ is limit, and therefore weakly inaccessible.*

Proof. Let $\mu \colon \mathscr{P}(\kappa) \to [0;1]$ be a κ-additive, non-singular, probability measure.

Suppose κ is singular, i.e. $\kappa = \sup_{i\in\gamma} \alpha_i$, with $\gamma < \kappa$ and $\alpha_i < \kappa$. By κ-additivity $\mu(\alpha) = \mu(\bigcup_{\beta\in\alpha} \{\beta\}) = 0$ for all $\alpha < \kappa$, and hence $\mu(X) = 0$ for any bounded $X \subseteq \kappa$. Therefore

$$\mu(\kappa) = \mu(\bigcup_{i\in\gamma}(\alpha_i \setminus \bigcup_{j<i} \alpha_j)) = \sum_{i\in\gamma} \mu(\alpha_i \setminus \bigcup_{j<i} \alpha_j) = 0$$

a contradiction. Thus κ is a regular cardinal.

If $\kappa = \lambda^+$ then by Ulam's Theorem 25.5 there are pairwise disjoint, non-null $A_\alpha \subseteq \kappa$ for $\alpha < \kappa$, against Exercise 26.30. Therefore κ is a limit cardinal. □

The import of Theorems 26.14 and 26.17 is that any real valued measurable cardinal with an atomless measure is $\leq 2^{\aleph_0}$, so that if the answer to Banach's Question 26.13 is affirmative, then the continuum must be very large. In Section 40 we will look at real valued measurable cardinals having a measure with atoms.

Exercises

Exercise 26.18. Let X be a topological space, and let P be the collection of all non-empty open subsets, ordered by $p \leq q \Leftrightarrow p \subseteq q$. Show that

(i) if $D \subseteq P$ is dense with respect to the downward topology of P then $\bigcup_{p\in D} p$ is open and dense in X;

(ii) if X is metric, then $\{p \in P \mid \operatorname{diam}(p) \leq 2^{-n}\}$ is dense in P.

Exercise 26.19. Let $P = \{p \subseteq \omega \times \omega \mid p \text{ is a finite function}\}$ ordered by $p \leq q \Leftrightarrow p \supseteq q$. Show that the sets $A_n = \{p \mid n \in \operatorname{dom}(p)\}$ and $B_n = \{p \mid n \in \operatorname{ran}(p)\}$ are dense in P.

Exercise 26.20. Show that

(i) $\langle {}^\omega 2, <_{\mathrm{lex}}\rangle$ is homeomorphic to Cantor's space;

(ii) $\langle {}^\omega \omega, <_{\mathrm{lex}}\rangle$ is isomorphic (and hence homeomorphic) to $\langle [0;1), <\rangle$. In particular $\langle {}^\omega \omega, <_{\mathrm{lex}}\rangle$ is not homeomorphic to the Baire space.

Exercise 26.21. Show that ${}^\omega\omega$ is homeomorphic to $\mathbb{R} \setminus D$ where D is countable and dense in $\mathbb{R}$.

Exercise 26.22. Fix an ordinal $1 < \xi < \omega_1$ and let $<$ be the lexicographic ordering on ${}^{<\omega}\xi$, that is

$$\begin{aligned} s < t \Leftrightarrow{} & \exists u \in {}^{<\omega}\xi\, (u \neq \emptyset \wedge s^\frown u = t) \vee \\ & \exists u, v, w \in {}^{<\omega}\xi\, \exists \alpha, \beta \in \xi\, (s = u^\frown \langle\alpha\rangle^\frown v \wedge t = u^\frown \langle\beta\rangle^\frown w \wedge \alpha < \beta). \end{aligned}$$

Let $I = {}^{<\omega}\xi \setminus \left\{ s^\frown \langle 0\rangle \mid s \in {}^{<\omega}\xi \right\}$ be the set of all sequences not ending with 0. For $s \in {}^{<\omega}\xi$ set $\bar{s}$ to be the unique element of I such that $s = \bar{s}^\frown 0^{(n)}$ for some $n < \omega$, where $0^{(n)}$ is as in (3.8)..

(i) Show that if $s = \bar{s}^\frown 0^{(n)}$ and $t = \bar{t}^\frown 0^{(m)}$ then

$$s < t \Leftrightarrow \bar{s} < \bar{t} \vee (\bar{s} = \bar{t} \wedge n < m).$$

(ii) Show that $\langle I, <\rangle$ is isomorphic to $\mathbb{Q} \cap [0; 1)$.

(iii) Conclude that $\langle {}^{<\omega}\xi, <\rangle$ is isomorphic to $(\mathbb{Q} \cap [0; 1)) \times \omega$ with the product ordering.

(iv) Explicitly describe an isomorphism between $\langle {}^{<\omega}2, <\rangle$ and $\langle {}^{<\omega}3, <\rangle$.

Exercise 26.23. Prove the following extension of Theorem 26.6: *Let C be a closed set in a separable complete metric space, and let $P \cup S$ be its decomposition into a perfect set P and a sparse set S (Theorem 13.47). Then either $P = \emptyset$ or else there is a continuous and injective map ${}^{\omega}2 \rightarrowtail P$.*

Conclude that a Polish space is either countable, or else it is in bijection with $\mathbb{R}$.

Exercise 26.24. Show that $\Psi \colon {}^{\omega}2 \to [0; 1]$, $x \mapsto \sum_{n=0}^{\infty} \frac{x(n)}{2^{n+1}}$ is surjective, monotone i.e. $x \leq_{\text{lex}} y \Rightarrow \Psi(x) \leq \Psi(y)$, and such that whenever $x <_{\text{lex}} y$ and $\Psi(x) = \Psi(y)$, then $x = s^\frown\langle 0\rangle^\frown 1^{(\omega)}$ and $y = s^\frown\langle 1\rangle^\frown 0^{(\omega)}$. Conclude that Ψ is continuous.

Exercise 26.25. Show that there exist continuous surjective maps $[0; 1] \twoheadrightarrow [0; 1]^n$ $(n \in \mathbb{N})$ and $[0; 1] \twoheadrightarrow [0; 1]^{\mathbb{N}}$. (When $n = 2$ the function is called **Peano curve**.)

Exercise 26.26. Show that if the function $X \to \mathbb{R}^{\mathbb{N}}$, $x \mapsto \langle d(x, q_n) \mid n \in \mathbb{N}\rangle$ defined in Section 13.G.3 is a homeomorphism from X onto its image, and that if d is a complete metric on X, then the image is a closed set in $\mathbb{R}^{\mathbb{N}}$. Conclude that, up to homeomorphism, all separable complete metric spaces are the closed subsets of $\mathbb{R}^{\mathbb{N}}$.

Exercise 26.27. Show that:

(i) For each $a < b$ and every sequence of reals $\vec{r} = \langle r_n \mid n \in \omega\rangle$ in $(0; 1)$, the sets ${}^{\omega}2$ and $\text{Cantor}([a; b], \vec{r})$ are homeomorphic, that is to say, all generalized Cantor sets (see (26.4)) are homeomorphic.

(ii) $\lambda\left(\text{Cantor}([a; b], r)\right) = 0$,

(iii) For each $0 \leq s < b - a$ there is a sequence $\vec{r}$ such that

$$\lambda\left(\text{Cantor}([a; b], \vec{r})\right) = 0.$$

Exercise 26.28. A **Fréchet space** is a vector space over $\mathbb{R}$ together with complete metric d such that addition $F \times F \to F$ and scalar multiplication

$\mathbb{R} \times F \to F$ are continuous. In particular every Banach space is a Fréchet space (but not conversely). Let F be an infinite dimensional Fréchet space. Show that every finite dimensional subspace is closed with empty interior. Conclude that the dimension of F is larger than $\aleph_0$.

Exercise 26.29. Show that is $\langle X, \mathcal{S}, \mu \rangle$ is a measure space, then

(a) μ is additive, that is if $A, B \in \mathcal{S}$ are disjoint, then $\mu(A \cup B) = \mu(A) + \mu(B)$, and hence it is monotone, $A \subseteq B \Rightarrow \mu(A) \leq \mu(B)$.

(b) $\mu(\bigcup_n A_n) = \sup_n \mu(A_n)$.

(c) $\mu(\bigcap_n A_n) = \inf_n \mu(A_n)$, if $\mu(\bigcap_{k \leq n} A_n) < +\infty$, for some k.

Exercise 26.30. Show that if $\mu \colon \mathcal{S} \to [0; 1]$ is a measure and $\{A_\alpha \mid \alpha < \kappa\} \subseteq \mathcal{S}$ are pairwise disjoint, then $\{\alpha < \kappa \mid \mu(A_\alpha) \neq 0\}$ is countable.

Exercise 26.31. Suppose $\mu \colon \mathcal{S} \to [0; +\infty]$ is atomless and $A \in \mathcal{S}$ with $\mu(A) > 0$. Show that:

(i) For all $\varepsilon > 0$ there is $B \subseteq A$, $B \in \mathcal{S}$ such that $0 < \mu(B) \leq \varepsilon$.

(ii) Assuming AC, for each $0 < r < \mu(A)$ there is $B \subseteq A$, $B \in \mathcal{S}$ such that $\mu(B) = r$.
[Hint: Apply Zorn's Lemma to the family of all $\vec{B} \in {}^{\gamma}S$ for some $\gamma < \omega_1$, such that $B_0 = A$ and $\forall \alpha, \beta < \gamma \, (B_\alpha \supset B_\beta \wedge \mu(B_\alpha) > \mu(B_\beta) \geq r)$.]

Notes and remarks

Exercise 26.22 is from [**Boo88**]. The axioms of countable choices AC_ω and dependent choices DC, are used throughout of mathematics, for example in order to show that a function is continuous (Exercise **??**), or in order to construct the Lebesgue measure (see page 498), or in order to show the Baire Category Theorem 26.8. The book [**Oxt80**] is an excellent introduction to measure and category. An encyclopædic treatise of measure theory is [**Fre04a, Fre03, Fre04b, Fre06, Fre08**]. Moreover, several pathologies occur if these axioms are not assumed: infinite but Dedekind-finite subsets of $\mathbb{R}$, functions that are discontinuous, but sequentially continuous in a point $\bar{x}$, etc. (see Exercises **??** and 28.17). For a survey of various "disasters" that can occur if either AC_ω or DC fails we refer to Herrlich's book [**Her06**]. The various "disasters" in analysis (no Lebesgue measurable sets, paradoxical decompositions of the sphere—see Section 28.B) obtained by means of AC, the full fledged axiom of choice, cannot be obtained by DC, by celebrated results of Robert M. Solovay from 1965 (see [**Jec03**, pag.??]). We refer the interested reader to the book [**Sch97**], a veritable encyclopedia for the foundational aspects of mathematical analysis. For an introduction to functional analysis, see the book by Walter Rudin [**Rud91**].

27. Ordinals and topology*

Recall from Section 13.I.1 the construction of X', the derivative of a topological space X, and of the sequence $X^{(\alpha)}$. By the Axiom of Replacement there is a least $\bar{\alpha}$ such that $X^{(\bar{\alpha})} = X^{(\bar{\alpha} \dotplus 1)}$, hence $X^{(\bar{\alpha})} = X^{(\beta)}$ for all $\beta > \bar{\alpha}$. Such $\bar{\alpha}$ is the Cantor-Bendixson rank of X and it is denoted by $\|X\|_{\mathrm{CB}}$.

The **height** of X is

$$\mathrm{ht}(X) = \sup \left\{ o(x) \mid x \in X \setminus X^{(\bar{\alpha})} \right\}.$$

Then $\mathrm{ht}(X) = \|X\|_{\mathrm{CB}}$ if $\|X\|_{\mathrm{CB}}$ is limit, and $\mathrm{ht}(X) \dotplus 1 = \|X\|_{\mathrm{CB}}$ otherwise.

Corollary 27.1. *If X is countable and compact, then $\|X\|_{\mathrm{CB}}$ is a successor ordinal.*

Proof. By the Cantor-Bendixson Theorem K can be decomposed in its perfect part P and its sparse part S. By the observation above, $P = K^{(\bar{\alpha})} = \emptyset$, where $\bar{\alpha} = \|K\|_{\mathrm{CB}}$. If $\bar{\alpha}$ were limit, then $K^{(\bar{\alpha})} = \bigcap_{\beta < \bar{\alpha}} K^{(\beta)}$ would be the empty intersection of a decreasing family of non-empty compact sets, against the finite intersection property. □

Therefore in a countable compact metric space K the ordinal $\gamma \overset{\text{def}}{=} \mathrm{ht}(K)$ is the predecessor of $\|K\|_{\mathrm{CB}}$, so that $K^{(\gamma)} \neq \emptyset$, but $K^{(\gamma \dotplus 1)} = \emptyset$. The set $K^{(\gamma)}$ cannot be infinite, otherwise $\{\{x\} \mid x \in K^{(\gamma)}\}$ would be an open cover without a finite subcover—its size n will be denoted by $\mathrm{wd}(K)$. The ordinal $\mathrm{ht}(K)$ can attain arbitrarily large values, as will be seen in the next Section, so we can characterize the first uncountable ordinal by

$$\omega_1 = \sup \{\mathrm{ht}(K) \mid K \text{ countable compact metric}\}.$$

Theorem 27.3 below shows that $\mathrm{ht}(K)$ and $\mathrm{wd}(K)$ characterize countable compact metric spaces up to homeomorphism.

27.A. Topology on the ordinals. By Exercise 13.74, if $\alpha < \omega_1$, then α is embeddable in $\mathbb{R}$, that is there is a function $f \colon \alpha \to \mathbb{R}$ that is order preserving and such that $\mathrm{ran}(f)$ is closed in $\mathbb{R}$. Therefore the spaces $\alpha \dotplus 1$ (with $\alpha < \omega_1$) are examples of compact, countable spaces which are completely metrizable spaces, that is they admit a complete metric which is compatible with the topology. Although they are all distinct as orders, they need not be distinct as topological spaces: if $\lambda \geq \omega$ is limit, then $\lambda \dotplus n$ and $\lambda \dotplus m$ are homeomorphic for each $0 < n, m < \omega$.

We now state three results that will be proved in the next Section. The first result classifies, up to homeomorphism, all countable ordinals.

Theorem 27.2. *A countable ordinal is homeomorphic to one and only one of the ordinals of the form*

(27.1a) $\quad n \qquad (n < \omega)$,

(27.1b) $\quad \omega^{\cdot\gamma} \cdot n \dotplus \omega^{\cdot\delta} \cdot m \qquad (0 < \delta < \gamma < \omega_1, 0 \leq n < \omega, 0 < m < \omega)$,

(27.1c) $\quad \omega^{\cdot\gamma} \cdot n \dotplus 1 \qquad (0 < \gamma < \omega_1, 0 < n < \omega)$.

The second result classifies, up to homeomorphism, all compact metric spaces.

Theorem 27.3. *If K is an infinite compact metric space and* $\mathrm{ht}(K) = \gamma$ *and* $\mathrm{wd}(K) = n$*, then K is homeomorphic to* $\omega^{\cdot\gamma} \cdot n \dotplus 1$*. In particular, two countable compact metric spaces K_1 and K_2 are homeomorphic if and only if* $\mathrm{ht}(K_1) = \mathrm{ht}(K_2)$ *and* $\mathrm{wd}(K_1) = \mathrm{wd}(K_2)$*.*

By Theorems 27.2 and 27.3 we obtain that the countable compact metric spaces are, up to homeomorphism, either the natural numbers or else the ordinals of the form $\omega^{\cdot\gamma} \cdot n \dotplus 1$, with $0 < n < \omega$ and $\gamma < \omega_1$.

Corollary 27.4. *A locally compact countable X is homeomorphic to a countable ordinal of the form*

(a) $\omega^{\cdot\,\mathrm{ht}(X)} \cdot n \dotplus 1$*, for some* $0 < n < \omega$*, if X is compact,*

(b) $\omega^{\cdot\,\mathrm{ht}(X)} \cdot n \dotplus \omega^{\cdot\delta} \cdot m$*, for some* $\delta < \mathrm{ht}(X)$*,* $0 < n < \omega$ *and* $0 \leq m < \omega$ *if X is not compact.*

Remark 27.5. The metrizability assumption in the statement of Theorem 27.3 and Corollary 27.4 can be removed, assuming AC. In fact a countable compact space is a first countable space [**Eng89**, Exercise 3.1.F(a), pag. 135] hence countability of the space implies that it is second countable. But every normal, second countable space is metrizable [**Eng89**, ??].

27.B. Characterization of countable compact spaces*. The isolating order is a topological invariant, in the sense that if $o^X(x) = \alpha$ and $f\colon X \to Y$ is a homeomorphism, then $o^Y(f(x)) = \alpha$, and f is a homeomorphism of $X^{(\alpha)}$ onto $Y^{(\alpha)}$. If $Y \subseteq X$ and $y \in Y$ then $o^Y(y) \leq o^X(y)$—the inequality could be strict since y could be isolated in Y and not in X, but if Y is open equality holds. In particular, if H is a clopen of a countable compact metric space K, then $o^H(x) = o^K(x)$ for every $x \in H$. Note that if $U \subseteq X$ is open and contains a point of order α, then it contains points of every order $\beta < \alpha$. Define $o(\alpha)$, the order of isolation of an ordinal α, to be $o^{\alpha \dotplus 1}(\alpha)$. Since an ordinal is an open set of a larger ordinal, $o(\alpha) = o^\beta(\alpha)$ for all $\beta > \alpha$. In analogy with what was done for topological spaces (which, by statue, are sets and not proper classes) for each $X \subseteq \mathrm{Ord}$ define

$$X' = X \setminus \{\alpha \in X \mid \exists \beta < \alpha\,((\beta;\alpha] \cap X = \{\alpha\})\}$$

and its iterations as in (**??**). In particular

$$\mathrm{Ord}^{(\alpha)} = \{\beta \mid o(\beta) \geq \alpha\}\,.$$

Since the space $Y = \gamma$ is an open set of Ord, one has that $Y^{(\alpha)} = Y \cap \mathrm{Ord}^{(\alpha)}$ for all α, so in order to analyze the derived classes $Y^{(\alpha)}$ it is enough to study the classes $\mathrm{Ord}^{(\alpha)}$.

Lemma 27.6. *If $\alpha > 0$, then*

$$\mathrm{Ord}^{(\alpha)} = \{\omega^{\cdot\alpha} \cdot \nu \mid 0 < \nu\}. \tag{27.2}$$

Proof. The non-isolated points of Ord are the limit ordinals that, by Exercise **??**, are of the form $\omega \cdot \nu$. Thus equation (27.2) holds for $\alpha = 1$. Similarly, if it holds for α, then the non-isolated points of $\mathrm{Ord}^{(\alpha)}$ are of the form $\omega^{\cdot\alpha} \cdot \nu$ with ν limite hence it can be written as $\omega \cdot \xi$. It follows that $\mathrm{Ord}^{(\alpha\dotplus1)} = \{\omega^{\cdot\alpha\dotplus1} \cdot \xi \mid 0 < \xi\}$, that is the formula (27.2) holds for $\alpha \dotplus 1$. Finally suppose that α is limit and that (27.2) holds for every $\alpha^* < \alpha$. Let $\lambda \in \mathrm{Ord}^{(\alpha)} = \bigcap_{\alpha^*<\alpha} \mathrm{Ord}^{(\alpha^*)}$: it is a limit ordinal and its Cantor normal form (Exercise 19.37(i)) is

$$\lambda = \omega^{\cdot\xi_0} \cdot n_0 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k \tag{27.3}$$

where $\xi_0 > \cdots > \xi_k > 0$ and $n_0, \ldots, n_k > 0$.

Since λ is of the form $\omega^{\cdot\alpha'} \cdot \nu^*$, for every $\alpha^* < \alpha$, it is easy to check (see Exercise 27.7 below) that $\xi_k \geq \alpha^*$. Thus λ is of the form $\omega^{\cdot\alpha} \cdot \nu$, with $\nu > 0$. Conversely, if $\lambda = \omega^{\cdot\alpha} \cdot \nu$ and $\alpha^* < \alpha$, then $\lambda = \omega^{\cdot\alpha^*} \cdot (\omega^{\cdot\eta} \cdot \nu)$, where η is such that $\alpha^* \dotplus \eta = \alpha$, hence $\lambda \in \mathrm{Ord}^{(\alpha^*)}$. Being α^* arbitrary, one has $\lambda \in \bigcap_{\alpha^*<\alpha} \mathrm{Ord}^{(\alpha^*)} = \mathrm{Ord}^{(\alpha)}$. Therefore the formula (27.2) holds also for limit α. □

Exercise 27.7. A limit ordinal $\lambda > 0$ is of the form $\omega^{\cdot\alpha} \cdot \nu$, with $\nu > 0$ if and only if $\alpha \leq \xi_k$, where ξ_k is the coefficient of the Cantor normal form of λ as in (27.3).

Therefore for $\alpha \neq 0$,

$$o(\alpha) = \gamma \Leftrightarrow \alpha = \omega^{\cdot\gamma} \cdot (\nu \dotplus 1).$$

An ordinal is topologically incompressible if it is not homeomorphic to a smaller ordinal.

Lemma 27.8. *If $\xi, n > 0$ then $\omega^{\cdot\xi} \cdot n$ is incompressible.*

Proof. Suppose, towards a contradiction, that $\omega^{\cdot\xi} \cdot n$ is homeomorphic to a smaller ordinal λ. By Proposition **??**, λ is limit and we can suppose that its Cantor normal form can be given by (27.3). If $\xi_0 < \xi$ a contradiction follows since

$$\left\{\omega^{\cdot\xi_0} \cdot m \mid m \in \omega\right\} \subseteq \omega^{\cdot\xi} \cdot n$$

shows that there are infinitely many points in $\omega^{\cdot\xi} \cdot n$ of order ξ_0, while λ has finitely many such points. Thus $\xi = \xi_0$ and $n_0 < n$. But $\omega^{\cdot\xi} \cdot n$ and λ cannot be homeomorphic as $\omega^{\cdot\xi} \cdot n$ contains at least n_0 points of order ξ, while λ has fewer such points. □

Exercise 27.9. Show that $\omega^{\cdot\gamma_0}\cdot n_0 \dotplus \omega^{\cdot\delta_0}\cdot m_0$ is homeomorphic to $\omega^{\cdot\gamma_1}\cdot n_1 \dotplus \omega^{\cdot\delta_1}\cdot m_1$, with $\gamma_i > \delta_i$ and $n_i, m_i > 0$ per $i = 0, 1$ if and only if $\gamma_0 = \gamma_1$, $\delta_0 = \delta_1$, $n_0 = n_1$ and $m_0 = m_1$.

Therefore the ordinals of the form (27.1a) and (27.1b) are pairwise non-homeomorphic.

By Exercise **??** the infinite incompressible ordinals are either of the form λ or else $\lambda \dotplus 1$ with limit λ. Fix an ordinal of the form $\lambda \dotplus 1$ with λ limit and consider its expansion in Cantor's normal form (Exercise 19.37(i))

$$\lambda \dotplus 1 = \omega^{\cdot\xi_0}\cdot n_0 \dotplus \cdots \dotplus \omega^{\cdot\xi_k}\cdot n_k \dotplus 1 \tag{27.4}$$

with $\xi_0 > \cdots > \xi_k > 0$ and $n_0, \ldots, n_k > 0$. Let $\gamma_0 = \omega^{\cdot\xi_0}\cdot n_0$ and $\gamma_{i+1} = \gamma_i \dotplus \omega^{\cdot\xi_{i+1}}\cdot n_{i+1}$ so that $\gamma_0 < \cdots < \gamma_k$. The sets

$$D_0^* = [0;\gamma_0],\ D_1^* = [\gamma_0 \dotplus 1;\gamma_1],\ \ldots,\ D_k^* = [\gamma_{k-1} \dotplus 1;\gamma_k]$$

are clopen, so they form a partition of $\lambda \dotplus 1$, and $\mathrm{ot}(D_i^*) = \omega^{\cdot\xi_i}\cdot n_i \dotplus 1$ per $i \leq k$. We need a simple result from topology.

Exercise 27.10. (i) Let $X = \bigcup_{i<\nu} D_i$ be a topological space and suppose that $\{D_i \mid i < \nu\}$ is a partition of the space in non-empty clopen sets. Suppose moreover that α_i is a successor ordinal and that $f_i\colon D_i \to \alpha_i$ is a homeomorphism, for all $i < \nu$. Then X is homeomorphic to $\dot{\sum}_{i<\nu}\alpha_i$, the ordinal defined on page 416.

(ii) Let X be a topological space, $\bar{x} \in X$ an isolated point, and let $X = V_0 \supset V_1 \supset \ldots$ be a basis of clopen subsets of $\bar{x}$. Suppose that f_i and α_i be as in part (i), where $D_i = V_i \setminus V_{i+1}$ and $i < \omega$. Then X is homeomorphic to $(\dot{\sum}_{i<\omega}\alpha_i) \dotplus 1$.

By part (i) of Exercise 27.10 applied to the space $X = \lambda \dotplus 1$ and to the sets $D_i = D_{k-i}^*$ (per $i \leq k$) one has that $\lambda \dotplus 1$ is homeomorphic to

$$(\omega^{\cdot\xi_k}\cdot n_k \dotplus 1) \dotplus (\omega^{\cdot\xi_{k-1}}\cdot n_{k-1} \dotplus 1) \dotplus \cdots \dotplus (\omega^{\cdot\xi_0}\cdot n_0 \dotplus 1)$$

and since $\omega^{\cdot\xi_0}$ is additively indecomposable (Exercise **??**) and $\omega^{\cdot\xi_i}\cdot n_i \dotplus 1 < \omega^{\cdot\xi_0}$ for each $0 < i \leq k$, this ordinal is $\omega^{\cdot\xi_0}\cdot n_0 \dotplus 1$.

We have thus proved that:

(27.5) If $\lambda \dotplus 1$ is as in (27.4) and λ is limite,

then $\lambda \dotplus 1$ is homeomorphic to $\omega^{\cdot\xi_0}\cdot n_0 \dotplus 1$.

Arguing as in the proof of Lemma 27.8 one checks that $\omega^{\cdot\gamma}\cdot n \dotplus 1$ is homeomorphic to $\omega^{\cdot\delta}\cdot m \dotplus 1$ if and only if $\gamma = \delta$ and $n = m$, that is

(27.6) $\alpha \dotplus 1 \geq \omega$ is incompressible if and only if $\alpha \dotplus 1 = \omega^{\cdot\gamma}\cdot n \dotplus 1$, for some $\gamma > 0$ and $n > 0$.

Therefore the incompressible successor ordinals are exactly those either of the form (27.1a) or else (27.1c).

We prove now that a limit ordinal is homeomorphic to an ordinal of the form $\omega^{\cdot\gamma}\cdot n$, or of the form $\omega^{\cdot\gamma}\cdot n \dotplus \omega^{\cdot\delta}\cdot m$. Suppose that λ is limit as in (27.3). If $k = 0$ then $\lambda = \omega^{\cdot\xi_0}\cdot n_0$, thus we can suppose that $k > 0$. By (27.5) $\alpha = \omega^{\cdot\xi_0}\cdot n_0 \dotplus \cdots \dotplus \omega^{\cdot\xi_{k-1}}\cdot n_{k-1} \dotplus 1$ is homeomorphic to $\alpha^* = \omega^{\cdot\xi_0}\cdot n_0 \dotplus 1$ and since these are clopen in the spaces $\alpha \dotplus \omega^{\cdot\xi_k}\cdot n_k = \lambda$ and $\alpha^* \dotplus \omega^{\cdot\xi_k}\cdot n_k = \omega^{\cdot\xi_0}\cdot n_0 \dotplus \omega^{\cdot\xi_k}\cdot n_k$, respectively, it follows that λ is homeomorphic to $\omega^{\cdot\xi_0}\cdot n_0 \dotplus \omega^{\cdot\xi_k}\cdot n_k$. We have thus proved that:
(27.7)

If λ is limite as in (27.3), then

$$\lambda \text{ is homeomorphic to } \begin{cases} \omega^{\cdot\xi_0}\cdot n_0 \dotplus \omega^{\cdot\xi_k}\cdot n_k & \text{if } k > 0,\\ \omega^{\cdot\xi_0}\cdot n_0 & \text{if } k = 0. \end{cases}$$

Proof of Theorem 27.2. Fix $\alpha < \omega_1$. A finite ordinal can be only be homeomorphic to itself, hence we can suppose that $\alpha \geq \omega$. If α is limit, then by (27.7) α is homeomorphic to a unique ordinal (Exercise 27.9) of the form $\omega^{\cdot\gamma}\cdot n$ or of the form $\omega^{\cdot\gamma}\cdot n \dotplus \omega^{\cdot\delta}\cdot m$, with $\gamma > \delta$. If α is successor, then it is homeomorphic to $\lambda \dotplus 1$ with λ limit by Exercise **??**, hence it is homeomorphic to exactly one ordinal of the form $\omega^{\cdot\xi}\cdot n \dotplus 1$ (27.5).

Finally, by Propositions 21.22 and **??** no ordinal of the form $\omega^{\cdot\gamma_0}\cdot n_0 \dotplus 1$ is homeomorphic to an ordinal of the form $\omega^{\cdot\gamma_1}\cdot n_1$ or of the $\omega^{\cdot\gamma_1}\cdot n_1 \dotplus 1 \dotplus \omega^{\cdot\delta_1}\cdot n_1$ with $\gamma_1 > \delta_1$. □

Proof of Theorem 27.3. We prove by induction on $\gamma = \mathrm{ht}(K)$ that K is homeomorphic to $\omega^{\cdot\gamma}\cdot n \dotplus 1$, where $n = \mathrm{wd}(K)$.

First of all note that it is enough to prove the result when $n = 1$. In fact if $x_1, \dots, x_n$ are points of order γ, fix $H_1, \dots, H_n$ clopen neighborhoods of $x_1, \dots, x_n$. Replacing H_1 with $K \setminus (H_2 \cup \cdots \cup H_n)$ if necessary, we may assume that $H_1, \dots, H_n$ form a partition of K. Since $\mathrm{ht}(H_i) = \gamma$ and $\mathrm{wd}(H_i) = 1$ then H_i is homeomorphic to $\omega^{\cdot\gamma} \dotplus 1$ and since K is the sum of the spaces H_i, by part (i) of Exercise 27.10 K is homeomorphic to $(\omega^{\cdot\gamma} \dotplus 1)\cdot n = \omega^{\cdot\gamma}\cdot n \dotplus 1$.

Therefore we may assume that $\mathrm{wd}(K) = 1$ and that $\bar{x} \in X$ is the only point such that $o(\bar{x}) = \gamma > 0$.

If $\gamma = \delta \dotplus 1$ then $\bar{x}$ is the only one accumulation point of $\{x_n \mid n < \omega\}$, the set of points of order δ. By Corollary 21.25, fix $K = V_0 \supset V_1 \supset V_2 \supset \dots$ a base of clopen neighborhoods of $\bar{x}$ such that $x_n \in V_n$ and $x_{n+1} \notin V_n$. Then the $D_i = V_i \setminus V_{i+1}$ form a disjoint clopen partition of $K \setminus \{\bar{x}\}$ such that $\mathrm{ht}(D_i) = \delta$ and $\mathrm{wd}(D_i) = 1$. It $\delta = 0$ is immediate to check that the D_i's are singletons and that K is homeomorphic to $\omega \dotplus 1$. Suppose that $\delta > 0$. By inductive assumption there are homeomorphisms $f_i\colon D_i \to \omega^{\cdot\delta} \dotplus 1$, hence by part (ii) of Exercise 27.10, K is homeomorphic to $\omega^{\cdot\delta\dotplus 1} \dotplus 1 = \omega^{\cdot\gamma} \dotplus 1$.

Finally suppose that γ is limit. By Corollary 21.25 fix a basis of clopen neighborhoods $X = V_0 \supset V_1 \supset V_2 \supset \dots$ of the point $\bar{x}$. Towards a contradiction, if $D_i \overset{\text{def}}{=} V_i \setminus V_{i+1}$ had height γ, then it should contain a point y such that $o^{D_i}(y) = o^X(y)$, hence by hypothesis $y = \bar{x}$, contradicting the fact that $\bar{x} \notin D_i$. By inductive assumption

(27.8) for every $i < \omega$ there is a homeomorphism $f_i\colon D_i \to \omega^{\cdot\gamma_i} \cdot m_i \dotplus 1$

for some γ_i and n_i. By part (ii) of Exercise 27.10 there is a homeomorphism $f\colon X \to \alpha \dotplus 1$ where

$$\alpha \dotplus 1 \overset{\text{def}}{=} \Bigl(\dot{\sum}_{i<\omega} \omega^{\cdot\gamma_i} \cdot m_i \dotplus 1\Bigr) \dotplus 1 \le \omega^{\cdot\gamma} \dotplus 1.$$

Towards a contradiction, suppose that $\alpha \dotplus 1 < \omega^{\cdot\gamma} \dotplus 1$ and let $\delta < \gamma$ be such that $\alpha \dotplus 1 < \omega^{\cdot\delta}$. Fix $y \in X^{(\delta)}$; by Corollary 21.25 let D be a clopen of X such that $D \cap X^{(\delta)} = \{y\}$. Since D is compact and contains exactly a point of order δ but no points of higher order, that is $\mathrm{ht}(D) = \delta$ and $\mathrm{wd}(D) = 1$, by inductive hypothesis D is homeomorphic to $\omega^{\cdot\delta} \dotplus 1$. The set $f[X \setminus D]$ is a clopen subset of $\alpha \dotplus 1$ that is isomorphic as order (and therefore homeomorphic as topological space) to an ordinal $\eta \dotplus 1 \le \alpha \dotplus 1$. By parte(i) of Exercise 27.10 the space X is homeomorphic to $\eta \dotplus 1 \dotplus \omega^{\cdot\delta} \dotplus 1 = \omega^{\cdot\delta} \dotplus 1$. In particular $\omega^{\cdot\delta} \dotplus 1$ is homeomorphic to $\alpha \dotplus 1$, against (27.6). □

Remark 27.11. The above proof of Theorem 27.3 uses the Axiom of Choice when the homeomorphisms f_i are chosen in (27.8). In order to see that the appeal to AC can be avoided, one can either suitably modify the proof, or else apply a deep result in set theory (Shoenfield's absoluteness theorem) to show that choice can be avoided.

Proof of Corollary 27.4. Let X be a locally compact, countable metric space. The case when X is compact is tackled in Theorem 27.3, so we may assume that X is not compact. Let $\hat{X}$ be **Alexandroff´s compactification** of X, that is the space $X \cup \{\infty\}$ where $\infty \notin X$ and the open sets of $\hat{X}$ are those of X together with sets of the form $\{\infty\} \cup X \setminus K$ with $K \subseteq X$ compact. Since X is open in $\hat{X}$, the order $o(x)$ of a point $x \in X$ is the same, computed in X or in $\hat{X}$, hence $\mathrm{ht}(X) \le \mathrm{ht}(\hat{X})$. In fact $\mathrm{ht}(\hat{X}) = \mathrm{ht}(X) \dotplus 1$ if and only if $o(\infty) = \mathrm{ht}(X) = \sup_{x\in X} o(x)$. The space $\hat{X}$ is metric, compact and countable, hence there is a homeomorphism from $\hat{X}$ onto $\omega^{\cdot\gamma} \cdot n$, where $\gamma = \mathrm{ht}(\hat{X})$ and $n = \mathrm{wd}(\hat{X})$. By construction ∞ is not isolated in $\hat{X}$ hence $f(\infty)$ is limit. If $f(\infty) = \omega^{\cdot\gamma} \cdot n$, then X is homeomorphic to $\omega^{\cdot\gamma} \cdot n$. If instead $f(\infty) = \lambda < \omega^{\cdot\gamma} \cdot n$, then X is homeomorphic to $(\omega^{\cdot\gamma} \cdot n \dotplus 1) \setminus \{\lambda\}$,which is partitioned in two clopen sets

$$D_0 = (\omega^{\cdot\gamma} \cdot n \dotplus 1) \setminus (\lambda \dotplus 1) \quad \text{and} \quad D_1 = \lambda.$$

Since $\omega^{\cdot\gamma}$ is additively indecomposable, $\operatorname{ot}(D_0) = \omega^{\cdot\gamma} \cdot n \dotplus 1$, hence by Exercise 27.10 X is homeomorphic to $\omega^{\cdot\gamma} \cdot n \dotplus 1 \dotplus \lambda = \omega^{\cdot\gamma} \cdot n \dotplus \lambda$. If $\omega^{\cdot\xi_0} \cdot n_0 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k$ is Cantor's normal form of λ, by (27.7) it follows that $\omega^{\cdot\gamma} \cdot n \dotplus \omega^{\cdot\xi_0} \cdot n_0 \dotplus \cdots \dotplus \omega^{\cdot\xi_k} \cdot n_k$ is homeomorphic to $\omega^{\cdot\gamma} \cdot n \dotplus \omega^{\cdot\xi_k} \cdot n_k$. □

Exercises

Exercise 27.12. Show that the ordinals of the form (27.1a), (27.1b) and (27.1c) in the statement of Theorem (27.2) are incompressible.

Notes and remarks

Theorems 27.2, 27.3 and 27.4 characterize countable locally compact spaces by means of ordinals and are due to ??. These characterizations are quite useful in the analysis of Banach spaces of the form $\mathscr{C}(K)$ with K countable and compact [**Ros03**].

28. Applications of the axiom of choice*

The axiom of choice has many consequences in mathematics. Here are some of the most important ones.

28.A. Theorems whose proof depend on the axiom of choice.

Assume AC throughout this Section

28.A.1. *Algebra.*

Theorem 28.1. *Let V be a vector space on a field $\Bbbk$.*

(a) *V is injective in the category of vector spaces $\Bbbk$, that is every linear map $f\colon U \to V$ from a linear subspace U of a vector space W can be extended to a linear map $\bar{f}\colon W \to V$.*

(b) *V is projective in the category of vector spaces on $\Bbbk$, that is given linear maps $f\colon V \to U$ and $g\colon W \to U$, there is a linear map $\bar{f}\colon V \to W$ such that $f = g \circ \bar{f}$.*

Proof.

□

Theorem 28.2 (Neilsen-Schreier)**.** *Every subgroup of a free group is free.*

Theorem 28.3. (a) *Every free abelian group is projective.*

(b) *Every divisible abelian group is injective.*

28.A.2. *Lattices and Boolean algebras.* By Theorem 25.2, every proper ideal in a lattice with maximum can be extended to a maximal ideal; dually, every proper filter in a lattice with minimum can be extended to a maximal filter. In general lattices, maximal ideals are not necessarily prime, so we cannot conclude that every proper ideal can be extended to a prime ideal; in fact prime ideals need not exists (Remark 25.4 and Exercise 25.11). Since in a distributive lattice, maximal ideals are prime, then

Proposition 28.4. *In un distributive lattice with maximum, every proper ideal can be extended to a maximal ideal. Dually, in a distributive lattice with minimum, every proper filter can be extended to a prime filter.*

The next result is known as Sikorski's extension Theorem.

Used somewhere?

Theorem 28.5 (Sikorski)**.** *Every complete Boolean algebra C is injective in the category of Boolean algebras, that is for every Boolean algebra B and every subalgebra A of B, a morphism $A \to C$ can be extended to a morphism $B \to C$.*

28.A.3. *Analysis.* The next result is known as the **generalized Ascoli-Arzelà theorem**.

Theorem 28.6. *Let X be a locally compact Hausdorff space, let Y be a metric space, and endow $\mathscr{C}(X,Y)$ the set of all continuous functions from X to Y with the* ***compact-open topology****, generated by the sets $\{f \mid f[K] \subseteq U\}$ with $K \subseteq X$ compact and $U \subseteq Y$ open. A set $\mathcal{F} \subseteq \mathscr{C}(X,Y)$ is compact if and only if*

- *$\{f(x) \mid f \in \mathcal{F}\}$ is compact in Y,*
- *$\mathcal{F}$ is a closed subset of Y^X with the product topology,*
- *$\mathcal{F}$ is* ***equicontinuous****, that is*

$$\forall x \in X\, \exists \varepsilon > 0\, \exists U \text{ open and } x \in U\, \forall f \in \mathcal{F}\, \forall y \in U\, [d(f(x), f(y)) < \varepsilon].$$

Theorem 28.6 is a generalization of the **classical Ascoli-Arzelà theorem**:

Theorem 28.7. *For $\mathcal{F} \subseteq \mathscr{C}(\mathbb{R},\mathbb{R})$ the following are equivalent:*

(a) *each sequence $(f_n)_n$ of functions in $\mathcal{F}$ has a subsequence $(f_{n_k})_k$ that is uniformly convergent on closed intervals,*

(b) *the set $\{f(x) \mid f \in \mathcal{F}\}$ is bounded, for each $x \in \mathbb{R}$, and $\mathcal{F}$ is equicontinuous.*

28.B. Pathological sets. AC yields also some undesirable results on the continuum.

In this Section we will assume that $\mathbb{R}$ is well-orderable

Clearly, any well-order on $\mathbb{R}$ induces a well-order on any $X \asymp \mathbb{R}$.

Every $\mathbb{R}^n$ can be seen as a vector space on $\mathbb{Q}$ and since $\mathbb{R}^n \asymp \mathbb{R}$, then $\mathbb{R}^n$ has a basis of size $2^{\aleph_0}$. A basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$ is called a **Hamel base**. Given a Hamel basis H, it is possibile to define a discontinuous homomorphism from $\langle \mathbb{R}, + \rangle$ in itself: every function $g \colon H \to \mathbb{R}$ can be extended to a $\mathbb{Q}$-linear function $f \colon \mathbb{R} \to \mathbb{R}$, thus if g is not monotone, the resulting morphism f is discontinuous.

The next result requires a few concepts from measure theory that will be introduced in Section 26.D.

Theorem 28.8 (Vitali). *There is a subset of $\mathbb{R}$ that is not Lebesgue measurable.*

The existence of a non-Lebesgue-measurable subset of some $\mathbb{R}^k$ implies the existence of non-Lebesgue-measurable subsets of $\mathbb{R}^n$, for all $n \geq 1$.

Remark 28.9. The existence of a discontinuous homomorphism $\langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ implies the existence of sets that are not Lebesgue-measurable [**Her06**, Theorem 5.5, p. 119] and the existence of an automorphism of $\langle \mathbb{C}, +, \cdot \rangle$ different from the identity and the conjugation, implies the existence of a discontinuous homomorphism $\langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ (Exercise 28.13).

Two subsets X and Y of $\mathbb{R}^n$ are equidecomposable if there are finite partitions $X = X_1 \cup \cdots \cup X_k$ and $Y = Y_1 \cup \cdots \cup Y_k$ and isometries $\sigma_1, \ldots, \sigma_k$ of $\mathbb{R}^n$ such that $\sigma_i[X_i] = Y_i$. The next result, known as the **Banach-Tarski paradox** is probably the most counter-intuitive consequence of the Axiom of Choice.

Theorem 28.10 (Banach-Tarski). *Suppose $n \geq 3$. Any two bounded subsets of $\mathbb{R}^n$ with non-empty interior are equidecomposable.*

In particular: it is possible to cut the unit ball of the three-dimensional space into a finite number of pieces, which can be rearranged, using rigid motions, into *two* balls identical to original one. The least number of pieces needed to duplicate a ball is 5. The pieces $X_1, \ldots, X_k, Y_1, \ldots, Y_k$ used in the decomposition in Theorem 28.10 are highly irregular and fail to be Lebesgue measurable, but can be taken to have some sort of tameness. For example, R. Dougherty and M. Foreman proved that the pieces can be taken have the property of Baire. Another startling result due to T. Wilson says that the pieces can be taken to be sufficiently disentangled so that the metamorphosis of X into Y can be achieved by a continuously parametrized isometries σ_i^t so that $\sigma_i^0[X_i] = X_i$, $\sigma_i^1[X_i] = Y_i$, and $\sigma_i^t[X_i] \cap \sigma_j^0[X_j] = \emptyset$ for all $t \in (0; 1)$ and all $1 \leq i < j \leq k$. The assumption that the dimension of the space is at least 3 is necessary, since when $n \leq 2$ two measurable bounded subsets of $\mathbb{R}^n$ are equidecomposable if and only if they have the same measure. Yet there are startling results even in dimension 2, for example: a square and a disc of the same area are equidecomposable via translations, and the pieces of the decomposition can be taken to be Borel.

28.C. Theorems that are equivalent to some form of the Axiom of Choice. Several of the results in mathematics turn out to be equivalent to some form of choice. The following are equivalent to AC:

AC-1 Krull's Lemma 14.4 for unique factorization domains [**Hod79**].

AC-2 Tychonoff's theorem for T_1 spaces (Exercise 28.12).

AC-3 Every proper filter in the lattice of closed subsets of a topological space can be extended to a maximal filter. Dually: every proper ideal in the lattice of open sets of a topological space can be extended to a maximal ideal.

AC-4 Two infinite sets, X, Y are in bijection if and only if the free groups $\boldsymbol{F}(X), \boldsymbol{F}(Y)$ are in bijection (Exercise 28.16).

AC-5 Every vector space has a basis [**Bla84**].

AC-6 Every vector space is injective.

AC-7 Every vector space is projective.

AC-8 Every free abelian is group projective [**Bla79**].

AC-9 Every divisible abelian group is injective [**Bla79**].

The following are equivalent to BPI:

BPI-1 In a commutative ring, every non-trivial ideal can be extended to a prime ideal.

BPI-2 Tychonoff's theorem for T_2 spaces.

BPI-3 Every proper ideal in the lattice of closed subsets of a topological space can be extended to a maximal ideal. Dually: every proper filter in the lattice of open subsets of a topological space can be extended to a maximal filter.

BPI-4 Two infinite sets X, Y are in bijection if and only if their free groups $\boldsymbol{F}(X), \boldsymbol{F}(Y)$ are isomorphic.

BPI-5 Alaoglu's Theorem [**Joh84**].

BPI-6 The generalized Ascoli-Arzelà Theorem 28.6.

BPI-7 The equivalence between the two definition of radical of an ideal of a commutative ring (see Section 9.B.1) [**Rav77**].

BPI-8 Stone's representation theorem for Boolean algebras (Exercise 25.17).

BPI-9 The compactness, completeness, and model existence theorems for first-order languages (Exercise 34.13).

Remark 28.11. Conditions AC-3 and BPI-3 highlight a subtle difference between the lattice of open and closed sets. By Proposition 28.4, AC-3 is equivalent to the existence of maximal filters in complete and in bounded distributive lattices.

BPI implies the existence and uniqueness of the algebraic closure of a field, Theorem **??**. The Hahn-Banach theorem follows from (but it is strictly weaker than) BPI, and it is equivalent to:

> If F is a proper filter in a Boolean algebra B, then there is a finitely additive measure $m\colon B \to [0;1]$ such that $m(x) = 1$ for all $x \in F$.

By [**FW91, Paw91**] the Hahn-Banach Theorem implies the Banach-Tarski Theorem 28.10 hence the existence of non-measurable sets.

Next we turn to AC_ω and the stronger DC. As we observed before, these principles are very important since they are weak enough to not generate the pathologies of Section 28.B, yet they are powerful enough to prove many useful results such as: the countable union of countable sets is countable, the existence of the Lebesgue measure, the Baire category theorem, ...

The following are equivalent to DC:

DC-1 The Baire category theorem (Exercise 28.21).

DC-2 Every descriptive tree without terminal nodes has a branch (Theorem 23.18).

DC-3 The existence of countable elementary substructures for countable languages (Theorem 31.19 and Exercise 31.51).

The following are equivalent to $\mathsf{AC}_\omega(\mathbb{R})$:

$\mathsf{AC}_\omega(\mathbb{R})$-1 The equivalence between continuity and sequential continuity su $\mathbb{R}$ (Exercise 28.19);

$\mathsf{AC}_\omega(\mathbb{R})$-2 If X is the surjective image of $\mathbb{R}$, then every second countable topology on X is separable (Exercise 28.20);

$\mathsf{AC}_\omega(\mathbb{R})$-3 The classical Ascoli-Arzelà Theorem 28.7.

Exercises

In the next exercise we will prove the following version of Tychonoff's Theorem implies AC:

(T) If $\langle (Y_i, \mathcal{T}_i) \mid i \in I\rangle$ is a collection of T_1 compact spaces, and if the *set* $\bigtimes_{i\in I} Y_i$ is non-empty, then the product space $\prod_{i\in I}(Y_i, \mathcal{T}_i)$ is compact.

(The assumption $\emptyset \neq \bigtimes_{i\in I} Y_i$ is necessary, as the statement that cartesian product of non-empty sets is non-empty is equivalent to AC.)

Exercise 28.12. Let $\langle X_i \mid i \in I\rangle$ be a family of non-empty sets, let $z \notin \bigcup_{i\in I} X_i$, let $Y_i = X_i \cup \{z\}$, and let $\mathcal{T}_i$ be the collection of all cofinite subsets of Y_i together with the addition of $\emptyset$ and $\{z\}$. Show that:

(i) $(Y_i, \mathcal{T}_i)$ is compact T_1,

(ii) (T) $\Rightarrow \bigtimes_{i\in I} X_i \neq \emptyset$.

Exercise 28.13. Show that

(i) a continuous automorphism of the complex field is either the identity or else the conjugation $z \mapsto \bar{z}$;

(ii) if $f \colon \mathbb{C} \to \mathbb{C}$ is a discontinuous automorphism of the complex field, then $\Re \circ f \restriction \mathbb{R} \colon \langle \mathbb{R}, +\rangle \to \langle \mathbb{R}, +\rangle$ is a discontinuous homomorphism of groups.

Exercise 28.14. Let $f \colon \mathbb{R} \to \mathbb{R}$ be a function satisfying the functional equation $f(x + y) = f(x) + f(y)$, and let $a = f(1)$. Show that

(i) $f \colon \langle \mathbb{R}, +\rangle \to \langle \mathbb{R}, +\rangle$ is a homomorphism and $\forall q \in \mathbb{Q}\ (f(q) = aq)$;

(ii) if f is continuous, then $\forall x \in \mathbb{R}\ (f(x) = ax)$.

Exercise 28.15. Suppose that $\mathbb{R}$ is well-orderable, and prove that $\langle \mathbb{R}, +\rangle$ is isomorphic to $\langle \mathbb{R}^n, +\rangle$ for every $n \geq 1$. In particular $\mathbb{R}$ and $\mathbb{C}$ are isomorphic as groups.

Exercise 28.16. Show that the statement AC-4 "if X_1, X_2 are infinite sets, then $X_1 \asymp X_2 \Leftrightarrow \boldsymbol{F}(X_1) \asymp \boldsymbol{F}(X_2)$" implies that every set is well-orderable by proving the following facts.

(i) Suppose $\emptyset \neq Y$, $Y \cap \mathrm{Ord} = \emptyset$, and $Y \asymp {}^{\omega}Y$, and let $\kappa = \mathrm{Hrtg}(Y)$. Then $\boldsymbol{F}(Y \times \kappa) \asymp Y \times \kappa \asymp \boldsymbol{F}(Y \cup \kappa)$.

(ii) Suppose X is infinite and let $Y = {}^{\omega}X$. Show that AC-4 together with (the proof of) Theorem 20.11 implies that Y is well-orderable, and so is X.

Exercise 28.17. Suppose that there is an infinite Dedekind-finite $A \subseteq \mathbb{R}$. (Clearly we are not allowed to assume AC_ω.) Show that A can be taken to be contained in $(0;1)$ and such that $0 = \inf A$. Check that the characteristic function $\boldsymbol{\chi}_A$ is discontinuous in 0, but sequentially continuous in 0.

Exercise 28.18. If $\emptyset \neq A_n \subseteq \mathbb{R}$ set $B_n = A_0 \times \cdots \times B_n \subseteq \mathbb{R}^n$. Show that there is a strictly increasing sequence of natural numbers $\langle n_i \mid i \in \omega\rangle$ and a sequence of real numbers $\langle b_i \mid i \in \omega\rangle$ such that $b_i \in B_{n_i}$, then there is a sequence of reals $\langle a_n \mid n \in \omega\rangle$ such that $a_n \in A_n$, for every n. Conclude that $\mathsf{AC}_\omega(\mathbb{R})$ is equivalent to the (seemingly weaker) statement: If $\emptyset \neq A_n \subseteq \mathbb{R}$, then there is a strictly increasing sequence of natural numbers $(n_i)_i$ and a sequence of reals $(b_i)_i$ such that $b_i \in A_{n_i}$.

Exercise 28.19. Let $\emptyset \neq A_n \subseteq (2^{-n-1}; 2^{-n})$ and let $f \colon \mathbb{R} \to \mathbb{R}$ be the characteristic function of $\bigcup_n A_n$. Show that f is discontinuous in 0 and that if $x_i \to 0$ is such that $f(x_i) \not\to 0$, then there is an increasing sequence of natural numbers $(n_i)_i$ and a sequence of reals $(b_i)_i$ such that $b_i \in A_{n_i}$.

Conclude that the statement (14.3) "for all $f \colon \mathbb{R} \to \mathbb{R}$ for all $x \in \mathbb{R}$, if f is sequentially continuous in x then f is continuous in x" implies $\mathsf{AC}_\omega(\mathbb{R})$.

Exercise 28.20. Show that $\mathsf{AC}_\omega(X)$ is equivalent to "every second countable topology on X is separable".

Exercise 28.21. Show that the following are equivalent:

(i) The Baire category Theorem 26.8;

(ii) The statement of Theorem 26.8 weakened to $\bigcap_n U_n \neq \emptyset$;

(iii) DC.

[Hint for (ii)⇒(iii): if $\forall x \in X\, \exists y \in X\, (x \mathrel{R} y)$, then $U_n = \{f \mid \exists m (f(n) \mathrel{R} f(m))\}$ is open and dense in ${}^{\omega}X$.]

Notes and remarks

The axiom of choice has a particular position in mathematics, since it has many useful consequences, and some other consequences that are counter-intuitive and bizarre. Since the first greatly outnumber the second, AC is taken to be a valid principle by the majority of mathematicians. In 1937 Gödel proved that if a contradiction is derived without the axioms of choice, then one could obtain such a contradiction even without AC. In other words: it is not possible to refute AC from MK or from ZF, unless these theories are inconsistent, in which case any statement would be provable. In 1963, Cohen proved an analogous result fro the negation of AC, hence it is not possible to prove AC from MK or ZF, unless these theories are inconsistent. For a survey of the various "disasters" that can happen in mathematics if AC or its negation is assumed, we refer the reader to [**Her06**]. The equivalence between DC and the Baire category theorem is due to C.E. Blair—see [**Her06**, Theorem 4.106]. The monograph [**TW16**] contains a detailed and up-to-date exposition of the Banach-Tarski paradox and its variants.

29. Ramsey's Theorem*

Ultrafilters on ω have important applications in many parts of mathematics, such as general topology, functional analysis, etc. In this Section we will see a few applications to combinatorics.

Recall a few concepts seen in Section 10. A graph $\langle V, E\rangle$ is a non-empty set of vertexes V together with the set $E \subseteq [V]^2$ of the edges; if $E = [V]^2$ then the graph is complete on V. A coloring (of the edges) is a function c with domani E: if $\operatorname{ran}(c) \subseteq k$ we speak of k-coloring. Equivalently, a k-coloring is a partition of the edges in at most k parts.

If c is a k-coloring of $\langle V, E\rangle$, we say that $H \subseteq V$ is **monochromatic** or **homogeneous** for c if $c \restriction E \cap [H]^2$ is constant, that is

$$\exists i \in k \forall x, y \in H\, (\{x, y\} \in E \Rightarrow c(\{x, y\}) = i)\,.$$

Equivalently, if $[V]^2 = C_0 \cup \cdots \cup C_{k-1}$, then $[H]^2 \subseteq C_i$, for some i.

Theorem 29.1 (Ramsey´s Theorem in the infinite case)**.** *Suppose V is a countable set and suppose*

$$[V]^r = C_0 \cup \cdots \cup C_{k-1}$$

where $k, r \in \omega \setminus \{0\}$ and $C_i \subseteq [V]^r$, then there is an infinite $H \subseteq V$ such that $[H]^r \subseteq C_i$, for some $i < k$.

Proof. We start with two simple observations. We may assume that the C_is are pairwise disjoint. The second observation is that it is enough to prove the theorem for $k = 2$. In fact the case $k = 1$ is trivial and for $k > 2$ proceed by induction: suppose the result holds for $k \geq 2$ and prove it for $k + 1$. By the theorem in case $k = 2$, there is an infinite $H \subseteq V$ such that either $[H]^r \subseteq C_0$ or else $[H]^r \subseteq C_1 \cup \cdots \cup C_k$. If the former holds, then the theorem is proved, hence we may assume that

$$[H]^r \subseteq (C_1 \cap [H]^r) \cup \cdots \cup (C_k \cap [H]^r)\,.$$

By inductive assumption there is an infinite $H' \subseteq H$ such that $[H]^r \subseteq C_i$ for some $1 \leq i \leq k$, as required.

Therefore we prove the result when $k = 2$. The proof proceeds by induction on $r \geq 1$.

Suppose $r = 1$: the set $[V]^1$ can be identified with V so the result becomes:

> If $V = C_0 \cup C_1$, then at least one among C_0 and C_1 is infinite,

and this follows at once from Proposition 13.20.

Assume the result is true for some r and let's prove it for $r+1$. For notational simplicity suppose that $V = \omega$. Let

$$f\colon [\omega]^{r+1} \to 2$$

be the coloring associated to the partition $\{C_0, C_1\}$, that is to say

$$f(\bar{x}) = i \;\Leftrightarrow\; \bar{x} \in C_i.$$

If C_i is finite, then

$$H = \{n \in \omega \mid \neg\exists \bar{x} \in [\omega]^r\,(n \in \bar{x} \wedge \bar{x} \in C_i)\}$$

is infinite and $[H]^r \subseteq C_{1-i}$, hence we may assume that C_0 and C_1 are both infinite. We construct a set $K \subseteq \omega$ such that

$$\forall \bar{x}, \bar{y} \in [K]^{r+1}\,(x_0 = y_0 \wedge \cdots \wedge x_{r-1} = y_{r-1} \Rightarrow f(\bar{x}) = f(\bar{y})) \tag{29.1}$$

that is to say: the value of $f(\bar{x})$ depends only on the first r elements of $\bar{x}$. We can thus define a function $g\colon [K]^r \to 2$ letting

$$g(\bar{x}) = f(\bar{x} \cup \{n\})$$

for some (equivalently: for all) $n \in K$ with $n > \max(\bar{x})$. By inductive assumption there is an infinite $H \subseteq K$ which is homogeneous for g. Fix $\bar{x}, \bar{y} \in [H]^{r+1}$. As K satisfies (29.1) and $H \subseteq K$, if $\bar{x}, \bar{y} \in [H]^{r+1}$ then

$$\begin{aligned} f(\bar{x}) &= g(\{x_0, \dots, x_{r-1}\}) \\ &= g(\{y_0, \dots, y_{r-1}\}) \\ &= f(\bar{y}), \end{aligned}$$

that is H is the homogeneous set we are looking for. Therefore it is enough to show the existence of a set K that satisfies (29.1).

Fix a non-principal ultrafilter U on ω. For every $\bar{x} \in [\omega]^r$ let

$$D_i(\bar{x}) = \{n \in \omega \mid n > \max \bar{x} \;\wedge\; f(\bar{x} \cup \{n\}) = i\}.$$

As

$$D_0(\bar{x}) \cup D_1(\bar{x}) = \omega \setminus (\max \bar{x} + 1) \in U$$

let

$$i(\bar{x}) = \text{the unique } i \in 2 \text{ such that } D_i(\bar{x}) \in U.$$

Construct by induction a sequence of natural numbers y_n as follows:

- since $r = \{0, 1, \dots, r-1\} \in [\omega]^r$, then

  $$Y_0 = D_{i(r)}(r)$$

  is well-defined; let

  $$y_0 = \min Y_0.$$

  Note that $y_0 > r$.

- Suppose we have defined $y_0, \ldots, y_n$. The set
$$\mathcal{X}_n = [r \cup \{y_0, \ldots, y_n\}]^r$$
is finite (it has exactly $\binom{r+n+1}{r}$ elements) and since U is closed under finite intersections,
$$Y_{n+1} = \bigcap_{\bar{x} \in \mathcal{X}_n} D_{i(\bar{x})}(\bar{x}) \in U.$$
As $\emptyset \notin U$, then $Y_{n+1} \neq \emptyset$. Let
$$y_{n+1} = \min Y_{n+1}.$$

It is easy to check that $r \leq y_0 < y_1 < \ldots$ and that $Y_0 \supset Y_1 \supset \ldots$. Let
$$K = \{y_n \mid n \in \omega\}.$$
Fix $\bar{x} \in [K]^r$ and let $y_n = \max \bar{x}$, such that $\bar{x} \in \mathcal{X}_n$. If $n < m, h$, then $y_m, y_h \in Y_{n+1} \subseteq D_{i(\bar{x})}(\bar{x})$ hence $f(\bar{x} \cup \{y_m\}) = f(\bar{x} \cup \{y_h\})$. Therefore K satisfies (29.1). □

Corollary 29.2. *If $<$ and $\prec$ are two linear ordering on an infinite set X, then there is an infinite subset $H \subseteq X$ on which $<$ agrees with either $\prec$ or else with the inverse ordering $\succ$, that is to say*
$$\forall x, y \in H\, (x < y \Leftrightarrow x \prec y) \vee \forall x, y \in H\, (x < y \Leftrightarrow y \prec x)\,.$$

The notation
$$\alpha \to (\beta)^n_k$$
means that for each coloring $f\colon [\alpha]^n \to k$ there is $H \subseteq \alpha$ of order type β that is homogeneous for f, that is $f \restriction [H]^n$ is constant. Therefore Ramsey's Theorem 29.1 can be stated as $\omega \to (\omega)^n_k$. The ordinal ω cannot be replaced by ω_1 (Exercise 29.7). In fact there is a coloring $f\colon [\omega_1]^2 \to \omega_1$ such that $\operatorname{ran}(f \restriction [X]^2) = \omega_1$ for *all* $X \subseteq \omega_1$. In other words: there is a commutative binary operation $*$ on ω_1 such that applying $*$ to the elements of any uncountable subset yields ω_1.

One can consider order-types, rather than ordinals. For example Exercise 29.8 shows that $\mathbb{Q} \to (\mathbb{Q})^1_k$, that is if $\mathbb{Q}$ is partitioned into finitely many pieces, then at least one of these pieces contains a subset isomorphic to $\mathbb{Q}$. Conversely $\mathbb{Q} \to (\mathbb{Q})^2_2$ fails, that is to say: there is a coloring $f\colon [\mathbb{Q}]^2 \to 2$ such that $f \restriction [X]^2$ assumes two values, for any subset X isomorphic to $\mathbb{Q}$ (Exercise 29.6). On the other hand, this is the worst it can happen, since if $f\colon [\mathbb{Q}]^2 \to k$, then there is $X \subseteq \mathbb{Q}$ isomorphic to $\mathbb{Q}$ such that $|f \restriction [X]^2| \leq 2$, for every k. In fact for each $n \in \omega$ there is a least $t_n \in \omega$ such that for all k-coloring $f\colon [\mathbb{Q}]^n \to k$ there is $X \subseteq \mathbb{Q}$ isomorphic to $\mathbb{Q}$ such that $|\operatorname{ran}(f \restriction [X]^n)| \leq t_n$.

29.A. Well-quasi-orders.

Definition 29.3. A quasi-order $(P, \leq)$ is a **well-quasi-order**, **wqo** for short, if

- the strict part $<$ of $\leq$ is well-founded on P (Definition 18.2), that is for all non-empty $X \subseteq P$ there is $p \in X$ such that there is no $q \in X$ such that $q < p$,
- and every independent set is finite, that is if $Y \subseteq P$ is such that $\forall p, q \in Y\, (p \nleq q \wedge q \nleq p)$, then $|Y| < \omega$.

Free subsets of (quasi-)orders are usually called **antichains**. A sequence $\langle p_n \mid n \in \omega \rangle$ in a quasi-order P is **bad** if $n < m \Rightarrow p_n \nleq p_m$.

Proposition 29.4. *Assume* DC. *For a quasi-order* $(P, \leq)$ *the following are equivalent:*

(1) $(P, \leq)$ *is a wqo,*

(2) $(P, \leq)$ *has no bad sequences,*

(3) $(\mathrm{Down}(P), \leq)$ *is well-founded.*

Proof. The equivalences (1)⇔(2) and (2)⇔(3) are obtained by taking the contrapositives.

(1)⇔(2). If $(p_n)_n$ is bad, let $f\colon [\omega]^2 \to 2$

$$f(\{n, m\}) = \begin{cases} 0 & \text{if } n < m \text{ and } p_m \leq p_n \\ 1 & \text{otherwise.} \end{cases}$$

By Ramsey's Theorem 29.1 let $\{n_k \mid k \in \omega\}$ be infinite and homogeneous for f. Then $(p_{n_k})_k$ is either $<$-descending, or else $\{p_{n_k} \mid k \in \omega\}$ is an infinite antichain.

Conversely if P is not wqo then there is an descending sequence (by DC) or there is an infinite antichain. In either case we have a bad sequence.

(2)⇔(3). By DC suppose $(D_n)_n$ is a $\subset$-decreasing sequence in $\mathrm{Down}(P)$, so that we can choose $p_n \in D_n \setminus D_{n+1}$. If $n < m$ and $p_n \leq p_m$, then $p_n \in D_m$ as D_m is a down-set, against the fact that $p_n \notin D_k$ when $k > n$. Therefore $n < m \Rightarrow p_n \nleq p_m$, that is $(p_n)_n$ is bad.

Vice-versa if $(p_n)_n$ is bad then $D_n = \downarrow\{p_k \mid n \leq k\}$ is an infinite $\subset$-descending chain. □

Exercises

Exercise 29.5. Show that for every sequence $\langle x_n \mid n \in \omega\rangle$ of distinct elements of an ordered set $\langle X, \leq\rangle$ has a subsequence $\langle x_{n_k} \mid k \in \omega\rangle$ which is increasing or decreasing, or such that $\{x_{n_k} \mid k \in \omega\}$ is an independent set (see page 43) of $\langle X, \leq\rangle$.

In particular, AC_ω implies that every infinite ordered set contains either an infinite chain or else an infinite independent set.

Exercise 29.6. Show that there is $f\colon [\mathbb{Q}]^2 \to 2$ such that $\forall X \subseteq \mathbb{Q}\,(X \cong \mathbb{Q} \Rightarrow |f \restriction [X]^2| = 2)$.

Exercise 29.7. Show that $2^{\aleph_0} \not\to (\omega)^2_2$.

Exercise 29.8. Show that

(i) if $\{X_1, \ldots, X_n\}$ is a partition of $\mathbb{Q}$, then some X_i contains an isomorphic copy of $\mathbb{Q}$;

(ii) if $\{X_1, \ldots, X_n\}$ is a partition of R_ω, then some X_i contains an isomorphic copy of R_ω.

Chapter VII

General structures and languages

30. Structures and languages

In this Section we develop in detail the notions of first-order language and first-order structure that were introduced in Chapter I.

30.A. Structures. A **signature** is a 4-uple $\tau = \langle I, J, K, \mathrm{ar}\rangle$ with I, J, K pairwise disjoint sets and $\mathrm{ar}\colon I \cup J \to \omega \setminus \{0\}$. We say that τ is **relational** if $J = K = \emptyset$, **functional** if $I = K = \emptyset$, **well-orderable** if I, J, K are well-orderable, **finite** if I, J, and K are finite. The **cardinality of the signature** τ is

$$\mathrm{card}(\tau) = \mathrm{card}(I) + \mathrm{card}(J) + \mathrm{card}(K) = \mathrm{card}(I \cup J \cup K),$$

that is $\mathrm{card}(\tau) = |I| + |J| + |K|$ when τ is well-orderable. A τ**-structure** is a 4-tuple

$$\mathcal{A} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle\rangle$$

such that $A = \|\mathcal{A}\|$ is a non-empty set called the **universe** of $\mathcal{A}$, $R_i^{\mathcal{A}} \subseteq A^{\mathrm{ar}(i)}$, for all $i \in I$, $f_j^{\mathcal{A}}\colon A^{\mathrm{ar}(j)} \to A$, for all $j \in J$, and $c_k^{\mathcal{A}} \in A$, for all $k \in K$. A τ-structure is relational/functional if so is τ. A **morphism** from $\mathcal{A}$ to $\mathcal{B}$ with $\mathcal{A}, \mathcal{B} \in \mathrm{Str}(\tau)$, is a function $F\colon \|\mathcal{A}\| \to \|\mathcal{B}\|$ such that

(A) $\forall \vec{a} \in A^{\mathrm{ar}(i)} \bigl(\vec{a} \in R_i^{\mathcal{A}} \Rightarrow F(\vec{a}) \in R_i^{\mathcal{B}}\bigr)$, for all $i \in I$,

(B) $\forall \vec{a} \in A^{\mathrm{ar}(j)} \bigl(\pi(f_j^{\mathcal{A}}(\vec{a})) = f_j^{\mathcal{B}}(F(\vec{a}))\bigr)$, for all $j \in J$,

(C) $F(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$, for all $k \in K$.

If (A) is strengthened to

(A$'$) $\forall \vec{a} \in A^{\mathrm{ar}(i)} \left(\vec{a} \in R_i^{\mathcal{A}} \Leftrightarrow F(\vec{a}) \in R_i^{\mathcal{B}} \right)$, for all $i \in I$,

we speak of **complete** or **full morphism**. An **embedding** of $\mathcal{A}$ into $\mathcal{B}$ is a complete injective morphism from $\mathcal{A}$ to $\mathcal{B}$; an **isomorphism** is a bijective morphism whose inverse is still a morphism; equivalently: it is a complete bijective morphism.

The collection of all τ-structures is a proper class $\mathrm{Str}(\tau)$, and it is and it is a category, taking the arrows to be the morphisms between structures. Two signatures $\tau = \langle I, J, K, \mathrm{ar} \rangle$ and $\tau' = \langle I', J', K', \mathrm{ar}' \rangle$ are **isomorphic** if there is a bijection $\varphi \colon I \cup J \cup K \to I' \cup J' \cup K'$ such that $\varphi[I] = I'$, $\varphi[J] = J'$, $\varphi[K] = K'$ and $\mathrm{ar}'(\varphi(x)) = \mathrm{ar}(x)$ for all $x \in I \cup J$. Every τ-structure can be construed as a τ'-structure and conversely, that is φ induces a bijective functional relation $\Phi \colon \mathrm{Str}(\tau) \to \mathrm{Str}(\tau')$. With abuse of notation, we will write $\tau \subseteq \tau'$ to say that $I \subseteq I'$, $J \subseteq J'$, $K \subseteq K'$ and $\mathrm{ar} = \mathrm{ar}' \restriction I \cup J$.

Two τ-structures are isomorphic $\mathcal{A} \cong \mathcal{B}$ if there is an isomorphism between them; an **automorphism** is an isomorphism of a structure in itself and $\mathrm{Aut}(\mathcal{A})$ is the group of all automorphisms of $\mathcal{A}$; if $\mathrm{Aut}(\mathcal{A}) = \{\mathrm{id}_{\|\mathcal{A}\|}\}$ then $\mathcal{A}$ is **rigid**. We say that $\mathcal{A}$ **embeds into** $\mathcal{B}$, in symbols

$$\mathcal{A} \Subset \mathcal{B}.$$

if there is an embedding of $\mathcal{A}$ in $\mathcal{B}$. When the embedding is not surjective write $\mathcal{A} \Subset \mathcal{B}$. In case the universe of $\mathcal{A}$ is contained in the universe of $\mathcal{B}$ and the relations, functions, constants of $\mathcal{A}$ agree with the restrictions of those of $\mathcal{B}$, i.e. the identity function $\mathcal{A} \hookrightarrow \mathcal{B}$ is an embedding, then $\mathcal{A}$ is a **substructure** of $\mathcal{B}$, in symbols $\mathcal{A} \subseteq \mathcal{B}$. If $\mathcal{A} \subseteq \mathcal{B}$ and $\|\mathcal{A}\| \neq \|\mathcal{B}\|$ we say that $\mathcal{A}$ is a **proper substructure** of $\mathcal{B}$, in symbols $\mathcal{A} \subset \mathcal{B}$. The **cardinality** of $\mathcal{A}$

$$\mathrm{card}(\mathcal{A})$$

is the cardinality of the universe $A = \|\mathcal{A}\|$. By Theorem 21.18 on page 434, if $X \subseteq \|\mathcal{A}\|$, then $\bigcap\{\|\mathcal{B}\| \mid X \subseteq \|\mathcal{B}\| \wedge \mathcal{B} \subseteq \mathcal{A}\}$ is the **substructure generated by** X and has cardinality $\leq \max(|J|, |K|, |X|, \aleph_0)$.

If $\mathcal{A}'$ is a τ'-structure and $\tau \subseteq \tau'$, the **reduction of** $\mathcal{A}'$ **to** τ is the τ-structure

$$\mathcal{A}' \restriction \tau = \langle \left\|\mathcal{A}'\right\|, \langle R_i^{\mathcal{A}'} \mid i \in I \rangle, \langle f_j^{\mathcal{A}'} \mid j \in J \rangle, \langle c_k^{\mathcal{A}'} \mid k \in K \rangle \rangle.$$

The map $\mathrm{Str}(\tau') \to \mathrm{Str}(\tau)$ is a forgetful functor. Conversely, if $\mathcal{A}$ is a τ-structure and $\mathcal{A}'$ is a τ'-structure whose reduction to τ is $\mathcal{A}$, then we will say that $\mathcal{A}'$ is an **expansion of** $\mathcal{A}$ **to** τ'. Every τ-structure admits a τ'-expansion, but, in general, such expansion is far from being unique. In other words, the reduction functor $\mathrm{Str}(\tau') \twoheadrightarrow \mathrm{Str}(\tau)$ is surjective, but not injective.

30.A.1. *Canonical expansions.* Suppose $\mathcal{A}$ is a τ-structure with $\tau = \langle I, J, K, \mathrm{ar}\rangle$. If $B \subseteq \|\mathcal{A}\|$, then the **canonical expansion of $\mathcal{A}$ by B** is the structure $\langle \mathcal{A}, b\rangle_{b\in B}$ obtained by making each $b \in B$ a distinguished element—formally $\langle \mathcal{A}, b\rangle_{b\in B} = \langle A, \langle R_i^{\mathcal{A}} \mid i \in I\rangle, \langle f_j^{\mathcal{A}} \mid j \in J\rangle, \langle c_k^{\mathcal{A}} \mid k \in K\rangle \cup \langle b \mid b \in B\rangle\rangle$ is a τ'-structure where $\tau' = \langle I, J, K \cup \{\mathring{b} \mid b \in B\}, \mathrm{ar}\rangle$ and $\{\mathring{b} \mid b \in B\}$ is disjoint from $I \cup J \cup K$. Similarly, if R is a relation and f is an operation on $\|\mathcal{A}\|$, the **canonical expansion of $\mathcal{A}$ by R and f** is the structure $\langle \mathcal{A}, R, f\rangle$ obtained by adding the relation R and the operation f— formally it is a τ^*-structure where $\tau^* = \langle I \cup \{i'\}, J \cup \{j'\}, K, \mathrm{ar}^*\rangle$ where $\{i', j'\}$ is disjoint from $I \cup J \cup K$ and $\mathrm{ar}^*(i')$ and $\mathrm{ar}^*(j')$ are the arities of R and f.

30.A.2. *Products.* First of all we check that the category $\mathrm{Str}(\tau)$ admits products, in fact products with an arbitrary number of factors. The construction of product of structures is a generalization of the product of orders and the product of groups. Let X be a non-empty set of indexes.[1] The **direct product** or simply **product** of a family of τ-structures $\langle \mathcal{A}_x \mid x \in X\rangle$ is the τ-structure $\mathcal{A} = \prod_x \mathcal{A}_x$ with universe $\bigtimes_{x\in X} \|\mathcal{A}_x\|$ and such that:

- if $\mathrm{ar}(i) = n$, then $(g_1, \dots, g_n) \in R_i^{\mathcal{A}} \Leftrightarrow \forall x \in X \left((g_1(x), \dots, g_n(x)) \in R_i^{\mathcal{A}_x}\right)$.
- if $\mathrm{ar}(j) = n$, then $f_j^{\mathcal{A}}(g_1, \dots, g_n) = \langle f_j^{\mathcal{A}_x}(g_1(x), \dots, g_n(x)) \mid x \in X\rangle$,
- if $k \in K$ let $c_k^{\mathcal{A}} = \langle c_k^{\mathcal{A}_x} \mid x \in X\rangle$.

For every $y \in X$ the maps $\pi_y\colon \bigtimes_{x\in X} \|\mathcal{A}_x\| \to \|\mathcal{A}_y\|$, $f \mapsto f(y)$ are morphisms of structures, and satisfy the universality property of products. In other words: the category $\mathrm{Str}(\tau)$ admits products. When $|X| = 2$ we write $\mathcal{A}_0 \times \mathcal{A}_1$ instead of $\prod_{x\in X} \mathcal{A}_x$.

Remark 30.1. If τ does not contain constants, then we need AC to guarantee that $\bigtimes_{x\in X} \|\mathcal{A}_x\| \neq \emptyset$, hence that a τ-structure is obtained.

Whenever F is a filter on X, an equivalence relation $g \sim_F h \Leftrightarrow \{x \in X \mid g(x) = h(x)\} \in F$ was defined on $\bigtimes_{x\in X} \|\mathcal{A}_x\|$ in Section 15.A, and we have denoted the quotient $\bigtimes_{x\in X} \|\mathcal{A}_x\| /{\sim_F}$ with $\prod_F \|\mathcal{A}_x\|$. The **reduced product modulo F of** $\langle \mathcal{A}_x \mid x \in X\rangle$ is the τ-structure $\prod_F \mathcal{A}_x$ with universe $\prod_F \|\mathcal{A}_x\|$, built in a similar way to what was done in Section 15.A.1 for orders and in Section 15.A.2 for fields:

- if $\mathrm{ar}(i) = n$ and $[g_1], \dots, [g_n] \in A_F$, then
$$([g_1], \dots, [g_n]) \in R_i^{\prod_F \mathcal{A}_x} \Leftrightarrow \{x \in X \mid (g_1(x), \dots, g_n(x)) \in R_i^{\mathcal{A}_x}\} \in F$$
- if $\mathrm{ar}(j) = n$ and $[g_1], \dots, [g_n] \in A_F$, then
$$f_j^{\prod_F \mathcal{A}_x}([g_1], \dots, [g_n]) = [\langle f_j^{\mathcal{A}_x}(g_1(x), \dots, g_n(x)) \mid x \in X\rangle]$$

[1] The choice of the letter X for a set of indexes may seem a bit peculiar, but the other letters commonly used for this task I, J, K are already taken.

- $c_k^{\prod_F \mathcal{A}_x} = [\langle c_k^{\mathcal{A}_x} \mid x \in X \rangle]$.

If $\mathcal{A}_x = \mathcal{A}$ for all $x \in X$, we say that $\prod_F \mathcal{A}_x = \mathcal{A}^N/F$ is a **reduced power**. If F is an ultrafilter on X we say that $\prod_F \mathcal{A}_x$ is an **ultraproduct**, and if $\mathcal{A}_x = \mathcal{A}$ for all $x \in X$, we will speak of **ultrapower**.

30.A.3. *Direct and inverse limits.* We have see the definition of increasing union of structures in Section 4.F.

To be written later

30.B. First-order languages. The goal of this section is to give a rigorous treatment within set theory of the notions seen in Chapter I. For each signature τ we construct a language $\mathcal{L}$ and from this we construct its terms $\boldsymbol{t}$ and its formulæ $\boldsymbol{\varphi}$. (Languages, terms, and formulæ will be sets.) Formulæ of $\mathcal{L}$ are the set-theoretic embodiment of the usual mathematical statements about τ-structures hence we will need a set-theoretic counterpart of the various logical symbols $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, and $\forall$. In order to avoid confusion, we will use distinguish the symbols of the object language from those of the informal language where the results are presented.

30.B.1. *Symbols.* A **first-order language** $\mathcal{L}$ is comprised of

- an ω-sequence of objects which we call **variables**

$$\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n, \dots$$

- two distinct objects which we call **connectives**: $\boldsymbol{\neg}$ and $\boldsymbol{\vee}$,
- an object which we call **equality symbol** $\doteq$
- three disjoint families of objects $\{\boldsymbol{R}_i \mid i \in I\}$, $\{\boldsymbol{f}_j \mid j \in J\}$, $\{\boldsymbol{c}_k \mid k \in K\}$, called **relation symbols** or **predicates**, **function symbols** or **operation symbol**, and **constant symbol**, respectively,
- a function $\mathrm{ar}\colon \{\boldsymbol{R}_i \mid i \in I\} \cup \{\boldsymbol{f}_j \mid j \in J\} \to \omega \setminus \{0\}$, called **arity**.

The nature of these objects is irrelevant—we stipulate that $\boldsymbol{\neg}$, $\boldsymbol{\vee}$, $\doteq$, $\boldsymbol{v}_n$, $\boldsymbol{R}_i$, $\boldsymbol{f}_j$, and $\boldsymbol{c}_k$, are shorthand for $(0,0)$, $(0,1)$, $(0,2)$, $\langle(1,n)\rangle$, $(2,i)$, $(3,j)$, and $\langle(4,k)\rangle$, respectively. (The rationale for requiring that $\boldsymbol{v}_n$ and $\boldsymbol{c}_k$ be sequences of length 1 will be clear when we define the terms.)

Definition 30.2. A **first-order language** $\mathcal{L}$ is a pair $(\mathcal{S}, \mathrm{ar})$ satisfying the following properties

- there are sets I, J and K such that

$$\mathcal{S} = \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Func}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}} \cup \{\boldsymbol{\neg}, \boldsymbol{\vee}, \doteq\} \cup \mathrm{Vbl}$$

  where $\mathrm{Vbl} = \{\boldsymbol{v}_n \mid n \in \omega\}$ and $\mathrm{Rel}_{\mathcal{L}} = \{2\} \times I$, $\mathrm{Func}_{\mathcal{L}} = \{3\} \times J$ and $\mathrm{Const}_{\mathcal{L}} = {}^1(\{4\} \times K)$.
- $\mathrm{ar}\colon\ \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Func}_{\mathcal{L}} \to \omega \setminus \{0\}$.

The **non-logical symbols** of $\mathcal{L}$ are the elements of $\mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Func}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}}$. Every signature τ yields a language $\mathcal{L}_\tau$ and, conversely, every language $\mathcal{L}$ yields a signature $\tau_{\mathcal{L}}$. Two languages are **isomorphic** if and only if their signatures are isomorphic. We say that $\mathcal{L}$ is a **sub-language** of $\mathcal{L}'$ or that $\mathcal{L}'$ is an **extension** of $\mathcal{L}$ if and only if $\tau_{\mathcal{L}} \subseteq \tau_{\mathcal{L}'}$.

Remark 30.3. As a language is completely identified by its signature, these two notions are often identified. Also the notion of arity is often suppressed, when it is clear from the context — for example we write $\mathcal{L}_{\mathrm{GRPS}} = \left\{\cdot, {}^{-1}, 1\right\}$ to denote the language of groups. This abuse of language will be perpetrated every time the set-theoretic notation enables us to state facts about languages in a concise form. Thus we write $\mathcal{L} \subseteq \mathcal{L}'$ to say that $\mathcal{L}'$ is an extension of $\mathcal{L}$, or $\mathcal{L} \cap \mathcal{L}'$ to denote the language whose non-logical symbols are those occurring both in $\mathcal{L}$ and in $\mathcal{L}'$, and so on.

A language $\mathcal{L}$ is **well-orderable** if its signature is well-orderable. The **cardinality** of $\mathcal{L}$ is

$$\mathrm{card}(\mathcal{L}) = \aleph_0 + \mathrm{card}(\tau_{\mathcal{L}}).$$

A **finite language** is a language whose signature is finite. An $\mathcal{L}$-structure is a $\tau_{\mathcal{L}}$-structure and let $\mathrm{Str}(\mathcal{L}) = \mathrm{Str}(\tau_{\mathcal{L}})$. In Chapter I and in particular in Section 9 we have seen many examples of finite, and hence well-orderable, languages. Instead the example of vector spaces over $\mathbb{R}$ described on page 242 yields a signature (and hence a language) which is uncountable, and that it is not well-orderable, unless AC is assumed. An important example of infinite, well-orderable language is the universal countable language $\mathcal{L}_\infty$ that has constant symbols $\boldsymbol{c}_n$ $(n \in \omega)$ and $\aleph_0$ relational symbols $\boldsymbol{R}_{n,m}$ and function symbols $\boldsymbol{f}_{n,m}$ of every arity, that is $\mathrm{ar}(\boldsymbol{R}_{n,m}) = \mathrm{ar}(\boldsymbol{f}_{n,m}) = m$ for all $n \geq 0$ and $m > 0$. Every countable language $\mathcal{L}$ is (isomorphic to) a sublanguage of $\mathcal{L}_\infty$, hence every $\mathcal{L}$-structure is the reduction of an $\mathcal{L}_\infty$-structure.

The set of all **terms of $\mathcal{L}$** is

$$\mathrm{Term}_{\mathcal{L}} = \mathrm{Expr}(\mathrm{Vbl} \cup \mathrm{Func} \cup \mathrm{Const}, a)$$

where $a(s) = 0$, if $s \in \mathrm{Vbl} \cup \mathrm{Const}$ and $a(s) = \mathrm{ar}(s)$, if $s \in \mathrm{Func}$. The elements of $\mathrm{Vbl} \cup \mathrm{Const}$ are sequences of length 1, so $\mathrm{Vbl} \cup \mathrm{Const} \subseteq \mathrm{Term}$ by Convention 23.2. Thus if $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n \in \mathrm{Term}$, $\boldsymbol{f} \in \mathrm{Func}$ and $\mathrm{ar}(\boldsymbol{f}) = n$ then $\langle \boldsymbol{f} \rangle^\frown \boldsymbol{t}_1{}^\frown \ldots {}^\frown \boldsymbol{t}_n \in \mathrm{Term}$. The **height of a term $\boldsymbol{t}$** is the height $\mathrm{ht}(\boldsymbol{t})$ as an expression. The letters $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ range on Vbl, while the letters $\boldsymbol{t}, \boldsymbol{u}, \boldsymbol{s}$ range over Term. Corollary 23.7 guarantees that a term that is neither a variable nor a constant must be of the form $\boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m)$ for a unique m-tuple $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m$ of terms.

Let $\mathrm{AtFml}^*(\mathcal{L})$ be the set of all sequences of the form

$$\langle \boldsymbol{R}_i \rangle^\frown \boldsymbol{t}_1{}^\frown \ldots {}^\frown \boldsymbol{t}_m \quad \text{or} \quad \langle \mathbin{\dot{=}} \rangle^\frown \boldsymbol{t}_1{}^\frown \boldsymbol{t}_2$$

where $\boldsymbol{R}_i$ is m-ary and $\boldsymbol{t}_1, \boldsymbol{t}_2, \dots, \boldsymbol{t}_m$ are terms. By Lemma 23.6 the terms $\boldsymbol{t}_1, \boldsymbol{t}_2, \dots, \boldsymbol{t}_m$ are uniquely determined. The set $\mathrm{AtFml}(\mathcal{L})$ of **atomic formulæ** of $\mathcal{L}$ is the set of all sequences of length 1 of the form $\langle u \rangle$ with $u \in \mathrm{AtFml}^*(\mathcal{L})$. An **$\mathcal{L}$-formula** is an element of the set

$$\mathrm{Fml}(\mathcal{L}) = \mathrm{Expr}(\mathrm{AtFml}(\mathcal{L}) \cup \{\neg, \vee\} \cup \mathrm{Vbl}, a)$$

where $a(\vee) = 2$, $a(\neg) = a(\boldsymbol{v}_n) = 1$ for all $n \in \omega$, and $a(\boldsymbol{\varphi}) = 0$ for all $\boldsymbol{\varphi} \in \mathrm{AtFml}(\mathcal{L})$. The letters $\boldsymbol{\varphi}, \boldsymbol{\psi}, \boldsymbol{\chi}, \dots$ range on Fml. As formulæ are expressions, we have a well-defined notion of **height**.

For ease of notation, we adopt the following conventions:

the writing...	is shorthand for...
$\boldsymbol{t}_1 = \boldsymbol{t}_2$	$\langle \langle = \rangle ^\frown \boldsymbol{t}_1 {}^\frown \boldsymbol{t}_2 \rangle$
$\boldsymbol{t}_1 \neq \boldsymbol{t}_2$	$\langle \neg, \langle = \rangle ^\frown \boldsymbol{t}_1 {}^\frown \boldsymbol{t}_2 \rangle$
$\boldsymbol{R}_i(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)$	$\langle \langle \boldsymbol{R}_i \rangle ^\frown \boldsymbol{t}_1 {}^\frown \dots {}^\frown \boldsymbol{t}_n \rangle$
$\neg \boldsymbol{\varphi}$	$\langle \neg \rangle ^\frown \boldsymbol{\varphi}$
$\boldsymbol{\varphi} \vee \boldsymbol{\psi}$	$\langle \vee \rangle ^\frown \boldsymbol{\varphi} {}^\frown \boldsymbol{\psi}$
$\exists \boldsymbol{v}_n \boldsymbol{\varphi}$	$\langle \boldsymbol{v}_n \rangle ^\frown \boldsymbol{\varphi}$

The connectives $\wedge$, $\Rightarrow$, and $\Leftrightarrow$, and the quantifier $\forall$ are introduced via the definitions:

the writing...	stands for...
$\boldsymbol{\varphi} \wedge \boldsymbol{\psi}$	$\neg(\neg \boldsymbol{\varphi} \vee \neg \boldsymbol{\psi})$
$\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$	$\neg \boldsymbol{\varphi} \vee \boldsymbol{\psi}$
$\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}$	$\neg(\neg(\neg \boldsymbol{\varphi} \vee \boldsymbol{\psi}) \vee \neg(\boldsymbol{\varphi} \vee \neg \boldsymbol{\psi}))$
$\boldsymbol{\varphi} \mathbin{\dot\vee} \boldsymbol{\psi}$	$\neg(\neg \boldsymbol{\varphi} \vee \boldsymbol{\psi}) \vee \neg(\boldsymbol{\varphi} \vee \neg \boldsymbol{\psi})$
$\forall \boldsymbol{x} \boldsymbol{\varphi}$	$\neg \exists \boldsymbol{x} \neg \boldsymbol{\varphi}$

By closing AtFml under negation and disjunction we obtain the set of **open** or **quantifier-free formulæ**. An **existential formula** is of the form $\exists \boldsymbol{x} \boldsymbol{\varphi}$; a **universal formula** is of the form $\forall \boldsymbol{x} \boldsymbol{\varphi}$, that is $\neg \exists \boldsymbol{x} \neg \boldsymbol{\varphi}$. A **primitive formula** is either an atomic or an existential formula. Every formula is obtained by applying $\neg$ and $\vee$ to primitive formulæ. A formula is in **prenex form** if it is obtained from open formulæ by closing under quantifications and negations.

The following notations will be used:

- $\mathrm{V{\scriptsize BL}}(\boldsymbol{t})$ is the set of **variables of the term $\boldsymbol{t}$**,
- $\mathrm{ClTerm} = \{\boldsymbol{t} \in \mathrm{Term} \mid \mathrm{V{\scriptsize BL}}(\boldsymbol{t}) = \emptyset\}$ is the set of **closed terms**,
- $\mathrm{Fv}(\boldsymbol{\varphi})$ is the set of all variables that occur free in $\boldsymbol{\varphi}$,
- $\mathrm{Sent}(\mathcal{L}) = \{\boldsymbol{\varphi} \mid \mathrm{Fv}(\boldsymbol{\varphi}) = \emptyset\}$ is the set of all **sentences**,

- the **universal** and the **existential closure** of a formula $\boldsymbol{\varphi}$ (defined in Chapter I on page 37) are the formulæ $\boldsymbol{\varphi}^{\forall} = \forall \boldsymbol{v}_{k_1} \dots \forall \boldsymbol{v}_{k_n} \boldsymbol{\varphi}$ and $\boldsymbol{\varphi}^{\exists} = \exists \boldsymbol{v}_{k_1} \dots \exists \boldsymbol{v}_{k_n} \boldsymbol{\varphi}$ where $\{\boldsymbol{v}_{k_1}, \dots, \boldsymbol{v}_{k_n}\} = \mathrm{Fv}(\boldsymbol{\varphi})$ and $k_1 < \cdots < k_n$,
- $\mathrm{Subst}(\boldsymbol{\varphi}; \boldsymbol{t}_1, \dots, \boldsymbol{t}_n; \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ means that the terms $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$ are *substitutable* for the variables $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$, that is to say: if we replace the free occurrences of the $\boldsymbol{x}_i$s with the $\boldsymbol{t}_i$, none of the variables occurring in a term fall under the scope of a quantifier of $\boldsymbol{\varphi}$,
- if $\mathrm{Subst}(\boldsymbol{\varphi}; \boldsymbol{t}_1, \dots, \boldsymbol{t}_n; \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ then $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$ is the formula obtained by replacing the free occurrences of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ with the terms $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$,
- $\exists! \boldsymbol{x} \boldsymbol{\varphi}$ is shorthand for $\exists \boldsymbol{x} \boldsymbol{\varphi} \wedge \forall \boldsymbol{y} (\boldsymbol{\varphi}(\!|\boldsymbol{y}/\boldsymbol{x}|\!) \Rightarrow \boldsymbol{y} = \boldsymbol{x})$, where $\boldsymbol{y}$ is the first variable such that $\mathrm{Subst}(\boldsymbol{\varphi}; \boldsymbol{y}; \boldsymbol{x})$.

Remarks 30.4. (a) In defining formulæ it is possible to start from a different set of symbols, for example $\{\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \exists, \forall\} \cup \{\boldsymbol{v}_n \mid n \in \omega\}$ so that all connectives and both quantifiers could be officially used. The advantage of our definition is that there are fewer cases to check when arguing by induction on the height of formulæ.

(b) By replacing $\boldsymbol{\varphi}$ with a suitable variant we may assume that $\mathrm{Subst}(\boldsymbol{\varphi}, \vec{\boldsymbol{t}}, \vec{\boldsymbol{x}})$ so that $\boldsymbol{\varphi}(\!|\vec{\boldsymbol{t}}, \vec{\boldsymbol{x}}|\!)$ can always be defined (Section 30.C.3).

(c) The sets of terms and formulæ depend on the signature, so we should write Term_τ and $\mathrm{Fml}(\tau)$ rather than $\mathrm{Term}_{\mathcal{L}}$ and $\mathrm{Fml}(\mathcal{L})$, but it is common in logic to blur the distinction between signature and language.

30.C. Syntax as manipulation of finite sequences*.

30.C.1. *Formulæ as expressions.* According to our definition, formulæ are expressions built from elements of AtFml using $\neg, \vee$ and variables. A key advantage of this approach is the unique readability of formulæ (Corollary 23.7). The set of formulæ can also be seen as a free induction system (Section 7.A.1), namely $(\mathrm{Fml}, \mathcal{F}, \mathrm{AtFml})$ where $\mathcal{F}$ is the set of all operations $\boldsymbol{\varphi} \mapsto \neg \boldsymbol{\varphi}$ and $(\boldsymbol{\varphi}, \boldsymbol{\psi}) \mapsto \boldsymbol{\varphi} \vee \boldsymbol{\psi}$, so by Theorem 12.10, in order to define a function on Fml it is enough to define it on AtFml and then describe how it behaves with respect to the operations in $\mathcal{F}$.

Since atomic formulæ are constructed from terms, relation symbols and $=$, it is natural to construe formulæ as elements of $\mathcal{S}^{<\omega}$, where

$$\mathcal{S} = \mathrm{Vbl} \cup \{\neg, \vee, =\} \cup \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Func}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}} . \tag{30.1}$$

Define

$$\mathrm{Fml}(\mathcal{L}) \to \mathcal{S}^{<\omega}, \qquad \boldsymbol{\varphi} \mapsto \boldsymbol{\varphi}^* \tag{30.2}$$

as follows. If $\boldsymbol{\varphi} = \langle u \rangle \in \mathrm{AtFml}$ then $\boldsymbol{\varphi}^* = u$; if $\boldsymbol{\varphi}$ is $\langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{\psi}$, or $\langle \boldsymbol{\vee} \rangle^\frown \boldsymbol{\psi}^\frown \boldsymbol{\chi}$, or $\langle \boldsymbol{v}_n \rangle^\frown \boldsymbol{\psi}$, then $\boldsymbol{\varphi}^*$ is $\langle \boldsymbol{\neg} \rangle^\frown \boldsymbol{\psi}^*$, or $\langle \boldsymbol{\vee} \rangle^\frown \boldsymbol{\psi}^{*\frown} \boldsymbol{\chi}^*$, or $\langle \boldsymbol{v}_n \rangle^\frown \boldsymbol{\psi}^*$, respectively. The function (30.2) is injective and $\mathrm{AtFml}^* = \{\boldsymbol{\varphi}^* \mid \boldsymbol{\varphi} \in \mathrm{AtFml}\}$.

Proposition 30.5. *Let $\mathcal{L}$ be a first-order language, and let $\mathcal{S}$ be as in* (30.1).

(a) $\mathrm{Term} \precsim \mathrm{AtFml} \subseteq \mathrm{Fml} \precsim \mathcal{S}^{<\omega}$.

(b) *The following sets are in bijection:*

$$\mathrm{AtFml}^{<\omega}, \quad \mathrm{QFFml}, \quad \mathrm{Fml}, \quad \mathrm{Sent}, \quad \mathrm{Fml}(\boldsymbol{x}), \quad \mathcal{S}^{<\omega},$$

where QFFml *is the set of all quantifier-free formulæ, and* $\mathrm{Fml}(\boldsymbol{x})$ *is the set of all formulæ with* $\boldsymbol{x}$ *as the only free variable.*

Thus if $\mathcal{L}$ is well-orderable, then $|\mathrm{AtFml}| = |\mathrm{QFFml}| = |\mathrm{Fml}| = |\mathrm{Sent}| = |\mathrm{Fml}(\boldsymbol{x})| = |\mathcal{S}| = \mathrm{card}(\mathcal{L})$.

Proof. (a) The map $\mathrm{Term} \to \mathrm{AtFml}$, $\boldsymbol{t} \mapsto \boldsymbol{t} \mathrel{=} \boldsymbol{t}$ witnesses that $\mathrm{Term} \precsim \mathrm{AtFml}$, while the map of (30.2) witnesses $\mathrm{Fml} \precsim \mathcal{S}^{<\omega}$.

(b) The map $\mathcal{S} \to \mathrm{AtFml}$, $s \mapsto \check{s}$ defined by

$$\check{s} = \begin{cases} \boldsymbol{v}_n = \boldsymbol{v}_n & \text{if } s = \boldsymbol{v}_n \in \mathrm{Vbl}, \\ \boldsymbol{R}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k) & \text{if } s = \boldsymbol{R} \text{ is a } k\text{-ary relation symbol}, \\ \boldsymbol{f}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k) = \boldsymbol{v}_0 & \text{if } s = \boldsymbol{f} \text{ is a } k\text{-ary function symbol}, \\ \boldsymbol{c} = \boldsymbol{c} & \text{if } s = \boldsymbol{c} \text{ is a constant symbol}, \end{cases}$$

is injective, so $\mathcal{S}^{<\omega} \precsim \mathrm{AtFml}^{<\omega}$. The map $\mathrm{AtFml}^{<\omega} \to \mathrm{QFFml}$, $\emptyset \mapsto \boldsymbol{v}_0 = \boldsymbol{v}_0$ and $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle \mapsto \boldsymbol{\varphi}_0 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{\varphi}_n$, is injective, and so are $\mathrm{QFFml} \to \mathrm{Sent}$, $\boldsymbol{\varphi} \mapsto \boldsymbol{\varphi}^\forall$ and $\mathrm{Sent} \to \mathrm{Fml}(\boldsymbol{x})$, $\boldsymbol{\sigma} \mapsto \boldsymbol{\sigma} \boldsymbol{\wedge} \boldsymbol{x} = \boldsymbol{x}$. Therefore the result follows from part (a) and the Cantor-Schröder-Bernstein Theorem 13.11.

If $\mathcal{L}$ is well-orderable then $\mathrm{card}(\mathcal{L}) = |\mathcal{S}|$ and by Theorem 18.31, $|\mathcal{S}| = |\mathcal{S}^{<\omega}|$ and $|\mathrm{AtFml}| = |\mathrm{AtFml}^{<\omega}|$. □

30.C.2. *Occurrences.* Recall the definition of $\boldsymbol{\varphi}^*$ in (30.2). An **occurrence** of $\boldsymbol{x} \in \mathrm{Vbl}$ in $\boldsymbol{\varphi} \in \mathrm{Fml}$ is an occurrence of $\boldsymbol{x}$ in $\boldsymbol{\varphi}^*$ in the sense of Section 23.B, and $\mathrm{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$, the set of **occurrences of $\boldsymbol{x}$ in $\boldsymbol{\varphi}$**, is a subset of $\mathrm{lh}\, \boldsymbol{\varphi}^*$. The set

$$\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) \subseteq \mathrm{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$$

of the **free occurrences** of $\boldsymbol{x}$ in $\boldsymbol{\varphi}$ is defined inductively as follow:

- if $\boldsymbol{\varphi} \in \mathrm{AtFml}$, then $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \mathrm{Occ}(\boldsymbol{x}; \boldsymbol{\varphi})$,
- if $\boldsymbol{\varphi} = \boldsymbol{\psi} \boldsymbol{\vee} \boldsymbol{\chi}$, then $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\psi})\} \cup \{1 + \mathrm{lh}\, \boldsymbol{\psi}^* + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\chi})\}$,
- if $\boldsymbol{\varphi} = \boldsymbol{\neg}\boldsymbol{\psi}$, then $\mathrm{FO}(\boldsymbol{x}; \boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x}; \boldsymbol{\psi})\}$,

- if $\boldsymbol{\varphi} = \exists \boldsymbol{y}\boldsymbol{\psi}$ and $\boldsymbol{y} \neq \boldsymbol{x}$, then $\mathrm{FO}(\boldsymbol{x};\boldsymbol{\varphi}) = \{1 + n \mid n \in \mathrm{FO}(\boldsymbol{x};\boldsymbol{\psi})\}$,
- if $\boldsymbol{\varphi} = \exists \boldsymbol{x}\boldsymbol{\psi}$, then $\mathrm{FO}(\boldsymbol{x};\boldsymbol{\varphi}) = \emptyset$.

30.C.3. *Substitution.* In Section 23.C we defined the substitution operation for expressions. Thus

$$\boldsymbol{t}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{s}_1, \dots, \boldsymbol{s}_n \in \mathrm{Term} \wedge \bigwedge_{1 \leq i < j \leq n} \boldsymbol{s}_i \neq \boldsymbol{s}_j \\ \Rightarrow \boldsymbol{t}[\boldsymbol{u}_1/\boldsymbol{s}_1, \dots, \boldsymbol{u}_n/\boldsymbol{s}_n] \in \mathrm{Term}\,.$$

Similarly, if $\boldsymbol{\varphi}$, $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$, $\boldsymbol{\chi}_1, \dots, \boldsymbol{\chi}_n \in \mathrm{Fml}$, and if $\boldsymbol{\chi}_i \neq \boldsymbol{\chi}_j$ for all $1 \leq i < j \leq n$, then $\boldsymbol{\varphi}[\boldsymbol{\psi}_1/\boldsymbol{\chi}_1, \dots, \boldsymbol{\psi}_n/\boldsymbol{\chi}_n]$ is the formula obtained from $\boldsymbol{\varphi}$ by replacing the formulæ $\boldsymbol{\chi}_1, \dots, \boldsymbol{\chi}_n$ with $\boldsymbol{\psi}_1, \dots, \boldsymbol{\psi}_n$.

If $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n \in \mathrm{Term}$ and $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ are distinct variables, then looking at all free occurrences of the $\boldsymbol{x}_i$s we write $\boldsymbol{\varphi}^* = u_1{}^\frown\boldsymbol{x}_{i_1}{}^\frown u_2{}^\frown\boldsymbol{x}_{i_2}{}^\frown \dots {}^\frown\boldsymbol{x}_{i_k}{}^\frown u_{k+1}$ where $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$, so let $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$ be the unique $\boldsymbol{\psi}$ such that $\boldsymbol{\psi}^* = u_1{}^\frown\boldsymbol{t}_{i_1}{}^\frown u_2{}^\frown\boldsymbol{t}_{i_2}{}^\frown \dots {}^\frown\boldsymbol{t}_{i_k}{}^\frown u_{k+1}$.

30.C.4. *Variants.* If $\boldsymbol{t} \in \mathrm{Term}$ and $\boldsymbol{\varphi} \in \mathrm{Fml}$ let $\mathcal{V}(\boldsymbol{t})$ be the least k such that every variable occurring in $\boldsymbol{t}$ has index $< k$ and $\mathcal{V}(\boldsymbol{\varphi})$ is the least k such that every variable occurring free in $\boldsymbol{\varphi}$ has index $< k$, that is

$$\mathcal{V}(\boldsymbol{t}) = \max\{n \mid \boldsymbol{v}_n \in \mathrm{V{\small BL}}(\boldsymbol{t})\} + 1 \quad \mathcal{V}(\boldsymbol{\varphi}) = \max\{n \mid \boldsymbol{v}_n \in \mathrm{F{\small V}}(\boldsymbol{\varphi})\} + 1.$$

When $n \geq \mathcal{V}(\boldsymbol{\varphi})$, the formula $\boldsymbol{\varphi}_{(n)}$ is obtained by replacing the bounded variables in $\boldsymbol{\varphi}$ with variables with index $\geq n$:

- if $\boldsymbol{\varphi}$ is atomic, then $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\varphi}$,
- if $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, then $\boldsymbol{\varphi}_{(n)} = \neg\boldsymbol{\psi}_{(n)}$,
- if $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, then $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)} \vee \boldsymbol{\chi}_{(n)}$,
- if $\boldsymbol{\varphi} = \exists \boldsymbol{v}_k\boldsymbol{\psi}$ with $k < n$, then $\boldsymbol{\varphi}_{(n)} = \exists \boldsymbol{v}_i\boldsymbol{\psi}_{(n)}[\boldsymbol{v}_i/\boldsymbol{v}_k]$ and $i = \mathcal{V}(\boldsymbol{\psi}_{(n)})$.

We say that $\boldsymbol{\varphi}$ is a **variant** of $\boldsymbol{\psi}$ if $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)}$ for some $n \geq \mathcal{V}(\boldsymbol{\varphi}), \mathcal{V}(\boldsymbol{\psi})$.

We are now ready to give the following:

Definition 30.6. If $\boldsymbol{\varphi}$ is a formula, $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$ are terms, and $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ are distinct variables, then $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$ is

- $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$, if $\boldsymbol{t}_1, \dots \boldsymbol{t}_n$ are substitutable for $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ in $\boldsymbol{\varphi}$,
- $\boldsymbol{\varphi}_{(m)}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$, otherwise, where $m \geq \max\{\mathcal{V}(\boldsymbol{\varphi}), \mathcal{V}(\boldsymbol{t}_1), \dots, \mathcal{V}(\boldsymbol{t}_n), \mathcal{V}(\boldsymbol{x}_1), \dots, \mathcal{V}(\boldsymbol{x}_n)\}$.

Exercises

Exercise 30.7. Give explicitly an inductive definition of $\mathrm{VBL}(\boldsymbol{t})$.

Exercise 30.8. Verify that

(i) $\boldsymbol{\varphi}_{(n)} \in \mathrm{Fml}$ and $\mathrm{Fv}(\boldsymbol{\varphi}_{(n)}) = \mathrm{Fv}(\boldsymbol{\varphi})$;

(ii) $\boldsymbol{\varphi}$ is a variant of $\boldsymbol{\psi}$ if $\boldsymbol{\varphi}_{(n)} = \boldsymbol{\psi}_{(n)}$ for all $n \geq \mathcal{V}(\boldsymbol{\varphi}), \mathcal{V}(\boldsymbol{\psi})$.

Exercise 30.9. For any τ-structure $\mathcal{A}$ let

$$\mathrm{FG}(\mathcal{A}) = \{\mathcal{B} \mid \mathcal{B} \subseteq \mathcal{A} \text{ and } \mathcal{B} \text{ is finitely generated}\}.$$

For $\mathcal{B} \subseteq \mathcal{C}$ finitely generated substructures of $\mathcal{A}$ let $\pi_{\mathcal{B},\mathcal{C}} \colon \mathcal{B} \hookrightarrow \mathcal{C}$ be the inclusion map. Show that $\langle \mathrm{FG}(\mathcal{A}), \subseteq \rangle$ is upward directed and that $\mathrm{FG}(\mathcal{A})$ with the maps $\pi_{\mathcal{B},\mathcal{C}}$ is an upward directed system of τ-structures and morphisms and that

$$\mathcal{A} \;\cong\; \varinjlim \langle \mathcal{B} \mid \mathcal{B} \in \mathrm{FG}(\mathcal{A}) \rangle\,.$$

Exercise 30.10. Suppose F is a filter on a non-empty set X. Check that:

(i) if $Y \in F$ and $\pi_y \colon \mathcal{A}_y \to \mathcal{B}_y$ is an isomorphism for each $y \in Y$, then $\prod_F \mathcal{A}_x \cong \prod_F \mathcal{B}_x$;

(ii) if $Y \in F$ and $F \restriction Y$ is the filter induced by F on Y (Exercise 25.15), then $\prod_F \mathcal{A}_x$ is isomorphic to the reduced product $\prod_{F \restriction Y} \mathcal{A}_y$ of $\langle \mathcal{A}_y \mid y \in Y \rangle$ modulo $F \restriction Y$. In particular, if $\{x_0\} \in F$ for some $x_0 \in X$, then $\prod_F \mathcal{A}_x \cong \mathcal{A}_{x_0}$.

31. Theories and models

31.A. The satisfaction relation. We now give a rigorous definition of the notion "the formula $\boldsymbol{\varphi}$ is true in the structure $\mathcal{A}$".

31.A.1. *Interpretation of terms in a structure.* An **assignment in a structure** $\mathcal{A}$ is a function $g \colon \mathrm{Vbl} \to \|\mathcal{A}\|$. Given an assignment g, for each $a \in \|\mathcal{A}\|$ let $g_{\boldsymbol{x}\mapsto a}$ be the assignment

$$g_{\boldsymbol{x}\mapsto a}(\boldsymbol{v}_n) = \begin{cases} a & \text{if } \boldsymbol{x} = \boldsymbol{v}_n, \\ g(\boldsymbol{v}_n) & \text{otherwise.} \end{cases}$$

Note that

$$\boldsymbol{x} \neq \boldsymbol{y} \Rightarrow (g_{\boldsymbol{x}\mapsto a})_{\boldsymbol{y}\mapsto b} = (g_{\boldsymbol{y}\mapsto b})_{\boldsymbol{x}\mapsto a} \tag{31.1}$$

for every $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ and $a, b \in \|\mathcal{A}\|$. The **interpretation of $\boldsymbol{t}$ in $\mathcal{A}$ via g** is

$$\boldsymbol{t}^{\mathcal{A}}[g] = \begin{cases} \boldsymbol{c}^{\mathcal{A}} & \text{if } \boldsymbol{t} = \boldsymbol{c} \in \mathrm{Const}, \\ g(\boldsymbol{x}) & \text{if } \boldsymbol{t} = \boldsymbol{x} \in \mathrm{Vbl}, \\ \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[g], \dots, \boldsymbol{u}_n^{\mathcal{A}}[g]) & \text{if } \boldsymbol{t} = \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n). \end{cases}$$

Lemma 31.1. *If $g, h\colon \mathrm{Vbl} \to \|\mathcal{A}\|$ and $g \restriction \textsc{Vbl}(\boldsymbol{t}) = h \restriction \textsc{Vbl}(\boldsymbol{t})$, then $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$.*

Proof. By induction on $\mathrm{ht}(\boldsymbol{t})$. If $\boldsymbol{t} \in \mathrm{Const} \cup \mathrm{Vbl}$, the result follows at once. Suppose that $\boldsymbol{t} = \boldsymbol{f}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$. Then $\textsc{Vbl}(\boldsymbol{t}) = \textsc{Vbl}(\boldsymbol{u}_1) \cup \dots \cup \textsc{Vbl}(\boldsymbol{u}_n)$ hence, by inductive assumption, $\boldsymbol{u}_m^{\mathcal{A}}[g] = \boldsymbol{u}_m^{\mathcal{A}}[h]$, for $m = 1, \dots, n$, hence $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[g], \dots, \boldsymbol{u}_n^{\mathcal{A}}[g]) = \boldsymbol{f}^{\mathcal{A}}(\boldsymbol{u}_1^{\mathcal{A}}[h], \dots, \boldsymbol{u}_n^{\mathcal{A}}[h]) = \boldsymbol{t}^{\mathcal{A}}[h]$. □

If $\boldsymbol{t}$ is closed, then let $\boldsymbol{t}^{\mathcal{A}} = \boldsymbol{t}^{\mathcal{A}}[g]$ for some/any g. If $\textsc{Vbl}(\boldsymbol{t}) \subseteq \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$ and $a_1, \dots, a_n$ are not necessarily distinct elements of $\|\mathcal{A}\|$ and g and h are assignments in $\mathcal{A}$ such that $g(\boldsymbol{x}_m) = h(\boldsymbol{x}_m) = a_m$, for $1 \le m \le n$, then Lemma 31.1 yields that $\boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[h]$, and this element will be denoted by

$$\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n].$$

Equivalently, consider the expansion $\langle \mathcal{A}, a_1, \dots, a_n \rangle$ of $\mathcal{A}$ obtained by augmenting $\mathcal{L}$ with new constant symbols $\mathring{a}_1, \dots, \mathring{a}_n$ to be interpreted as $a_1, \dots, a_n$ — note that the $\mathring{a}_m$s, unlike the a_ms, *must be distinct.* The interpretation in $\mathcal{A}'$ of the closed term $\boldsymbol{t}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n]$ coincides with $\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]$, that is

$$(\boldsymbol{t}[\mathring{a}_1/\boldsymbol{x}_1, \dots, \mathring{a}_n/\boldsymbol{x}_n])^{\mathcal{A}'} = \boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n].$$

Lemma 31.2. *If $\boldsymbol{t}$ is a term whose variables are among $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$, and if $\pi\colon \mathcal{A} \to \mathcal{B}$ is a morphism, then*

$$\forall a_1, \dots, a_n \in \|\mathcal{A}\| \bigl(\pi\bigl(\boldsymbol{t}^{\mathcal{A}}[a_1, \dots, a_n]\bigr) = \boldsymbol{t}^{\mathcal{B}}[\pi(a_1), \dots, \pi(a_n)]\bigr).$$

Proof. By induction on $\mathrm{ht}(\boldsymbol{t})$. If $\mathrm{ht}(\boldsymbol{t}) = 0$, then either $\boldsymbol{t} = \boldsymbol{x}_m$ or $\boldsymbol{t} = \boldsymbol{c}_k$, so $\boldsymbol{t}^{\mathcal{A}}[\vec{a}] = a_m$ and $\boldsymbol{t}^{\mathcal{B}}[\pi(\vec{a})] = \pi(a_m)$ or else $\boldsymbol{t}^{\mathcal{A}}[\vec{a}] = \boldsymbol{c}_k^{\mathcal{A}}$ and $\boldsymbol{t}^{\mathcal{B}}[\pi(\vec{a})] = \boldsymbol{c}_k^{\mathcal{B}}$. If $\mathrm{ht}(\boldsymbol{t}) > 0$, then $\boldsymbol{t} = \boldsymbol{f}_j(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m)$ for some $j \in J$ and $\boldsymbol{t}_1, \dots, \boldsymbol{t}_m \in \mathrm{Term}$. Then by definition of morphism and by inductive assumption,

$$\begin{aligned} \pi(\boldsymbol{t}^{\mathcal{A}}[\vec{a}]) &= \pi\bigl(\boldsymbol{f}_j^{\mathcal{A}}\bigl(\boldsymbol{t}_1^{\mathcal{A}}[\vec{a}], \dots, \boldsymbol{t}_m^{\mathcal{A}}[\vec{a}]\bigr)\bigr) \\ &= \boldsymbol{f}_j^{\mathcal{B}}\bigl(\pi\bigl(\boldsymbol{t}_1^{\mathcal{A}}[\vec{a}]\bigr), \dots, \pi\bigl(\boldsymbol{t}_m^{\mathcal{A}}[\vec{a}]\bigr)\bigr) \\ &= \boldsymbol{f}_j^{\mathcal{B}}\bigl(\boldsymbol{t}_1^{\mathcal{B}}[\pi(\vec{a})], \dots, \boldsymbol{t}_m^{\mathcal{B}}[\pi(\vec{a})]\bigr) \\ &= \boldsymbol{t}^{\mathcal{B}}\bigl[\pi(\vec{a})\bigr]. \end{aligned}$$

□

31.B. Satisfaction of a formula in a structure.

31.B.1. *The definition of the satisfaction relation.* We define when a formula $\boldsymbol{\varphi}$ is **true in $\mathcal{A}$ according to an assignment** g, in symbols

$$\mathcal{A} \vDash_g \boldsymbol{\varphi}.$$

The writing above also read as: $\mathcal{A}$ **satisfies $\boldsymbol{\varphi}$ with the assignment** g, or $\mathcal{A}$ is a **model of $\boldsymbol{\varphi}$ for the assignment** g. Whenever this does not happen, we write $\mathcal{A} \nvDash_g \boldsymbol{\varphi}$ and say that $\boldsymbol{\varphi}$ is **false in $\mathcal{A}$ for the assignment** g. The definition of $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ is by recursion on the complexity of $\boldsymbol{\varphi}$:

$$\begin{aligned}
\mathcal{A} \vDash_g \boldsymbol{t}_1 \mathrel{\boldsymbol{=}} \boldsymbol{t}_2 &\Leftrightarrow \boldsymbol{t}_1^{\mathcal{A}}[g] = \boldsymbol{t}_2^{\mathcal{A}}[g] \\
\mathcal{A} \vDash_g \boldsymbol{R}_i(\boldsymbol{t}_1, \dots, \boldsymbol{t}_m) &\Leftrightarrow \langle \boldsymbol{t}_1^{\mathcal{A}}[g], \dots, \boldsymbol{t}_m^{\mathcal{A}}[g]\rangle \in \boldsymbol{R}_i^{\mathcal{A}} \\
\mathcal{A} \vDash_g \boldsymbol{\neg\varphi} &\Leftrightarrow \mathcal{A} \nvDash_g \boldsymbol{\varphi} \\
\mathcal{A} \vDash_g \boldsymbol{\varphi} \boldsymbol{\vee} \boldsymbol{\psi} &\Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\varphi} \vee \mathcal{A} \vDash_g \boldsymbol{\psi} \\
\mathcal{A} \vDash_g \boldsymbol{\exists x \varphi} &\Leftrightarrow \exists a \in \|\mathcal{A}\| \, (\mathcal{A} \vDash_{g_{\boldsymbol{x} \mapsto a}} \boldsymbol{\varphi}) \, .
\end{aligned}$$

Remark 31.3. From the definition it follows that either $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ or else $\mathcal{A} \vDash_g \boldsymbol{\neg\varphi}$, for any $\mathcal{A}$, g, and $\boldsymbol{\varphi}$. This does not mean that we are actually able to determine which one of the two alternatives hold.

Let us recall a few notions from Section 3. A formula $\boldsymbol{\varphi}$ is

- **satisfiable in a structure** $\mathcal{A}$ if $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ for some assignment g;
- **satisfiable** if it is satisfiable in *some* structure; a formula that it is not satisfiable is called **unsatisfiable** or **false**;
- **true in a structure** $\mathcal{A}$ if $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ for *every* assignment g. In this case we write that $\mathcal{A} \vDash \boldsymbol{\varphi}$;
- **valid** or **true** if it is true in every structure.

Two formulæ $\boldsymbol{\varphi}, \boldsymbol{\psi}$ are **logically equivalent** if $\boldsymbol{\varphi} \boldsymbol{\Leftrightarrow} \boldsymbol{\psi}$ is valid; as noted in Remark 3.36(a) this is stronger than saying that $\boldsymbol{\varphi}^{\forall}, \boldsymbol{\psi}^{\forall}$ are logically equivalent.

Lemma 31.4. *If $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ is an $\mathcal{L}$-formula and $g, h \colon \mathrm{Vbl} \to \|\mathcal{A}\|$ are assignments such that $g \restriction \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\} = h \restriction \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_n\}$,*

$$\mathcal{A} \vDash_g \boldsymbol{\varphi} \Leftrightarrow \mathcal{A} \vDash_h \boldsymbol{\varphi}.$$

Proof. By induction on $\mathrm{ht}(\boldsymbol{\varphi})$. The case when $\boldsymbol{\varphi}$ is atomic follows from Lemma 31.1. If either $\boldsymbol{\varphi} = \boldsymbol{\neg\psi}$ or else $\boldsymbol{\varphi} = \boldsymbol{\psi} \boldsymbol{\vee} \boldsymbol{\chi}$, the result is trivial. Suppose then $\boldsymbol{\varphi}$ is of the form $\exists \boldsymbol{y}\, \boldsymbol{\psi}$. If $\mathcal{A} \vDash_g \exists \boldsymbol{y}\, \boldsymbol{\psi}$, then there is $a \in \|\mathcal{A}\|$ such that $\mathcal{A} \vDash_{g_{\boldsymbol{y} \mapsto a}} \boldsymbol{\psi}$. By inductive assumption $\mathcal{A} \vDash_{g_{\boldsymbol{y} \mapsto a}} \boldsymbol{\psi} \Leftrightarrow \mathcal{A} \vDash_{h_{\boldsymbol{y} \mapsto a}} \boldsymbol{\psi}$ hence $\mathcal{A} \vDash_h \exists \boldsymbol{y}\, \boldsymbol{\psi}$. □

For every $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ and $a_1, \ldots, a_n \in \|\mathcal{A}\|$ (not necessarily distinct), set

$$\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n] \quad \text{if and only if} \quad \mathcal{A} \vDash_g \boldsymbol{\varphi}$$

for some (equivalently: for all) g such that $g(\boldsymbol{x}_m) = a_m$, $(1 \leq m \leq n)$. If $\boldsymbol{\varphi}$ has just one free variable $\boldsymbol{x}$ we write $\mathcal{A} \vDash \boldsymbol{\varphi}[a]$ for $\mathcal{A} \vDash_g \boldsymbol{\varphi}$, for some (equivalently: for every) assignment g such that $g(\boldsymbol{x}) = a$. We write $\mathcal{A} \vDash \boldsymbol{\varphi}$ if $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ for all assignments. If $\boldsymbol{\sigma}$ is a statement, then the assignment becomes irrelevant, i.e. $\mathcal{A} \vDash_g \boldsymbol{\sigma}$ for *some* assignment if and only if $\mathcal{A} \vDash_g \boldsymbol{\sigma}$ for *all* assignment, so also in this case we write $\mathcal{A} \vDash \boldsymbol{\sigma}$. Note that $\mathcal{A} \vDash \boldsymbol{\varphi}$ is equivalent to $\mathcal{A} \vDash \boldsymbol{\varphi}^{\forall}$.

Remark 31.5. In view of Lemma 31.4 we could have defined the satisfaction relation using finite assignments, i.e. maps defined on finitely many variables. More precisely we could have defined $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ with $g\colon \mathrm{Fv}(\boldsymbol{\varphi}) \to \|\mathcal{A}\|$. This approach is completely equivalent to the one presented here: it has indeed a few advantages (see Section **??**) but it is technically awkward.

Recall from Section 3.G that the **truth set** of a formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ in $\mathcal{A}$ is

$$\mathbf{T}^{\mathcal{A}}_{\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)} = \{\langle a_1, \ldots, a_n\rangle \in A^n \mid \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]\}.$$

A set $X \subseteq \|\mathcal{A}\|^n$ is **definable with parameters in** $P \subseteq \|\mathcal{A}\|$ if there is a formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_k)$ and there are $p_1, \ldots, p_k \in P$ such that

$$\begin{aligned} X &= \{\langle a_1, \ldots, a_n\rangle \in A^n \mid \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n, p_1, \ldots, p_k]\} \\ &= \mathbf{T}^{\mathcal{A}}_{\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_k)} \cap \|\mathcal{A}\|^n \times \{\langle p_1, \ldots, p_k\rangle\}. \end{aligned}$$

The integer n is the dimension of X. When $P = A$ we say that X is definable with parameters in $\mathcal{A}$. If $P = \emptyset$ then X is definable without parameters. The set of all definable subsets of dimension n of $\mathcal{A}$ with parameters P is $\mathrm{Def}^n_{\mathcal{A}}(P)$.

If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ then $\mathcal{A} \vDash \Sigma$ means that $\mathcal{A} \vDash \boldsymbol{\sigma}$ for all $\boldsymbol{\sigma} \in \Sigma$. Let

$$\mathrm{Mod}(\Sigma) = \{\mathcal{A} \in \mathrm{Str} \mid \mathcal{A} \vDash \Sigma\}.$$

The **theory of a class of structures** $\mathscr{C} \subseteq \mathrm{Str}(\mathcal{L})$ is

$$\mathrm{Th}(\mathscr{C}) = \{\boldsymbol{\sigma} \in \mathrm{Sent} \mid \forall \mathcal{A} \in \mathscr{C}\,(\mathcal{A} \vDash \boldsymbol{\sigma})\}.$$

When $\mathscr{C} = \{\mathcal{A}\}$ and $T = \{\boldsymbol{\sigma}\}$ we write $\mathrm{Th}(\mathcal{A})$ and $\mathrm{Mod}(\boldsymbol{\sigma})$.

Let $\mathscr{U}_\Sigma = \bigcup_{\boldsymbol{\sigma} \in \Sigma} \mathrm{Mod}(\boldsymbol{\sigma})$. As $\mathrm{Mod}(\neg\boldsymbol{\sigma}) = \mathrm{Str} \setminus \mathrm{Mod}(\boldsymbol{\sigma})$ and $\mathrm{Mod}(\boldsymbol{\sigma}) \cap \mathrm{Mod}(\boldsymbol{\tau}) = \mathrm{Mod}(\boldsymbol{\sigma} \wedge \boldsymbol{\tau})$, then $\mathscr{U}_\Sigma \cap \mathscr{U}_\Delta = \bigcup_{\boldsymbol{\sigma} \in \Sigma, \boldsymbol{\delta} \in \Delta} \mathrm{Mod}(\boldsymbol{\sigma} \wedge \boldsymbol{\delta})$ so that

$$\{\mathscr{U}_\Sigma \mid \Sigma \subseteq \mathrm{Sent}\} \text{ is a zero-dimensional topology on Str.} \tag{31.2}$$

Note that $\mathrm{Mod}(\Sigma) = \mathrm{Str} \setminus \mathscr{U}_{\neg\Sigma}$ is a closed set, where $\neg\Sigma = \{\boldsymbol{\neg\sigma} \mid \boldsymbol{\sigma} \in \Sigma\}$, and that this topology is not T_0, since two structures $\mathcal{A}, \mathcal{B}$ belong to the same open sets if and only if $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$.

The maps $\Sigma \mapsto \mathrm{Mod}(\Sigma)$ and $\mathscr{C} \mapsto \mathrm{Th}(\mathscr{C})$ are antitone with respect to inclusion, and moreover $\Sigma \subseteq \mathrm{Th}(\mathrm{Mod}(\Sigma))$ and $\mathscr{C} \subseteq \mathrm{Mod}(\mathrm{Th}(\mathscr{C}))$. Thus $(\mathrm{Mod}, \mathrm{Th})$ is a Galois connection between $\mathscr{P}(\mathrm{Sent})$, the set of all theories, and the collection of all subclasses of Str, and hence

$$\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathscr{C}))) = \mathrm{Th}(\mathscr{C}) \quad \text{and} \quad \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Sigma))) = \mathrm{Mod}(\Sigma). \tag{31.3}$$

Remark 31.6. The proofs of (31.2) and (31.3) need some attention, since the notions of topology and of Galois connection are formulated for *sets*, and do not cover the case of collections of sub*classes* of Str. Yet standard arguments in topology as well as the ones in Section 7.B can be easily adapted to yield these results. For example one can argue that for the first identity in (31.3) as follows. From $\mathscr{C} \subseteq \mathrm{Mod}(\mathrm{Th}(\mathscr{C}))$ we get that $\mathrm{Th}(\mathscr{C}) \supseteq \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathscr{C})))$. If $\boldsymbol{\sigma} \notin \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathscr{C})))$ then there is $\mathcal{A} \in \mathrm{Mod}(\mathrm{Th}(\mathscr{C}))$ such that $\mathcal{A} \nvDash \boldsymbol{\sigma}$. Since $\mathcal{A} \vDash \mathrm{Th}(\mathscr{C})$ then $\boldsymbol{\sigma} \notin \mathrm{Th}(\mathscr{C})$. Therefore $\mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathscr{C}))) = \mathrm{Th}(\mathscr{C})$.

If $\Sigma, \Delta \subseteq \mathrm{Sent}(\mathcal{L})$, then Δ is **logical consequence of** Σ, in symbols $\Sigma \models_{\mathcal{L}} \Delta$, if $\mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\Delta)$. As usual we will write $\Sigma \models \Delta$ when $\mathcal{L}$ is clear. If $\Sigma = \emptyset$ we write $\models \Delta$ and if Σ and/or Δ are singletons we will drop the braces and write e.g. $\Sigma \models \boldsymbol{\tau}$. If $\mathrm{Mod}(\Sigma) = \mathrm{Mod}(\Delta)$ then Σ and Δ are **logically equivalent**.

A theory Σ is **satisfiable** if $\mathrm{Mod}(\Sigma) \neq \emptyset$. An **axiom system** for a theory Σ is a set Δ of sentences (i.e. a theory) such that Σ and Δ are logically equivalent. A theory Σ is finitely axiomatizable if it admits a finite set of axioms, or equivalently if it is logically equivalent to a single $\boldsymbol{\sigma} \in \mathrm{Sent}$. Recall (Section 4.K) that $\mathscr{C} \subseteq \mathrm{Str}(\mathcal{L})$ is **axiomatizable** if $\mathscr{C} = \mathrm{Mod}(\Sigma)$ for some theory Σ; if Σ is finitely axiomatizable, then $\mathscr{C}$ is **finitely axiomatizable**. These notions are also known in model theory as **generalized elementary class** $\mathrm{EC}_\Delta(\mathcal{L})$, and **elementary class** $\mathrm{EC}(\mathcal{L})$, respectively. When $\mathscr{C} \subseteq \mathrm{Str}(\mathcal{L})$ is the class of all reductions of some (generalized) elementary class in some larger language $\mathcal{L}'$, then $\mathscr{C}$ is said to be a **(generalized) pseudo-elementary class** $\mathrm{PC}_\Delta(\mathcal{L})$ and $\mathrm{PC}(\mathcal{L})$, respectively. The Compactness Theorem 4.46 which was stated in Section 4.K and that will be proved in Section 31.G, can be used to construct many examples of generalized elementary classes that are not elementary, i.e. classes that are in $\mathrm{EC}_\Delta(\mathcal{L}) \setminus \mathrm{EC}(\mathcal{L})$—see Section 4.K. The other inclusions in the Venn diagram of Figure 25 are also proper (Exercises 31.61–31.63).

change to basic elementary class

31.C. Easy facts about satisfaction.

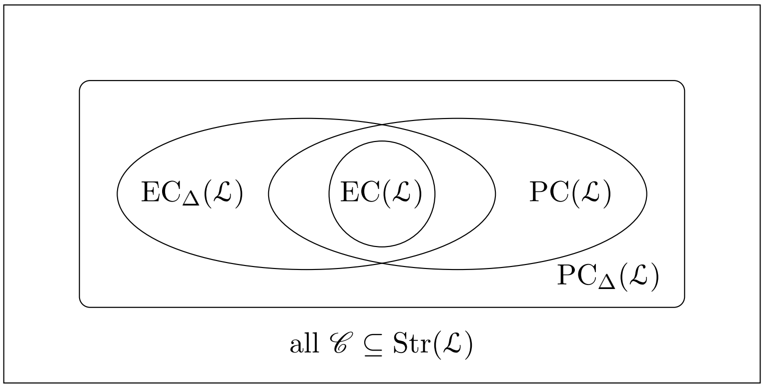

$\mathrm{EC}_\Delta(\mathcal{L})$
$\mathrm{EC}(\mathcal{L})$
$\mathrm{PC}(\mathcal{L})$
$\mathrm{PC}_\Delta(\mathcal{L})$
all $\mathscr{C} \subseteq \mathrm{Str}(\mathcal{L})$

Figure 25. Elementary and pseudo-elementary (generalized) classes

Proposition 31.7. *Let $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ be a formula, $\mathcal{A}$ a structure and let $a_1, \ldots, a_n \in \|\mathcal{A}\|$.*

(a) *If $\boldsymbol{y} \notin \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$, then*

$$\mathcal{A} \vDash \boldsymbol{\exists y \varphi}[a_1, \ldots, a_n] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\forall y \varphi}[a_1, \ldots, a_n] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n].$$

(b) *If $\boldsymbol{y} = \boldsymbol{x}_m$ for some $1 \leq m \leq n$, then*

$$\begin{aligned} &\mathcal{A} \vDash \boldsymbol{\exists x}_m \boldsymbol{\varphi}[a_1, \ldots, a_n] \\ &\qquad\qquad \Leftrightarrow \exists a \in \|\mathcal{A}\| \left(\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n]\right), \\ &\mathcal{A} \vDash \big(\boldsymbol{\forall x}_m \boldsymbol{\varphi}\big)[a_1, \ldots, a_n] \\ &\qquad\qquad \Leftrightarrow \forall a \in \|\mathcal{A}\| \left(\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_{m-1}, a, a_{m+1}, \ldots, a_n]\right). \end{aligned}$$

Proof. (a) Suppose that $\mathcal{A} \vDash \boldsymbol{\exists y \varphi}[a_1, \ldots, a_n]$, that is to say $\mathcal{A} \vDash_g \boldsymbol{\exists y \varphi}$ for some (equivalently: for every) assignment g such that $g(\boldsymbol{x}_m) = a_m$ $(1 \leq m \leq n)$. Then $\mathcal{A} \vDash_{g_{\boldsymbol{y} \mapsto a}} \boldsymbol{\varphi}$ for some $a \in \|\mathcal{A}\|$. By assumption on $\boldsymbol{y}$, $g_{\boldsymbol{y} \mapsto a}(\boldsymbol{x}_i) = a_i$ hence $\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]$. Similarly, $\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n]$ implies that $\mathcal{A} \vDash \boldsymbol{\exists y \varphi}[a_1, \ldots, a_n]$, and hence

$$\mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n] \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\exists y \varphi}[a_1, \ldots, a_n]. \tag{31.4}$$

As the free variables of $\boldsymbol{\neg\varphi}$ are exactly those of $\boldsymbol{\varphi}$, we have that

$$\begin{aligned} \mathcal{A} \vDash \boldsymbol{\forall y \varphi}[a_1, \ldots, a_n] &\Leftrightarrow \mathcal{A} \nvDash \boldsymbol{\exists y \neg \varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \nvDash \boldsymbol{\neg\varphi}[a_1, \ldots, a_n] \\ &\Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}[a_1, \ldots, a_n], \end{aligned}$$

where in the second row we used the equivalence (31.4) for $\boldsymbol{\neg\varphi}$.

Part (b) is left to the reader. □

Proposition 31.8. *If* $\mathrm{Subst}(\boldsymbol{\varphi};\boldsymbol{t};\boldsymbol{x})$ *and* $a = \boldsymbol{t}^{\mathcal{A}}[g] \in \|\mathcal{A}\|$ *where* g *is an assignment in an* $\mathcal{L}$*-structure* $\mathcal{A}$*, then* $\mathcal{A} \vDash_g \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!) \Leftrightarrow \mathcal{A} \vDash_{g_{\boldsymbol{x}\mapsto a}} \boldsymbol{\varphi}$.

Proof. If $\boldsymbol{\varphi}$ is atomic, or $\boldsymbol{\varphi}$ is $\neg\boldsymbol{\psi}$, or $\boldsymbol{\varphi}$ is $\boldsymbol{\psi} \vee \boldsymbol{\chi}$, the result is trivial. Suppose that $\boldsymbol{\varphi}$ is $\exists \boldsymbol{y}\boldsymbol{\psi}$ and distinguish two cases.

Case 1: $\boldsymbol{y} = \boldsymbol{x}$. Then $\boldsymbol{x}$ does not occur free in $\boldsymbol{\varphi}$, hence $\boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$ is $\boldsymbol{\varphi}$ and g and $g_{\boldsymbol{x}\mapsto a}$ agree on the free variables of $\boldsymbol{\varphi}$. It follows that

$$\begin{aligned} \mathcal{A} \vDash_g \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!) &\Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\varphi} \\ &\Leftrightarrow \mathcal{A} \vDash_{g_{\boldsymbol{x}\mapsto a}} \boldsymbol{\varphi} && \text{(by Lemma 31.4).} \end{aligned}$$

Case 2: $\boldsymbol{y} \neq \boldsymbol{x}$. Then $\boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$ is $\exists \boldsymbol{y}\boldsymbol{\psi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$ and since $\boldsymbol{y}$ does not occur in $\boldsymbol{t}$, for each $b \in A$ one has that

$$a = \boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{t}^{\mathcal{A}}[g_{\boldsymbol{y}\mapsto b}]. \tag{31.5}$$

Therefore

$$\begin{aligned} \mathcal{A} \vDash_g \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!) &\Leftrightarrow \exists b \in A\, \mathcal{A} \vDash_{g_{\boldsymbol{y}\mapsto b}} \boldsymbol{\psi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!) \\ &\Leftrightarrow \exists b \in A\, \mathcal{A} \vDash_{(g_{\boldsymbol{y}\mapsto b})_{\boldsymbol{x}\mapsto a}} \boldsymbol{\psi} && \text{by ind. hyp. and (31.5)} \\ &\Leftrightarrow \exists b \in A\, \mathcal{A} \vDash_{(g_{\boldsymbol{x}\mapsto a})_{\boldsymbol{y}\mapsto b}} \boldsymbol{\psi} && \text{by (31.1)} \\ &\Leftrightarrow \mathcal{A} \vDash_{g_{\boldsymbol{x}\mapsto a}} \exists \boldsymbol{y}\boldsymbol{\psi} \\ &\Leftrightarrow \mathcal{A} \vDash_{g_{\boldsymbol{x}\mapsto a}} \boldsymbol{\varphi}. \end{aligned}$$

□

31.D. Logical axioms.

31.D.1. *Tautologies.* Recall from Section 3.C.1 that a **primitive formula** is either an atomic formula or an existential formula. We associate to every $\boldsymbol{\varphi}$ a set $\mathcal{P}(\boldsymbol{\varphi})$ of primitive formulæ as follows:

- if $\boldsymbol{\varphi}$ is primitive, then $\mathcal{P}(\boldsymbol{\varphi}) = \{\boldsymbol{\varphi}\}$,
- if $\boldsymbol{\varphi} = \neg\boldsymbol{\psi}$, then $\mathcal{P}(\boldsymbol{\varphi}) = \mathcal{P}(\boldsymbol{\psi})$,
- if $\boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}$, then $\mathcal{P}(\boldsymbol{\varphi}) = \mathcal{P}(\boldsymbol{\psi}) \cup \mathcal{P}(\boldsymbol{\chi})$.

Associate to each $\boldsymbol{\varphi} \in \mathrm{Fml}(\mathcal{L})$ a proposition $\boldsymbol{p}_{\boldsymbol{\varphi}}$ on the letters $\{\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_n\} = \mathcal{P}(\boldsymbol{\varphi})$:

$$\boldsymbol{p}_{\boldsymbol{\varphi}} = \begin{cases} \boldsymbol{\varphi} & \text{if } \boldsymbol{\varphi} \text{ is primitive,} \\ \neg \boldsymbol{p}_{\boldsymbol{\psi}} & \text{if } \boldsymbol{\varphi} = \neg\boldsymbol{\psi}, \\ \boldsymbol{p}_{\boldsymbol{\psi}} \vee \boldsymbol{p}_{\boldsymbol{\chi}} & \text{if } \boldsymbol{\varphi} = \boldsymbol{\psi} \vee \boldsymbol{\chi}. \end{cases}$$

Lemma 31.9. *Let* $\boldsymbol{\varphi}$ *and* $\mathcal{P}(\boldsymbol{\varphi}) = \{\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_n\}$*, and let* $\boldsymbol{p}_{\boldsymbol{\varphi}}$ *be as above. Let* $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$*, let* $g\colon \mathrm{Vbl} \to \|\mathcal{A}\|$*, and let* $v\colon \mathcal{P}(\boldsymbol{\varphi}) \to \{0,1\}$ *be the evaluation defined by*

$$v(\boldsymbol{\psi}_i) = 1 \Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\psi}_i.$$

Then $v(\boldsymbol{p}_{\boldsymbol{\varphi}}) = 1 \Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\varphi}$.

Proof. If $\mathrm{ht}(\boldsymbol{p}_{\varphi}) = 0$ then φ is primitive and the result follows at once. If $\mathrm{ht}(\boldsymbol{p}_{\varphi}) > 0$ then either $\varphi = \neg\psi$ or else $\varphi = \psi \vee \chi$, that is either $\boldsymbol{p}_{\varphi} = \neg \boldsymbol{p}_{\psi}$ or else $\boldsymbol{p}_{\varphi} = \boldsymbol{p}_{\psi} \vee \boldsymbol{p}_{\chi}$ and the result follows from the definition of $\vDash$. □

A formula $\varphi \in \mathrm{Fml}(\mathcal{L})$ is a **tautology** if and only if the propositional formula $\boldsymbol{p}_{\varphi}$ is a propositional tautology (Definition **??**).

Corollary 31.10. *If $\varphi \in \mathrm{Fml}(\mathcal{L})$ is a tautology then φ is valid.*

A **tautology axiom** is a sentence obtained by universally quantifying a tautology.

31.D.2. *Equality axioms.* A **logical identity** is a formula of the form

- $\boldsymbol{t} = \boldsymbol{t}$,
- $\boldsymbol{s} = \boldsymbol{t} \Rightarrow \boldsymbol{t} = \boldsymbol{s}$,
- $\boldsymbol{s} = \boldsymbol{t} \wedge \boldsymbol{t} = \boldsymbol{u} \Rightarrow \boldsymbol{s} = \boldsymbol{u}$,
- $\boldsymbol{s}_1 = \boldsymbol{t}_1 \wedge \ldots \wedge \boldsymbol{s}_n = \boldsymbol{t}_n \Rightarrow \boldsymbol{f}_j(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) = \boldsymbol{f}_j(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$,
- $\boldsymbol{s}_1 = \boldsymbol{t}_1 \wedge \ldots \wedge \boldsymbol{s}_n = \boldsymbol{t}_n \wedge \boldsymbol{R}_i(\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) \Rightarrow \boldsymbol{R}_i(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n)$.

It is immediate to check that the logical identities are valid. An **equality axiom** is a sentence obtained by universally quantifying a logical identity.

31.D.3. *Axioms for quantification.* An **axiom for quantification** is the universal closure of a formula of the form

(A) $\varphi \Rightarrow \forall \boldsymbol{x} \varphi$, with $\boldsymbol{x} \notin \mathrm{Fv}(\varphi)$,

(B) $\varphi(\!| \boldsymbol{t}_1/\boldsymbol{x}_1, \ldots, \boldsymbol{t}_n/\boldsymbol{x}_n |\!) \Rightarrow \exists \boldsymbol{x}_1 \ldots \exists \boldsymbol{x}_n \varphi$,

(C) $\forall \boldsymbol{x} \neg \varphi \Rightarrow \neg \exists \boldsymbol{x} \varphi$,

(D) $\forall \boldsymbol{x}(\varphi \Rightarrow \psi) \Rightarrow (\forall \boldsymbol{x} \varphi \Rightarrow \forall \boldsymbol{x} \psi)$.

Remarks 31.11. (a) The requirement in (A) that $\boldsymbol{x} \notin \mathrm{Fv}(\varphi)$ cannot be dropped.

(b) The axioms of type (B) cover the case when not every $\boldsymbol{x}_i$ occurs free in φ; in particular, if φ is a sentence, then $\varphi \Rightarrow \exists \boldsymbol{x}_1 \ldots \exists \boldsymbol{x}_n \varphi$ is an axiom.

(c) As $\forall \boldsymbol{x} \ldots$ is shorthand for $\neg \exists \boldsymbol{x} \neg \ldots$, the axioms of type (C) say that $\neg \exists \boldsymbol{x} \neg \neg \varphi \Rightarrow \neg \exists \boldsymbol{x} \varphi$.

Let us check that the axioms for quantification are valid.

The validity of axioms of type (A) follows from part (a) of Proposition 31.7, and the case of the axioms of type (B) and of type (C) is immediate. Suppose $\mathcal{A} \vDash \forall \boldsymbol{x}(\varphi \Rightarrow \psi)$, but $\mathcal{A} \vDash \forall \boldsymbol{x} \varphi$ and $\mathcal{A} \nvDash \forall \boldsymbol{x} \psi$. Let $g \colon \mathrm{Vbl} \to \|\mathcal{A}\|$ be an assignment: then $\mathcal{A} \vDash_g \varphi \Rightarrow \psi$ and $\mathcal{A} \vDash_g \varphi$, and hence $\mathcal{A} \vDash_g \psi$. As g is arbitrary we have that $\mathcal{A} \vDash \forall \boldsymbol{x} \psi$: a contradiction. Therefore axioms of type (D) are valid.

31.E. Elementary equivalence. By Definitions 3.31 and 4.25 in Chapter I we say that two $\mathcal{L}$-structures $\mathcal{A}$ and $\mathcal{B}$ are **elementarily equivalent** $\mathcal{A} \equiv \mathcal{B}$ if and only if $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$, and that a morphism $\pi \colon \mathcal{A} \to \mathcal{B}$ is an **elementary embedding** if $\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \Leftrightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(\vec{a})]$, for each formula $\boldsymbol{\varphi}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ and each $\vec{a} \in A^n$. If there is an elementary embedding of $\mathcal{A}$ into $\mathcal{B}$ we say that $\mathcal{A}$ **elementarily embeds into** $\mathcal{B}$, and if $\mathcal{A} \subseteq \mathcal{B}$ and the inclusion map is an elementary embedding we say that $\mathcal{A}$ is an **elementary substructure** of $\mathcal{B}$, in symbols

$$\mathcal{A} \preccurlyeq \mathcal{B} \quad \text{and} \quad \mathcal{A} \preccurlyeq \mathcal{B}.$$

Let $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$, let $\mathcal{L}_A = \mathcal{L} \cup \{\mathring{a} \mid a \in A\}$ be the expanded language with a new constant symbols for each element of A, and let $\langle \mathcal{A}, a \rangle_{a \in A}$ be the canonical expansion of $\mathcal{A}$ to A. The **elementary diagram** of $\mathcal{A}$ is the set of all sentences that hold in $\langle \mathcal{A}, a \rangle_{a \in A}$,

$$\mathrm{EDiag}(\mathcal{A}) = \mathrm{Th}(\langle \mathcal{A}, a \rangle_{a \in A}).$$

The **diagram of** $\mathcal{A}$ is the set of all atomic and negated-atomic formulæ that are true in $\langle \mathcal{A}, a \rangle_{a \in A}$

$$\mathrm{Diag}(\mathcal{A}) = \mathrm{EDiag}(\mathcal{A}) \cap \bigl(\mathrm{AtFml}(\mathcal{L}_A) \cup \{\boldsymbol{\neg\psi} \mid \boldsymbol{\psi} \in \mathrm{AtFml}(\mathcal{L}_A)\}\bigr).$$

By Theorems 15.7 and 15.8, if $\mathcal{A}, \mathcal{B}$ are $\mathcal{L}$-structures, then

- $\mathcal{A} \preccurlyeq \mathcal{B}$ if and only if there is an expansion $\tilde{\mathcal{B}}$ of $\mathcal{B}$ in the language $\mathcal{L}_A = \mathcal{L} \cup \{\mathring{a} \mid a \in A\}$ such that $\tilde{\mathcal{B}} \vDash \mathrm{EDiag}(\mathcal{A})$;
- $\mathcal{A} \subseteq \mathcal{B}$ if and only if there is an expansion $\tilde{\mathcal{B}}$ of $\mathcal{B}$ in the language $\mathcal{L}_A = \mathcal{L} \cup \{\mathring{a} \mid a \in A\}$ such that $\tilde{\mathcal{B}} \vDash \mathrm{Diag}(\mathcal{A})$.

Lemma 31.12. *Let T be a satisfiable $\mathcal{L}$-theory, and let Δ be a set of $\mathcal{L}$-sentences closed under disjunctions. The following are equivalent:*

(1) *T has a set of axioms from Δ.*

(2) *Suppose M, N are $\mathcal{L}$-structures such that $N \vDash T$ and if $N \vDash \sigma$ then $M \vDash \sigma$, for all σ in Δ. Then $M \vDash T$.*

Proof. (1) $\Rightarrow$ (2) is obvious, so we may focus on the other direction. It is clear that $T \models \Sigma$ where $\Sigma = \{\sigma \in \Delta \mid T \models \sigma\}$, so it is enough to prove that $\Sigma \models T$. So fix M a model of Σ, towards proving that $M \vDash T$. Let

$$\Sigma^- = \{\neg\sigma \mid \sigma \in \Delta \text{ and } M \vDash \neg\sigma\}.$$

Claim 31.12.1. *$T \cup \Sigma^-$ is satisfiable.*

Proof of the Claim. Suppose $T \cup \Sigma^-$ is unsatisfiable. By compactness there are $\neg\sigma_1, \dots, \neg\sigma_n \in \Sigma^-$ such that $T \cup \{\neg\sigma_1, \dots, \neg\sigma_n\}$ is unsatisfiable. Therefore $T \models \neg(\neg\sigma_1 \wedge \dots \wedge \neg\sigma_n)$ that is $T \models \sigma_1 \vee \dots \vee \sigma_n$. As $\sigma_1 \vee \dots \vee \sigma_n \in$

Δ, then $\sigma_1 \vee \cdots \vee \sigma_n \in \Sigma$, and hence $M \vDash \sigma_1 \vee \cdots \vee \sigma_n$. Therefore $M \vDash \sigma_i$ for some $1 \leq i \leq n$. But $\neg\sigma_i \in \Sigma^-$, so $M \vDash \neg\sigma_i$: a contradiction. □

Suppose $N \vDash T \cup \Sigma^-$. We claim that for any $\sigma \in \Delta$, if $M \vDash \sigma$ then $N \vDash \sigma$. To see this suppose $M \vDash \sigma_0$ but $N \vDash \neg\sigma_0$ for some $\sigma_0 \in \Delta$: then $\neg\sigma_0 \in \Sigma^-$, and hence $M \vDash \neg\sigma_0$, a contradiction. Therefore the hypotheses of (2) are fulfilled and $M \vDash T$ as required. □

Theorem 31.13 (Tarski-Łos). *Let T be a satisfiable $\mathcal{L}$-theory. Then*

(i) *T can be axiomatized by $\forall$-sentences if and only if for all $\mathcal{L}$-structures $N \subseteq M$, if $M \vDash T$ then $N \vDash T$.*

(ii) *T can be axiomatized by $\exists$-sentences if and only if for all $\mathcal{L}$-structures $N \subseteq M$, if $N \vDash T$ then $M \vDash T$.*

Proof. We prove (i) leaving (ii) to the reader. By Proposition 4.8 we only need to prove the right-to-left direction of the equivalence. As the collection of all $\forall$-sentences is closed under disjunctions (see Section 3.C.4), it is enough

□

31.F. Skolem functions. Let $\mathcal{A}$ be an $\mathcal{L}$-structure and let $\lhd$ be a well-order of $A = \|\mathcal{A}\|$. To each formula $\boldsymbol{\varphi}$ with free variables $\boldsymbol{y}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ we associate $h_{\boldsymbol{\varphi}} \colon A^n \to A$, the **Skolem function for $\exists\boldsymbol{y}\boldsymbol{\varphi}$** defined by

$$h_{\boldsymbol{\varphi}}(a_1, \ldots, a_n) = \begin{cases} \text{the } \lhd\text{-least } b \text{ such that } \mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{a}] & \text{if } \mathcal{A} \vDash (\exists\boldsymbol{y}\boldsymbol{\varphi})[\vec{a}] \\ a^* & \text{otherwise,} \end{cases}$$

where a^* is the $\lhd$-minimum of A. Note that if $\boldsymbol{y}$ is the unique free variable of $\boldsymbol{\varphi}$, then $h_{\boldsymbol{\varphi}} \colon A^0 \to A$ is — essentially — an element of A: either a witness of the fact that $\mathcal{A} \vDash \exists\boldsymbol{y}\boldsymbol{\varphi}$ or else a^*. The set of all Skolem functions for $\mathcal{A}$ is $\mathrm{Sk}(\mathcal{A})$.

Theorem 31.14. *If $\mathcal{A}$ is well-orderable, then $\mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(X) \preccurlyeq \mathcal{A}$ for all $X \subseteq A$, that is: the closure of X under the functions in $\mathrm{Sk}(\mathcal{A})$ is an elementary substructure of $\mathcal{A}$.*

Proof. The Skolem function of the formula $\boldsymbol{y} \neq \boldsymbol{y}$ guarantees that $a^* \in C = \mathrm{Cl}_{\mathrm{Sk}(\mathcal{A})}(X)$, hence $C \neq \emptyset$. By the Tarski-Vaught Theorem it is enough to check that if $\mathcal{A} \vDash \exists\boldsymbol{y}\boldsymbol{\varphi}[\vec{c}]$ for some $\vec{c} \in C^n$, then there is $b \in C$ such that $\mathcal{A} \vDash \boldsymbol{\varphi}[b, \vec{c}]$. This is immediate taking $b = h_{\boldsymbol{\varphi}}(\vec{c})$. □

The next result, known as the **downward Löwenheim-Skolem Theorem** says that any uncountable structure in a countable language has an elementary countable substructure.

Theorem 31.15. *Assume $\mathcal{L}$ and $\mathcal{A} \in \operatorname{Str}(\mathcal{L})$ are well-orderable. If $X \subseteq \|\mathcal{A}\|$ with $|X| \leq \kappa$ and $\operatorname{card}(\mathcal{L}) \leq \kappa \leq \operatorname{card}(\mathcal{A})$, then for all there is $\mathcal{B} \preccurlyeq \mathcal{A}$ such that $X \subseteq \|\mathcal{B}\|$ and $\operatorname{card}(\mathcal{B}) = \kappa$.*

Proof. Let $Y \subseteq A = \|\mathcal{A}\|$ be such that $X \subseteq Y$ and $|Y| = \kappa$. As $|\operatorname{Sk}(\mathcal{A})| \leq |\operatorname{Fml}(\mathcal{L})| = \operatorname{card}(\mathcal{L})$, Theorem 21.18 implies that $\kappa \leq |Y| \leq |\operatorname{Cl}_{\operatorname{Sk}(\mathcal{A})}(Y)| \leq \kappa$. By Theorem 31.14 we may take $B = \operatorname{Cl}_{\operatorname{Sk}(\mathcal{A})}(Y)$. □

Corollary 31.16. *Assume* AC. *If $\mathcal{A} \in \operatorname{Str}(\mathcal{L})$ is infinite and $\operatorname{card}(\mathcal{L}) \leq \kappa \leq \operatorname{card}(\mathcal{A})$, then there is a $\mathcal{B} \preccurlyeq \mathcal{A}$ with $|\mathcal{B}| = \kappa$.*

Remark 31.17. If there is a model of ZFC, that is a set N and $E \subseteq N \times N$ such that $\langle N, E \rangle \vDash$ ZFC, then by Corollary 31.16 there must be a *countable* model $\langle M, E' \rangle$ of ZFC, where $M \subseteq N$ and $E' = E \cap M \times M$. Since "there is an uncountable set" is a theorem of ZFC, it follows that there is an $a \in M$ such that $\langle M, E' \rangle \vDash$"$a$ is an uncountable set", although $\{b \in M \mid b \; E' \; a\}$ is a countable set, since M itself is countable. This counter-intuitive phenomenon is called the **Löwenheim-Skolem paradox**.

Then notion of elementary substructure is tightly connected with that of closed and unbounded sets seen in Section 21.E.

Theorem 31.18. *Suppose $\mathcal{A} \in \operatorname{Str}(\mathcal{L})$ whose universe is a cardinal κ, that is $\|\mathcal{A}\| = \kappa$. Letting $C = \{\alpha < \kappa \mid \langle \alpha, \ldots \rangle \preccurlyeq \mathcal{A}\}$,*

- *C is closed in κ, and*
- *if $\omega < \operatorname{cof}(\kappa)$ and $\operatorname{card}(\mathcal{L}) < \kappa$, then C is also unbounded in κ.*

Proof. Suppose $\lambda < \kappa$ is limit and $C \cap \lambda$ is unbounded in λ: we must prove that $\lambda \in C$. Then λ is an increasing union of elementary substructures of $\mathcal{A}$ and hence $\langle \lambda, \ldots \rangle \preccurlyeq \mathcal{A}$ by Proposition 4.29. Therefore $\lambda \in C$ as required.

Suppose now $\operatorname{cof}(\kappa) > \omega$ and that $\operatorname{card}(\mathcal{L}) < \kappa$, and let $\beta < \kappa$. Applying Corollary 21.31 when $\mathcal{F} = \operatorname{Sk}(\mathcal{A})$ we have that

$$C \supseteq \{\alpha < \kappa \mid \alpha \text{ is closed under every } f \in \mathcal{F}\}$$

is closed and unbounded in κ. □

By Theorem 31.15, if $\mathcal{L}$ is countable and choice is assumed, then any $\mathcal{L}$-structure has a countable elementary substructure. The next result shows that AC can be replaced by DC (see Section 20.D).

Theorem 31.19 (DC). *If $\mathcal{L}$ is a countable language, then every $\mathcal{L}$-structure has a countable elementary substructure. In fact if $\mathcal{A} \in \operatorname{Str}(\mathcal{L})$ and $C \subseteq \|\mathcal{A}\|$ is countable, then there is a countable $\mathcal{B} \preccurlyeq \mathcal{A}$ with $C \subseteq \|\mathcal{B}\|$.*

Proof. By Proposition 30.5, $\mathrm{Fml}^{\exists}(\mathcal{L})$, the set of all existential formulæ of $\mathcal{L}$, is countable. Let $\langle \exists \boldsymbol{x}_n \boldsymbol{\varphi}_n \mid n < \omega \rangle$ be an enumeration of $\mathrm{Fml}^{\exists}(\mathcal{L})$ such that every formula is listed infinitely often. The plan is to build a descriptive tree T on $\|\mathcal{A}\|$ without terminal nodes, and whose branches[2] encode an elementary substructure of $\mathcal{A}$ containing C. By dependent choices T has a branch, and the result follows.

The construction of T is by induction on the length of the nodes: given $t \in T$ we must determine what are its immediate successors in T. Let $\langle c_n \mid n \in \omega \rangle$ be an enumeration (possibly with repetitions) of C, if this set is non-empty; otherwise the c_ns are some fixed element $a \in \|\mathcal{A}\|$.

- If $\mathrm{lh}\, t = 2n$, then $t^\frown \langle c_n \rangle$ is the unique immediate successor of t.
- If $\mathrm{lh}\, t = 2n + 1$, then consider the formula $\exists \boldsymbol{x}_n \boldsymbol{\varphi}_n$ whose free variables are $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_m}$ with $i_1 < \cdots < i_m$:
  – if $i_m \leq 2n$ and $\mathcal{A} \vDash \exists \boldsymbol{x}_n \boldsymbol{\varphi}_n [a_{i_1}, \ldots, a_{i_m}]$, then
  $$\forall a \in \|\mathcal{A}\| \left(t^\frown \langle a \rangle \in T \Leftrightarrow \mathcal{A} \vDash \boldsymbol{\varphi}_n [a, a_{i_1}, \ldots, a_{i_m}] \right);$$
  – otherwise the only node of length $2n + 1$ extending t is $t^\frown \langle c_0 \rangle$.

By construction T is has no terminal nodes, so $[T] \neq \emptyset$. If $f \in [T]$, then $C \subseteq \operatorname{ran} f \subseteq \|\mathcal{A}\|$, and in order to show that $\operatorname{ran} f$ is (the universe of) an elementary substructure of $\mathcal{A}$, it is enough to apply the Tarski-Vaught criterion. Suppose that $\mathcal{A} \vDash \exists \boldsymbol{y} \boldsymbol{\varphi} [a_1, \ldots, a_m]$ where $a_1, \ldots, a_m \in \operatorname{ran} f$, and $\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_m}$ are distinct, and $\{\boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{i_m}\} = \mathrm{Fv}(\exists \boldsymbol{y} \boldsymbol{\varphi})$. We must find $a \in \operatorname{ran} f$ such that $\mathcal{A} \vDash \boldsymbol{\varphi}[a, a_1, \ldots, a_m]$. Let $k_j \in \omega$ be least such that $f(k_j) = a_j$, for $1 \leq j \leq m$. Let us notice that without loss of generality we may make some further assumptions.

- The a_js are distinct. If, for example, $a_1 = a_2$, then replace $\boldsymbol{\varphi}$ with $\boldsymbol{\psi} = \boldsymbol{\varphi}(\!| \boldsymbol{v}_{i_2} / \boldsymbol{v}_{i_1} |\!)$ so that $\mathcal{A} \vDash \exists \boldsymbol{y} \boldsymbol{\varphi} [a_1, a_2, \ldots, a_m]$ is equivalent to $\mathcal{A} \vDash \exists \boldsymbol{y} \boldsymbol{\psi} [a_2, \ldots, a_m]$.
- $1 \leq i < j \leq m \Rightarrow k_i < k_j$. To see this use $\boldsymbol{\varphi}(\!| \boldsymbol{v}_{\pi(i_1)} / \boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{\pi(i_m)} / \boldsymbol{v}_{i_m} |\!)$ in place $\boldsymbol{\varphi}$, for a suitable permutation π of $\{i_1, \ldots, i_m\}$.
- $i_j = k_j$ for $1 \leq j \leq m$. To see this use $\boldsymbol{\varphi}(\!| \boldsymbol{v}_{k_1} / \boldsymbol{v}_{i_1}, \ldots, \boldsymbol{v}_{k_m} / \boldsymbol{v}_{i_m} |\!)$ in place of $\boldsymbol{\varphi}$.

Then there is n such that $\exists \boldsymbol{y} \boldsymbol{\varphi} = \exists \boldsymbol{x}_n \boldsymbol{\varphi}_n$ and $i_m \leq 2n$. By construction $f(2n + 2)$ is an element $a \in \|\mathcal{A}\|$ such that $\mathcal{A} \vDash \exists \boldsymbol{x}_n \boldsymbol{\varphi}_n [a, a_1, \ldots, a_n]$, which is what we had to prove. □

31.F.1. *Applications.* Assume AC throughout this section.

[2] See Section 23.D.

Suppose N is a transitive set and that $\langle N, \in\rangle \vDash \mathsf{ZFC}$. For any $X \subseteq N$ the set $\mathrm{Cl}(X) = \mathrm{Cl}_{\mathrm{Sk}(N)}(X)$ is infinite, since $\mathrm{Cl}(X) \preccurlyeq N$, and has size $|X| + \aleph_0$. The structure $\langle \mathrm{Cl}(X), \in\rangle$ satisfies the axiom of extensionality, since $\langle N, \in\rangle$ does. Moreover every $\emptyset \neq Y \subseteq \mathrm{Cl}(X)$ has an $\in$-minimal element by the axiom of foundation. Therefore $\mathrm{Cl}(X)$ is isomorphic to a transitive set M via the Mostowski collapse $\boldsymbol{\pi}\colon \mathrm{Cl}(X) \to M$ (see Section 19.C.3). The inverse of $\boldsymbol{\pi}$ is an elementary embedding $j\colon M \to N$. As the set X can be of any cardinality $\omega \leq \lambda \leq \kappa$, and since M and N are elementarily equivalent, it follows that:

Proposition 31.20. *If N is a transitive model of* ZFC*, then for any $\omega \leq \lambda \leq |N|$ there is a transitive set M of size λ such that $M \preccurlyeq N$.*

If κ is strongly inaccessible then V_κ is an uncountable transitive model of ZFC by Theorem 21.39, so that the hypothesis of Proposition 31.20 is not vacuous. By Exercise 21.63 if $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$ then κ is a strong limit cardinal, and $|\mathrm{V}_\kappa| = \kappa$. The next result shows that if $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$ then κ need not be inaccessible. (Recall that the theory of closed unbounded sets can be developed for any cardinal of uncountable cofinality—Remark 21.36.)

Lemma 31.21. *If* $\mathrm{cof}(\kappa) > \omega$ *then* $\{\alpha < \kappa \mid \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\kappa\}$ *is closed and unbounded in κ.*

Proof. Let $C = \{\alpha < \kappa \mid \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\kappa\}$.

If $\lambda < \kappa$ is limit and $\bigcup(C \cap \lambda) = \lambda$, then $\mathrm{V}_\lambda = \bigcup_{\alpha \in C \cap \lambda} \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\kappa$ by Proposition 4.29, and hence $\lambda \in C$. Therefore C is closed in κ.

Next we prove that C is unbounded. For any $\beta \in \kappa$ we want α such that $\mathrm{V}_\beta \subseteq \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\kappa$. Let $\mathrm{Cl}(X)$ be the closure of $X \subseteq \mathrm{V}_\kappa$ under some fixed set of Skolem functions for V_κ. We construct by recursion α_n and X_n by letting $\alpha_0 = \beta$, $X_n = \mathrm{Cl}(\mathrm{V}_{\alpha_n})$, and $\alpha_{n+1} = \sup(X_n \cap \mathrm{Ord})$. Since $\mathrm{V}_{\alpha_n} \subseteq X_n \subseteq \mathrm{V}_{\alpha_{n+1}}$ then $\bigcup_n X_n = \bigcup_n \mathrm{V}_{\alpha_n} = \mathrm{V}_\alpha$, where $\alpha = \sup_n \alpha_n$, and since $X_n \preccurlyeq \mathrm{V}_\kappa$, it follows that $\mathrm{V}_\beta \subseteq \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\kappa$ by Proposition 4.29. □

Theorem 31.22. *If* $\mathrm{V}_\kappa \vDash \mathsf{ZFC}$ *and* $\mathrm{cof}(\kappa) > \omega$ *then* $\{\alpha < \kappa \mid \mathrm{V}_\alpha \vDash \mathsf{ZFC}\}$ *contains a closed and unbounded set in κ. Therefore the least λ such that* $\mathrm{V}_\lambda \vDash \mathsf{ZFC}$ *has cofinality ω.*

Proof. Let λ be of uncountable cofinality and such that $\mathrm{V}_\lambda \vDash \mathsf{ZFC}$. By Lemma 31.21 $C = \{\alpha < \lambda \mid \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\lambda\}$ is closed and unbounded in λ, and $C \subseteq \{\alpha < \lambda \mid \mathrm{V}_\alpha \vDash \mathsf{ZFC}\}$. So the result applies when $\lambda = \kappa$ is strongly inaccessible.

If $\mathrm{V}_\lambda \vDash \mathsf{ZFC}$ and $\mathrm{cof}(\lambda) > \omega$ then by Lemma 31.21 $\{\alpha < \lambda \mid \mathrm{V}_\alpha \preccurlyeq \mathrm{V}_\lambda\}$ is closed and unbounded and, in particular, non-empty. Any α belonging to this set would witness that $\mathrm{V}_\alpha \vDash \mathsf{ZFC}$. Therefore the least λ such that $\mathrm{V}_\lambda \vDash \mathsf{ZFC}$ has cofinality ω. □

Theorem 31.23 (Łos). *Let $\langle \mathcal{A}_x \mid x \in X \rangle$ be $\mathcal{L}$-structures and let U be an ultrafilter on X. Let $\lhd_x$ be a well-order on $\|\mathcal{A}_x\|$. For every formula $\varphi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ and every $g_1, \ldots, g_n \in \bigtimes_{x \in X} A_x$*

$$\prod_U \mathcal{A}_x \vDash \varphi[[g_1], \ldots, [g_n]] \quad \Leftrightarrow \quad X_{\varphi, g_1, \ldots, g_n} \in U,$$

where $X_{\varphi, g_1, \ldots, g_n} = \{x \in X \mid \mathcal{A}_x \vDash \varphi[g_1(x), \ldots, g_n(x)]\}$.

Proof. The proof is by induction on $\mathrm{ht}(\varphi)$. If φ is atomic, the result follows from the definition of $\prod_U \mathcal{A}_x$. For the other cases, suppose fo simplicity that $n = 2$. If $\varphi = \neg\psi$, then

$$\begin{aligned}\prod_U \mathcal{A}_x \vDash \varphi[[g_1], [g_2]] &\Leftrightarrow \prod_U \mathcal{A} \nvDash \psi[[g_1], [g_2]] \\ &\Leftrightarrow X_{\psi, g_1, g_2} \notin U \\ &\Leftrightarrow X_{\varphi, g_1, g_2} \in U\end{aligned}$$

where in the last passage we used that $X_{\varphi, g_1, g_2} = X \setminus X_{\psi, g_1, g_2}$.

If $\varphi = \psi \vee \chi$, then

$$\begin{aligned}\prod_U \mathcal{A}_x \vDash \varphi[[g_1], [g_2]] &\Leftrightarrow \big(\prod_U \mathcal{A} \vDash \psi[[g_1], [g_2]]\big) \vee \big(\prod_U \mathcal{A} \vDash \chi[[g_1], [g_2]]\big) \\ &\Leftrightarrow X_{\psi, g_1, g_2} \in U \ \vee \ X_{\chi, g_1, g_2} \in U \\ &\Leftrightarrow X_{\psi, g_1, g_2} \cup X_{\chi, g_1, g_2} \in U \\ &\Leftrightarrow X_{\psi \vee \chi, g_1, g_2} \in U\end{aligned}$$

where we used that $X_{\psi \vee \chi, g_1, g_2} = X_{\psi, g_1, g_2} \cup X_{\chi, g_1, g_2}$.

Suppose now $\varphi = \exists \boldsymbol{y} \psi$. If $\prod_U \mathcal{A}_x \vDash \varphi[[g_1], [g_2]]$ then there is $h \in \bigtimes_{x \in X} A_x$ such that $\prod_U \mathcal{A}_x \vDash \psi[[h], [g_1], [g_2]]$ hence, by inductive hypothesis, $X_{\psi, h, \bar{g}} \in U$. As $X_{\varphi, g_1, g_2} \supseteq X_{\psi, h, g_1, g_2}$, it follows that $X_{\varphi, g_1, g_2} \in U$. Conversely, suppose that $X_{\varphi, g_1, g_2} \in U$. Let $h \in \bigtimes_{x \in X} A_x$ be the function

$$h(x) = \begin{cases} \text{the } \lhd_x\text{-least } a \text{ such that } \mathcal{A}_x \vDash \psi[a, g_1(x), g_2(x)] & \text{if } x \in X_{\varphi, g_1, g_2}, \\ a_x^* & \text{otherwise,} \end{cases}$$

where a_x^* is the $\lhd_x$-least element of A_x. Then X_{φ, g_1, g_2} is contained in X_{ψ, h, g_1, g_2} (in fact: the two sets are the same) hence $X_{\psi, h, g_1, g_2} \in U$. By inductive assumption, this implies that $\prod_U \mathcal{A}_x \vDash \psi[[h], [g_1], [g_2]]$ hence $\prod_U \mathcal{A}_x \vDash \varphi[[g_1], [g_2]]$. □

Corollary 31.24. *Let $\mathcal{A}$ be a well-orderable structure, let U be an ultrafilter on X, and let $\pi \colon \mathcal{A} \to \prod_U \mathcal{A}$ be the map defined by $\pi(a) = [c_a]$ where $c_a \colon X \to \{a\}$. Then π is an elementary embedding. In particular $\mathcal{A}$ is elementarily equivalent to any of its ultrapowers.*

Corollary 31.25 (AC). *A PC_Δ-class is closed under ultraproducts.*

The ultrapower of $\langle \omega, \leq \rangle$ by a non-principal ultrafilter on ω is a linear order that is not well-founded (Section 15.A.1), and therefore:

Corollary 31.26. *Assume there is a non-principal ultrafilter on ω (which is a consequence of* BPI*). Then the class of all well-orders is not* $\mathrm{PC}_\Delta(\mathcal{L}_{\mathit{Ordr}})$.

31.G. Compactness. The next result, known as the **Compactness Theorem**, is one of the cornerstones of mathematical logic. It was stated (Theorem 4.46) for countable languages in Section 4.K.

Theorem 31.27. *Assume either* BPI *or that $\mathcal{L}$ is well-orderable. If $\Sigma \subseteq$* $\mathrm{Sent}(\mathcal{L})$ *is **finitely satisfiable**, that is* $\mathrm{Mod}(\Sigma_0) \neq \emptyset$ *for every finite $\Sigma_0 \subseteq \Sigma$, then Σ is satisfiable.*

Proof. Let $X = \{x \subseteq \Sigma \mid x \text{ is finite}\}$ and for all $x \in X$ choose $\mathcal{A}_x \vDash x$. Let $S(x) = \{y \in X \mid x \subseteq y\}$. As $S(x_1) \cap \cdots \cap S(x_n) = S(x_1 \cup \cdots \cup x_n)$, then $\{S(x) \mid x \in X\} \subseteq \mathscr{P}(X)$ is a base for the filter F on X. Let $U \supseteq F$ be an ultrafilter extending F. We want to show that for each $\boldsymbol{\sigma} \in \Sigma$

$$\prod_U \mathcal{A}_x \vDash \boldsymbol{\sigma}.$$

This follows at once from Łos' Theorem and from $\{x \in X \mid \mathcal{A}_x \vDash \boldsymbol{\sigma}\} \supseteq S(\{\boldsymbol{\sigma}\}) \in F \subseteq U$. □

Remarks 31.28. (a) By Example 7.K.2, Theorem 31.27 generalizes the Compactness Theorem 14.20 for propositional calculus.

(b) As the closed subclasses of $\mathrm{Str}(\mathcal{L})$ with respect to the topology defined in (31.2) are the $\mathrm{Mod}(\Sigma)$s, it follows that Theorem 31.27 says that this topology is compact, whence the name.

(c) The proof of Theorem 31.27 given above uses the full power of the axiom of choice, since for each $x \in X$ we must choose an $\mathcal{A}_x$ which must be well-orderable, in order to apply Łos' Theorem 31.23. But Corollary 34.5 in Section 34 shows that the compactness theorem is provable under the stated assumptions.

Let us recall several easy consequences of the compactness theorem form Section 4.K:

- If $\Sigma \models \tau$, then there is a finite $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \tau$ (Corollary 4.47).
- If $\{\sigma_n \mid n \in \omega\} \cup \Delta'$ is a system of axioms for Δ, and if for every n there is an $m > n$ such that $\{\sigma_0, \ldots, \sigma_n\} \cup \Delta' \not\models \sigma_m$, then Δ is not finitely axiomatizable modulo Δ' (Theorem 4.49).
- If $\mathscr{C}, \mathscr{C}_0, \mathscr{C}_1 \subseteq \mathrm{Str}(\mathcal{L})$ are axiomatizable and $\mathscr{C}_0 \cup \mathscr{C}_1 = \mathscr{C}$ and $\mathscr{C}_0 \cap \mathscr{C}_1 = \emptyset$, then $\mathscr{C}_0, \mathscr{C}_1$ are finitely axiomatizable modulo $\mathscr{C}$ (Theorem 4.52).

- If $\mathscr{C}' \subseteq \mathscr{C} \subseteq \mathrm{Str}(\mathcal{L})$ are axiomatizable and $\mathscr{C}'$ is not finitely axiomatizable modulo $\mathscr{C}$, then $\mathscr{C} \setminus \mathscr{C}'$ is not axiomatizable (Theorem 4.53).

The following result is known as the **Upward Löwenheim-Skolem Theorem** is a generalization of Theorem 4.48.

Theorem 31.29. *Assume either* BPI *or that $\mathcal{L}$ is well-orderable. Suppose for each $n > 0$ there is a model of $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ with at least n elements. (In particular this holds if Σ has an infinite model.) Then Σ has models of arbitrarily large cardinality,*

$$\forall \kappa\, \exists \mathcal{B} \in \mathrm{Mod}(\Sigma)\, (\mathrm{card}(\mathcal{B}) \geq \kappa).$$

Proof. Let $\tilde{\mathcal{L}} = \mathcal{L} \cup \{\boldsymbol{d}_\alpha \mid \alpha < \kappa\}$ be the expansion of $\mathcal{L}$ with new constants, and let $\tilde{\Sigma} = \Sigma \cup \{\boldsymbol{d}_\alpha \neq \boldsymbol{d}_\beta \mid \alpha < \beta < \kappa\} \subseteq \mathrm{Sent}(\tilde{\mathcal{L}})$. Let $\Delta \subseteq \tilde{\Sigma}$ be a finite subset: then there exist $n \in \omega$ and $\{\alpha_i \mid i < n\} \subseteq \kappa$ such that

$$\Delta \subseteq \Sigma \cup \{\boldsymbol{d}_{\alpha_i} \neq \boldsymbol{d}_{\alpha_j} \mid 0 \leq i < j < n\}.$$

Let $\mathcal{A} \vDash \Sigma$ be a model with at least n elements $a_0, \ldots, a_{n-1}$ and let $\tilde{\mathcal{A}}$ be the expansion of $\mathcal{A}$ to the language $\tilde{\mathcal{L}}$ defined as follows:

$$\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} = \begin{cases} a_i & \text{if } \alpha = \alpha_i \\ a_0 & \text{otherwise.} \end{cases}$$

It is immediate to check that $\tilde{\mathcal{A}} \vDash \Delta$. Therefore we have shown that $\tilde{\Sigma}$ is finitely satisfiable. By compactness there is a model $\tilde{\mathcal{B}} \vDash \tilde{\Sigma}$ whose cardinality is at least that of κ, since $\boldsymbol{d}_\alpha^{\tilde{\mathcal{A}}} \neq \boldsymbol{d}_\beta^{\tilde{\mathcal{A}}}$ when $0 < \alpha < \beta < \kappa$. Then $\mathcal{B}$, the reduction of $\tilde{\mathcal{B}}$ to $\mathcal{L}$, is the model we were looking for. □

Corollary 31.30. *Assume $\mathcal{L}$ and $\mathcal{A}$ are well-orderable. If $\mathcal{A}$ is infinite, then*

$$\forall \kappa \geq \max\left(\mathrm{card}(\mathcal{L}), \mathrm{card}(\mathcal{A})\right) \exists \mathcal{B}\ (\mathcal{A} \preccurlyeq \mathcal{B} \wedge \kappa = \mathrm{card}(\mathcal{B}))\,.$$

Proof. By Theorem 15.7 it is enough to find a model of $\mathrm{EDiag}(\mathcal{A})$ of size κ. The theory $\mathrm{EDiag}(\mathcal{A})$ is satisfiable and has size $\leq \kappa$, hence by Theorem 31.29 it has a model of cardinality $\geq \kappa$ which by Theorem 31.15 has an elementary substructure of size κ. □

Corollary 31.31. *Let Σ be a finitely axiomatizable theory in a language $\mathcal{L}$ such that for every $n > 0$ there is a model of Σ with at least n elements. (This encompasses the case when Σ has an infinite model.) Then*

$$\forall \kappa \in \mathrm{Card} \setminus \omega\, \exists \mathcal{A} \in \mathrm{Mod}(\Sigma)\, (\mathrm{card}(\mathcal{A}) = \kappa).$$

Proof. Let $\boldsymbol{\sigma}$ be an $\mathcal{L}$-sentence that axiomatizes Σ, and let $\mathcal{L}_0$ be the finite language whose non-logical symbols are exactly the symbols occurring in $\boldsymbol{\sigma}$. By compactness there is an $\mathcal{L}_0$-structure $\mathcal{A}$ of size $\aleph_0$ such that $\mathcal{A} \vDash \boldsymbol{\sigma}$, and by the Löwenheim-Skolem Theorems 31.15 and 31.29 we can find $\mathcal{L}_0$-structures satisfying $\boldsymbol{\sigma}$ of any prescribed infinite cardinality. Since every $\mathcal{L}_0$-structure satisfying $\boldsymbol{\sigma}$ can be expanded to a $\mathcal{L}$-structure that is a model Σ, the result is proved. □

Remark 31.32. The use of compactness in the proof of Corollary 31.31 in order to get the countable $\mathcal{A}$ seems to require AC, but Exercise 34.14(ii) in Section 34 shows that such $\mathcal{A}$ can be obtained irrespective of choice.

Corollary 31.33. *Assume either* BPI *or that $\mathcal{L}$ is well-orderable. Let Σ be a set of statements whose models are of finite size. Then the models of Σ have uniformly bounded size, that is*

$$\exists n \in \omega \, \forall \mathcal{A} \in \operatorname{Mod}(\Sigma) \; (\operatorname{card}(\mathcal{A}) \leq n) \, .$$

Theorem 31.34. *Assume* BPI *and suppose $\mathscr{C}$ is $\mathrm{PC}_\Delta(\mathcal{L})$. Then $\mathcal{A} \in \operatorname{Str}(\mathcal{L})$ is embeddable in some structure in $\mathscr{C}$ if and only if every finitely generated substructure of $\mathcal{A}$ is embeddable in some structure in $\mathscr{C}$.*

Proof. By replacing $\mathcal{L}$ with some larger $\mathcal{L}'$, we may assume that $\mathscr{C} = \operatorname{Mod}(T)$. If $\mathcal{A} \subseteq \mathcal{B} \in \mathscr{C}$, then every substructure of $\mathcal{A}$ embeds into $\mathcal{B}$. Conversely, suppose every finitely generated substructure of $\mathcal{A}$ embeds into some structure of $\mathscr{C}$. It is enough to show that $\Sigma = \operatorname{Diag}(\mathcal{A}) \cup T$ is satisfiable, which follows at once from compactness and the assumption. □

Corollary 31.35 (BPI)**.** *Every field can be embedded into an algebraically closed field.*

Proof. □

31.G.1. *Categoricity.* A theory is

- **categorical** if it has a unique (up to isomorphism) model;
- κ-**categorical** if it has a unique (up to isomorphism) model of size κ, where κ is an infinite cardinal;
- **totally categorical** if it has a unique (up to isomorphism) model of size κ, for any infinite cardinal κ.

By the upward Löwenheim-Skolem Theorem, if T is categorical, then its unique model is finite.

A deep theorem of Morley says that if a theory in a countable language is κ-categorical for *some* $\kappa > \omega$, then it is κ-categorical for *all* uncountable cardinals κ. Thus a complete first-order theory in a countable language can be totally categorical, never categorical, ω-categorical but not uncountably categorical, or uncountably categorical but not ω-categorical. Here are some examples.

- The empty theory in the empty language is κ-categorical for every κ, since a model is just a non-empty set and two sets are isomorphic just in case they are in bijection.

- The theory of groups (even abelian ones) is never categorical, since $\bigoplus_{\alpha<\kappa}\mathbb{Z}$ and $\bigoplus_{\alpha<\kappa}\mathbb{Z}/2\mathbb{Z}$ have size κ but are not isomorphic.

- By Theorem 13.32 the theory of dense linear orders without endpoints is ω-categorical, but it is not $2^{\aleph_0}$-categorical (see Section 13.E.4). Therefore the theory of dense linear orders without endpoints is not uncountably categorical.

- The theory ACF_p of algebraically closed fields of characteristic p, where p is either prime or else $p = 0$, is uncountably categorical, but not ω-categorical.

  Let us first argue that it is uncountably categorical. Let $\mathbb{F} \vDash \mathrm{ACF}_p$, let $\mathbb{F}'$ be its prime subfield, and let $X \subseteq \mathbb{F}$ be a transcendence base of $\mathbb{F}$ over $\mathbb{F}'$. Note that $\mathbb{F}'$ is $\mathbb{Z}/p\mathbb{Z}$, if p is prime, or $\mathbb{Q}$ if $p = 0$; thus $\mathbb{F}'$ is countable. The transcendence base of X exists by Zorn's Lemma and has the cardinality of $\mathbb{F}$, if $\mathbb{F}$ is uncountable. If X and Y are two transcendence base for the fields $\mathbb{F}$ and $\mathbb{G}$ of equal characteristic, and if $\pi\colon X \to Y$ is a bijection, then π extends to an isomorphism $\pi\colon \mathbb{F} \to \mathbb{G}$. Therefore, if $\mathbb{F}$, $\mathbb{G}$ are uncountable algebraically closed fields of the same characteristic, then their transcendence bases have the same cardinality and hence they are isomorphic. We have thus proved that ACF_p is κ-categorical, if $\kappa > \omega$. To see that ACF_p is not ω-categorical, consider two algebraically closed fields with different finite transcendence degree.

The next result generalizes Theorem 4.37 that was stated without proof in Chapter I.

Theorem 31.36. *Assume* AC. *If* Σ *is a* κ*-categorical theory with only infinite models and* $\mathrm{card}(\mathcal{L}) \leq \kappa$*, then* Σ *is complete.*

Proof. Suppose $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L})$ witnesses that Σ is not complete, and let $\mathcal{A}$ and $\mathcal{B}$ be models of Σ satisfying $\boldsymbol{\sigma}$ and $\neg\boldsymbol{\sigma}$, respectively. By assumption $\mathcal{A}$ and $\mathcal{B}$ are infinite, and by the upward Löwenheim-Skolem Theorem 31.29 we may assume that $\mathrm{card}(\mathcal{A}), \mathrm{card}(\mathcal{B}) \geq \kappa$. By AC $\mathcal{A}$ and $\mathcal{B}$ are well-orderable, so we may assume that $\mathrm{card}(\mathcal{A}) = \mathrm{card}(\mathcal{B}) = \kappa$ by the downward Löwenheim-Skolem Theorem 31.15. By κ-categoricity $\mathcal{A} \cong \mathcal{B}$, against the assumption that $\mathcal{A} \vDash \boldsymbol{\sigma}$ and $\mathcal{B} \vDash \neg\boldsymbol{\sigma}$. □

Exercises

Exercise 31.37. Show that if $\boldsymbol{t}$ is a closed term of the language of $\mathcal{A}$, and $\mathcal{A}'$ is an expansion of $\mathcal{A}$, and $\mathcal{A} \subseteq \mathcal{B}$, then $\boldsymbol{t}^{\mathcal{A}} = \boldsymbol{t}^{\mathcal{A}'} = \boldsymbol{t}^{\mathcal{B}}$.

Exercise 31.38. Let $\mathcal{L}' \subseteq \mathcal{L}$ and $\boldsymbol{\varphi} \in \mathrm{Fml}(\mathcal{L}')$. Show that $\mathcal{A} \vDash_g \boldsymbol{\varphi} \Leftrightarrow (\mathcal{A} \upharpoonright \mathcal{L}') \vDash_g \boldsymbol{\varphi}$ for all $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ and all $g \colon \mathrm{Vbl} \to \|\mathcal{A}\|$.

Exercise 31.39. Show that:

(i) $\mathcal{A} \vDash_g \boldsymbol{\varphi} \wedge \boldsymbol{\psi} \Leftrightarrow (\mathcal{A} \vDash_g \boldsymbol{\varphi} \wedge \mathcal{A} \vDash_g \boldsymbol{\psi})$;

(ii) $\mathcal{A} \vDash_g \forall \boldsymbol{x} \boldsymbol{\varphi} \Leftrightarrow \forall a \in \|\mathcal{A}\| \ (\mathcal{A} \vDash_{g_{\boldsymbol{x} \mapsto a}} \boldsymbol{\varphi})$;

(iii) $\mathcal{A} \vDash_g \neg\neg\boldsymbol{\varphi} \Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\varphi}$;

(iv) $\mathcal{A} \vDash_g \boldsymbol{\varphi} \vee \boldsymbol{\psi} \Leftrightarrow \mathcal{A} \vDash_g \neg(\neg\boldsymbol{\varphi} \wedge \neg\boldsymbol{\psi})$;

(v) $\mathcal{A} \vDash_g \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi} \Leftrightarrow (\mathcal{A} \vDash_g \boldsymbol{\varphi} \Rightarrow \mathcal{A} \vDash_g \boldsymbol{\psi})$;

(vi) $\mathcal{A} \vDash_g (\boldsymbol{\varphi} \Leftrightarrow \boldsymbol{\psi}) \Leftrightarrow (\mathcal{A} \vDash_g \boldsymbol{\varphi} \Leftrightarrow \mathcal{A} \vDash_g \boldsymbol{\psi})$.

Exercise 31.40. Generalize Proposition 31.7 to the case of formulæ with blocks of quantifiers of the same kind (for example $\exists \boldsymbol{y}_1 \exists \boldsymbol{y}_2 \ldots \exists \boldsymbol{y}_m \boldsymbol{\varphi}$, or $\forall \boldsymbol{y}_1 \forall \boldsymbol{y}_2 \ldots \forall \boldsymbol{y}_m \boldsymbol{\varphi}$).

Exercise 31.41. Suppose that $\boldsymbol{s}, \boldsymbol{t}$ are substitutable in $\boldsymbol{\varphi}$ for $\boldsymbol{x}$. Show that $\boldsymbol{s} = \boldsymbol{t} \Rightarrow (\boldsymbol{\varphi}(\!|\boldsymbol{s}/\boldsymbol{x}|\!) \Leftrightarrow \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!))$ is valid.

Exercise 31.42. Show that the formulæ below are valid:

(i) $\exists \boldsymbol{x} (\boldsymbol{\varphi} \vee \boldsymbol{\psi}) \Leftrightarrow (\exists \boldsymbol{x} \boldsymbol{\varphi} \vee \exists \boldsymbol{x} \boldsymbol{\psi})$.

(ii) $\forall \boldsymbol{x} (\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Leftrightarrow (\forall \boldsymbol{x} \boldsymbol{\varphi} \wedge \forall \boldsymbol{x} \boldsymbol{\psi})$.

(iii) $\exists \boldsymbol{x} (\boldsymbol{\varphi} \wedge \boldsymbol{\psi}) \Rightarrow (\exists \boldsymbol{x} \boldsymbol{\varphi} \wedge \exists \boldsymbol{x} \boldsymbol{\psi})$.

(iv) $(\forall \boldsymbol{x} \boldsymbol{\varphi} \vee \forall \boldsymbol{x} \boldsymbol{\psi}) \Rightarrow \forall \boldsymbol{x} (\boldsymbol{\varphi} \vee \boldsymbol{\psi})$.

(v) $\forall \boldsymbol{x} (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}) \Rightarrow (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\psi})$, if $\boldsymbol{x}$ does not occur free in $\boldsymbol{\varphi}$.

Exercise 31.43. Show that the following formulæ are not valid:

(i) $(\exists \boldsymbol{x} \boldsymbol{\varphi} \wedge \exists \boldsymbol{x} \boldsymbol{\psi}) \Rightarrow \exists \boldsymbol{x} (\boldsymbol{\varphi} \wedge \boldsymbol{\psi})$.

(ii) $\forall \boldsymbol{x} (\boldsymbol{\varphi} \vee \boldsymbol{\psi}) \Rightarrow (\forall \boldsymbol{x} \boldsymbol{\varphi} \vee \forall \boldsymbol{x} \boldsymbol{\psi})$.

(iii) $\forall \boldsymbol{x} (\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}) \Rightarrow (\boldsymbol{\varphi} \Rightarrow \forall \boldsymbol{x} \boldsymbol{\psi})$, if $\boldsymbol{x}$ occurs free in $\boldsymbol{\varphi}$.

Exercise 31.44. Show that

(i) $\boldsymbol{\varphi}$ is valid if and only if $\boldsymbol{\varphi}^{\forall}$ is valid;

(ii) $\boldsymbol{\varphi}$ is satisfiable if and only if $\boldsymbol{\varphi}^{\exists}$ is satisfiable.

Exercise 31.45. If $\mathcal{L}' \subseteq \mathcal{L}$ and $\Sigma, \Delta \subseteq \mathrm{Sent}(\mathcal{L}')$, then $\Sigma \models_{\mathcal{L}} \Delta \Leftrightarrow \Sigma \models_{\mathcal{L}'} \Delta$.

Exercise 31.46. Let $\pi\colon \mathcal{A} \to \mathcal{B}$ be a morphism. Show that:

(i) If π is an isomorphism then it is an elementary embedding.

(ii) If π is elementary then it is injective.

(iii) If $\mathcal{A} \vDash \boldsymbol{\varphi}[\vec{a}] \Rightarrow \mathcal{B} \vDash \boldsymbol{\varphi}[\pi(\vec{a})]$ for all formulæ $\boldsymbol{\varphi}$ and all $\vec{a}$, then π is elementary.

Exercise 31.47. Let $\mathcal{A}, \mathcal{B} \in \mathrm{Str}(\mathcal{L})$.

(i) Show that the following are equivalent:
- $\mathcal{A} \subseteq \mathcal{B}$,
- there is an expansion $\tilde{\mathcal{B}}$ of $\mathcal{B}$ in the language $\mathcal{L} \cup \{\mathring{a} \mid a \in \|\mathcal{A}\|\}$ such that $\tilde{\mathcal{B}} \vDash \mathrm{Diag}(\mathcal{A})$.

(ii) Show that the following are equivalent:
- $\mathcal{A} \preccurlyeq \mathcal{B}$,
- $\tilde{\mathcal{A}} \subseteq \tilde{\mathcal{B}}$ and $\tilde{\mathcal{A}} \equiv \tilde{\mathcal{B}}$, where $\tilde{\mathcal{A}}$, $\tilde{\mathcal{B}}$ are the expansions of $\mathcal{A}$, $\mathcal{B}$ to $\|\mathcal{A}\|$.

Exercise 31.48. (i) If $X \in \mathrm{Def}^n_{\mathcal{A}}(\{q_1, \ldots, q_m\} \cup P')$ and $\{q_1\}, \ldots, \{q_m\} \in \mathrm{Def}^1_{\mathcal{A}}(P)$ then $X \in \mathrm{Def}^n_{\mathcal{A}}(P \cup P')$.

(ii) Suppose $R \in \mathrm{Def}^m_{\mathcal{A}}(P)$ and $X \in \mathrm{Def}^n_{\langle\mathcal{A},R\rangle}(Q)$, where $\langle\mathcal{A}, R\rangle$ is the expansion of $\mathcal{A}$ obtained by adding the relation R. Then $X \in \mathrm{Def}^n_{\mathcal{A}}(P \cup Q)$.

Exercise 31.49. Complete the proof of Proposition 4.29.

Exercise 31.50. Let $\mathcal{L} = \{U\}$ be the language with a 1-ary relational symbol. The $\mathcal{L}$-structures $\langle A, B\rangle$ are non-empty sets with a specified subset.

(i) How many $\mathcal{L}$-structures of cardinality n are there, up to isomorphism? How many of size $\kappa \geq \omega$?

(ii) Find a set of sentences Σ such that $\langle A, B\rangle \vDash \Sigma$ if and only if A, B, $A \setminus B$ are infinite.

Exercise 31.51. Let $\mathcal{L}$ be a countable language, and assume the following weakening of the downward Löwenheim-Skolem Theorem 31.15: Every $\mathcal{L}$-structure has a countable elementary substructure. Show that:

(i) If $\mathcal{L}$ is the empty language, then there are no Dedekind-finite, infinite sets (see page 353).

(ii) If $\mathcal{L}$ has infinitely many unary predicates, then AC_ω holds.

(iii) If $\mathcal{L}$ has a binary predicate symbol, then DC holds.

Exercise 31.52 (AC)**.** Show that $\prod_U \mathbb{R}$ where U is a non-principal ultrafilter on ω, is a non-Archimedean field which is elementarily equivalent to $\mathbb{R}$.

Exercise 31.53 (BPI)**.** Let G be a group with elements with arbitrarily large finite torsion, e.g. the group of roots of unity $\{z \in \mathbb{C} \mid \exists n \in \mathbb{Z}\,(z^n = 1)\}$. Show that there is a group H a torsion-free element and such that $G \preccurlyeq H$.

Exercise 31.54 (AC). Let $\Bbbk$ be a finite field. Show that:

(i) the theory of $\Bbbk$-vector spaces is κ-categorical for all $\kappa \geq \omega$, but it is not complete;

(ii) the theory of infinite dimensional $\Bbbk$-vector spaces (see Exercise 9.33) is κ-categorical for all $\kappa \geq \omega$ and complete.

Exercise 31.55 (AC). Show that the following theories are ω-categorical, but not κ-categorical for uncountable κs:

(i) The theory of the random graph.

(ii) The theory of atomless boolean algebras.

Exercise 31.56 (AC). Show that the theories of:

(i) of vector spaces over a countable infinite field $\Bbbk$, (Section 9.B.3),

(ii) of divisible torsion-free abelian groups,

(iii) $\Sigma_{(\mathbb{N},S)}$, $\Sigma_{(\mathbb{N},<)}$ from Section 11.A,

(iv) of torsion-free divisible abelian groups,

(v) of $\mathbb{Z}$-groups (see page 240),

are κ-categorical for $\kappa > \omega$, but are not ω-categorical.

Exercise 31.57. Let $\mathcal{L}$ be the language for orders extended with a constant symbol $\mathring{r}$ for each $r \in \mathbb{R}$. Let T be the $\mathcal{L}$-theory with axioms for dense linear orders without endpoints and

- $\mathring{0} \mathrel{\overset{\circ}{=}} \mathring{1} \boldsymbol{\Rightarrow} \mathring{r} \mathrel{\overset{\circ}{=}} \mathring{0}$ for each $r \in \mathbb{R}$,
- $\mathring{0} \mathrel{\overset{\circ}{\neq}} \mathring{1} \boldsymbol{\Rightarrow} \mathring{r} < \mathring{s}$ for each $r < s$ with $r, s \in \mathbb{R}$.

Show that T is ω-categorical, but not complete.

Exercise 31.58 (AC). Given a first-order language $\mathcal{L}$, show that:

(i) if $\mathscr{C}_i$ $(i \in I)$ is axiomatizable, then $\bigcap_{i \in I} \mathscr{C}_i$ is axiomatizable;

(ii) if $\mathscr{C}_0$ is axiomatizable and $\mathscr{C}_1$ is finitely axiomatizable, then $\mathscr{C}_0 \cup \mathscr{C}_1$ is axiomatizable;

(iii) if $\mathscr{C}_0 = \mathrm{Mod}(T_0)$ and $\mathscr{C}_1 = \mathrm{Mod}(T_1)$ where T_i is a countable set of $\mathcal{L}$-sentences,[3] then $\mathscr{C}_0 \cup \mathscr{C}_1$ is axiomatizable;

(iv) if the classes $\mathscr{C}'$ and $\mathscr{C}_i$ $(i \in I)$ are axiomatizable and such that $i < j \Rightarrow \mathscr{C}' \supseteq \mathscr{C}_i \supset \mathscr{C}_j$ where $(I, <)$ is totally ordered and without maximum, then $\bigcap_{i \in I} \mathscr{C}_i$ is not finitely axiomatizable modulo $\mathscr{C}'$;

(v) if the classes $\mathscr{C}_i$ $(i \in I)$ are finitely axiomatizable modulo $\mathscr{C}'$ and are such that$i < j \Rightarrow \mathscr{C}_i \subset \mathscr{C}_j \subseteq \mathscr{C}'$ where $(I, <)$ is totally ordered and

[3] This is the case if $\mathcal{L}$ has countably many non-logical symbols—see Section 30.B.

without maximum, then $\bigcup_{i\in I}\mathscr{C}_i$ is not axiomatizable. Use this to give a different proof of Theorem 4.48.

Exercise 31.59 (AC)**.** Suppose $\mathscr{C}\subseteq \mathrm{Str}(\mathcal{L})$ is EC and that $\mathscr{C}$ has structures of arbitrarily large finite cardinality. Show that $\mathscr{C}'=\{\mathcal{M}\in\mathscr{C}\mid \mathrm{card}(\mathcal{M})<\omega\}$ is not PC_Δ and that $\mathscr{C}\setminus\mathscr{C}'$ is PC and EC_Δ, but not EC.

Exercise 31.60. Let $\mathcal{L}$ be the language with a unary predicate symbol. Show that:

(i) the class of all $\mathcal{L}$-structures $\langle M,P\rangle$ such that P and $M\setminus P$ are both infinite is EC_Δ and not EC, and that the theory axiomatizing this class is ω-categorical, but not κ-categorical, for $\kappa>\omega$;

(ii) the class of all $\mathcal{L}$-structures $\langle M,P\rangle$ such that $P\asymp M\setminus P$ is PC, but not EC_Δ.

Exercise 31.61 (AC)**.** Show that the following classes of $\mathcal{L}$-structures are $\mathrm{PC}(\mathcal{L})$ and $\mathrm{EC}_\Delta(\mathcal{L})$ but not $\mathrm{EC}(\mathcal{L})$:

(i) the class of acyclic graphs, $\mathcal{L}=\mathcal{L}_{\textsc{Grph}}$;

(ii) the class of all bipartite graphs, $\mathcal{L}=\mathcal{L}_{\textsc{Grph}}$;

(iii) the class of all torsion-free abelian groups, $\mathcal{L}=\mathcal{L}_{\textsc{Grps}}$.

Exercise 31.62 (AC)**.** Show that the following classes of $\mathcal{L}$-structures are $\mathrm{PC}(\mathcal{L})$ but not $\mathrm{EC}_\Delta(\mathcal{L})$:

(i) the class of homogeneous dense linear orders without endpoints, $\mathcal{L}=\mathcal{L}_{\textsc{Ordr}}$;

(ii) the class of ill-founded linear orders, $\mathcal{L}=\mathcal{L}_{\textsc{Ordr}}$.

Exercise 31.63 (AC)**.** Let $\mathscr{C}$ be PC. Show that $\{\mathcal{A}\in\mathscr{C}\mid \mathcal{A}\text{ is uncountable}\}$ is PC_Δ but not PC.

Exercise 31.64. (i) An unfriendly coloring of a graph (V,E) is a map $c\colon V\to 2$ such that $|\{w\in V\mid w\ E\ v\wedge c(w)=c(v)\}|\leq|\{w\in V\mid w\ E\ v\wedge c(w)\neq c(v)\}|$. Show that the class of graphs that admit an unfriendly coloring is $\mathrm{PC}(\mathcal{L}_{\textsc{Grph}})$.

(ii) Every finite graph admits an unfriendly coloring [**AMP90**]. Use the Compactness Theorem to extend this result to locally finite graphs.

Exercise 31.65. Let $\mathcal{L}$ be a language with a binary relation symbol $\boldsymbol{R}$ and let $\boldsymbol{\sigma}$ be the sentence $\boldsymbol{\forall x\exists y(x\ R\ y)}$. Assume BPI together with the negation of AC. By Exercise **????** fix a non-empty set A together with $R\subseteq A\times A$ such that $\mathcal{A}=\langle A,R\rangle$ satisfies $\boldsymbol{\sigma}$, yet there is no $f\colon A\to A$ such that $\forall x\in A\ (x\ R\ f(x))$, that is $S(f)\neq A$ for any $f\in A^A$ where $S(f)=\{a\in A\mid a\ R\ f(a)\}$. Show that:

(i) the family $\{S(f) \mid f \in A^A\}$ generates a proper ideal J on A,

(ii) the ultrapower $\prod_U \mathcal{A}$ does not satisfy $\boldsymbol{\sigma}$, where U is any ultrafilter extending $\check{J}$.

Conclude that BPI together with Corollary 31.24 restricted to the language $\mathcal{L}$ and to the $\forall\exists$-statement $\boldsymbol{\sigma}$ imply AC.

Exercise 31.66. Show that AC is equivalent to each of the following statements, which are variants of the downward and upward Löwenheim-Skolem theorems.

(i) If $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ is infinite, then for every infinite $B \precsim \|\mathcal{A}\|$ there is $\mathcal{B} \in \mathrm{Str}(\mathcal{L})$ such that $\|\mathcal{B}\| = B$ and $\mathcal{B} \equiv \mathcal{A}$.

(ii) Same as (i), but with $\mathcal{L}$ finite.

(iii) If $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ has size $\aleph_0$ and $\mathcal{L}$ is finite, then for every infinite set B there is a $\mathcal{B} \in \mathrm{Str}(\mathcal{L})$ such that $\|\mathcal{B}\| = B$ and $\mathcal{B} \equiv \mathcal{A}$.

(iv) Every $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ such that $\mathrm{card}(\mathcal{L}) \leq \mathrm{card}(\mathcal{A})$ has an elementary substructure $\mathcal{B}$ such that $\mathrm{card}(\mathcal{B}) \leq \mathrm{card}(\mathcal{L})$.

[Hint: using a binary function symbol to formalize 'there is a pairing function' and apply Theorem 20.11 and Corollary 18.35.]

Exercise 31.67. Show that the Compactness Theorem 31.27 implies BPI.

Notes and remarks

Most of the applications of Łos' Theorem 31.23 use the axiom of choice, but the statement of the theorem, even extended to non-necessarily well-orderable structures, *does not imply* AC. In fact the existence of non-principal ultrafilters is unprovable in MK or in ZF [**Bla77**], hence if every ultrafilter is principal, then $\prod_U \mathcal{A}_x \cong \mathcal{A}_{x_0}$ where $\{x_0\}$ is the generator of U, hence Łos' Theorem holds for trivial reasons. On the other hand, Exercise 31.65 (from [**Bel09**]) shows that Łos' Theorem and BPI imply AC.

32. Application of compactness

Throughout this section, assume always BPI, unless otherwise stated.

32.A. Undefinability results.

Proposition 32.1. *Let G be a group with elements of arbitrarily large torsion, that is $\forall n\, \exists g \in G\ (n \leq o(g) < \infty)$. Then there is a group H with an element of infinite torsion and such that $G \preccurlyeq H$.*

Proof. Let $\Sigma = \mathrm{EDiag}(G) \cup \{\boldsymbol{c}^n \neq 1 \mid n \geq 1\}$, where $\boldsymbol{c}$ is a new symbol of constant. Every finite subset of Σ is satisfied by an expansion of G and hence

Σ is finitely satisfiable. Therefore a model of Σ is a group H with an element of infinite order and such that $G \preccurlyeq H$. □

Proposition 32.2. *Suppose $G = \langle V, E\rangle$ is a connected graph such that $\forall k \in \omega\, \exists v, w \in V\, (k \leq d(v, w) < \infty)$. Then there is a disconnected graph H such that $G \preccurlyeq H$.*

Proof. The theory $\mathrm{EDiag}(G) \cup \{d(\boldsymbol{c}, \boldsymbol{d}) > n \mid n \in \omega\}$, where $\boldsymbol{c}, \boldsymbol{d}$ are two new symbols for constants, is finitely satisfiable—for any n we can always find two vertices in G whose distance is greater than n. Therefore any model of Σ is a graph H with two vertices in distinct connected components, and such that $G \preccurlyeq H$. □

32.B. Non-standard models of arithmetic.

Part of this has been moved to section 8, so I need to revise this!

Recall from Section 12.D that the language $\mathcal{L}_{\mathsf{PA}}$ of Peano arithmetic (PA) has $\mathsf{S}, \overline{0}, +, \cdot, <$ as non-logical symbols. If $\mathcal{M} = \langle M; S_M, +_M, \cdot_M, <_M, 0_M\rangle$ is a model of PA then the map $F\colon \mathbb{N} \to M$ defined recursively by $F(0) = 0_M$ and $F(S(n)) = S_M(F(n))$ is an embedding and the **standard part of** $\mathcal{M}$

$$\operatorname{ran} F = \mathbb{N}_M = \{S_M(n) \mid n \in \omega\}$$

is an initial segment of $\langle M, <\rangle$. If $\mathbb{N}_M = M$ then F is an isomorphism, and $\mathcal{M}$ is said to be standard; otherwise it is said to be a **non-standard model** of PA. A model of PA is a model of Presburger arithmetic, so by the remarks after Proposition 11.23 the order structure of a non-standard model of PA is $\mathbb{N} \uplus Q \times \mathbb{Z}$ with Q a dense linear order without endpoints. If $\mathcal{M}$ is non-standard then $\mathbb{N}_M$ has no least upper bound by Lemma 12.13, so $\langle M, <_M\rangle$ is not a well-order.

By the upward Löwenheim-Skolem Theorem 31.29 there are uncountable (necessarily non-standard) models of PA. Another way to obtain an uncountable non-standard model of PA is to take $\prod_U \langle \mathbb{N}, S, 0, +, \cdot, <\rangle$ with U a non-principal ultrafilter on ω. If $\mathcal{M}$ is an inductive structure, that is if it satisfies the second-order induction principle Ind^2 on page 289 of Section 12.A, then $\mathcal{M}$ is standard by Theorem 12.2, so Ind^2 is not equivalent to a first-order formula.

Theorem 32.3. *Every satisfiable theory T in a language $\mathcal{L} \supseteq \mathcal{L}_{\mathsf{PA}}$ such that $T \models \mathsf{PA}$ has a non-standard model. Moreover, this model can be taken to be countable, if $\mathcal{L}$ is countable.*

Proof. Extend $\mathcal{L}$ to $\mathcal{L}' = \mathcal{L} \cup \{\boldsymbol{c}\}$ by adding a new constant symbol and let $\Sigma = T \cup \{\mathsf{S}^{(n)}(\overline{0}) < \boldsymbol{c} \mid n \in \omega\}$. If $\Sigma_0 \subseteq \Sigma$ is finite, then $\Sigma_0 \subseteq T \cup \left\{\mathsf{S}^{(n)}(\overline{0}) < \boldsymbol{c} \mid n < k\right\}$ for some $k \in \omega$. If $\mathcal{N}$ is a model of T then let $\mathcal{N}'$ be its expansion to $\mathcal{L}'$ where we assign to $\boldsymbol{c}$ the value $\big(\mathsf{S}^{(k)}(\bar{0})\big)^{\mathcal{N}}$. Then $\mathcal{N}' \vDash \Sigma_0$ and since Σ_0 is arbitrary, it follows that Σ is finitely satisfiable. By compactness there is an $\mathcal{L}'$-structure $\mathcal{M}'$ such that $\mathcal{M}' \vDash \Sigma$, hence its reduction $\mathcal{M} = \mathcal{M}' \restriction \mathcal{L}$ is a non-standard model of T. □

Remark 32.4. By Theorem 32.3 there are countable non-standard models of PA, and by a result of Tennenbaum's a countable non-standard model of PA is not computable. Therefore there exist effectively axiomatizable theories that have countable models, but without computable models.

32.C. The finite Ramsey Theorem. In Section 29 we proved Ramsey's Theorem 29.1 in the infinite case: for every infinite set A, if the elements of $[A]^r$ are colored with k many colors, then there is an infinite $H \subseteq A$ such that $[H]^r$ is monochromatic. By the Compactness Theorem we can prove its finite version.

Theorem 32.5 (Ramsey's Theorem in the finite case)**.** *For all $r, k, n > 0$ there is m such that every coloring $f\colon [m]^r \to k$ has a monochromatic subset $H \subseteq m$ of cardinality n.*

Proof. For ease of notation assume $r = 2$. Fix $k \geq 2$. Consider the language $\mathcal{L}$ with k many 2-ary predicate symbols $\boldsymbol{C}_0, \dots, \boldsymbol{C}_{k-1}$ that represent the colors. Consider the set of sentences asserting that every unordered pair is colored with a single color and that there are infinitely many elements:

(i) $\forall \boldsymbol{x} \forall \boldsymbol{y}\, (\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \Rightarrow \boldsymbol{C}_h(\boldsymbol{y}, \boldsymbol{x}))$, for all $h < k$,

(ii) $\forall \boldsymbol{x} \forall \boldsymbol{y} \left(\boldsymbol{x} \neq \boldsymbol{y} \Rightarrow \bigvee_{h \leq k} \boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y})\right)$,

(iii) $\neg \exists \boldsymbol{x} \exists \boldsymbol{y}\, (\boldsymbol{C}_h(\boldsymbol{x}, \boldsymbol{y}) \wedge \boldsymbol{C}_i(\boldsymbol{x}, \boldsymbol{y}))$, for all $h < i < k$,

(iv) $\boldsymbol{\varepsilon}_{\geq n}$, for $n > 1$, where $\boldsymbol{\varepsilon}_{\geq n}$ is the statement defined on page 18.

By (iv) if an $\mathcal{L}$-structure $\mathcal{A} = \langle A, \boldsymbol{C}_0^{\mathcal{A}}, \dots, \boldsymbol{C}_{k-1}^{\mathcal{A}} \rangle$ satisfies Σ then A is infinite, and setting $\bar{C}_i = \{\{x, y\} \in [A]^2 \mid (x, y) \in \boldsymbol{C}_i^{\mathcal{A}}\}$, the sets $\bar{C}_0, \dots, \bar{C}_{k-1}$ are pairwise disjoint and $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$. Conversely, if A is infinite and $[A]^2$ is colored with k many colors, that is there are $\bar{C}_0, \dots, \bar{C}_{k-1}$ pairwise disjoint subsets of A such that $\bar{C}_0 \cup \dots \cup \bar{C}_{k-1} = [A]^2$, then letting $\boldsymbol{C}_i^{\mathcal{A}} = \{(x, y) \mid \{x, y\} \in \bar{C}_i\}$ one has that $\mathcal{A} \vDash \Sigma$. Fix a model $\mathcal{A}$ of Σ. By the infinite Ramsey Theorem 29.1 there is an infinite homogeneous subset of A. For any given n, $\mathcal{A}$ satisfies the statement $\boldsymbol{\varphi}_n$ saying:

($\boldsymbol{\varphi}_n$) There are distinct elements $\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}$ such that $[\{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{n-1}\}]^2$ is monocrhomatic of color $\boldsymbol{C}_h$, for some $h < k$

in symbols

$$\exists \boldsymbol{x}_0 \dots \exists \boldsymbol{x}_{n-1} \Big[\bigwedge_{i<j<n} \boldsymbol{x}_i \neq \boldsymbol{x}_j \wedge \big(\bigvee_{h<k} \bigwedge_{i<j<n} \boldsymbol{C}_h(\boldsymbol{x}_i, \boldsymbol{x}_j) \big) \Big].$$

As $\mathcal{A} \in \mathrm{Mod}(\Sigma)$ is arbitrary, this proves that $\Sigma \models \boldsymbol{\varphi}_n$ for every n. By compactness, given n there is a finite $\Sigma' \subset \Sigma$ such that $\Sigma' \models \boldsymbol{\varphi}_n$. Let m be largest such that $\boldsymbol{\varepsilon}_{\geq m} \in \Sigma'$. A coloring of $[m]^2$ with k colors induces a model $\mathcal{A}'$ of Σ' of size m. As $\mathcal{A}' \vDash \boldsymbol{\varphi}_n$, there is a monochromatic $H \subset m$ of size n. □

32.D. Further applications*.

32.D.1. *Proof of Proposition 11.16.* Since isomorphic structures can be identified, Proposition 11.16 follows form the next result.

Proposition 32.6. *Let $\mathcal{L}$ be a language with at least one constant symbol $\boldsymbol{c}$, let T be an $\mathcal{L}$-theory, and let $\boldsymbol{\varphi}(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ be an $\mathcal{L}$-formula that is conjunction of atomic and negated atomic formulæ. The following are equivalent:*

(a) *there is a quantifier-free $\mathcal{L}$-formula $\boldsymbol{\theta}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ with the same free variables as $\boldsymbol{\exists y \varphi}$ such that*

$$T \models \boldsymbol{\forall \vec{x}}[\boldsymbol{\exists y \varphi} \Leftrightarrow \boldsymbol{\theta}]$$

(b) *if M and N are models of T and K is an $\mathcal{L}$-structures contained in $M \cap N$, then*

$$M \vDash \boldsymbol{\exists y \varphi}[a_1, \dots, a_n] \Leftrightarrow N \vDash \boldsymbol{\exists y \varphi}[a_1, \dots, a_n],$$

for all $a_1, \dots, a_n \in K$.

Proof. The only non-trivial direction is (b)⇒(a). Suppose $\varphi(y, x_1, \dots, x_n)$ is as above. If $T \models \boldsymbol{\forall \vec{x} \exists y \varphi}$, then take $\boldsymbol{\theta}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ to be $\boldsymbol{x}_1 = \boldsymbol{x}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{x}_n = \boldsymbol{x}_n$, if $n \geq 1$, or $\boldsymbol{c} = \boldsymbol{c}$ otherwise. Similarly, if $T \models \boldsymbol{\forall \vec{x} \neg \exists y \varphi}$, then take $\boldsymbol{\theta}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ to be $\boldsymbol{x}_1 \neq \boldsymbol{x}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{x}_n \neq \boldsymbol{x}_n$, if $n \geq 1$, or $\boldsymbol{c} \neq \boldsymbol{c}$ otherwise. Therefore we may assume that

finish

□

32.D.2. *Lefschetz's principle.*

Theorem 32.7. *For every $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L}_{\textsc{Rings}})$, the following are equivalent:*

(1) $\mathrm{ACF}_0 \models \boldsymbol{\sigma}$.

(2) $\boldsymbol{\sigma}$ *holds in some algebraically closed field of characteristic* 0.

(3) $\boldsymbol{\sigma}$ *holds in every algebraically closed field of sufficiently large finite characteristic, that is* $\exists n \forall p > n\ \mathrm{ACF}_p \models \boldsymbol{\sigma}$.

(4) $\forall n \exists p > n\, \exists \mathbb{F} (\mathbb{F} \vDash \mathrm{ACF}_p \wedge \boldsymbol{\sigma})$.

Proof. Conditions (1) and (2) are equivalent, since ACF_0 is complete. If (1) holds, then by compactness $\mathrm{ACF}_p \models \boldsymbol{\sigma}$ for all sufficiently large primes p, so

(3) holds. Since (3) implies (4) trivially, it is enough to show that (4) implies (2). Choose primes p_n and fields $\mathbb{F}_n$ such that $p_n < p_{n+1}$ and $\mathbb{F}_n \vDash \mathrm{ACF}_{p_n} \wedge \boldsymbol{\sigma}$. Let U be an ultrafilter on ω such that $\{p_n \mid n \in \omega\} \in U$. Then $\mathbb{F} = \prod_U \mathbb{F}_n$ satisfies $\boldsymbol{\sigma}$ and $\operatorname{char} \mathbb{F} = 0$. □

32.D.3. *Rings of algebraic integers.*

Theorem 32.8. *Let R be an integral domain such that any element belongs to finitely many prime ideals, if any.*[4] *Let $\boldsymbol{\sigma}$ be a statement of $\mathcal{L}_{\mathrm{CRings}} \cup \{\mathring{a} \mid a \in R\}$. Then $\boldsymbol{\sigma}$ holds in every field extending R if and only if $\boldsymbol{\sigma}$ holds in every fields extending R/I, for all but finitely many prime ideals I.*

Proof. The theorem is trivially true if R has finitely many prime ideals, so assume otherwise. By assumption $\Sigma_{\mathrm{Flds}} \cup \mathrm{Diag}(R) \models \boldsymbol{\sigma}$, so by compactness there are $\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n \in \mathrm{Diag}(R)$ such that $\Sigma_{\mathrm{Flds}} \cup \{\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n\} \models \boldsymbol{\sigma}$. The statements $\boldsymbol{\tau}_i$ are either atomic formulæ, that is of the form

$$\mathring{a} \doteq \mathring{b}, \quad \mathring{a} \dotplus \mathring{b} \doteq \mathring{c}, \quad \mathring{a} \mathbin{\dot{\cdot}} \mathring{b} \doteq \mathring{c}$$

with $a, b, c \in R$, or else they are negated atomic formulæ. Note that the formula $\neg(\mathring{a} \dotplus \mathring{b} \doteq \mathring{c})$ is logical consequence of the formulæ $\mathring{a} \dotplus \mathring{b} \doteq \mathring{d}$ and $\neg(\mathring{c} \doteq \mathring{d})$, where $d = a + b \in R$; similarly $\neg(\mathring{a} \mathbin{\dot{\cdot}} \mathring{b} \doteq \mathring{c})$ is logical consequence of the two formulæ $\mathring{a} \mathbin{\dot{\cdot}} \mathring{b} \doteq \mathring{d}$ and $\neg(\mathring{c} \doteq \mathring{d})$, where $d = a \cdot b \in R$. Finally formulæ of the form $\neg(\mathring{a} \doteq \mathring{b})$ with $a, b \in R \setminus \{0_R\}$ are logical consequence of $\neg(\mathring{c} \doteq \mathbf{0})$, with $c = a - b \in R \setminus \{0_R\}$. Therefore we may assume that the statements $\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n$ are either positive or else of the form $\neg(\mathring{a} \doteq \mathbf{0})$ with $a \in R \setminus \{0_R\}$. Let $a_1, \dots, a_m$ be the non-zero elements of R such that $\mathring{a}_1, \dots, \mathring{a}_n$ are the constants occurring in the $\boldsymbol{\tau}_i$. By assumption, there is a finite number, possibly zero, of prime ideals I that contain $\{a_1, \dots, a_m\}$. Given such an ideal, let $\pi \colon R \to R/I$ be the canonical projection: this preserves the positive statements, and since $\pi(a_j) \neq 0_{R/I}$ it also preserves statements of the form $\neg(\mathring{a} \doteq \mathbf{0})$. Then R/I, or better: its canonical expansion to the language $\mathcal{L}_{\mathrm{CRings}} \cup \{\mathring{a} \mid a \in R\}$, satisfies $\{\boldsymbol{\tau}_1, \dots, \boldsymbol{\tau}_n\}$, whence every field extending it satisfies $\boldsymbol{\sigma}$. □

Recall that a polynomial $f \in R[X_1, \dots, X_n]$ is irreducible on R if it cannot be factorized as $f = g \cdot h$, with non-constant $g, h \in R[X_1, \dots, X_n]$. It f is irreducible on every field extending R we say that it is absolutely irreducible on R.

Corollary 32.9. *Let R be an integral domain such that every element belongs to finitely many prime ideals, if any, and suppose that $f \in R[X_1, \dots, X_n]$ is absolutely irreducible on R. Then f is absolutely irreducible on R/I, for all but finitely many prime ideals I.*

[4] For example, the ring of algebraic integers of an extension of the rationals.

Proof. It is enough to check that the property "f is irreducible" is formalizable as a statement of $\mathcal{L}_{\mathrm{CRings}} \cup \{\mathring{a} \mid a \in R\}$: for every pair (d_1, d_2) such that $d = d_1 + d_2$ and $1 \leq d_1, d_2$, consider the statement $\boldsymbol{\sigma}_{(d_1,d_2)}$ asserting that f cannot be factorized in polynomials od degree d_1 and d_2, then take the conjunction of these statements. □

Exercises

Exercise 32.10. Use Hall's Theorem 14.26 to prove that the following are consequences of BPI.

(i) Two bases of a vector space are in bijection.

(ii) Two transcendence bases of a field are in bijection.

(iii) If $\mathcal{A}$ is a family of non-empty finite sets such that $|A_1 \cup \cdots \cup A_n| \geq n$ for any choice of distinct $A_1, \ldots, A_n \in \mathcal{A}$, then there is an injective choice function $f \colon \mathcal{A} \to \bigcup \mathcal{A}$.

Exercise 32.11. Show that there is $\mathcal{A}$ a countable family of countable sets such that $|A_1 \cup \cdots \cup A_n| \geq n$ for distinct $A_1, \ldots, A_n \in \mathcal{A}$, and yet there is no injective choice function. (Contrast this with Exercise 32.10(iii).) Use this to construct a bipartite graph $\langle A \uplus B, E \rangle$ such that $|A| = |B| = \omega$ and $n + 1 \leq |\{b \in B \mid \exists i \leq n\,(b \mathrel{E} a_i)\}|$ for distinct $a_0, \ldots, a_n \in A$, and yet there is no injective $f \colon A \to B$ such that $\forall a \in A\,(a \mathrel{E} f(a))$.

Exercise 32.12. Show that relation of logical consequence is a pre-order on $\mathscr{P}(\mathrm{Sent}(\mathcal{L}))$ whose minimal elements are unsatisfiable theories.

Exercise 32.13. Use the Compactness Theorem to show that:

(i) An abelian group is orderable (see page **??**) if and only if any of its finitely generated subgroup is orderable.

(ii) A graph is k-colorable if and only if any its finite subgraph is k-colorable.

(iii) An ordered set is the union of $\leq k$ chains if and only if every finite suborder is the union of $\leq k$ chains, where $1 \leq k < \omega$. Prove a similar result with "independent set" instead of "chain" (see page 43 for the definition of independent set).

Exercise 32.14. Let $\langle P, \leq \rangle$ be an ordered set.

(i) Show that if P is the union of n chains, then every independent subset of P has size $\leq n$.

(ii) Dilworth proved the converse of (i) for *finite* orders: If P is finite and every independent subset has cardinality $\leq n$, then there are chains $C_0, \ldots, C_{n-1} \subseteq P$ such that $\bigcup_{i<n} C_i = P$.

Generalize this to arbitrary orders.

Exercise 32.15. Recall (see page 102) that a total order is homogeneous if given two elements a, b of the order there is an automorphism mapping a to b; it is ultrahomogeneous if any partial isomorphism between two finite subsets of the same size can be extended to an automorphism. Use Exercise 4.90 to show that the classes of total orders that are homogeneous and those that are ultrahomogeneous are, respectively, PC and PC_Δ but not EC_Δ in the language $\mathcal{L}_{\mathrm{ORDR}}$.

Exercise 32.16. Suppose $\langle P, \leq\rangle$ is an ordered set with chains of length $\geq n$, for each $n \in \omega$. Show that there is an ordered set $\langle P^*, \leq^*\rangle$ which is ill-founded and such that $\langle P, \leq\rangle \preccurlyeq \langle P^*, \leq^*\rangle$ and $|P| = |P^*|$. In particular, the class of well-founded orders is not PC_Δ.

Exercise 32.17. Let U be an ultrafilter on a set $I \neq \emptyset$ and let $\mathcal{A}_i \in \mathrm{Str}(\mathcal{L})$, with $i \in I$. Show that if $\mathcal{L}' \subseteq \mathcal{L}$ then

$$\bigl(\prod_U \mathcal{A}_i\bigr) \restriction \mathcal{L}' = \prod_U \bigl(\mathcal{A}_i \restriction \mathcal{L}'\bigr) .$$

Conclude that a PC_Δ class is closed under ultraproducts.

Exercise 32.18. Show that every ordered field has a non-Archimedean elementary extension.

Exercise 32.19. Prove the infinite Ramsey's Theorem 29.1 from its finite version (Theorem 32.5).

Exercise 32.20. Show that an abelian group is simple if it is isomorphic to $\mathbb{Z}(p)$ for some prime p. Conclude that the class of simple groups is not PC_Δ.

Exercise 32.21. Show that the class of connected graphs is not axiomatizable.

Exercise 32.22. Show that if Σ is a set of sentences in an arbitrary language which has finite models of arbitrarily large cardinality, then it has a model $\mathcal{M}$ whose universe is the surjective image of $\mathbb{R}$. Therefore assuming AC (or even just that $\mathbb{R}$ is well-orderable) $\operatorname{card} \mathcal{M} \leq 2^{\aleph_0}$.

Give an example of a theory (in a necessarily uncountable language) with finite models of arbitrarily large size, that has a model of cardinality of the continuum, but has no infinite model of size strictly less than the cardinality of $\mathbb{R}$.

Exercise 32.23. Let T be a theory in the language $\mathcal{L}' \supseteq \mathcal{L}$. Show that $\mathcal{M} \in \mathrm{Str}(\mathcal{L})$ is embeddable in a model of T if and only if every finitely generated substructure of $\mathcal{M}$ is embeddable in a model of T.

Exercise 32.24. Show that if $f_1, \ldots, f_n \in \mathbb{Q}[x_1, \ldots, x_m]$ the system

$$\begin{cases} f_1(x_1, \ldots, x_m) \\ \vdots \\ f_n(x_1, \ldots, x_m) \end{cases}$$

has at most k solutions in an extension of $\mathbb{Q}$ if and only if the system has at most k solutions in field of characteristic p, for all but finitely many primes p.

Repeat the exercise when *at most* is replaced by *exactly* and by *at least*.

Exercise 32.25. (i) Show that a graph with vertices with arbitrarily high degree is elementarily embeddable in a graph containing a degree with infinite order.

(ii) A graph is **locally finite** if every vertex has finite degree. Show that the class of locally finite graphs is not PC_Δ.

33. Syntax

33.A. Derivations. A **logical axiom** for a language $\mathcal{L}$ is an $\mathcal{L}$-sentence that is either a tautology axiom, or else an equality axiom (Section 31.D.2), or else an axiom for quantification (Section 31.D.3). The set of all logical axioms for $\mathcal{L}$ is $\mathrm{LAx}(\mathcal{L})$. Let us recall the ***Modus Ponens* rule**, first seen on page 9: infer $\boldsymbol{\varphi}$ from $\boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi}$ and $\boldsymbol{\psi}$, in symbols

$$\text{(MP)} \qquad \frac{\boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi} \qquad \boldsymbol{\psi}}{\boldsymbol{\varphi}} \, .$$

In what follows Σ is an $\mathcal{L}$-theory, for some fixed $\mathcal{L}$.

Definition 33.1. The set of all **theorems of** Σ is the smallest subset $\mathrm{Thm}(\Sigma)$ of $\mathrm{Sent}(\mathcal{L})$ containing $\Sigma \cup \mathrm{LAx}(\mathcal{L})$, and closed under (MP).

We write $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\varphi}$ for $\boldsymbol{\varphi} \in \mathrm{Thm}(\Sigma)$. In order to say that a sentence $\boldsymbol{\varphi}$ is a theorem of Σ we need to derive $\boldsymbol{\varphi}$ from Σ.

Definition 33.2. A **derivation from** Σ is a finite sequence of $\mathcal{L}$-sentences $\langle \boldsymbol{\varphi}_0, \ldots, \boldsymbol{\varphi}_n \rangle$ such that for all $i \leq n$:

(1) $\boldsymbol{\varphi}_i \in \Sigma \cup \mathrm{LAx}(\mathcal{L})$, or else

(2) there are $j, k < i$ such that $\boldsymbol{\varphi}_i$ is obtained from $\boldsymbol{\varphi}_j$ and $\boldsymbol{\varphi}_k$ via (MP).

A sentence $\boldsymbol{\sigma}$ is **derivable from** Σ if there is a derivation $\langle \boldsymbol{\varphi}_0, \ldots, \boldsymbol{\varphi}_n \rangle$ from Σ such that $\boldsymbol{\sigma} = \boldsymbol{\varphi}_n$.

Therefore $\boldsymbol{\sigma}$ is derivable from Σ if and only if $\boldsymbol{\sigma} \in \mathrm{Thm}(\Sigma) = \bigcup_{n \in \omega} \Sigma_n$ where

$$\begin{aligned}\Sigma_0 &= \Sigma \cup \mathrm{LAx}(\mathcal{L})\\ \Sigma_{n+1} &= \Sigma_n \cup \{\boldsymbol{\varphi} \mid \exists \boldsymbol{\psi}\, (\boldsymbol{\psi} \in \Sigma_n \wedge \boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi} \in \Sigma_n)\}.\end{aligned}$$

Note that an initial segment of a derivation from Σ is still a derivation from Σ. When the language $\mathcal{L}$ is clear from the context, we just write $\Sigma \vdash \boldsymbol{\varphi}$; if $\Sigma = \{\boldsymbol{\psi}\}$ or $\Sigma = \emptyset$, we write, respectively, $\boldsymbol{\psi} \vdash \boldsymbol{\varphi}$ and $\vdash \boldsymbol{\varphi}$.

Remarks 33.3. (a) If $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\sigma}$, and $\Sigma \subseteq \Sigma' \subseteq \mathrm{Sent}(\mathcal{L}')$ with $\mathcal{L}' \supseteq \mathcal{L}$, then $\Sigma' \vdash_{\mathcal{L}'} \boldsymbol{\sigma}$.

(b) The relation $\vdash$ is transitive: if $\Sigma \vdash \boldsymbol{\sigma}$ and $\boldsymbol{\sigma} \vdash \boldsymbol{\tau}$, then $\Sigma \vdash \boldsymbol{\tau}$.

(c) $\Sigma \vdash \boldsymbol{\sigma}$ if and only if $\Sigma_0 \vdash \boldsymbol{\sigma}$ for some finite $\Sigma_0 \subseteq \Sigma$.

By 31.D.3, 31.D.2 and by Corollary 31.10, every logical axiom is valid.

The following **Soundness Theorem** shows that derivations yield logical consequences.

Theorem 33.4. *If* $\Sigma \cup \{\boldsymbol{\sigma}\} \subseteq \mathrm{Sent}$, *then* $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow \Sigma \models \boldsymbol{\sigma}$.

Proof. Suppose $\mathcal{A} \vDash \Sigma$ and let $\langle \boldsymbol{\varphi}_0, \ldots, \boldsymbol{\varphi}_n \rangle$ be a derivation from Σ. It is enough to check by induction on $i \leq n$ that $\mathcal{A} \vDash \boldsymbol{\varphi}_i$. If $\boldsymbol{\varphi}_i$ is a logical axiom or else $\boldsymbol{\varphi}_i \in \Sigma$ the result is immediate, hence we may assume that $\boldsymbol{\varphi}_i$ is obtained via (MP) from $\boldsymbol{\varphi}_j$ and $\boldsymbol{\varphi}_k = \boldsymbol{\varphi}_j \Rightarrow \boldsymbol{\varphi}_i$ for $j, k < i$. Then $\mathcal{A} \vDash \boldsymbol{\varphi}_j$ and $\mathcal{A} \vDash \boldsymbol{\varphi}_j \Rightarrow \boldsymbol{\varphi}_i$ by inductive assumption, so $\mathcal{A} \vDash \boldsymbol{\varphi}_i$. □

33.B. Derived inference rules. In the official definition of derivation only the *Modus Ponens* rule is allowed, but several other rules, called *derived rules*, can be used inside a derivation. These derived rules are just abbreviations for longer arguments using (MP).

Tautological consequence rule. If $\boldsymbol{\varphi}$ is tautological consequence of $\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_n$, then $\boldsymbol{\varphi}$ is obtained from $\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_n$, that is to say: if $\Sigma \vdash \boldsymbol{\psi}_1, \ldots, \Sigma \vdash \boldsymbol{\psi}_n$, then $\Sigma \vdash \boldsymbol{\varphi}$.

Proof. Saying that $\boldsymbol{\varphi}$ is tautological consequence of $\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_n$ amounts to saying that $\boldsymbol{\psi}_1 \Rightarrow (\boldsymbol{\psi}_2 \Rightarrow \ldots (\boldsymbol{\psi}_n \Rightarrow \boldsymbol{\varphi}) \ldots)$ is a tautology, so $\boldsymbol{\varphi}$ follows from repeated applications of (MP). □

As $\boldsymbol{\varphi}_0 \wedge \boldsymbol{\varphi}_1$ is tautological consequence of $\boldsymbol{\varphi}_0, \boldsymbol{\varphi}_1$ and since $\boldsymbol{\varphi}_i$ is tautological consequence of $\boldsymbol{\varphi}_0 \wedge \boldsymbol{\varphi}_1$ we obtain

Conjunction rule. $\Sigma \vdash \boldsymbol{\varphi}$ and $\Sigma \vdash \boldsymbol{\psi}$ if and only if $\Sigma \vdash \boldsymbol{\varphi} \wedge \boldsymbol{\psi}$.

As $\boldsymbol{\psi}$ is tautological consequence of $\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ and $\neg \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ one has the:

Proof-by-cases rule. If $\Sigma \vdash \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ and $\Sigma \vdash \neg\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ then $\Sigma \vdash \boldsymbol{\psi}$.

As $\boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ is tautologically equivalent to $\neg\boldsymbol{\psi} \Rightarrow \neg\boldsymbol{\varphi}$ one has the:

Contraposition rule. $\Sigma \vdash \boldsymbol{\varphi} \Rightarrow \boldsymbol{\psi}$ if and only if $\Sigma \vdash \neg\boldsymbol{\psi} \Rightarrow \neg\boldsymbol{\varphi}$.

$\forall$-elimination rule. If $\Sigma \vdash \forall \boldsymbol{x}_1 \dots \forall \boldsymbol{x}_n \boldsymbol{\varphi}$ and $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$ are closed terms, then $\Sigma \vdash \boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$.

Proof. Suppose $n = 1$. By the contraposition rule applied to the type (B) axiom for quantification $\neg\boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!) \Rightarrow \exists \boldsymbol{x} \neg\boldsymbol{\varphi}$, we have $\vdash \neg\exists\boldsymbol{x}\neg\boldsymbol{\varphi} \Rightarrow \neg\neg\boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$. By the tautological consequence rule and by definition of $\forall$, we have that $\vdash \forall\boldsymbol{x}\boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$, so if $\Sigma \vdash \forall\boldsymbol{x}\boldsymbol{\varphi}$ then $\Sigma \vdash \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$.

The case $n > 1$ follows by induction and by the fact that since $\boldsymbol{t}_1, \dots, \boldsymbol{t}_n$ are closed, then $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!) = (\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_{n-1}/\boldsymbol{x}_{n-1}|\!))(\!|\boldsymbol{t}_n/\boldsymbol{x}_n|\!)$. □

Remark 33.5. By Remark 31.11(b), the $\forall$-elimination rule applies also when $\boldsymbol{\varphi}$ is a sentence, so that $\Sigma \vdash \forall\boldsymbol{x}_1 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi} \Rightarrow \Sigma \vdash \boldsymbol{\varphi}$.

Since $\boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!) \Rightarrow \exists\boldsymbol{x}_1 \dots \exists\boldsymbol{x}_n\boldsymbol{\varphi}$ is a type (B) axiom for quantification, then by (MP) we have at once the:

$\exists$-introduction rule. If $\Sigma \vdash \boldsymbol{\varphi}(\!|\boldsymbol{t}_1/\boldsymbol{x}_1, \dots, \boldsymbol{t}_n/\boldsymbol{x}_n|\!)$ then $\Sigma \vdash \exists\boldsymbol{x}_1 \dots \exists\boldsymbol{x}_n\boldsymbol{\varphi}$.

Dummy quantifiers rule. Suppose that $\boldsymbol{\varphi} \in \mathrm{Sent}$. Then $\Sigma \vdash \boldsymbol{\varphi}$ if and only if $\Sigma \vdash \forall\boldsymbol{x}_1 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi}$ if and only if $\Sigma \vdash \exists\boldsymbol{x}_1 \dots \exists\boldsymbol{x}_n\boldsymbol{\varphi}$.

Proof. Suppose $\Sigma \vdash \boldsymbol{\varphi}$: by repeated applications of (MP) to the type (A) axioms for quantification

$$\boldsymbol{\varphi} \Rightarrow \forall\boldsymbol{x}_n\boldsymbol{\varphi}, \quad \forall\boldsymbol{x}_n\boldsymbol{\varphi} \Rightarrow \forall\boldsymbol{x}_{n-1}\forall\boldsymbol{x}_n\boldsymbol{\varphi}, \quad \dots \quad \forall\boldsymbol{x}_2 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi} \Rightarrow \forall\boldsymbol{x}_1 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi}$$

one has $\Sigma \vdash \forall\boldsymbol{x}_1 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi}$. The converse implication follows from the $\forall$-elimination rule, so $\Sigma \vdash \boldsymbol{\varphi}$ if and only if $\Sigma \vdash \forall\boldsymbol{x}_1 \dots \forall\boldsymbol{x}_n\boldsymbol{\varphi}$.

The other equivalence is left to the reader. □

Lemma 33.6. *If* $\Sigma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\varphi}$ *then* $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}$.

Proof. Suppose $\langle \boldsymbol{\varphi}_0, \dots, \boldsymbol{\varphi}_n \rangle$ is a derivation of $\boldsymbol{\varphi}$ from $\Sigma \cup \{\boldsymbol{\sigma}\}$. We prove by induction on $i \leq n$ that $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$. We take cases:

- If $\boldsymbol{\varphi}_i \in \Sigma \cup \mathrm{LAx}(\mathcal{L})$, then $\langle \boldsymbol{\varphi}_i \Rightarrow (\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i), \boldsymbol{\varphi}_i, \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i \rangle$ is a derivation in Σ.
- If $\boldsymbol{\varphi}_i = \boldsymbol{\sigma}$ then $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ is a tautology, hence it is derivable.
- If $\boldsymbol{\varphi}_i$ follows by (MP) from $\boldsymbol{\varphi}_m$ and $\boldsymbol{\varphi}_k$, where $m, k < i$ and $\boldsymbol{\varphi}_k$ is $\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i$, then by inductive assumption $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_m$ and $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow (\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i)$. As $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ is tautological consequence of $\boldsymbol{\sigma} \Rightarrow (\boldsymbol{\varphi}_m \Rightarrow \boldsymbol{\varphi}_i)$ and of $\boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_m$, then $\Sigma \vdash \boldsymbol{\sigma} \Rightarrow \boldsymbol{\varphi}_i$ by the rule of tautological consequence.

Therefore $\Sigma \vdash \sigma \Rightarrow \varphi_i$ for all $i \leq n$, as required. □

In mathematics, when proving $\forall x \varphi(x)$ one usually argues as follows: take a generic element c and show that φ holds for c; as c is arbitrary, one obtains $\forall x \varphi(x)$. The next result justifies the correctness of this argumentation.

Theorem 33.7. *Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$, let φ be an $\mathcal{L}$-formula with exactly one free variable x, and let c be a new constant symbol. Then*

$$\Sigma \vdash_{\mathcal{L}} \forall x \varphi \Leftrightarrow \Sigma \vdash_{\mathcal{L} \cup \{c\}} \varphi(\!|c/x|\!).$$

Proof. If $\Sigma \vdash_{\mathcal{L}} \forall x \varphi$ then $\Sigma \vdash_{\mathcal{L} \cup \{c\}} \forall x \varphi$, and hence $\Sigma \vdash_{\mathcal{L} \cup \{c\}} \varphi(\!|c/x|\!)$ by the $\forall$-elimination rule.

Conversely, suppose $\langle \psi_0, \dots, \psi_n \rangle$ witnesses that $\Sigma \vdash_{\mathcal{L} \cup \{c\}} \varphi(\!|c/x|\!)$. By taking a subset of Σ if needed, we may assume that every sentence in Σ is used in this derivation, that is $\Sigma \subseteq \{\psi_0, \dots, \psi_n\}$. Pick a variable y that does not occur in any ψ_i, and let $\psi'_i = \psi_i[y/x]$ be the expression obtained from ψ_i by replacing x with y. Then each ψ'_i is an $\mathcal{L} \cup \{c\}$-sentence, and let $\Sigma' = \{\psi'_i \mid \psi_i \in \Sigma\}$.

Claim 33.7.1. *$\langle \psi'_0, \dots, \psi'_n \rangle$ is a derivation from Σ' in $\mathcal{L} \cup \{c\}$ of $\varphi(\!|c/x|\!)$.*

Proof. If $\psi_i \in \Sigma$, then $\psi'_i \in \Sigma'$. If ψ_i is either an equality axiom, or a tautology axiom, or else an axiom for quantification then ψ'_i is an axiom of the same kind. If ψ_i is obtained via (MP) from ψ_j and $\psi_k = \psi_j \Rightarrow \psi_i$ with $j, k < i$ then by inductive assumption $\Sigma' \vdash_{\mathcal{L} \cup \{c\}} \psi'_j$ and $\Sigma' \vdash_{\mathcal{L} \cup \{c\}} \psi'_j \Rightarrow \psi'_i$, so $\Sigma' \vdash_{\mathcal{L} \cup \{c\}} \psi'_i$ by (MP).

Finally observe that $\psi'_n = \psi_n = \varphi(\!|c/x|\!)$. □

Letting $\varphi_i = \psi'_i[x/c]$, each φ_i is an $\mathcal{L}$-formula, and $\varphi_n = \varphi$.

Claim 33.7.2. *$\Sigma' \vdash_{\mathcal{L}} \forall x \varphi_i$, for $i \leq n$.*

Proof. If $\psi'_i \in \Sigma'$, then c does not occur in it so $\varphi_i = \psi'_i$, and since $\varphi_i \Rightarrow \forall x \varphi_i$ is a type (A) axiom for quantification, then $\Sigma' \vdash \forall x \varphi_i$. If ψ'_i is a logical axiom of some kind (tautology, equality, quantification), then $\forall x \varphi_i$ is a logical axiom of the same kind, so $\Sigma' \vdash \forall x \varphi_i$. If ψ'_i follows by (MP) from ψ'_j and $\psi_k = \psi'_j \Rightarrow \psi'_i$ with $j, k < i$, then by inductive hypothesis $\Sigma' \vdash_{\mathcal{L}} \forall x \varphi_j$ and $\Sigma' \vdash_{\mathcal{L}} \forall x(\varphi_j \Rightarrow \varphi_i)$, and since $\forall x(\varphi_j \Rightarrow \varphi_i) \Rightarrow (\forall x \varphi_j \Rightarrow \forall x \varphi_i)$ is a type (D) axiom for quantification, then $\Sigma' \vdash_{\mathcal{L}} \forall x \varphi_i$ by (MP). □

Finally, if $\langle \tau'_0, \dots, \tau'_m \rangle$ witnesses that $\Sigma' \vdash_{\mathcal{L}} \forall x \varphi$, then $\langle \tau_0, \dots, \tau_m \rangle$ witnesses that $\Sigma \vdash_{\mathcal{L}} \forall x \varphi$ where $\tau_i = \tau'_i[x/y]$. □

Corollary 33.8. *If $\Sigma \cup \{\sigma\} \subseteq \mathrm{Sent}(\mathcal{L})$ and c is a new symbol for a constant, then $\Sigma \vdash_{\mathcal{L} \cup \{c\}} \sigma$ if and only if $\Sigma \vdash_{\mathcal{L}} \sigma$.*

Proof. If $\Sigma \vdash_{\mathcal{L}\cup\{\boldsymbol{c}\}} \boldsymbol{\sigma}$ then $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\forall x \sigma}$, so that $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\sigma}$ by the $\boldsymbol{\forall}$-elimination rule and Remark 33.5.

The other implication is trivial. □

33.C. Consistency. We say that $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is **inconsistent** if $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\varphi}$ and $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\neg\varphi}$ for some sentence $\boldsymbol{\varphi}$; otherwise Σ is **consistent**. Equivalently, by the conjunction rule, Σ is consistent if and only if $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\varphi \wedge \neg\varphi}$ for some statement $\boldsymbol{\varphi}$. As every sentence is tautological consequence of a propositional contradiction, Σ is inconsistent if and only $\mathrm{Sent} = \mathrm{Thm}(\Sigma)$.

Proposition 33.9. *Let* $\Sigma \cup \{\boldsymbol{\sigma}\} \subseteq \mathrm{Sent}(\mathcal{L})$.

(a) Σ *is consistent if and only if every finite subset is so;*

(b) *if* $\mathcal{C} \subseteq \mathscr{P}(\mathrm{Sent}(\mathcal{L}))$ *is upward directed under* $\subseteq$ *and if all* $\Sigma \in \mathcal{C}$ *are consistent, then* $\bigcup \mathcal{C}$ *is consistent;*

(c) $\Sigma \cup \{\boldsymbol{\sigma}\}$ *is consistent if and only if* $\Sigma \nvdash \boldsymbol{\neg\sigma}$.

Proof. (a) Any derivation of a contradiction from Σ uses only a finite number of statements from Σ.

(b) If $\bigcup \mathcal{C}$ were inconsistent, then there would be $\boldsymbol{\varphi}_1, \dots, \boldsymbol{\varphi}_n \in \bigcup \mathcal{C}$ such that $\{\boldsymbol{\varphi}_1, \dots, \boldsymbol{\varphi}_n\}$ is inconsistent. Choose $\Sigma_i \in \mathcal{C}$ such that $\boldsymbol{\varphi}_i \in \Sigma_i$, and let $\Sigma \in \mathcal{C}$ containing all Σ_is. Then Σ would be inconsistent.

(c) If $\Sigma \vdash \boldsymbol{\neg\sigma}$, then $\Sigma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\sigma \wedge \neg\sigma}$. Conversely suppose that $\Sigma \cup \{\boldsymbol{\sigma}\}$ is inconsistent: then $\Sigma \cup \{\boldsymbol{\sigma}\} \vdash \boldsymbol{\sigma \wedge \neg\sigma}$. By Lemma 33.6, $\Sigma \vdash \boldsymbol{\sigma \Rightarrow (\sigma \wedge \neg\sigma)}$ hence $\Sigma \vdash \boldsymbol{(\sigma \vee \neg\sigma) \Rightarrow \neg\sigma}$. But $\boldsymbol{\sigma \vee \neg\sigma}$ is a tautology, hence by (MP) $\Sigma \vdash \boldsymbol{\neg\sigma}$. □

If $\Delta \subseteq \mathrm{Sent}(\mathcal{L})$, the relation

$$\boldsymbol{\varphi} \preceq_\Delta \boldsymbol{\psi} \Leftrightarrow \Delta \cup \{\boldsymbol{\varphi}\} \vdash_{\mathcal{L}} \boldsymbol{\psi}$$

is a pre-order on $\mathrm{Sent}(\mathcal{L})$ and the induced equivalence relation $\sim_\Delta$ is called **equi-derivability modulo Δ**, and $\boldsymbol{\varphi} \sim_\Delta \boldsymbol{\psi}$ reads '$\boldsymbol{\varphi}$ and $\boldsymbol{\psi}$ are **equi-derivable modulo Δ**'. Therefore Δ is consistent if and only if the relation $\sim_\Delta$ is non-trivial. If $\Delta \subseteq \Sigma$ then the equivalence relation $\sim_\Delta$ refines $\sim_\Sigma$, that is to say $\boldsymbol{\varphi} \sim_\Delta \boldsymbol{\psi} \Rightarrow \boldsymbol{\varphi} \sim_\Sigma \boldsymbol{\psi}$. By Lemma 33.6,

$$\boldsymbol{\sigma} \sim_\Delta \boldsymbol{\tau} \Leftrightarrow \Delta \vdash (\boldsymbol{\sigma \Leftrightarrow \tau}).$$

The quotient

$$\mathrm{Lnd}_\Delta(\mathcal{L}) = \mathrm{Sent}(\mathcal{L})/{\sim_\Delta}$$

with the induced order is a bounded, complemented, distributive lattice, with the operations $[\boldsymbol{\sigma}] \curlyvee [\boldsymbol{\tau}] = [\boldsymbol{\sigma \vee \tau}]$, $[\boldsymbol{\sigma}] \curlywedge [\boldsymbol{\tau}] = [\boldsymbol{\sigma \wedge \tau}]$, $[\boldsymbol{\sigma}]^* = [\boldsymbol{\neg\sigma}]$. If Δ is consistent, then $\mathbf{1} \neq \mathbf{0}$ so it is a boolean algebra, called the **Lindenbaum**

algebra generated by Δ. When $\Delta = \emptyset$ we simply write $\mathrm{Lnd}(\mathcal{L})$ or Lnd, if $\mathcal{L}$ is clear from the context.

An $\mathcal{L}$-theory Σ is

- **syntactically closed** if $\Sigma = \mathrm{Thm}(\Sigma)$;
- **semantically closed** if $\Sigma \models \boldsymbol{\sigma}$ implies $\boldsymbol{\sigma} \in \Sigma$;
- **syntactically complete** if $\Sigma \vdash \boldsymbol{\sigma} \Leftrightarrow \Sigma \nvdash \boldsymbol{\neg\sigma}$ for every $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L})$;
- **semantically complete** if $\Sigma \models \boldsymbol{\sigma} \Leftrightarrow \Sigma \not\models \boldsymbol{\neg\sigma}$ for every $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L})$.

By the Soundness Theorem 33.4 a semantically closed theory is syntactically closed, and a syntactically complete theory is semantically complete. The converse implications follow from the Completeness Theorem 34.3, so, after this will be proved, we will simply talk of closed/complete theories. (A *semantically complete theory* is what was called a *complete theory* in Definition 3.31 in Section 3.F of Chapter I.) Note that a syntactically/semantically closed theory Σ is syntactically/semantically complete if and only $\boldsymbol{\sigma} \notin \Sigma \Leftrightarrow \boldsymbol{\neg\sigma} \in \Sigma$.

Proposition 33.10. *Suppose* $\Sigma, \Delta \subseteq \mathrm{Sent}(\mathcal{L})$ *and that* Σ *is consistent. Let* $F = \{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Delta\} \subseteq \mathrm{Lnd}_\Sigma$.

(a) $\Sigma \cup \Delta$ *is consistent if and only if the filter generated by* F *is proper.*

(b) *Suppose* $\Delta \supseteq \Sigma$ *is syntactically closed. Then* F *is a filter, and* $[\boldsymbol{\sigma}] \in F$ *implies that* $\boldsymbol{\sigma} \in \Delta$ *for any* $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L})$.

(c) *Suppose* $\Delta \supseteq \Sigma$ *is syntactically closed. Then* Δ *is syntactically complete if and only if* F *is an ultrafilter.*

Proof. (a) The filter generated by F is $\uparrow\{[\bigwedge \Delta_0] \mid \Delta_0 \subseteq \Delta \text{ is finite}\}$. It is proper if and only if there is no finite $\Delta_0 \subseteq \Delta$ such that $\Sigma \cup \Delta_0$ is inconsistent if and only if $\Sigma \cup \Delta$ is consistent, by Proposition 33.9.

(b) If $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \in \Delta$, then $\boldsymbol{\sigma}_1 \boldsymbol{\wedge} \boldsymbol{\sigma}_2 \in \Delta$ by syntactic closure, so $[\boldsymbol{\sigma}_1] \curlywedge [\boldsymbol{\sigma}_2] \in F$. If $\boldsymbol{\sigma} \in \Delta$ and $[\boldsymbol{\sigma}] \leq [\boldsymbol{\tau}]$, then $\Sigma \vdash \boldsymbol{\sigma} \boldsymbol{\Rightarrow} \boldsymbol{\tau}$, so $\Delta \vdash \boldsymbol{\tau}$ by (MP), and hence $[\boldsymbol{\tau}] \in F$. Therefore F is a filter.

Towards a contradiction, suppose $[\boldsymbol{\sigma}] \in F$ and $\boldsymbol{\sigma} \notin \Delta$. Then there is $\boldsymbol{\tau} \in \Delta$ such that $\Sigma \vdash \boldsymbol{\tau} \boldsymbol{\Leftrightarrow} \boldsymbol{\sigma}$, and hence $\Delta \vdash \boldsymbol{\sigma}$ by (MP), so that $\boldsymbol{\sigma} \in \Delta$ by syntactic closure: a contradiction.

(c) By part (b) we have that F is a filter.

Suppose Δ is syntactically complete. Then Δ is consistent, and hence F is proper by part (a); moreover if $[\boldsymbol{\sigma}] \notin F$ then $\boldsymbol{\sigma} \notin \Delta$ so that $\boldsymbol{\neg\sigma} \in \Delta$ and hence $[\boldsymbol{\neg\sigma}] = [\boldsymbol{\sigma}]^* \in F$. Therefore F is an ultrafilter.

Conversely suppose F is an ultrafilter. By part (b), if $\boldsymbol{\sigma} \notin \Delta$ then $[\boldsymbol{\sigma}] \notin F$, so $[\boldsymbol{\neg\sigma}] \in F$, and hence $\boldsymbol{\neg\sigma} \in \Delta$. □

Corollary 33.11. *The map $\Sigma \mapsto \{[\boldsymbol{\sigma}] \mid \boldsymbol{\sigma} \in \Sigma\}$ is a bijection between the set of all syntactically closed and complete $\mathcal{L}$-theories and* $\mathrm{St}(\mathrm{Lnd}(\mathcal{L}))$*.*

From the previous results we obtain at once the next result, known as **Lindenbaum's Lemma**.

Lemma 33.12. *Let $\mathcal{L}$ be a first-order language, and assume* $\mathsf{BPI}(\mathrm{Lnd}(\mathcal{L}))$*. Every consistent set of $\mathcal{L}$-sentences can be extended to a maximal consistent set of $\mathcal{L}$-sentences.*

Note that if $\mathcal{L}$ is well-orderable, then so is $\mathrm{Sent}(\mathcal{L})$ and therefore $\mathrm{Lnd}(\mathcal{L})$ is well-orderable, so that $\mathsf{BPI}(\mathrm{Lnd}(\mathcal{L}))$ holds.

Exercises

Exercise 33.13. Show that:

(i) The Lindenbaum algebra $\mathrm{Lnd}_\Sigma(\mathcal{L})$ is indeed a boolean algebra whenever Σ is consistent.

(ii) If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is consistent and maximal, then it is syntactically closed.

(iii) $\Sigma \subseteq \mathrm{Sent}$ is semantically closed if and only if $\Sigma = \mathrm{Th}(\mathrm{Mod}(\Sigma))$.

Exercise 33.14. Show that $\mathrm{Thm}(\Sigma)$ can be seen as the closure of a suitable induction system $(\mathrm{Sent}, \mathcal{F}, \Sigma)$ (see Section 7.A.1).

Exercise 33.15. For X a topological space, let $\approx$ be the equivalence relation on X defined by $x \approx y \Leftrightarrow \mathrm{Cl}\,\{x\} = \mathrm{Cl}\,\{y\}$.

(i) Describe the open sets of the quotient space $X/{\approx}$ and show that $X/{\approx}$ is T_0.

(ii) Use the Completeness Theorem 34.3 to show that $\mathrm{Str}(\mathcal{L})/{\approx}$ is homeomorphic to $\mathrm{St}(\mathrm{Lnd}(\mathcal{L}))$.

34. The completeness theorem

Proposition 34.1. *If* $\mathrm{Mod}(\Sigma) \neq \emptyset$ *then Σ is consistent. In other words: a satisfiable set of sentences is consistent.*

Proof. Suppose that $\Sigma \subseteq \mathrm{Sent}$ is inconsistent, that is $\Sigma \vdash \boldsymbol{\sigma} \wedge \neg\boldsymbol{\sigma}$. Then $\Sigma \models \boldsymbol{\sigma} \wedge \neg\boldsymbol{\sigma}$, thus if $\mathcal{A}$ is a model of Σ, then $\mathcal{A} \vDash \boldsymbol{\sigma} \wedge \neg\boldsymbol{\sigma}$: a contradiction. Therefore Σ is unsatisfiable. □

The next result shows that the converse of the Soundness Theorem 33.4 and of Proposition 34.1 are equivalent.

Proposition 34.2. *Let $\mathcal{L}$ be a first-order language. The following are equivalent:*

(a) $\forall \Sigma \subseteq \mathrm{Sent}(\mathcal{L}) \bigl(\Sigma$ *is consistent* $\Rightarrow \mathrm{Mod}(\Sigma) \neq \emptyset\bigr)$*;*

(b) $\forall \Sigma \cup \{\boldsymbol{\tau}\} \subseteq \mathrm{Sent}(\mathcal{L}) \bigl(\Sigma \models \boldsymbol{\tau} \Rightarrow \Sigma \vdash \boldsymbol{\tau}\bigr)$

Proof. Assume (a) towards proving (b). We may assume that Σ is consistent, otherwise the proof is trivially true. If $\Sigma \nvdash \boldsymbol{\tau}$ then $\Sigma \cup \{\neg\boldsymbol{\tau}\}$ is consistent by Proposition 33.9, hence it has a model $\mathcal{A}$. But then $\mathcal{A}$ witnesses that $\Sigma \not\models \boldsymbol{\tau}$.

Assume $\neg$(a) towards proving $\neg$(b). So let Σ be consistent and unsatisfiable: then $\Sigma \nvdash \boldsymbol{\tau} \wedge \neg\boldsymbol{\tau}$, yet $\Sigma \models \boldsymbol{\tau} \wedge \neg\boldsymbol{\tau}$ holds vacuously. □

The converse of the Soundness Theorem 33.4 is known as the **Completeness Theorem**: it says that the logical axioms and the rule of *Modus Ponens* are *complete*, i.e. they are powerful enough to derive all logical consequences.

Theorem 34.3. *Let $\Sigma \cup \{\boldsymbol{\sigma}\} \subseteq \mathrm{Sent}(\mathcal{L})$. If either* BPI *holds, or if $\mathcal{L}$ is well-orderable, then $\Sigma \models \boldsymbol{\sigma} \Rightarrow \Sigma \vdash \boldsymbol{\sigma}$.*

The Completeness Theorem follows from the converse of Proposition 34.1, known as the **Model Existence Theorem**.

Theorem 34.4. *Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ be consistent.*

(a) *If* BPI *holds, then* $\mathrm{Mod}(\Sigma) \neq \emptyset$.

(b) *If $\mathcal{L}$ is well-orderable, then Σ has a model of size $\leq \mathrm{card}(\mathcal{L})$.*

The Model Existence Theorem yields a new, more enlightening proof of the Compactness Theorem 31.27.

Corollary 34.5. *Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ be finitely satisfiable.*

(a) *If we assume* BPI *then Σ has a model.*

(b) *If $\mathcal{L}$ is well-orderable, then Σ has a well-orderable model of size $\leq \mathrm{card}(\mathcal{L})$.*

Proof. If Σ is finitely satisfiable, then each finite subset is consistent, hence Σ is consistent. □

Finally, note that for a finitely axiomatizable theory, we don't need to appeal to choice.

Corollary 34.6. *If $\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L})$ is consistent, then there is a countable $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ satisfying $\boldsymbol{\sigma}$.*

Proof. Let $\mathcal{L}_0$ be the sublanguage of $\mathcal{L}$ containing only the symbols of *logic*σ. Since $\boldsymbol{\sigma} \vdash_{\mathcal{L}} \boldsymbol{\exists x}(\boldsymbol{x} \neq \boldsymbol{x})$ if and only if $\boldsymbol{\sigma} \vdash_{\mathcal{L}_0} \boldsymbol{\exists x}(\boldsymbol{x} \neq \boldsymbol{x})$, it follows that $\{\boldsymbol{\sigma}\}$ is a consistent $\mathcal{L}_0$-theory. As $\mathcal{L}_0$ is well-orderable, then there is a countable $\mathcal{A}_0 \in \mathrm{Str}(\mathcal{L}_0)$ such that $\mathcal{A}_0 \vDash \boldsymbol{\sigma}$. Any expansion of $\mathcal{A}_0$ to an $\mathcal{A} \in \mathrm{Str}(\mathcal{L})$ satisfies $\boldsymbol{\sigma}$. □

34.A. The role of choice in the completeness theorem. In the assumptions of Theorems 34.3 and 34.4 there is a reference to some form of choice principle — the language must be well-orderable or we must assume BPI. In particular, if $\mathcal{L}$ is finite or countable, then $\Sigma \vdash \boldsymbol{\sigma} \Leftrightarrow \Sigma \models \boldsymbol{\sigma}$, independently of the axiom of choice. But when arbitrary languages are considered, the appeal to some form of choice is inevitable, as Theorem 34.4 for arbitrary languages is equivalent to BPI (Exercise 34.13).

Let Σ be a theory with a recursive set of axioms, in a countable language, so that the pathologies mentioned above have no reason to exist. Thus ZF proves that $\Sigma \vdash \boldsymbol{\sigma} \Leftrightarrow \Sigma \models \boldsymbol{\sigma}$ for any sentence $\boldsymbol{\sigma}$. So in order to prove that $\boldsymbol{\sigma}$ follows from Σ it is enough to show that $\mathcal{M} \vDash \boldsymbol{\sigma}$ for any $\mathcal{M}$ that satisfies Σ. But suppose that in order to prove this we use AC: does this mean that a derivation (which is a concrete, finite object) exists only if AC is assumed? Theorem 39.21 in Chapter VIII shows that this is not the case—in other words, if ZFC proves that $\Sigma \models \boldsymbol{\sigma}$, then a proof of this fact can be given in ZF alone.

Example 34.7. Let R be a commutative ring. We say that $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ is primitive if $I(f) \overset{\text{def}}{=} \langle a_0, \ldots, a_n \rangle$, the ideal generated by the coefficients of f, is improper, that is it contains 1_R. Then [**AM69**, Chapter 1, Exercise 2]

$$(*) \qquad \forall f, g \in \mathbb{R}[X]\ (f \cdot g \text{ is primitive} \Leftrightarrow f \text{ and } g \text{ are primitive}) .$$

The forward implication of $(*)$ is immediate, while for the other direction assume that $f \cdot g$ is not primitive, towards proving that either f or g are not primitive. By Krull's lemma (which follows from AC) let $\mathfrak{m} \supseteq I(f \cdot g)$ be a maximal ideal. Then $F = R/\mathfrak{M}$ is a field and $F[X]$ is an integral domain, and π denotes the canonical projection $R \to R/\mathfrak{M}$ as well as the induced homomorphism $F \to F[X]$. Then $\pi(f \cdot g) = 0_{F[X]}$, so $\pi(f) = 0_{F[X]}$ or $\pi(g) = 0_{F[X]}$, that is $I(f) \subseteq \mathfrak{m}$ and hence f is not primitive, or $I(g) \subseteq \mathfrak{m}$ and hence g is not primitive.

We claim that $(*)$ can be proved without choice, by showing that it is equivalent to the fact that Σ_{CRings}, the theory of commutative rings, proves certain first-order sentences. First observe that "$a_0 + a_1 X + \cdots + a_n X^n$ is primitive" amounts to say that "$\exists c_0, \ldots, c_n\, (a_0 \cdot c_0 + \cdots + a_n \cdot c_n = 1)$", so $(*)$ is equivalent to $\Sigma_{\text{CRings}} \vdash \boldsymbol{\sigma}_{n,m}$ for all $n, m \geq 1$, where $\boldsymbol{\sigma}_{n,m}$ is the universal closure of

$$\exists e_0, \dots, e_{n+m}\, ((a_0 b_0) e_0 + (a_0 b_1 + a_1 b_0) e_1 + \cdots + (a_n b_m) e_{n+m} = 1)$$
$$\Leftrightarrow \exists c_0, \dots, c_n\, (\textstyle\sum_{i=0}^{n} a_i c_i = 1) \vee \exists d_0, \dots, d_m\, (\textstyle\sum_{j=0}^{m} b_j d_j = 1).$$

34.B. The Model Existence Theorem. In order to prove the Model Existence Theorem, we need some preliminary results.

Lemma 34.8. *Let Σ be a consistent $\mathcal{L}$-theory, let $\boldsymbol{c}$ be a new constant, and let $\boldsymbol{\varphi}(\boldsymbol{x})$ be an $\mathcal{L}$-formula with exactly one free variable. Then the $\mathcal{L} \cup \{\boldsymbol{c}\}$-theory $\Sigma \cup \{\boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)\}$ is consistent.*

Proof. Towards a contradiction, suppose that $\Sigma \cup \{\boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)\} \vdash_{\mathcal{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\sigma \wedge \neg \sigma}$. By Lemma 33.6 one has that $\Sigma \vdash_{\mathcal{L} \cup \{\boldsymbol{c}\}} (\boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)) \boldsymbol{\Rightarrow \sigma \wedge \neg \sigma}$, and by the rule of the tautological consequence $\Sigma \vdash_{\mathcal{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\neg}(\boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!))$, that is $\Sigma \vdash_{\mathcal{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\exists x \varphi}$ and $\Sigma \vdash_{\mathcal{L} \cup \{\boldsymbol{c}\}} \boldsymbol{\neg \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)$. By Corollary 33.8 $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\exists x \varphi}$ and by Theorem 33.7 $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\forall x \neg \varphi}$. As $\boldsymbol{\forall x \neg \varphi \Rightarrow \neg \exists x \varphi}$ is an type (C) axiom for quantification, by the rule of tautological consequence $\Sigma \vdash_{\mathcal{L}} \boldsymbol{\neg \exists x \varphi}$, and hence Σ is inconsistent. □

Lemma 34.9. *If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is consistent, then there is a set of new constants C and $\tilde{\Sigma} \subseteq \mathrm{Sent}(\tilde{\mathcal{L}})$ where $\tilde{\mathcal{L}} = \mathcal{L} \cup C$ such that $\tilde{\Sigma} \supset \Sigma$ is consistent and if $\boldsymbol{\varphi}(\boldsymbol{x})$ is an $\mathcal{L}$-formula with exactly one free variable, then $\tilde{\Sigma} \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)$ for some $\boldsymbol{c} \in C$.*

Moreover, if $\mathcal{L}$ is well-orderable, then C can be taken to be of size $\mathrm{card}(\mathcal{L})$.

Proof. Let F be the set of all $\mathcal{L}$-formulæ $\boldsymbol{\varphi}$ with only one free variable $\boldsymbol{x}_{\boldsymbol{\varphi}}$, let $C = \{\boldsymbol{c}_{\boldsymbol{\varphi}} \mid \boldsymbol{\varphi} \in F\}$ and let $\tilde{\Sigma} = \Sigma \cup \{\boldsymbol{\exists x_{\varphi} \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}_{\boldsymbol{\varphi}}/\boldsymbol{x}_{\boldsymbol{\varphi}}|\!) \mid \boldsymbol{\varphi} \in F\}$. We must check that $\tilde{\Sigma}$ is consistent: towards a contradiction, if $\tilde{\Sigma}$ were inconsistent, then so would be $\Sigma \cup \{\boldsymbol{\exists x_{\varphi} \varphi \Rightarrow \varphi}(\!|\boldsymbol{c}_{\boldsymbol{\varphi}}/\boldsymbol{x}_{\boldsymbol{\varphi}}|\!) \mid \boldsymbol{\varphi} \in F_0\}$ for some finite $F_0 \subseteq F$. By repeated applications of Lemma 34.8 a contradiction is obtained.

If $\mathcal{L}$ is well-orderable, then $|F| = \mathrm{card}(\mathcal{L})$ by Proposition 30.5, and hence $|C| = \mathrm{card}(\mathcal{L})$. □

Definition 34.10. $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ **has witnesses** if for every $\mathcal{L}$-formula $\boldsymbol{\varphi}$ with exactly one free variable $\boldsymbol{x}$ there is a closed term $\boldsymbol{t}$ such that $\Sigma \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$. We say that $\boldsymbol{t}$ is the **witness** for the formula $\boldsymbol{\exists x \varphi}$.

Thus if a theory has witnesses, then whenever it proves existential statement $\boldsymbol{\exists x \varphi}$, it can prove also $\boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$ for a suitable closed term $\boldsymbol{t}$.

Remarks 34.11. (a) If Σ has witnesses, then $\mathcal{L}$ has constants. Thus not every theory has witnesses.

(b) If $\Sigma \subseteq \Delta \subseteq \mathrm{Sent}(\mathcal{L})$ and Σ has witnesses, then also Δ has witnesses.

Theorem 34.12. *If* $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *is consistent, then there are a set of new constants* C*, and* $\Sigma_\infty \subseteq \mathrm{Sent}(\mathcal{L}_\infty)$ *where* $\mathcal{L}_\infty = \mathcal{L} \cup C$*, such that* $\Sigma_\infty \supset \Sigma$ *is consistent and has witnesses, and every witness is a constant of* C*.*

Moreover, if $\mathcal{L}$ *is well-orderable, then* C *can be taken to be of size* $\mathrm{card}(\mathcal{L})$*.*

Proof. We construct by induction

- languages $\mathcal{L} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_n \subset \ldots$ such that $\mathcal{L}_{n+1} = \mathcal{L}_n \cup C_n$ where C_n is a set of constants that do not belong to $\mathcal{L}_n$,
- consistent sets $\Sigma_n \subseteq \mathrm{Sent}(\mathcal{L}_n)$ such that
  (i) $\Sigma = \Sigma_0 \subset \Sigma_1 \subset \cdots \subset \Sigma_n \subset \cdots$ and
  (ii) for every $\mathcal{L}_n$-formula $\boldsymbol{\varphi}$ with exactly one free variable $\boldsymbol{x}$ there is $\boldsymbol{c} \in C_n$ such that $\Sigma_{n+1} \vdash \boldsymbol{\exists x \varphi \Rightarrow \varphi} (\!| \boldsymbol{c}/\boldsymbol{x} |\!)$.

If $\mathcal{L}_0, \ldots, \mathcal{L}_n$, $C_0, \ldots, C_{n-1}$ and $\Sigma_0, \ldots, \Sigma_n$ have been constructed and satisfy the requirement, then Lemma 34.9 guarantees the existence of C_n (hence of $\mathcal{L}_{n+1}$) and of Σ_{n+1} as required. Letting $C = \bigcup_n C_n$, $\mathcal{L}_\infty = \bigcup_n \mathcal{L}_n$ and $\Sigma_\infty = \bigcup_n \Sigma_n$ we have that

- $\Sigma_\infty \subseteq \mathrm{Sent}(\mathcal{L}_\infty)$ is consistent by Proposition 33.9
- Σ_∞ has witnesses: given an $\mathcal{L}_\infty$-formula $\boldsymbol{\varphi}(\boldsymbol{x})$ with a single free variable, let n be least such that $\boldsymbol{\varphi}(\boldsymbol{x}) \in \mathrm{Fml}(\mathcal{L}_n)$. By construction there is $\boldsymbol{c} \in C_n$ such that $\Sigma_{n+1} \vdash_{\mathcal{L}_{n+1}} \boldsymbol{\exists x \varphi \Rightarrow \varphi} (\!| \boldsymbol{c}/\boldsymbol{x} |\!)$ hence $\Sigma_\infty \vdash_{\mathcal{L}_\infty} \boldsymbol{\exists x \varphi \Rightarrow \varphi} (\!| \boldsymbol{c}/\boldsymbol{x} |\!)$.

Finally note that if $\mathcal{L}$ is well-orderable, then $|C_n| = \mathrm{card}(\mathcal{L})$ hence $|C| = \mathrm{card}(\mathcal{L})$. □

34.C. Proof of the Model Existence Theorem 34.4. Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ be consistent: by Lemma 34.9 fix a set of new constants C and extend Σ to a coherent set $\Sigma' \subseteq \mathrm{Sent}(\overline{\mathcal{L}})$, where $\overline{\mathcal{L}} = \mathcal{L} \cup C$ so that Σ' has witnesses, and the witnesses are constants of C.

Claim 34.12.1. *There is* $\overline{\Sigma} \subseteq \mathrm{Sent}(\overline{\mathcal{L}})$ *which is consistent and maximal among the ones containing* Σ'*.*

Proof. We have two possibilities: either $\mathcal{L}$ is well-orderable, and hence so is $\mathrm{Lnd}(\overline{\mathcal{L}})$ and therefore $\mathsf{BPI}(\mathrm{Lnd}(\overline{\mathcal{L}}))$ holds, or else BPI holds. In either case Lindenbaum's Lemma 33.12 can be applied. □

By Exercise 33.13 $\overline{\Sigma}$ is syntactically closed. By Remark 34.11(b) $\overline{\Sigma}$ has witnesses, so $\boldsymbol{\exists x \varphi \Rightarrow \varphi} (\!| \boldsymbol{c}/\boldsymbol{x} |\!) \in \overline{\Sigma}$ for some $\boldsymbol{c} \in C$; thus if $\boldsymbol{\exists x \varphi} \in \overline{\Sigma}$, then $\boldsymbol{\varphi} (\!| \boldsymbol{c}/\boldsymbol{x} |\!) \in \overline{\Sigma}$ by (MP) and closure.

We shall construct $\overline{\mathcal{A}} \in \mathrm{Str}(\overline{\mathcal{L}})$ such that $\overline{\mathcal{A}} \vDash \overline{\Sigma}$ so that the reduction $\mathcal{A} = \overline{\mathcal{A}} \restriction \mathcal{L}$ we obtain a model of Σ. Let $\sim$ be the equivalence relation on

$\mathrm{ClTerm}(\overline{\mathcal{L}})$ defined by

$$\boldsymbol{t} \sim \boldsymbol{u} \quad \Leftrightarrow \quad (\boldsymbol{t} \mathrel{\boldsymbol{=}} \boldsymbol{u}) \in \overline{\Sigma}.$$

The universe of the structure $\overline{\mathcal{A}}$ (and therefore of the structure $\mathcal{A}$) is the set

$$A = \mathrm{ClTerm}(\overline{\mathcal{L}})/{\sim}$$

and the interpretation of the non-logical symbols of $\overline{\mathcal{L}}$ is defined as follows:

- If $\boldsymbol{R} \in \mathrm{Rel}_{\overline{\mathcal{L}}} = \mathrm{Rel}_{\mathcal{L}}$ is n-ary, set

  $$\boldsymbol{R}^{\overline{\mathcal{A}}} = \{\langle [\boldsymbol{t}_1]_\sim, \dots, [\boldsymbol{t}_n]_\sim \rangle \mid \boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \in \overline{\Sigma}\} \subseteq A^n.$$

  The relation $\boldsymbol{R}^{\overline{\mathcal{A}}}$ is well-defined: if $\boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \in \bar{\Sigma}$ and if $\boldsymbol{t}_i \sim \boldsymbol{u}_i$ then $\boldsymbol{t}_1 \mathrel{\boldsymbol{=}} \boldsymbol{u}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{t}_n \mathrel{\boldsymbol{=}} \boldsymbol{u}_n \in \overline{\Sigma}$ and since

  $$\boldsymbol{t}_1 \mathrel{\boldsymbol{=}} \boldsymbol{u}_1 \boldsymbol{\wedge} \dots \boldsymbol{\wedge} \boldsymbol{t}_n \mathrel{\boldsymbol{=}} \boldsymbol{u}_n \boldsymbol{\wedge} \boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n) \boldsymbol{\Rightarrow} \boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$$

  is an equality axiom, we have $\overline{\Sigma} \vdash_{\overline{\mathcal{L}}} \boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, that is $\boldsymbol{R}(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n) \in \overline{\Sigma}$.
- If $\boldsymbol{f} \in \mathrm{Func}_{\overline{\mathcal{L}}} = \mathrm{Func}_{\mathcal{L}}$ is n-ary, set

  $$\boldsymbol{f}^{\overline{\mathcal{A}}} \colon A^n \to A \qquad \langle [\boldsymbol{t}_1]_\sim, \dots, [\boldsymbol{t}_n]_\sim \rangle \mapsto [\boldsymbol{f}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)]_\sim .$$

  Also in this case one checks that the definition of $\boldsymbol{f}^{\overline{\mathcal{A}}}$ does not depend on the representatives.
- If $\boldsymbol{c} \in \mathrm{Const}_{\overline{\mathcal{L}}} \supset \mathrm{Const}_{\mathcal{L}}$, set $\boldsymbol{c}^{\overline{\mathcal{A}}} = [\boldsymbol{c}]_\sim$.

If $\boldsymbol{t} \in \mathrm{ClTerm}$, let $\boldsymbol{c} \in C$ be the witness to the formula $\boldsymbol{\exists x}(\boldsymbol{x} \mathrel{\boldsymbol{=}} \boldsymbol{t})$. As $\boldsymbol{t} \mathrel{\boldsymbol{=}} \boldsymbol{t} \boldsymbol{\Rightarrow} \boldsymbol{\exists x}(\boldsymbol{x} \mathrel{\boldsymbol{=}} \boldsymbol{t})$ is a substitution axiom, $\boldsymbol{t} \mathrel{\boldsymbol{=}} \boldsymbol{t}$ is an equality axiom, and $\boldsymbol{\exists x}(\boldsymbol{x} \mathrel{\boldsymbol{=}} \boldsymbol{t}) \boldsymbol{\Rightarrow} \boldsymbol{c} \mathrel{\boldsymbol{=}} \boldsymbol{t} \in \overline{\Sigma}$, it follows that $\boldsymbol{c} \sim \boldsymbol{t}$, and therefore

$$A = \{[\boldsymbol{c}]_\sim \mid \boldsymbol{c} \in C\}.$$

We must check that $\overline{\mathcal{A}} \vDash \overline{\Sigma}$. The definition of $\overline{\mathcal{A}}$ guarantees that

$$\boldsymbol{\sigma} \in \overline{\Sigma} \Leftrightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\sigma}$$

for all atomic sentences $\boldsymbol{\sigma}$. We check by induction on $\mathrm{ht}(\boldsymbol{\sigma})$ that this equivalence holds for all $\boldsymbol{\sigma} \in \mathrm{Sent}(\overline{\mathcal{L}})$. As $\overline{\Sigma}$ is maximal, then $\boldsymbol{\sigma} \notin \overline{\Sigma} \Leftrightarrow \boldsymbol{\neg\sigma} \in \overline{\Sigma}$ and $\boldsymbol{\sigma} \boldsymbol{\vee} \boldsymbol{\tau} \in \overline{\Sigma} \Leftrightarrow \boldsymbol{\sigma} \in \overline{\Sigma} \vee \boldsymbol{\tau} \in \overline{\Sigma}$, so

- if $\boldsymbol{\sigma} = \boldsymbol{\neg\tau}$ then $\boldsymbol{\neg\tau} \in \overline{\Sigma} \Leftrightarrow \boldsymbol{\tau} \notin \overline{\Sigma} \Leftrightarrow \overline{\mathcal{A}} \nvDash \boldsymbol{\tau} \Leftrightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\neg\tau}$;
- if $\boldsymbol{\sigma} = \boldsymbol{\tau} \boldsymbol{\vee} \boldsymbol{\chi}$ then

  $$\boldsymbol{\tau} \boldsymbol{\vee} \boldsymbol{\chi} \in \overline{\Sigma} \Leftrightarrow \bigl(\boldsymbol{\tau} \in \overline{\Sigma}\bigr) \vee \bigl(\boldsymbol{\chi} \in \overline{\Sigma}\bigr) \Leftrightarrow \bigl(\overline{\mathcal{A}} \vDash \boldsymbol{\tau}\bigr) \vee \bigl(\overline{\mathcal{A}} \vDash \boldsymbol{\chi}\bigr) \Leftrightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\tau} \boldsymbol{\vee} \boldsymbol{\chi}.$$

- Suppose that $\boldsymbol{\sigma} = \exists \boldsymbol{x}\boldsymbol{\varphi}$. As $\overline{\Sigma}$ has witnesses, $\exists \boldsymbol{x}\boldsymbol{\varphi} \Rightarrow \boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!) \in \overline{\Sigma}$ for some $\boldsymbol{c} \in C$. Therefore

$$\begin{aligned} \exists \boldsymbol{x}\boldsymbol{\varphi} \in \overline{\Sigma} &\Rightarrow \boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!) \in \overline{\Sigma} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!) && \text{(ind. hyp.)} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \boldsymbol{\varphi}[\boldsymbol{c}^{\overline{\mathcal{A}}}] && \text{(Proposition 31.8)} \\ &\Rightarrow \overline{\mathcal{A}} \vDash \exists \boldsymbol{x}\boldsymbol{\varphi}. \end{aligned}$$

Conversely, suppose that $\overline{\mathcal{A}} \vDash \exists \boldsymbol{x}\boldsymbol{\varphi}$ hence $\overline{\mathcal{A}} \vDash \boldsymbol{\varphi}[\boldsymbol{c}^{\overline{\mathcal{A}}}]$ for some $\boldsymbol{c} \in C$. It follows that $\overline{\mathcal{A}} \vDash \boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!)$ by Proposition 31.8, hence $\boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!) \in \overline{\Sigma}$ by inductive hypothesis. The sentence $\boldsymbol{\varphi}(\!|\boldsymbol{c}/\boldsymbol{x}|\!) \Rightarrow \exists \boldsymbol{x}\boldsymbol{\varphi}$ is a type (B) axiom for quantification, so it belongs to $\overline{\Sigma}$, hence $\exists \boldsymbol{x}\boldsymbol{\varphi} \in \overline{\Sigma}$ as required.

Finally, if $\mathcal{L}$ is well-orderable, then $|A| \leq |C| = \operatorname{card}(\mathcal{L})$. This concludes the proof of the Model Existence Theorem.

Exercises

Exercise 34.13. Show that each of the following results, stated for arbitrary languages, is equivalent to BPI:

- the Model Existence Theorem: if Σ is consistent, then Σ is satisfiable;
- the Completeness Theorem: if $\Sigma \models \boldsymbol{\tau}$ then $\Sigma \vdash \boldsymbol{\tau}$;
- the Compactness Theorem: if Σ is finitely satisfiable, then it is satisfiable.

Exercise 34.14. Suppose $\forall n\, \exists \mathcal{A} \in \operatorname{Mod}(\Sigma)\, (n \leq \operatorname{card}(\mathcal{A}))$ with $\Sigma \subseteq \operatorname{Sent}(\mathcal{L})$. (In particular, this holds if Σ has an infinite model.) Show that:

(i) if $\mathcal{L}$ is well-orderable, then Σ has models of every size $\kappa \geq \operatorname{card}(\mathcal{L})$;

(ii) if Σ is well-orderable, then it has infinite models of every size $\kappa \geq |\Sigma|$; in particular, if $|\Sigma| \leq \omega$, then it has models of every size $\kappa \in \mathrm{Card} \setminus \omega$;

(iii) if we assume BPI then Σ has models of arbitrarily large size, that is for every set X there is $\mathcal{A} \vDash \Sigma$ such that $X \precsim \|\mathcal{A}\|$.

Exercise 34.15. Show that the statement "$\forall \mathcal{L}\, \forall \Sigma \subseteq \operatorname{Sent}(\mathcal{L})$ (if Σ has an infinite model then it has models of arbitrarily large size)" implies BPI.

Exercise 34.16. Prove the following strengthening of Theorem 34.4(a): *Given a first-order language $\mathcal{L}$, let $\mathcal{S} = \mathrm{Vbl} \cup \mathrm{Rel}_{\mathcal{L}} \cup \mathrm{Func}_{\mathcal{L}} \cup \mathrm{Const}_{\mathcal{L}}$ and let C be a set of new constants such that $C \asymp \mathcal{S}^{<\omega}$. Assume* $\mathsf{BPI}(\mathrm{Lnd}_{\mathcal{L} \cup C})$*. If $\Sigma \subseteq \operatorname{Sent}(\mathcal{L})$ is consistent, then it has a model whose universe is the surjective image of C.*

Chapter VIII

Metamathematics

35. Concrete, finitistic arguments vs. abstract, non-constructive proofs

Many facts about formulæ can be stated and proved in a very weak framework, while other results in first-order logic require the power of set-theoretic arguments. Examples of the first kind are the results on the syntax of the first-order language—we only need some basic manipulation of finite sequences. Examples of results on the second kind are the notion of structure and satisfaction, the completeness theorem, etc. The environment used to prove results of the first kind is called **metatheory**, and the study of the underpinnings of provability is called **metamathematics**. Objects in the metatheory are concrete, finitistic entities, and *are not* (or better: we do not construe them as) structured sets—for example the natural number n can be thought to be n consecutive tallies $\mathsf{II}\cdots\mathsf{I}$, a finite sequence of objects $a_1, a_2, \ldots, a_n$ is just an explicit list, and we do not care how this list can be coded in arithmetic (by means of one of the coding procedures described in Section 11.B) or formalized in set theory (as a function with domain $\{1, 2, \ldots, n\}$). The methods and proofs in the metatheory are elementary and eschew the abstract, infinitistic reasoning typical of modern mathematics; the only kind of infinity allowed is that of the set of natural numbers, and we should never consider the collection of *all* subsets of the integers as a given object. When an existential sentence is proved, we are supposed to provide an explicit witness; similarly in order to assert $\mathrm{A} \vee \mathrm{B}$ we must be able to assert A or to assert B. (This should be contrasted with Examples 2.2 and 2.3 in Section 2.) A function in the metatheory is always assumed to be computable, and it is identified with the explicit algorithm that performs the computation. For example, a function that is constantly equal to 0 or 1 depending on the truth of some hard-to-decide problem (see Remark 8.1(a)) should not be considered.

In the metatheory

$$\boxed{\text{a language } \mathsf{L} \text{ will always be computable,}}$$

meaning that we have an algorithm to recognize the non-logical symbols and their arities; this guarantees that we can effectively determine whether a given string is a formula or not, and in the affirmative case we can effectively determine the free occurrences of a variable, and so on. Thus there is an effective enumeration of all L-formulæ and all L-sentences. Similarly

$$\boxed{\text{an } \mathsf{L}\text{-theory } \mathsf{T} \text{ will always be a computable set of } \mathsf{L}\text{-sentences,}}$$

meaning that we have an algorithm to determine whether a sentence is in T or not. In general, a theory T will just be a computable set of axioms, not a closed theory, i.e. a collection of sentences containing all theorems provable from it. If T is non-empty, then it can be effectively enumerated—if T is finite this is trivial, while if T is infinite, then list an all L-sentences $\sigma_0, \sigma_1, \ldots$, and focus only on those n such that σ_n is in T. One might ask if the notion of a T that is a semi-computable set of axioms is more general than that of computable set of axioms—by Exercise 36.7 it is not. To summarize: an effective theory T is just a computable set of L-sentences, and it is identified with its effective enumeration.

So the theories of arithmetic ($\bar{\mathsf{Q}}$, Q, PA, ...) axiomatic set-theory (ZF, NGB, MK, ...), and many theories from algebra (the theory of groups, rings, boolean algebras, ...) can be formulated in the metatheory; on the other hand the first-order theory of $\mathbb{R}$-vector spaces cannot.

35.A. Syntax and semantics in the encoding theory.

35.A.1. *Coding of syntax.* Metamathematics—being just another piece of mathematics—can be coded within some axiomatic system such as PA or ZF. But it is important to be able to distinguish if a given argument takes place in the metatheory, or within some axiomatic system such as PA or ZF. We describe a translation procedure (the *encoding*) from an austere environment (the *metatheory*) to a rich environment (the *encoding theory*, typically arithmetic or set theory). In order to ease the distinction between the two environments, we will adopt[1] the following notational convention:

[1] We will stick to this notational convention, unless it becomes too heavy. Mathematicians should never capitulate to their self-imposed notations.

- syntactic items of the metatheory are denoted using sans-serif fonts. Therefore $\mathsf{x}, \mathsf{y}, \dots$ range over the set of variables $\mathsf{v}_0, \mathsf{v}_1, \dots$, while L and T range over the set of effective languages and effective theories;
- the coded version of an object $\mathsf{L}, \mathsf{T}, \mathsf{x}, \varphi, \dots$ of the metatheory is denoted by $\ulcorner \mathsf{L} \urcorner, \ulcorner \mathsf{T} \urcorner, \ulcorner \mathsf{x} \urcorner, \ulcorner \varphi \urcorner, \dots$,
- boldface letters like $\boldsymbol{x}, \boldsymbol{\varphi}, \dots$ range over the set of codes for variables, formulæ, ...

Working in the metatheory one can verify in that, given L and T as above, the sets

$$\mathsf{Fml}_{\mathsf{L}}, \quad \mathsf{Sent}_{\mathsf{L}}, \quad \mathsf{LAx}_{\mathsf{L}}, \quad \mathsf{Prf}_{\mathsf{T}} \tag{35.1}$$

of formulæ, sentences, logical axioms, derivations, are effective. Similarly the substitution operation $\varphi, \mathsf{t}, \mathsf{x} \rightsquigarrow \varphi(\!|\mathsf{t}/\mathsf{x}|\!)$, is effective. On the other hand the set $\mathsf{Thm}_{\mathsf{T}}$ of all theorems is not (in general) effective, since in order to affirm that σ is in this set, one needs to exhibit a derivation. As there is an algorithm enumerating all possible derivations from T, we obtain that $\mathsf{Thm}_{\mathsf{T}}$ is effectively enumerable. The coded versions of the objects in (35.1) are

$$\mathrm{Fml}(\ulcorner \mathsf{L} \urcorner), \quad \mathrm{Sent}(\ulcorner \mathsf{L} \urcorner), \quad \mathrm{LAx}(\ulcorner \mathsf{L} \urcorner), \quad \mathrm{Prf}(\ulcorner \mathsf{T} \urcorner),$$

while $\boldsymbol{\varphi}, \boldsymbol{t}, \boldsymbol{x} \rightsquigarrow \boldsymbol{\varphi}(\!|\boldsymbol{t}/\boldsymbol{x}|\!)$ is the coded version of the substitution operation. These can be proved to be computable, while

$$\mathrm{Thm}(\ulcorner \mathsf{T} \urcorner) = \{\boldsymbol{\sigma} \in \mathrm{Sent} \mid \exists p \in \mathrm{Prf}(\ulcorner \mathsf{T} \urcorner)\ (\boldsymbol{\sigma} = p(\mathrm{lh}(p) - 1))\},$$

the set of all codes for theorems of T, is semi-computable.

Let us see how to encode an effective language L in arithmetic and in set theory.

Example 35.1. *Arithmetical coding.* We start defining a number $c(\mathsf{s})$ for s a symbol (logical or otherwise) of L. For example $\mathsf{v}_0, \mathsf{v}_1, \mathsf{v}_2, \dots$ are coded as $0, 2, 4, \dots$, and the remaining symbols are listed using the odd numbers, starting first with the logical symbols (the connectives $\neg$, $\vee$, ..., the equality symbol $=$) and then with non-logical symbols (of which there are at most $\aleph_0$-many). Terms and formulæ, being finite sequences can be coded using the Gödel $\boldsymbol{\beta}$-function of Section 11.B. In particular $\ulcorner \mathsf{T} \urcorner$ is a definable subset of $\mathbb{N}$ so it is identified the formula $\varphi_{\mathsf{T}}(x)$ defining it.

The encoding theory can be any theory extending $\bar{\mathsf{Q}}$ or Q, which are finitely axiomatized sub-theory of PA, since in Section 24.D we showed that every computable set and function is representable in them. More precisely: for all computable $A \subseteq \mathbb{N}^k$ there is a $\varphi(\mathsf{x}_1, \dots, \mathsf{x}_k)$ such that

$$\langle a_1, \dots, a_k \rangle \in A \Rightarrow \mathsf{Q} \vdash \varphi(\!|\overline{a_1}/\mathsf{x}_1, \dots, \overline{a_k}/\mathsf{x}_k|\!)$$
$$\langle a_1, \dots, a_k \rangle \notin A \Rightarrow \mathsf{Q} \vdash \neg\varphi(\!|\overline{a_1}/\mathsf{x}_1, \dots, \overline{a_k}/\mathsf{x}_k|\!)$$

and for every computable $f\colon \mathbb{N}^k \to \mathbb{N}$ there is a $\varphi(\mathsf{x}_1, \dots, \mathsf{x}_k, \mathsf{y})$ such that

$$\mathsf{Q} \vdash \forall \mathsf{y}(\varphi\llbracket\overline{a_1}/\mathsf{x}_1, \dots, \overline{a_k}/\mathsf{x}_k\rrbracket \Leftrightarrow \mathsf{y} \doteq \overline{f(a_1, \dots, a_k)}),$$

where the term $\overline{a}$ is the numeral for all $a \in \mathbb{N}$—see Definition 11.5.

Example 35.2. *Set-theoretic coding.* Most of the work was implicitly done in Section 30.B.1. The syntax of L is coded as elements of V_ω: the codes for variables are $\boldsymbol{v}_0 = \langle(1,0)\rangle, \boldsymbol{v}_1 = \langle(1,1)\rangle, \boldsymbol{v}_2 = \langle(1,2)\rangle, \dots$, the codes for connectives are $\boldsymbol{\neg} = (0,0)$ and $\boldsymbol{\vee} = (0,1)$, the code $\boldsymbol{\doteq}$ is $(0,2)$, and so on. All terms, formulæ, derivations, ... of L can thus be seen as elements of V_ω. As in Example 35.1, the code $\ulcorner\mathsf{T}\urcorner$ is a formula $\varphi_{\mathsf{T}}(x)$ in the language of set theory defining a certain subset of V_ω of all codes of sentences of T. The encoding theory could be taken to be ZF, but it is clearly overkill, and in Definition 24.33 we will introduce a finitely axiomatizable, very weak set theory that plays the role of Robinson's arithmetic.

There is a small wrinkle that needs to be ironed out. The language of set theory has no terms other than variables, so an element $a \in \mathrm{V}_\omega$ must be identified with the formula $\delta_a(x)$ of Proposition 24.6(a) defining a in V_ω.

Moving from a basic, concrete environment (the metatheory) to an abstract mathematical theory (the encoding theory) allows us to prove many theorems, but takes its toll.

- If in the metatheory we state that $\mathsf{T} \vdash \sigma$, then in the encoding theory we can prove that $\mathrm{Thm}_{\ulcorner\mathsf{T}\urcorner}(\ulcorner\sigma\urcorner)$. If the encoding theory proves that $\mathrm{Thm}_{\ulcorner\mathsf{T}\urcorner}(\ulcorner\sigma\urcorner)$, then we conclude that there is a proof of σ from T, but we may not have clues as to what this proof might be. In other words: the coding procedure cannot be reversed. (See Example 35.6 for a case in point.)
- If $\sigma \in \mathsf{T}$, then $\ulcorner\sigma\urcorner \in \ulcorner\mathsf{T}\urcorner$, so that $\{\ulcorner\sigma\urcorner \mid \sigma \in \mathsf{T}\} \subseteq \ulcorner\mathsf{T}\urcorner$. The reverse inclusion sounds highly plausible, but cannot be proved since there is no way to "invert" the coding procedure (Example 35.10.)

The situation described above is, in some ways, similar to what happens in Analysis when Cauchy's ε-δ-definition of continuity is introduced in order to formalize the intuitive notion of a function that "varies with no abrupt breaks or jumps"—on one hand it allows us to state and rigorously prove many results previously unattainable, and on the other hand it yields new objects that were not contemplated in the naïve conception of continuity, such as functions that are everywhere continuous, yet nowhere differentiable.

35.A.2. *Semantics within set theory.* We now take a closer look at what we did in Section 31.B.1. Working inside (some suitable sub-theory of) ZF a formula $\mathrm{Sat}(\tau, \mathcal{A}, \boldsymbol{\varphi}, g, i)$ is obtained such that

- τ is a signature, $\mathcal{A}$ is a τ-structure, $\boldsymbol{\varphi} \in \mathrm{Fml}(\mathcal{L}_\tau)$, $g\colon \mathrm{Fv}(\boldsymbol{\varphi}) \to \|\mathcal{A}\|$, and $i \in 2$;

- $\mathsf{ZF} \vdash \forall \mathcal{A}, \tau, \boldsymbol{\varphi}, g \, \exists! i \in 2 \; \mathrm{Sat}(\tau, \mathcal{A}, \boldsymbol{\varphi}, g, i)$

and we set

$$\mathcal{A} \vDash_g \boldsymbol{\varphi} \Leftrightarrow \mathrm{Sat}(\tau, \mathcal{A}, \boldsymbol{\varphi}, g, 1).$$

By definition, if $\mathcal{A}$ is a τ-structure, then $\mathcal{A} \vDash T$ if and only if $\forall \boldsymbol{\sigma} \in T \, (\mathcal{A} \vDash \boldsymbol{\sigma})$. This applies in particular when $\mathcal{L} = \ulcorner \mathsf{L} \urcorner$ and $T = \ulcorner \mathsf{T} \urcorner$. If T is a finite list of sentences $\sigma_1, \ldots, \sigma_n$ this means that $\mathcal{A} \vDash \ulcorner \sigma_1 \urcorner \boldsymbol{\wedge} \ldots \boldsymbol{\wedge} \ulcorner \sigma_n \urcorner$. If T is an infinite list of sentences then asserting $\mathcal{A} \vDash \ulcorner \mathsf{T} \urcorner$ means that in set theory we can prove in one shot that every sentence in $\ulcorner \mathsf{T} \urcorner \subseteq \mathrm{V}_\omega$ holds in $\mathcal{A}$, so it is stronger than saying that for every axiom σ of T there is a proof in set theory that $\mathcal{A} \vDash \ulcorner \sigma \urcorner$ (Example 35.10).

Remark 35.3. A reader may question the rationale for writing $\mathcal{A} \vDash_g \ulcorner \varphi \urcorner$ and $\mathcal{A} \vDash \ulcorner \mathsf{T} \urcorner$ rather than $\mathcal{A} \vDash_g \varphi$ and $\mathcal{A} \vDash \mathsf{T}$ as we did in the earlier chapters. The reason is that $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ asserts that a certain relation $\vDash$ holds for a triple of *sets* $(\mathcal{A}, \boldsymbol{\varphi}, g)$, so if we are given an L-formula φ or an L-theory T in the metatheory we must first encode them in set-theory as $\ulcorner \varphi \urcorner$ and $\ulcorner \mathsf{T} \urcorner$. For example, saying that "ZF proves that V_ω is a model of the axiom of pairing" means that $\mathsf{ZF} \vdash \mathrm{V}_\omega \vDash \ulcorner \forall x \forall y \exists z \forall w (w \in z \Leftrightarrow w = x \vee w = y) \urcorner$, or better

$$\mathsf{ZF} \vdash \exists v \, \exists u \, \exists t \, (\varphi(v) \wedge \psi(u) \wedge \chi(t) \wedge \mathrm{Sat}(t, v, u, \emptyset, 1))$$

where φ, ψ, χ are $\mathcal{L}_\in$-formulæ such that

- $\varphi(v)$ holds true if and only if v is V_ω,
- $\psi(u)$ holds true if and only if $u \in \mathrm{V}_\omega$ is the code of the $\mathcal{L}_\in$-formula $\forall x \forall y \exists z \forall w (w \in z \Leftrightarrow w = x \vee w = y)$,
- $\chi(t)$ holds true if and only if $t \in \mathrm{V}_\omega$ is the code of the signature for set theory.

Most of the time there is no need to be so careful about metamathematical issues, and following standard usage we will write $\mathcal{A} \vDash_g \varphi$ and $\mathcal{A} \vDash \mathsf{T}$.

If we work in NGB or MK rather than in ZF, then the τ-structures can be proper classes (Section 37.E). In particular one can argue in MK that $\langle \mathrm{V}, \in \rangle \vDash \ulcorner \mathsf{ZF} \urcorner$, where as usual $\mathrm{V} = \{x \mid \exists y (x \in y)\}$ is the class of all sets.

35.B. Theory vs. metatheory. In this chapter, we will look at three central results, due to Gödel, in mathematical logic, each of them highlighting different aspects of the subtle relation between theory and metatheory. The discussion below is meant to acquaint the reader with these notions. For the sake of definiteness we may assume that both the language of the encoding theory is that of arithmetic, and thus we use the arithmetical encoding.

35.B.1. *The first incompleteness theorem.* Suppose T is a consistent, effectively axiomatized theory, and suppose it is *sufficiently strong*, meaning that it can encode its own syntax. A sufficient condition is that any (elementary) computable function is representable in T, so Robinson's arithmetic $\bar{\mathsf{Q}}$ and Q and elementary set theory EST would do. In particular, this applies to PA and the usual axiomatizations of set theory, such as ZF, NGB, and MK. Then T is **incomplete**, that is there are sentences σ that are **independent of** T, that is neither $\mathsf{T} \vdash \sigma$ nor $\mathsf{T} \vdash \neg\sigma$. Moreover T is **undecidable**, i.e. there is no effective method to determine whether or not a given sentence is a theorem of T (Definition 11.7). The next result (whose proof is modelled after that of Theorem 8.38) shows that completeness implies decidability.

Theorem 35.4. *If* T *is effectively axiomatized and complete, then* T *is decidable.*

Proof. As L, the language of T, is effective, we can fix an effective enumeration $n \mapsto \sigma_n$ of $\mathsf{Sent}_{\mathsf{L}}$. Thus there is an effective enumeration of all finite sequences of sentences. Since the set of all derivations from T is effective, i.e. there is an algorithm to determine whether a finite sequence is a derivation from T, this yields an effective enumeration $n \mapsto \tau_n$ of all theorems of T. Let us describe an algorithm to determine whether or not $\mathsf{T} \vdash \sigma$ for any σ in $\mathsf{Sent}_{\mathsf{L}}$. Since T is complete, either $\mathsf{T} \vdash \sigma$ or else $\mathsf{T} \vdash \neg\sigma$, so it is enough to look for the least n such that σ is τ_n or $\neg\sigma$ is τ_n. □

The proof of the incompleteness theorem shows that there is an algorithm $\mathsf{T} \rightsquigarrow \gamma_{\mathsf{T}} \in \mathsf{Sent}_{\mathsf{L}}$ with γ_{T} independent of T, so adding γ_{T} to T yields a theory T' extending T, and satisfying the hypotheses of the incompleteness theorem. This would yield a new sentence $\gamma_{\mathsf{T}'}$ which is independent of T' and hence of T, so adding finitely many (or even an infinite effective list of) sentences to T does not avoid the incompleteness phenomenon.

The requirement that the list of the new axioms be computable is essential—$\mathrm{Th}(\mathbb{N})$ is a complete theory extending, but it is far from being effectively axiomatizable. In fact $\mathrm{Th}(\mathbb{N})$ lives in the realm of set theory, and not in the metatheory.

Definition 35.5. An effectively axiomatized theory is **essentially incomplete** if it is incomplete, and every effectively axiomatized theory extending it is incomplete.

Gödel's first incompleteness theorem says that any sufficiently strong, consistent, effective theory is essentially incomplete.

One might wonder: if σ is independent from PA, what can we say about the truth of σ in the real world, i.e. in the structure $\langle \mathbb{N}, S, +, \cdot, 0, < \rangle$? Say that $\varphi(x_1, \dots, x_k)$ is computable if it defines a k-ary computable predicate of

$\mathbb{N}$. The proof of Gödel's first incompleteness theorem shows that γ_{T} is of the form $\forall x \varphi(x)$, with $\varphi(x)$ computable (in fact: elementary computable). This means that γ_{T} must be true in $\mathbb{N}$: if $\mathbb{N} \vDash \ulcorner \neg\varphi \urcorner [n]$ then by Theorem 24.31 $\mathsf{T} \vdash \neg\varphi(\!|\overline{n}/x|\!)$, and hence $\mathsf{T} \vdash \neg\gamma_{\mathsf{T}}$, against our assumption that γ_{T} is independent of T. The sentence γ_{T} produced by Gödel's proof is true, yet unprovable (and irrefutable) from T, so in some sense it witnesses T's lack of skills in proving theorems. But the above argument does not apply to sentences of higher logical complexity. For example is σ is of the form $\forall x \exists y \varphi(x, y)$, with $\varphi(x, y)$ computable, then knowing that σ is independent from Tdoes not yield any information on whether $\mathbb{N} \vDash \sigma$ or $\mathbb{N} \vDash \neg\sigma$.

By Exercise 24.39, it is easy to find sentences that are independent of $\bar{\mathsf{Q}}$ or Q, but what about PA or stronger theories? Are there natural mathematical problems, i.e. problems that mathematicians might encounter in their daily work, that are independent of PA? The answer is affirmative—there are variants of the Ramsey theorem that are provable in ZF, yet are unprovable in PA.

35.B.2. *The second incompleteness theorem.* Among the hypotheses in the first incompleteness theorem is that T is consistent, in symbols $\mathsf{Con}_{\mathsf{T}}$. When in the metatheory we say that $\neg\mathsf{Con}_{\mathsf{T}}$, we are asserting the existence of a contradiction from T, that is we assert that there is a derivation from T of some false sentence, e.g. $\exists \mathsf{v}_0 (\mathsf{v}_0 \neq \mathsf{v}_0)$, which will be abbreviated with $\perp$. On the other hand stating in the metatheory that $\mathsf{Con}_{\mathsf{T}}$ amounts to say that T is empirically free from contradictions, that is to say: there is no known derivation of a contradiction from T,

$$\mathsf{Con}_{\mathsf{T}} : \quad \neg\exists p \in \mathsf{Prf}_{\mathsf{T}} \; (p(\mathrm{lh}\, p - 1) = \perp)$$

Moving to the encoding theory, the formal version of $\mathsf{Con}_{\mathsf{T}}$ is

$$\mathrm{Con}(\ulcorner \mathsf{T} \urcorner) : \quad \neg\exists p \in \mathrm{Prf}(\ulcorner \mathsf{T} \urcorner) \; (p(\mathrm{lh}\, p - 1) = \ulcorner \perp \urcorner) \, .$$

Gödel's second incompleteness theorem says that a consistent, effectively axiomatized, and *reasonably strong* theory cannot prove its own consistency. (Reasonably strong means that it extends PA—so the assumptions for the second incompleteness theorem are more demanding than those for the first incompleteness.) More precisely, if T is effectively axiomatized theory, reasonably strong, then any derivation witnessing $\mathsf{T} \vdash \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$ can be turned into a derivation of a contradiction in T, that is $\neg\mathsf{Con}_{\mathsf{T}}$.

For a theory T being free of contradictions, that is $\mathsf{Con}_{\mathsf{T}}$, is certainly an essential, but hardly the only, requirement. Consider the case of Peano's arithmetic: not only the vast majority of mathematicians would concur that it is consistent, but they would also deem that its theorems assert facts about the natural numbers that agree with our intuition of the integers. This does not follow from coherence, as the next example shows.

Example 35.6. Assume that PA is consistent, that is $\mathsf{Con}_{\mathsf{PA}}$. By Gödel's second incompleteness theorem $\mathsf{PA} \nvdash \mathrm{Con}(\ulcorner \mathsf{PA} \urcorner)$, so $\mathsf{T} = \mathsf{PA} + \neg \mathrm{Con}(\ulcorner \mathsf{PA} \urcorner)$, the theory obtained by adding "PA is incinsistent to PA", must be consistent. Yet $\mathsf{T} \vdash \neg \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$, that is to say: T is a consistent theory proving its own inconsistency! Observe that T claims that *there is* a proof of a contradiction, yet this proof cannot be uncovered in the real world.

Example 35.7. Suppose T is like in Example 35.6, a consistent theory that proves its inconsistency, that is $\mathsf{Con}_{\mathsf{T}}$ and $\mathsf{T} \vdash \neg \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$. Let $\mathcal{M}$ be a model of T and let $d \in \|\mathcal{M}\|$ be such that

$$\mathcal{M} \vDash d \text{ codes a derivation of } \bot \text{ from } \mathsf{T}.$$

Then $\omega^{\mathcal{M}} = \{x \in \|\mathcal{M}\| \mid \mathcal{M} \vDash x \text{ is a natural number}\}$ cannot be isomorphic to $\mathbb{N}$, since otherwise d would witness in the real world that T is inconsistent against our assumption. Although people living in $\mathcal{M}$ think that "d encodes a finite string of sentences", one cannot expect to turn this into an honest derivation of $\bot$ from T, since it might happen that the length of this derivation or the codes of these sentences be non-standard numbers. To be more specific, consider the case when $\mathsf{T} = \mathsf{ZF} + \neg\mathsf{Con}_{\mathsf{ZF}}$, and let $n \mapsto \boldsymbol{\sigma}_n$ be a primitive recursive enumeration of ZF. As argued above any $\mathcal{M} = \langle M, E \rangle$ model of T is not **ω-standard**, that is $\omega^{\mathcal{M}}$ is a non-standard model of arithmetic. Without loss of generality we may assume that ω is a proper initial segment of $\omega^{\mathcal{M}}$. Let $n \mapsto \boldsymbol{\sigma}_n$ be a primitive recursive enumeration (of the axioms) of ZF, so that it induces a bijection $a \colon \omega \to \ulcorner \mathsf{ZF} \urcorner$. Let $d \in \omega^{\mathcal{M}}$ witness in $\mathcal{M}$ that $\mathsf{ZF} \vdash \bot$, and let

$$I = \{n \in \omega^{\mathcal{M}} \mid a^{\mathcal{M}}(n) \text{ occurs in the derivation coded by } d\}.$$

Then I has non-standard integers, that is to say: any d coding a proof of $\mathsf{ZF} \vdash \bot$ in $\mathcal{M}$ must use non-standard axioms of ZF (Exercise 38.13).

A reasonably strong theory T is **n-consistent** if $\mathsf{Con}_{\mathsf{T}^{(n)}}$ where

$$\mathsf{T}^{(0)} = \mathsf{T}, \qquad \mathsf{T}^{(n+1)} = \mathsf{T}^{(n)} + \mathrm{Con}(\ulcorner \mathsf{T}^{(n)} \urcorner).$$

If T is not n-consistent, then it is n-inconsistent. Thus if T is n-consistent, it is also m-consistent, for all $m < n$, T is 0-consistent if and only if $\mathsf{Con}_{\mathsf{T}}$, and T is $n + 1$-inconsistent if and only if $\mathsf{T}^{(n)} \vdash \neg \mathrm{Con}(\ulcorner \mathsf{T}^{(n)} \urcorner)$. In particular, the theory of Example 35.6 is consistent, but 1-inconsistent. A theory T which is n-consistent and $n + 1$-inconsistent asserts the existence of a proof (of the existence of contradictions in $\mathsf{T}^{(n)}$) that do not exist in the real world; in other words, it proves existential facts about natural numbers that are false in $\mathbb{N}$. Since we believe that PA proves true facts about natural numbers, we believe that it is n-consistent, for all ns. This belief is substantiated in ZF, where we construct $\langle \omega, \mathbf{S}, +, \cdot, <, 0 \rangle$ which is a model of every $\mathsf{PA}^{(n)}$.

Remark 35.8. The model existence theorem states a theory is consistent if and only if it has a model,

$$\mathsf{ZF} + \mathsf{BPI} \vdash \forall T\,(\mathrm{Con}(T) \Leftrightarrow \mathrm{Mod}(T) \neq \emptyset)\,.$$

When dealing with an effectively axiomatizable theory T the principle BPI can be dropped since the language is well-orderable, so

$$\mathsf{ZF} \vdash \mathrm{Con}(\ulcorner\mathsf{T}\urcorner) \Leftrightarrow \mathrm{Mod}(\ulcorner\mathsf{T}\urcorner) \neq \emptyset. \tag{35.2}$$

As MK extends ZF, then (35.2) holds with MK in place of ZF, and since $\mathsf{MK} \vdash \langle \mathrm{V}, \in\rangle \vDash \ulcorner\mathsf{ZFC}\urcorner$, then $\mathsf{MK} \vdash \mathrm{Con}(\ulcorner\mathsf{ZFC}\urcorner)$.

Example 35.9. In Section 38.A we will prove for any finite sub-theory of ZF, there is a proof in ZF that such sub-theory has a model, i.e. if $\sigma_1, \dots, \sigma_n$ are axioms of ZF, then $\mathsf{ZF} \vdash \exists \mathcal{A}(\mathcal{A} \vDash \ulcorner\sigma_1\urcorner \wedge \ldots \wedge \ulcorner\sigma_n\urcorner)$. This is weaker than saying

$$\mathsf{ZF} \vdash \forall \Sigma \subseteq \ulcorner\mathsf{ZF}\urcorner\,(|\Sigma| < \omega \Rightarrow \mathrm{Mod}(\Sigma) \neq \emptyset) \tag{†}$$

since (†) would imply by compactness that $\mathsf{ZF} \vdash \mathrm{Mod}(\ulcorner\mathsf{ZF}\urcorner) \neq \emptyset$, that is $\mathsf{ZF} \vdash \ulcorner\mathrm{Con}(\mathsf{ZF})\urcorner$, against Gödel's second incompleteness theorem. Therefore (†) is false, that is to say: it is not true that ZF proves that any of its finite sub-theories is satisfiable. In plain words: for any finite $\Sigma \subseteq \mathsf{ZF}$ there is a proof in ZF of the satisfiability of Σ, but there is no single proof in ZF that works for all sub-theories at once.

There is one more surprising fact that can be inferred from the above: even if ZF proves $\psi(n)$ for any $n \in \mathbb{N}$, it might not be able to prove that $\forall n \in \omega\, \psi(n)$. To see this work in ZF, and let $\omega \ni n \mapsto \boldsymbol{\sigma}_n$ be an enumeration of $\ulcorner\mathsf{ZF}\urcorner$, and let $\psi(n)$ be $\mathrm{Con}(\{\boldsymbol{\sigma}_0 \wedge \ldots \wedge \boldsymbol{\sigma}_n\})$. For every n let $\delta_n(x)$ be the $\mathcal{L}_\in$-formula that defines the number n. Then $\mathsf{ZF} \vdash \forall x(\delta_n(x) \Rightarrow \psi(x))$ for any n, but $\mathsf{ZF} \nvdash \forall x \in \omega\, \psi(x)$.

Example 35.10. If $n \mapsto \sigma_n$ is an explicit enumeration of ZF, then working in ZF let $I = \{n \in \omega \mid \ulcorner\bigwedge_{i \leq n} \sigma_i\urcorner \text{ is satisfiable}\}$. Then I is an initial segment of ω, and by the arguments in Example 35.9 $\mathsf{ZF} \vdash n \in I$ for each $n \in \omega$, and yet $\mathsf{ZF} \nvdash I = \omega$. Therefore $T = \{\ulcorner\sigma_n\urcorner \mid n \in I\} \subseteq \ulcorner\mathsf{ZF}\urcorner$, and by compactness ZF proves that there is $\mathcal{M} \vDash T$, a statement that is *weaker* than saying that there is a model of ZF, that is $\exists \mathcal{M}\, \forall \boldsymbol{\sigma} \in \ulcorner\mathsf{ZF}\urcorner\,(\mathcal{M} \vDash \boldsymbol{\sigma})$.

35.B.3. *Undefinability of truth.* Consider $\mathcal{N} = \langle \mathbb{N}, +, \cdot, S, 0, <\rangle$, the structure for arithmetic. The theory PA is effective and $\ulcorner\mathsf{PA}\urcorner \subseteq \mathbb{N}$ is a computable set, and $\mathrm{Thm}(\ulcorner\mathsf{PA}\urcorner)$, the set of all (codes for) theorems provable from PA is semi-computable, and hence a Σ_1 definable subset on $\mathbb{N}$. Is the set

$$\mathrm{Th}(\mathcal{N}) = \{\boldsymbol{\sigma} \mid \mathcal{N} \vDash \boldsymbol{\sigma}\}$$

semi-computable, i.e. definable in $\mathcal{N}$ via a $\boldsymbol{\Sigma}_1$ formula? Tarski proved that this is not the case. In fact $\mathrm{Th}(\mathcal{N})$ is not definable in $\mathcal{N}$, it is not Σ_n for any n. In simple words, truth in $\mathcal{N}$ is not definable within $\mathcal{N}$.

35.B.4. *Relative consistency.* If T is 1-consistent, then T and $\mathsf{T}^{(1)} = \mathsf{T} + \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$ are consistent, so both $\mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$ and $\mathrm{Con}(\ulcorner \mathsf{T}^{(1)} \urcorner)$ are true sentences about natural numbers, yet the implication $\mathrm{Con}(\ulcorner \mathsf{T} \urcorner) \Rightarrow \mathrm{Con}(\ulcorner \mathsf{T}^{(1)} \urcorner)$ cannot be established in $\mathsf{T}^{(1)}$, and *a fortiori* in T. In fact if, towards a contradiction, $\mathsf{T}^{(1)} \vdash \mathrm{Con}(\ulcorner \mathsf{T} \urcorner) \Rightarrow \mathrm{Con}(\ulcorner \mathsf{T}^{(1)} \urcorner)$, then since $\mathsf{T}^{(1)} \vdash \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$ it would follow that $\mathsf{T}^{(1)} \vdash \mathrm{Con}(\ulcorner \mathsf{T}^{(1)} \urcorner)$ against the second incompleteness theorem.

Definition 35.11. The theory T_1 has **higher consistency strength** than T_0, in symbols $\mathsf{T}_0 <_{\mathsf{Con}} \mathsf{T}_1$ if $\mathsf{T}_1 \vdash \mathrm{Con}(\ulcorner \mathsf{T}_0 \urcorner)$.

By the second incompleteness theorem, no consistent theory has higher consistency strength than itself, and an inconsistent theory has higher consistency strength than any consistent theory. In plain words, if T_1 has higher consistency strength than T_0, then working with T_1 is "riskier" than working with T_0. Note that:

- $\mathsf{T}^{(n)} <_{\mathsf{Con}} \mathsf{T}^{(m)}$ if and only if $n < m$;
- $\mathsf{PA}^{(n)} <_{\mathsf{Con}} \mathsf{ZFC}$ for any n, since in ZFC one constructs the structure $\langle \omega, \mathbf{S}, +, \cdot, 0, < \rangle$ which models any $\mathsf{PA}^{(n)}$;
- $\mathsf{ZFC} + \forall \beta \, \exists \alpha > \beta \, (\mathrm{V}_\alpha \vDash \ulcorner \mathsf{ZFC} \urcorner) <_{\mathsf{Con}} \mathsf{ZFC} +$ (there is an inaccessible cardinal) by Theorems 21.39 and 31.22.

There is a very concrete, algebraic embodiment of the notion of relative consistency. Recall that a Diophantine subset of the natural numbers is of the form $\mathbb{N} \cap \mathrm{ran}(f)$, where $f \in \mathbb{Z}[x_1, \dots, x_n]$, and by the Matiyasevich-Robinson-Davis-Putnam theorem, Diophantine subsets of the natural numbers are exactly the semi-computable sets. In particular, for any T there is $f_{\mathsf{T}} \in \mathbb{Z}[x_1, \dots, x_N]$ such that $\mathsf{T} \vdash \upsigma$ if and only if there are $k_1, \dots, k_N \in \mathbb{N}$ such that $f_{\mathsf{T}}(k_1, \dots, k_N) = \ulcorner \upsigma \urcorner$.[2] Therefore $\mathsf{Con}_{\mathsf{T}}$ is equivalent to saying that the equation $f_{\mathsf{T}}(x_1, \dots, x_N) - \ulcorner \perp \urcorner = 0$ has no solution in $\mathbb{N}$, with $\perp$ our standard false sentence. The set $\mathfrak{D}_{\mathsf{T}} = \{ f \in \mathbb{Z}[x_1, \dots, x_m] \mid \mathsf{T} \vdash \forall \vec{x} \in \mathbb{N} \, f(\vec{x}) \neq 0 \}$ of all Diophantine equations that (provably in T) have no solutions can be used to gauge the consistency strength: if T_1 extends T_0 then

$$\mathsf{T}_1 \text{ has higher consistency strength than } \mathsf{T}_0 \Rightarrow \mathfrak{D}_{\mathsf{T}_1} \supset \mathfrak{D}_{\mathsf{T}_0}.$$

In particular, there is an algorithm assigning to any T a polynomial $f(\vec{x})$ with coefficients in $\mathbb{Z}$ such that $\mathsf{Con}_{\mathsf{T}}$ if and only if $f(\vec{x})$ has no roots in $\mathbb{N}$.

Definition 35.12. Given $\mathsf{T}_0, \mathsf{T}_1$ then

[2] It can be showh that the number N is independent of T.

- T_1 is **consistent relative to** T_0 if and only if $\mathsf{Con}_{\mathsf{T}_0}$ implies $\mathsf{Con}_{\mathsf{T}_1}$,
- T_0 and T_1 are **equiconsistent** if and only if they are consistent relative to each other.

In other words, T_1 is consistent relative to T_0 means that T_1 is no "riskier" than T_0, and $\mathsf{T}_0, \mathsf{T}_1$ are equiconsistent if and only if they are equally "dangerous".

Although Definition 35.12 is worded in a positive form, it really should be stated using the contrapositive: T_1 is consistent relative to T_0 if and only if there is an algorithm transforming derivations from T_1 into derivations from T_0, such that any contradiction from T_1 is turned into a contradiction from T_0.

One of the central results in set theory is Gödel's proof that $\mathsf{ZFC} + \mathsf{GCH}$ is consistent relative to ZF, so that the theories ZF and $\mathsf{ZFC} + \mathsf{GCH}$ are equiconsistent, and hence $\mathfrak{D}_{\mathsf{ZF}} = \mathfrak{D}_{\mathsf{ZFC+GCH}}$. Therefore there is an algorithm (some sort of a doomsday machine) such that if (heaven forbid!) a contradiction were to emerge from $\mathsf{ZFC} + \mathsf{GCH}$, then the algorithm would turn this into a proof of a contradiction in ZF. In other words, the theories ZF and $\mathsf{ZFC} + \mathsf{GCH}$ share the same fate form here to eternity—either they both survive forever without a contradiction, or they both collapse at the same time.

Equiconsistency proofs occupy a central place in contemporary set theory. For example ZFC + "there is an inaccessible cardinal" and ZFC + "every projective set is Lebesgue measurable" are equiconsistent, where a subset of the real line is projective if it can be obtained from Borel sets by means of continuous images and complements. Thus if a mathematician is suspicious of the existence of inaccessible cardinals, as their existence is "riskier" than $\mathsf{Con}_{\mathsf{ZFC}}$, then (s)he should harbour a similar distrust towards the measurability of projective sets.

35.C. Interpretability. How can we prove a relative consistency result like $\mathsf{Con}_{\mathsf{T}_0} \Rightarrow \mathsf{Con}_{\mathsf{T}_1}$? One way could be to find a method for transforming a model of T_0 into a model of T_1, but this approach wouldn't yield a concrete, finitistic proof of the consistency of T_1 from the consistency of T_0, since the notion of satisfaction (and hence of model) subsumes some set theory on the background. Moreover for a reasonably strong theory, the existence of a model for it is an assumption that transcends the theory. Interpretations are the syntactic analogues of models: by interpreting T_1 inside T_0 a surrogate model for T_1 is defined within T_0 so that any contradiction from T_1 would yield a contradiction from T_0.

Let T_0 and T_1 be effective theories in the languages L_0 and L_1, respectively. An **interpretation $\mathfrak{I}$ of T_1 into T_0** is an effective procedure to transform any L_1-sentence σ into an L_0-sentence $\sigma^{\mathfrak{I}}$ so that

- $(\neg\sigma)^{\mathfrak{I}}$ is $\neg\sigma^{\mathfrak{I}}$,
- $(\sigma \odot \tau)^{\mathfrak{I}}$ is $\sigma^{\mathfrak{I}} \odot \tau^{\mathfrak{I}}$, where $\odot$ is a binary connective,
- if σ is either an axiom of T_1 or else a logical axiom of L_1, then $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}$.

Proposition 35.13. *Suppose $\mathfrak{I}$ is an interpretation of T_1 into T_0, and let L_i be the language of T_i.*

(a) *If $\mathsf{T}_1 \vdash_{\mathsf{L}_1} \sigma$ then $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}$.*

(b) *If $\mathsf{Con}_{\mathsf{T}_0}$ then $\mathsf{Con}_{\mathsf{T}_1}$.*

(c) *If T_1 is essentially incomplete, then T_0 is also essentially incomplete.*

Proof. (a) It is enough to show that if $\langle \varphi_0, \ldots, \varphi_n \rangle$ is a derivation in T_1, then $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \varphi_i^{\mathfrak{I}}$ for all $i \leq n$. If φ_i is an axiom of T_1 or else a logical axiom of L_1 the result follows from the definition of interpretation, so we may assume that φ_i is obtained by (MP) from φ_j, φ_k with $j, k < i$. Then $\varphi_i^{\mathfrak{I}}$ is obtained by (MP) from $\varphi_j^{\mathfrak{I}}, \varphi_k^{\mathfrak{I}}$.

(b) If $\mathsf{T}_1 \vdash_{\mathsf{L}_1} \sigma \wedge \neg\sigma$ then $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}} \wedge \neg\sigma^{\mathfrak{I}}$, so the result follows by taking the contrapositive.

(c) Towards a contradiction, suppose T_0 has a complete, computably axiomatized extension T_0'. Then $\mathfrak{I}$ is also an interpretation of T_1 in T_0'. The theory $\Sigma = \left\{\sigma \in \mathsf{Sent}_{\mathsf{L}_1} \mid \mathsf{T}_0' \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}\right\}$ is complete, extends T_1 as $\mathfrak{I}$ is an interpretation, and it is decidable, as so is T_0' by Theorem 35.4. But this contradicts the first incompleteness theorem. □

Although interpretations need to be defined only for sentences, it is often handy to define it for all formulæ. The next result serves as a template for constructing interpretations.

Theorem 35.14. *Let T_i be an L_i-theory, for $i = 0, 1$, and let $\upsilon(\mathsf{x})$ be an L_0-formula such that $\mathsf{T}_0 \vdash \exists \mathsf{x}\, \upsilon(\mathsf{x})$. Suppose there are L_0-formulæ*

- *$\psi_R(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ one for each n-ary relational symbol R of L_1,*
- *$\psi_f(\mathsf{x}_1, \ldots, \mathsf{x}_n, \mathsf{y})$ one for each n-ary function symbol f of L_1, such that $\mathsf{T}_0 \vdash \forall \mathsf{x}_1, \ldots, \mathsf{x}_n \exists! \mathsf{y} \psi_f(\mathsf{x}_1, \ldots, \mathsf{x}_n, \mathsf{y})$,*
- *$\psi_c(\mathsf{x})$ one for each constant symbol c of L_1, such that $\mathsf{T}_0 \vdash \exists! \mathsf{y} \psi_c(\mathsf{y})$.*

Then there is an effective map $\varphi \rightsquigarrow \varphi^{\mathfrak{I}}$ from the L_1-formulæ to the L_0-formulæ such that $\varphi^{\mathfrak{I}}$ has the same free variables as φ, and

- *$(\neg\varphi)^{\mathfrak{I}}$ is $\neg\varphi^{\mathfrak{I}}$,*

- $(\varphi \odot \psi)^{\mathfrak{I}}$ *is* $\varphi^{\mathfrak{I}} \odot \psi^{\mathfrak{I}}$, *where* $\odot$ *is a binary connective,*
- $(\exists x \varphi)^{\mathfrak{I}}$ *is* $\exists x(\upsilon(x) \wedge \varphi^{\mathfrak{I}})$ *and* $(\forall x \varphi)^{\mathfrak{I}}$ *is* $\forall x(\upsilon(x) \Rightarrow \varphi^{\mathfrak{I}})$,
- *if* σ *is a logical axiom of* T_1, *then* $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}$.

Moreover, if $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}$ *whenever* σ *is an axiom of* T_1, *then* $\mathfrak{I}$ *is an interpretation of* T_1 *into* T_0.

Proof. For each L_0-term $t(x_1, \ldots, x_n)$ which is not a variable let $\psi_t(x_1, \ldots, x_n, y)$ be the L_1-formula defined as follows:

- if $t(\vec{x})$ is $f(\vec{x})$ with f a function symbol, then $\psi_t(\vec{x}, y)$ is $\psi_f(\vec{x}, y)$,
- if $t(\vec{x})$ is a constant symbol c, then $\psi_t(\vec{x}, y)$ is $\psi_c(y)$,
- if $t(\vec{x})$ is $f(u_1(\vec{x}), \ldots, u_n(\vec{x}))$ then $\psi_t(\vec{x}, y)$ is

$$\exists z_1, \ldots, z_n(\psi_f(z_1, \ldots, z_n, y) \wedge \psi_{u_1}(\vec{x}, z_1) \wedge \cdots \wedge \psi_{u_n}(\vec{x}, z_n)).$$

Thus $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \forall \vec{x} \exists ! y \psi_t(\vec{x}, y)$.

The first goal is to define $\varphi^{\mathfrak{I}}$ when φ is atomic:

if φ is...	then $\varphi^{\mathfrak{I}}$ is...
$x = y$	$x = y$
$t(\vec{x}) = y$ or $y = t(\vec{x})$	$\psi_t(\vec{x}, y)$
$s(\vec{x}) = t(\vec{x})$	$\exists y\, (\psi_s(\vec{x}, y) \wedge \psi_t(\vec{x}, y))$
$R(t_1(\vec{x}), \ldots, t_n(\vec{x}))$	$\exists y_1, \ldots, y_n\, (\psi_{t_1}(\vec{x}, y_1) \wedge \cdots \wedge \psi_{t_n}(\vec{x}, y_n)$ $\wedge\, \psi_R(y_1, \ldots, y_n))$

Thus the definition of the map $\varphi \rightsquigarrow \varphi^{\mathfrak{I}}$ extends to all formulæ.

The proof is complete once we show that if $\sigma \in \mathsf{LAx}_{\mathsf{L}_1}$, then $\mathsf{T}_0 \vdash_{\mathsf{L}_0} \sigma^{\mathfrak{I}}$. We will prove that $\mathcal{A} \vDash \ulcorner \sigma^{\mathfrak{I}} \urcorner$ for all $\mathcal{A}$ models of T_0, and the appeal to the completeness theorem. All logical axioms σ are the form $\forall x_1, \ldots, x_n\, \theta$ so $\sigma^{\mathfrak{I}}$ is $\forall x_1, \ldots, x_n\, (\upsilon(x_1) \wedge \cdots \wedge \upsilon(x_n) \Rightarrow \theta^{\mathfrak{I}})$, and therefore it is enough to show that $\theta^{\mathfrak{I}}$ is a valid L_0-formula.

If σ is a tautology axiom, the result is trivial. If σ is an equality axiom, then θ is a logical identity of L_1:

(i) $t = t$,

(ii) $t = s \Rightarrow s = t$,

(iii) $t_1 = s_1 \wedge \cdots \wedge t_n = s_n \Rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$,

(iv) $t_1 = s_1 \wedge \cdots \wedge t_n = s_n \wedge R(t_1, \ldots, t_n) \Rightarrow R(s_1, \ldots, s_n)$,

where for the sake of brevity we have suppressed the dependence on $\vec{x}$ of the terms in the formulæ above. The verification that if θ is as in (i)–(iv) then $\theta^{\mathfrak{I}}$ is valid is straightforward. If σ is an axiom of quantification, then θ is of the form

(A) $\varphi \Rightarrow \forall \mathsf{x}\varphi$, with x not free in φ,

(B) $\varphi(\!|\mathsf{t}_1/\mathsf{x}_1, \dots, \mathsf{t}_n/\mathsf{x}_n|\!) \Rightarrow \exists \mathsf{x}_1 \dots \exists \mathsf{x}_n \varphi$,

(C) $\forall \mathsf{x} \neg \varphi \Rightarrow \neg \exists \mathsf{x} \varphi$,

(D) $\forall \mathsf{x}(\varphi \Rightarrow \psi) \Rightarrow (\forall \mathsf{x}\varphi \Rightarrow \forall \mathsf{x}\psi)$.

Let us argue that if θ is of type (A) then $\theta^{\mathfrak{I}}$ is valid: if $\varphi^{\mathfrak{I}} \Rightarrow \forall \mathsf{x}(\upsilon(\mathsf{x}) \Rightarrow \varphi^{\mathfrak{I}})$ were not valid, there would be an L_1-structure $\mathcal{A}$ and an assignment g such that $\mathcal{A} \vDash_g \ulcorner \varphi^{\mathfrak{I}} \urcorner$ but $\mathcal{A} \vDash \ulcorner \exists \mathsf{x}(\upsilon(\mathsf{x}) \wedge \neg \varphi^{\mathfrak{I}}) \urcorner$, which is absurd, since $\mathsf{x} \notin \mathrm{Fv}(\varphi)$. The case of the axioms of type (B)–(D) is similar. □

Example 35.15. PA is interpretable in $\mathsf{ZF} - \mathsf{Inf}$. Let $\upsilon(x)$ be the formula $x \in \omega$, that is $x \in \mathrm{Ord} \wedge \forall y \in x\,(y = \emptyset \vee \exists z \in y\,(\mathbf{S}(z) = y))$, and let $\varphi_{\mathsf{S}}(x, y)$, $\varphi_{+}(x, y, z)$, $\varphi_{\cdot}(x, y, z)$ be the formulæ defining the successor operation and addition and multiplication on ω.

Conversely, $\mathsf{ZF} - \mathsf{Inf}$ is interpretable in PA by means of the map $\mathfrak{a}^{-1} \colon \mathrm{V}_\omega \to \omega$ of Section 24.B. In this case $\upsilon(x)$ is simply $x = x$, and $(x \in y)^{\mathfrak{I}}$ becomes $\mathfrak{a}^{-1}(x) \mathrel{\mathfrak{E}} \mathfrak{a}^{-1}(y)$, where $\mathfrak{E}$ is as in (24.1).

Corollary 35.16. *The theories* PA *and* $\mathsf{ZF} - \mathsf{Inf}$ *are equiconsistent.*

36. Undecidability

36.A. Undecidability in number theory. For T a theory in a language with numerals, and for $\varphi(\mathsf{v}_0)$ a formula let

$$P_T(\varphi) = \{n \in \mathbb{N} \mid T \vdash \varphi(\!|\overline{n}/\mathsf{v}_0|\!)\}. \tag{36.1}$$

If T is inconsistent, then $P_T(\varphi) = \mathbb{N}$ for all φ, so this notion is of interest only when T is consistent.

Proposition 36.1. *If T is a consistent theory extending* Q *and $A \subseteq \mathbb{N}$ is computable, then there is $\varphi \in \mathrm{Fml}(\mathsf{v}_0)$ such that $A = P_T(\varphi)$.*

Proof. Let $\varphi(\mathsf{v}_0)$ be a formula representing A in Q. If $n \in A$ then $\mathsf{Q} \vdash \varphi(\!|\overline{n}/\mathsf{v}_0|\!)$, and hence $T \vdash \varphi(\!|\overline{n}/\mathsf{v}_0|\!)$, so that $n \in P_T(\varphi)$. If $n \notin A$, then $\mathsf{Q} \vdash \neg\varphi(\!|\overline{n}/\mathsf{v}_0|\!)$, and hence $T \vdash \neg\varphi(\!|\overline{n}/\mathsf{v}_0|\!)$, so $T \nvdash \varphi(\!|\overline{n}/\mathsf{v}_0|\!)$ by the consistency, and hence $n \notin P_T(\varphi)$. □

The next result, **Gödel's First Incompleteness Theorem** is one of the most celebrated theorems of mathematical logic.

Theorem 36.2. Q *is essentially incomplete.*

Proof. Let T be a consistent theory extending Q: we will argue that T is not decidable. Let $\bar{P}$ be the set of all pairs (φ, n) such that $\mathsf{T} \vdash \varphi(\!|\overline{n}/\mathsf{v}_0|\!)$, so working inside Q, the encoding theory, we define

$$\bar{P} = \{(m, n) \in \mathrm{Fml} \times \mathbb{N} \mid \mathrm{Sbst}(m, \overline{n}, \boldsymbol{v}_0) \in \mathrm{Thm}(\ulcorner \mathsf{T} \urcorner)\}.$$

Then $\{n \in \mathbb{N} \mid (m,n) \in \bar{P}\} = P_{\mathsf{T}}(m)$ for each $m \in \mathrm{Fml}$, where P_{T} is as in (36.1). The set

$$G = \{n \in \mathbb{N} \mid (n,n) \notin \bar{P}\} = \{n \in \mathbb{N} \mid \mathrm{Sbst}(n, \overline{n}, \boldsymbol{v}_0) \notin \mathrm{Thm}(\ulcorner \mathsf{T} \urcorner)\}$$

is the set of all $\boldsymbol{\varphi}(\boldsymbol{v}_0)$ such that $\mathsf{T} \nvdash \boldsymbol{\varphi}(\!|\overline{n}/\boldsymbol{v}_0|\!)$ with $n = \boldsymbol{\varphi}$. (Keep in mind that coded objects such as $\boldsymbol{\varphi}$, $\boldsymbol{v}_0$, and $\overline{n}$ are natural numbers!) We claim that G is not computable. Otherwise $G = P_{\ulcorner \mathsf{T} \urcorner}(k)$ for some $k \in \mathrm{Fml}$, and therefore

$$k \in G \Leftrightarrow (k,k) \notin \bar{P} \Leftrightarrow k \notin P_{\ulcorner \mathsf{T} \urcorner}(k)$$

a contradiction! If T were decidable, then $\mathrm{Thm}(\ulcorner \mathsf{T} \urcorner)$ would be computable, then so would be G, and hence the result is proved. □

36.B. Undecidability in set theory.

36.C. Undecidability in logic. In particular, Q is undecidable, that is to say: $\{\varphi \mid \bigwedge_{1 \leq i \leq 9} \mathsf{Q}i \vdash \varphi\}$ is not computable. By Lemma 33.6 this is the same as $\{\varphi \mid \vdash \bigwedge_{1 \leq i \leq 9} \mathsf{Q}i \Rightarrow \varphi\}$, so this amounts to say that the set of all valid formulæ of the language of Q is undecidable. This implies that if $\mathcal{L}$ is any first-order language with two binary function symbols, one unary function symbol, and one constant symbol, then $\{\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L}) \mid \vdash \boldsymbol{\sigma}\}$ is not computable. The next result summarizes what is known.

Theorem 36.3. *Let $\mathcal{L}$ be a computable first-order language and let $V = \{\boldsymbol{\sigma} \in \mathrm{Sent}(\mathcal{L}) \mid \vdash \boldsymbol{\sigma}\}$ be the set of all valid $\mathcal{L}$-sentences.*

(a) *If $\mathcal{L}$ satisfies any of the following*
- *it has at least one n-ary predicate symbol, with $n \geq 2$;*
- *it has at least one n-ary function symbol, with $n \geq 2$;*
- *it has at least two unary function symbols,*

then V is not computable.

(b) *If $\mathcal{L}$ satisfies has only unary predicate symbols, or else has just one unary function symbol, then V is computable.*

In other words, there is no method to effectively determine whether a certain statement in the $\mathcal{L}_{\mathsf{Q}}$ is logically valid. By Corollary **??** the empty theory in the language $\mathcal{L}_{\mathsf{Q}}$ is incomplete, but it is not essentially incomplete: adding the axiom $\forall x, y (x = y)$ yields a complete theory.

36.D. Unprovability of consistency. The next result is known as **Gödel's Second Incompleteness Theorem**: it says that no consistent, sufficiently strong, effectively axiomatizable theory can prove its own consistency.

Theorem 36.4. *If T is a consistent, effectively axiomatizable theory in $\mathcal{L}_{\mathsf{PA}}$ extending PA, then $\mathsf{T} \nvdash \mathrm{Con}(\ulcorner \mathsf{T} \urcorner)$.*

We end this section with Tarski's result on undefinability of truth, a result that is closely related to Gödel's First Incompleteness Theorem 36.2. Recall that if $\mathcal{M} = \langle M, \dots \rangle$ is an $\mathcal{L}$-structure, then $\mathrm{Def}^k_{\mathcal{M}}(P)$ is the collection of all subsets of M^k definable in $\mathcal{M}$ with parameters in $P \supseteq M$.

Theorem 36.5. *If* $\mathcal{M}$ *is a model of* PA*, then*

$$\{\boldsymbol{\sigma} \in \mathrm{Sent} \mid \mathcal{M} \vDash \boldsymbol{\sigma}\} \notin \mathrm{Def}^1_{\mathcal{M}}(\emptyset),$$

$$\{(\boldsymbol{\varphi}, m) \in \mathrm{Fml}(\boldsymbol{x}) \times M \mid \mathcal{M} \vDash \boldsymbol{\varphi}[m]\} \notin \mathrm{Def}^2_{\mathcal{M}}(M).$$

36.E. Undecidable structures.

To be written later

Exercises

Exercise 36.6. Give an example of a theory T in an effective language such that $\mathrm{Thm}(T)$ is decidable, yet T is not computable.

Exercise 36.7. Suppose that $T \subseteq \mathrm{Sent}$ is effectively enumerable. Show that it is effectively axiomatizable.

37. Metamathematics of set theory

37.A. Another look at the axioms of ZF. We recall the axioms of ZF, and for future reference, we introduce specific acronyms for them:

Ext: $\forall x, y\ (\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$, the axiom of extensionality

Prn: $\forall x \forall y \exists z\, (x \in z \wedge y \in z)$, the axiom of pairing

Unn: $\forall x \exists u \forall y \forall z\, (z \in y \wedge y \in x \Rightarrow z \in u)$, the axiom of union

Pwr: $\forall x \exists y \forall z\, (z \subseteq x \Rightarrow z \in y)$, the powerset axiom

Inf: $\exists x\, (\emptyset \in x \wedge \forall y \in x\, (\mathbf{S}(y) \in x))$, the axiom of infinity

Fnd: $\forall x(\exists y(y \in x) \Rightarrow \exists y(y \in x \wedge \neg \exists z(z \in x \wedge z \in y)))$, the axiom of foundation

Spr: the axiom-schema of separation, if y does not occur free in $\varphi(x, z, \vec{w})$, then $\forall z \forall \vec{w} \exists y \forall x\, (x \in y \Leftrightarrow x \in z \wedge \varphi(x, z, \vec{w}))$

Rpl: the axiom-schema of replacement, if B does not occur free in $\varphi(x, y, A, \vec{w})$,

$$\forall A \forall \vec{w}\, (\forall x \in A \exists! y \varphi \Rightarrow \exists B \forall x \in A \exists y \in B \varphi(x, y, A, \vec{w}))$$

The axiom of pairing Prn requires that given two sets x, y there is a third set z to which x, y belong. This axiom can be strengthened by requiring that z has only x and y as elements. Similarly, the axioms of union and power-set can be stated in a slightly sharper form.

Prn^+: $\forall x \forall y \exists z \forall w\, (w \in z \Leftrightarrow w = x \vee w = y)$,

Unn^+: $\forall x \exists u \forall w\, (w \in u \Leftrightarrow \exists y (w \in y \wedge y \in x))$,

Pwr^+: $\forall x \exists y \forall z\, (z \subseteq x \Leftrightarrow z \in y)$.

By separation, these sharper versions follow from the regular ones.

Zermelo's set theory Z is obtained from ZF by removing Rpl, and ZC is $\mathsf{Z} + \mathsf{AC}$.

37.A.1. *Alternative formulations of replacement and foundation.* The **axiom of collection** Clct is the following schema of statements: if B does not occur free in $\varphi(x, y, A, w_1, \dots, w_n)$, then

$$\forall A \forall \vec{w}\, (\forall x \in A \exists y \varphi(x, y, A, \vec{w}) \Rightarrow \exists B \forall x \in A \exists y \in B \varphi(x, y, A \vec{w}))\,.$$

Collection is a strengthening of replacement, since we are dealing with relations rather than functions. On the other hand, in the presence of the other axioms of ZF it is not a real strengthening.

Theorem 37.1. *The axiom schema of collection is provable in* ZF*, so* ZF *can be axiomatized by* $\mathsf{Z} + \mathsf{Clct}$*.*

Proof. Assume that $\forall x \in A \exists y \varphi(x, y, A, \vec{w})$: given $x \in A$ let $B = \bigcup_{x \in A} Y_x$, where $Y_x = \{y \mid \varphi(x, y, A, \vec{w}) \wedge \operatorname{rank}(y) \text{ is minimal}\}$. Then $\forall x \in A \exists y \in B \varphi(x, y, A, \vec{w})$. □

Although Rpl and Clct are equivalent over Z, the same need not be true for other sub-theories of ZF. In the absence of the powerset axiom, Clct is stronger than Rpl. For this reason when working with $\mathsf{ZF} - \mathsf{Pwr}$, the Zermelo-Frænkel set theory minus the powerset axiom, it is customary to list among the axioms Clct rather than Rpl.

Another axiomatization of ZF is obtained by using tight replacement instead of the two axiom schemata of separation and replacement (Exercise 37.20). The **axiom schema of tight replacement** tRpl says that

$$\begin{aligned}\forall A \forall \vec{w} (\forall x \in A \neg \exists y, y' (y \neq y' \wedge \varphi(x, y, A, \vec{w}) \wedge \varphi(x, y', A, \vec{w}))\\ \Rightarrow \exists B \forall y (y \in B \Leftrightarrow \exists x \in A \varphi(x, y, A, \vec{w})))\end{aligned}$$

for every formula $\varphi(x, y, A, w_1, \dots, w_n)$ and every variable B that does not occur free in it.

The **axiom schema of set-induction** $\mathsf{Ind}_\in$ says that: for any $\varphi(x, \vec{w})$

$$\forall \vec{w} [\forall x\, (\forall y \in x\, \psi(y, \vec{w}) \Rightarrow \psi(x, \vec{w}))\ \Rightarrow \forall x \psi(x, \vec{w})].$$

By taking the contrapositive, $\mathsf{Ind}_\in$ can be stated as: for any $\varphi(x, \vec{w})$

$$\forall \vec{w} [\exists x \varphi(x, \vec{w}) \Rightarrow \exists x\, (\varphi(x, \vec{w}) \wedge \forall y \in x\, \neg \varphi(y, \vec{w}))].$$

If $A \neq \emptyset$ then applying $\mathsf{Ind}_{\in}$ to the formula $x \in A$ yields an $a \in A$ such that $a \cap A = \emptyset$, so set-induction implies foundation. Conversely, assuming foundation and working in ZF, if $\varphi(x, \vec{w})$ holds for some x, then take such x of least rank, and hence $\mathsf{Ind}_{\in}$ holds. Therefore we have proved:

Proposition 37.2. *$\mathsf{Ind}_{\in}$ and Fnd are equivalent over $\mathsf{ZF} - \mathsf{Fnd}$.*

37.B. The Levy hierarchy of formulæ. By Definition 19.17 and 19.18, a $\mathcal{L}_{\in}$-formula is $\Delta_0 = \Sigma_0 = \Pi_0$ if it belongs to the smallest collection of formulæ containing the atomic ones, and closed under connectives and bounded quantifications; a formula is Σ_1 if it is the existential quantification of a Δ_0 formula, and a formula is Π_1 if it is the universal quantification of a Δ_0 formula.

Definition 37.3. A $\mathcal{L}_{\in}$-formula is

- Σ_{n+1} if it is of the form $\exists x\, \varphi$ with φ a Π_n-formula,
- Π_{n+1} if it is of the form $\forall x\, \varphi$ with φ a Σ_n-formula.

If T is an effective $\mathcal{L}_{\in}$-theory, we say that a formula is

- Σ_n^{T} if it is (provably in T) equivalent to a Σ_n-formula,
- Π_n^{T} if it is (provably in T) equivalent to a Π_n-formula,
- Δ_n^{T} if it is both Σ_n^{T} and Π_n^{T}.

By the prenex normal form algorithm, and by adding some dummy quantifiers if needed, every formula is logically equivalent to a Σ_n and to a Π_n formula. For example "r is a well-founded relation on x" is (logically equivalent to) a Π_1 formula

$$\begin{aligned}&\forall c \in r\, \exists a \in x\, \exists b \in x\, (c = (a, b))\\ &\qquad\qquad\qquad \wedge\ \forall y\, (\emptyset \neq y \subseteq x \Rightarrow \exists a \in y\, \forall b \in y\, \forall c \in r\, (c \neq (b, a))).\end{aligned}$$

Here we are using that "$c = (a, b)$" is Δ_0—see Section 19.F.1. By replacement it is also equivalent to the Σ_1 formula

$$\begin{aligned}&\forall c \in r\, \exists a \in x\, \exists b \in x\, (c = (a, b))\\ &\qquad \wedge\ \exists f\, (\mathsf{Fn}(f) \wedge \operatorname{dom} f = x \wedge \forall y, z \in x\, ((y, z) \in r \Rightarrow f(y) \in f(z))),\end{aligned}$$

where $\mathsf{Fn}(f)$ stands for "f is a function". Therefore "r is a well-founded relation on x" is Δ_1^{ZF}, but in the absence of replacement this might fail.

The next result is the analogue of Corollary 24.5.

Lemma 37.4. (a) *If $\mathsf{T} \vdash \mathsf{Ext} \wedge \mathsf{Prn}$, and φ and ψ are Σ_1^{T}, then $\exists x \varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, and $\exists x \in w\, \varphi$ are Σ_1^{T}.*

(b) *If $\mathsf{T} \vdash \mathsf{Clct}$ and φ is Σ_1^{T} then $\forall y \in x\, \varphi$ is Σ_1^{T}.*

Proof. (a) Suppose T proves that φ and ψ are equivalent to $\exists y \varphi'$ and $\exists z \psi'$, with φ' and ψ' in Δ_0. Without loss of generality we may assume that y and z are distinct variables, and different from w. Arguing in T

- $\exists x \varphi$ is equivalent to $\exists u \exists x \in u \, \exists y \in u \, \varphi'$;
- $\varphi \wedge \psi$ is equivalent to $\exists y \exists z(\varphi' \wedge \psi')$ and $\varphi \vee \psi$ is equivalent to $\exists y \exists z(\varphi' \vee \psi')$, so we apply the previous point;
- $\exists x \in w \, \varphi$ is $\exists x(x \in w \wedge \exists y \varphi')$, which is Σ_1 by the previous points.

(b) Without loss of generality we may assume that φ is $\exists z \, \theta$ with θ a Δ_0-formula. Then $\mathsf{T} \vdash \forall y \in x \, \exists z \, \theta \Leftrightarrow \exists u \forall y \in x \, \exists z \in u \, \theta$, since the forward implication follows from collection, and the reverse implication is trivial. □

If Γ is either Σ^{T}_n, or Π^{T}_n, or Δ^{T}_n, then a Γ **predicate** is a class defined by a Γ formula, and a Γ **operation** is a class-function defined by a Γ formula. Arguing as in Proposition 24.8:

Lemma 37.5. *Suppose* $\mathsf{T} \vdash \mathsf{Ext} \wedge \mathsf{Prn}$.

(a) *If F is a Σ^{T}_1 operation, then its domain and its range are Σ^{T}_1 predicates.*

(b) *The composition of Σ^{T}_1 operations is a Σ^{T}_1 operation.*

(c) *If F is a Σ^{T}_1 operation whose domain is a Δ^{T}_1 predicate, then F is a Δ^{T}_1 operation.*

(d) *The composition of Δ^{T}_1 operations is a Δ^{T}_1 operation; the substitution of Δ^{T}_1 operation inside a Δ^{T}_1 predicate is a Δ^{T}_1 predicate.*

(e) *Suppose $S_j(\vec{x})$ and $G_j(\vec{x})$ $(j \leq n)$ are Δ^{T}_1 predicates, and that $\mathsf{T} \vdash \forall \vec{x} \bigvee_{j \leq n} S_j(\vec{x})$ and $\mathsf{T} \vdash \forall \vec{x} \neg (S_i(\vec{x}) \wedge S_j(\vec{x}))$ for $i < j \leq n$. Then*

$$R(\vec{x}) \Leftrightarrow \begin{cases} G_0(\vec{x}) & \textit{if } S_0(\vec{x}), \\ \vdots & \\ G_n(\vec{x}) & \textit{if } S_n(\vec{x}), \end{cases}$$

is Δ^{T}_1 predicate.

(f) *Moreover if $\mathsf{T} \vdash \mathsf{Ind}_\in$, and $\mathsf{T} \vdash \forall \vec{x} \exists y \, (\mathsf{Ord}(y) \wedge G(\vec{x}, y))$, where $G(\vec{x}, y)$ is a Δ^{T}_1 predicate, then the operation $F(\vec{x}) = \boldsymbol{\mu} \alpha \, G(\vec{x}, \alpha)$ is Δ^{T}_1.*

37.C. Relativization and inner models.

Definition 37.6. Let $\upsilon(x, \vec{z})$ and $\varepsilon(x, y, \vec{z})$ be formulæ with x occurring free in υ and x, y occurring free in ε, but neither of x, y occurring in $\varphi(x_1, \ldots, x_n)$. The **relativization of φ to υ, ε** is the formula $\varphi^{(\upsilon,\varepsilon)}$ defined as follows:

- if φ is $x_1 = x_2$ then $\varphi^{(\upsilon,\varepsilon)}$ is φ,
- if φ is $x_1 \in x_2$ then $\varphi^{(\upsilon,\varepsilon)}$ is $\varepsilon(x_1, x_2)$,

- if φ is $\neg\psi$, then $\varphi^{(\upsilon,\varepsilon)}$ is $\neg\psi^{(\upsilon,\varepsilon)}$,
- if φ is $\psi \vee \chi$, then $\varphi^{(\upsilon,\varepsilon)}$ is $\psi^{(\upsilon,\varepsilon)} \vee \chi^{(\upsilon,\varepsilon)}$,
- if φ is $\exists y\psi$, then $\varphi^{(\upsilon,\varepsilon)}$ is $\exists y(\upsilon(y,\vec{z}) \wedge \psi^{(\upsilon,\varepsilon)})$.

If $\varepsilon(x,y)$ is $x \in y$ then it is customary to write $\varphi^{(\upsilon)}$. In particular, if z is a variable then $\varphi^{(z)}$ is $\varphi^{(\upsilon)}$ where $\upsilon(x,z)$ is $x \in z$.

If υ has only x as free variable, $\mathsf{T}_1 \vdash \exists x\upsilon(x)$ and $\mathsf{T}_1 \vdash \sigma^{(\upsilon)}$ for all $\sigma \in \mathsf{T}_0$, then we have an interpretation of T_0 in T_1.

As $(\forall y\varphi)^{(\psi)}$ is just $\forall y(\psi(y,\vec{z}) \Rightarrow \varphi^{(\psi)})$, it follows that relativizing φ to ψ is tantamount to restricting all quantified variables of φ to range over the class $\{x \mid \psi(x,\vec{v})\}$.

Work in some set theory where the only acceptable objects are *sets*, for example (a strengthening or weakening of) ZF. Thus a class M is of the form $M = \{x \mid \upsilon(x,\vec{z})\}$, and let $\varphi^{(M)}$ be $\varphi^{(\upsilon)}$—if M is actually a set, then υ is the formula $x \in M$. If M is a set and $a_1,\dots,a_n \in M$, an easy induction on the complexity of φ shows that

$$\varphi(a_1,\dots,a_n)^{(M)} \Leftrightarrow \langle M,\in\rangle \vDash \ulcorner\varphi\urcorner[a_1,\dots,a_n]. \tag{37.1}$$

Therefore relativization is the syntactic counterpart of the satisfaction relation. In particular, when M is a proper class, writing $\varphi(a_1,\dots,a_n)^{(M)}$ amounts to say that $\varphi(a_1,\dots,a_n)$ is true in M.

A list of formulæ $\varphi_1,\dots,\varphi_n$ is said to be closed under sub-formulæ if any sub-formula of φ_i is a φ_j. Any finite list of formulæ can be expanded to a finite list which is closed under sub-formulæ. The following is the syntactic analogue of Theorem 4.26, the Tarski-Vaught criterion for being an elementary substructure.

Lemma 37.7. *Let $M \subseteq N$ be classes and suppose $\varphi_1,\dots,\varphi_n$ is closed under sub-formulæ. The following are equivalent*

(a) *$\varphi_1,\dots,\varphi_n$ are absolute between M and N,*

(b) *if φ_i is $\exists x\varphi_j(x,y_1,\dots,y_k)$, then*

$$\forall y_1,\dots,y_k \in M\,(\exists x \in N\,\varphi_j^{(N)}(x,y_1,\dots,y_k) \Rightarrow \exists x \in M\,\varphi_j^{(N)}(x,y_1,\dots,y_k)).$$

Proof. (a)⇒(b): Suppose $\vec{y} \in M$ and $\exists x \in N\,\varphi_j^{(N)}(x,\vec{y})$, that is $\varphi_i^{(N)}(\vec{y})$. By absoluteness $\varphi_i^{(M)}(\vec{y})$ that is $\varphi_j^{(M)}(\bar{x},\vec{y})$, for some $\bar{x} \in M$. By absoluteness $\varphi_j^{(N)}(\bar{x},\vec{y})$, so $\exists x \in M\,\varphi_j^{(N)}(x,\vec{y})$.

(b)⇒(a): Let us prove by induction on the complexity that φ_i is absolute between M and N. If φ_i is atomic, or elseis of the form $\neg\varphi_j$ or $\varphi_j \vee \varphi_h$, the result follows at once. If φ_i is $\exists x \varphi_j$ then by inductive assumption φ_j is absolute between M and N, so

$$\varphi_i^{(M)} \Leftrightarrow \exists x \in M\, \varphi_j^{(M)} \Leftrightarrow \exists x \in M\, \varphi_j^{(N)} \Rightarrow \exists x \in N\, \varphi_j^{(N)} \Leftrightarrow \varphi_i^{(N)}.$$

Conversely using (b):

$$\varphi_i^{(N)} \Leftrightarrow \exists x \in N\, \varphi_j^{(N)} \Rightarrow \exists x \in M\, \varphi_j^{(N)} \Leftrightarrow \exists x \in M\, \varphi_j^{(M)} \Leftrightarrow \varphi_i^{(M)}. \qquad \square$$

Generalizing Definition 19.19 we have:

Definition 37.8. If $M \subseteq N$ are classes, we say that $\varphi(x_1, \dots, x_n)$ is

- **upward absolute** between M and N if $\forall \vec{x} \in M \left(\varphi^{(M)} \Rightarrow \varphi^{(N)} \right)$;
- **downward absolute** between M and N if $\forall \vec{x} \in M \left(\varphi^{(N)} \Rightarrow \varphi^{(M)} \right)$;
- **absolute** between M and N if it is both upward and downward absolute, that is $\forall \vec{x} \in M \left(\varphi^{(M)} \Leftrightarrow \varphi^{(N)} \right)$.

Arguing as in Lemmata 19.20 and 19.21:

Lemma 37.9. *If $\emptyset \neq M \subseteq N$ are classes and $\varphi(\vec{x})$ is quantifier-free, then $\forall \vec{x} \in M \left(\varphi^{(M)} \Leftrightarrow \varphi^{(N)} \right)$.*

Lemma 37.10. *Suppose $M \subseteq N$ are classes with $M \neq \emptyset$ transitive, and let $\varphi(\vec{x})$ be a formula.*

(a) *If $\varphi(\vec{x})$ is Δ_0, then $\forall \vec{x} \in M \left(\varphi^{(M)} \Leftrightarrow \varphi^{(N)} \right)$.*

(b) *If $\varphi(\vec{x})$ is Σ_1 then $\forall \vec{x} \in M\, (\varphi^{(M)} \Rightarrow \varphi^{(N)})$; if φ is Π_1 then $\forall \vec{x} \in M\, (\varphi^{(N)} \Rightarrow \varphi^{(M)})$.*

Definition 37.11. Let T be an effective $\mathcal{L}_\in$-theory. A transitive class M is an **inner model of** T if $\sigma^{(M)}$ holds for every axiom σ of T.

Examples 37.12. Let M be a transitive inner model of ZF.

(a) $\mathsf{Ord}(x)$ is Δ_0, so $\mathrm{Ord} \cap M = \{x \in M \mid \mathsf{Ord}(x)^{(M)}\}$.

(b) The formula $\mathsf{Card}(x)$ saying that "x is a cardinal" is logically equivalent to a Π_1 formula:

$$\mathsf{Ord}(x) \wedge \forall \nu \in x\, \neg \exists f\, (\underbrace{f \colon \nu \to x \text{ is a bijection}}_{\varphi(f,\nu,x)})$$

and $\varphi(f, \nu, x)$ is Δ_0—see Table 3 on page 411. Therefore $\mathsf{Card}(\kappa) \Rightarrow \mathsf{Card}(\kappa)^{(M)}$, but the converse implication may fail.

(c) Similarly, "γ is a singular ordinal" is logically equivalent to a Σ_1 formula:

$$\mathsf{Ord}(\gamma) \wedge \exists f\, \exists \nu \in \gamma\, (f \colon \nu \to \gamma \text{ is cofinal}).$$

Therefore κ is regular $\Rightarrow$ (κ is regular)$^{(M)}$, but the converse implication may fail.

(d) If $\varphi(\alpha, x)$ is the formula asserting that $x = \mathrm{V}_\alpha$, then

$$\forall \alpha \in M\,(\mathrm{V}_\alpha \cap M \in M \ \wedge\ \varphi(\alpha, \mathrm{V}_\alpha \cap M)^{(M)}).$$

When $\alpha = 0$ or α limit, this is clear. If $\alpha = \mathbf{S}(\beta)$ then by inductive assumption $y = \mathrm{V}_\beta \cap M \in M$ and $\varphi(\beta, y)^{(M)}$, so

$$x = \mathrm{V}_\alpha \cap M = \mathscr{P}(\mathrm{V}_\beta) \cap M = \mathscr{P}(y) \cap M \in M$$

and hence $\varphi(\alpha, x)^{(M)}$.

When dealing with transitive inner models, it is convenient to extend the notation adopted for relativization to terms and classes. For example:

- $\mathscr{P}(x)^{(M)}$ is the set in M that collects every subset of x belonging to M, and hence $\mathscr{P}(x)^{(M)} = \mathscr{P}(x) \cap M$;
- $\mathrm{Card}^{(M)} = \{\alpha \in M \mid \mathsf{Card}(\alpha)^{(M)}\}$ is the class of all sets that M believes to be cardinals, and hence $\mathrm{Card} \subseteq \mathrm{Card}^{(M)}$;
- $(\kappa^+)^{(M)}$ is the least element that M believes to be a cardinal bigger than κ, and hence $(\kappa^+)^{(M)} \leq \kappa^+$;

and so on.

Proposition 37.13. *Suppose M is an inner model of* ZF*, and let $G(\alpha, x, w)$ be a Δ_1^{ZF} operation. If $w \in M$ then the function $F\colon \mathrm{Ord} \cap M \to \mathrm{V}$, $F(\alpha) = G(\alpha, F \restriction \alpha, w)$ is absolute between M and* V*, and* $\operatorname{ran} F \subseteq M$.

Proof. $F(\alpha) = y$ if and only if

$$\begin{aligned}\mathsf{Ord}(\alpha) \wedge \exists f \bigl[&\mathsf{Fn}(f) \wedge \mathsf{Trans}(\operatorname{dom} f) \wedge \alpha \in \operatorname{dom} f \wedge f(\alpha) = y \\ &\wedge \forall \beta \in \operatorname{dom} f\,(f(\beta) = G(\beta, f \restriction \beta, w))\bigr].\end{aligned}$$

The formula above Σ_1^{ZF} so F is a Δ_1^{ZF}-operation and hence absolute between M and V. If $\alpha \in \mathrm{Ord}$ then $\alpha \in M$ and since $\exists y\,(y = F(\alpha))$ holds in V, then $\exists y \in M\,(y = F(\alpha))^{(M)}$, that is $F(\alpha) \in M$. Therefore $\operatorname{ran} F \subseteq M$. □

A similar argument proves that

Proposition 37.14. *Suppose M is an inner model of* ZF *and $G(n, x, w)$ is a Δ_1^{ZF}-operation. If $w \in M$ then the function $F\colon \omega \to \mathrm{V}$ defined by $F(0) = y_0 \in M$ and $F(n+1) = G(n, F(n), w)$ is absolute between M and* V*,* $\operatorname{ran} F \in M$*, and $\bigcup_{n \in \omega} F(n) \in M$.*

Using the notation introduced at the beginning of this section, and arguing as in Theorem 19.22:

Theorem 37.15. *Suppose $M \neq \emptyset$ is a transitive class. Then*

(a) $\mathsf{Ext}^{(M)}$ *and* $\mathsf{Fnd}^{(M)}$.

(b) $(\mathsf{Prn}^+)^{(M)}$ *if and only if* $\forall a, b \in M\,(\{a,b\} \in M)$.

(c) $(\mathsf{Unn}^+)^{(M)}$ *if and only if* $\forall a \in M\,(\bigcup a \in M)$.

(d) $(\mathsf{Pwr}^+)^{(M)}$ *if and only if* $\forall a \in M\; (\mathscr{P}(a) \cap M \in M)$.

(e) *If* $\omega \in M$ *then* $\mathsf{Inf}^{(M)}$.

(f) *If* $\forall a \in M\,(\mathscr{P}(a) \subseteq M)$ *then* $\mathsf{Spr}^{(M)}$.

(g) *If* $\forall a \in M\, \forall f\colon a \to M\, \exists b \in M\, (\operatorname{ran} f \subseteq b)$, *then* $\mathsf{Rpl}^{(M)}$.

(h) $\mathsf{AC}^{(M)}$ *if and only if* $\forall \mathcal{A} \in M\, (\forall A \in \mathcal{A}\, (A \neq \emptyset) \Rightarrow \exists f \in M\, (f$ *is a choice function for* $\mathcal{A}))$.

A class M is **almost universal** if for every set $x \subseteq M$ there is $y \in M$ such that $x \subseteq y$. Note that an almost universal class must be a proper class. If $M \cap \mathrm{V}_\alpha \in M$ for a proper class of αs, then M is almost universal. In particular, Ord is almost universal.

Proposition 37.16. *Suppose M is a transitive, almost universal class. If* $\mathsf{Spr}^{(M)}$*, then M is an inner model for* ZF.

Proof. The result is a straightforward application of Theorem 37.15 and $\mathsf{Spr}^{(M)}$. The case of Ext and Fnd is immediate, and for Prn, Unn, and Pwr argue as follows:

- if $a, b \in M$ then $x = \{a, b\} \subseteq M$ and $\exists y \in M\,(x \subseteq y)$, so $x = \{z \in y \mid z = a \vee z = b\} \in M$ by $\mathsf{Spr}^{(M)}$;
- if $a \in M$ then $x = \bigcup a \subseteq M$ by transitivity of M, and $\exists y \in M\,(x \subseteq y)$, so $x = \{z \in y \mid \exists w \in a\,(z \in w)\} \in M$ by $\mathsf{Spr}^{(M)}$;
- if $a \in M$ then $x = \mathscr{P}(a) \cap M \subseteq M$ and $\exists y \in M\,(x \subseteq y)$, so $x = \{z \in y \mid z \subseteq a\} \in M$ by $\mathsf{Spr}^{(M)}$.

In order to prove $\mathsf{Inf}^{(M)}$ it is enough to show that $\omega \in M$. As M is closed under unions and the operation of taking singletons, $\omega \subseteq M$ and hence $\omega \subseteq y \in M$ for some $y \in M$. By $\mathsf{Spr}^{(M)}$ the set $z = \{x \in y \mid \mathsf{Ord}(x)\} = \{x \in y \mid \mathsf{Ord}^{(M)}(x)\}$ belongs to M, and $\omega \subseteq z$. If $z = \omega$ we are done, otherwise there is $\alpha \in z \setminus \omega$, and $\omega \leq \alpha \in M$, so $\omega \in M$ in any case.

To complete the proof we verify $\mathsf{Rpl}^{(M)}$. Given $\varphi(x, y, z, \vec{w})$ we must show that

$$\big(\forall \vec{w}, z\ (\forall x \in z\, \exists! y\, \varphi \Rightarrow \exists u\, \forall x \in z\, \exists y \in u\, \varphi)\big)^{(M)}.$$

Fix $\vec{w}, z \in M$ and suppose that $(\forall x \in z\, \exists! y\, \varphi)^{(M)}$. Then $(\forall x \in z\, \exists y\, \varphi)^{(M)}$ and hence by transitivity of M, $\forall x \in z\, \exists y \in M\, \varphi^{(M)}$. Then $u = \{y \in M \mid \exists x \in z\, \varphi^{(M)}\} \subseteq M$ is a set, so there is $v \in M$ such that $u \subseteq v$, and hence $u = \{y \in v \mid \exists x \in z\, \varphi^{(M)}\}$ belongs to M by $\mathsf{Spr}^{(M)}$. Therefore we have shown that $(\exists u\, \forall x \in z\, \exists y \in u\, \varphi)^{(M)}$, which is what we had to prove. □

37.C.1. *Binding quantifiers by new variables.* Every formula can be transformed into a Δ_0-formula by adding new variables used to bind the quantifiers. To be more precise, we define a transformation $\varphi(x_1,\dots,x_n) \rightsquigarrow \varphi_{\mathrm{b}}(x_1,\dots,x_n,y_1,\dots,y_k)$ where k is the numbers of quantifiers occurring in φ, so that all quantifiers of φ_{b} are bounded:

- if φ is atomic, then φ_{b} is φ;
- $(\neg\varphi)_{\mathrm{b}}$ is $\neg\varphi_{\mathrm{b}}$ and $(\varphi \odot \psi)_{\mathrm{b}}$ is $\varphi_{\mathrm{b}} \odot \psi_{\mathrm{b}}$, with $\odot$ a binary connective;
- $(\exists x\, \varphi)_{\mathrm{b}}$ is $\exists x \in y\, \varphi_{\mathrm{b}}$ and $(\forall x\, \varphi)_{\mathrm{b}}$ is $\forall x \in y\, \varphi_{\mathrm{b}}$, where y is a variable different from x and not occurring in φ.

Lemma 37.17. *Suppose M is transitive and almost universal. For every $a \in M$ there are $y_1,\dots,y_k \in M$ such that*

$$\forall x_1,\dots,x_n \in a\,(\varphi^{(M)}(x_1,\dots,x_n) \Leftrightarrow \varphi_{\mathrm{b}}(x_1,\dots,x_n,y_1,\dots,y_k)).$$

Proof. We proceed by induction on the complexity of φ. If φ is atomic, the result follows by Lemma 37.9 with $N = \mathrm{V}$, and if φ is a negation or a disjunction, the result follows at once from the inductive hypothesis. So we may assume that $\varphi(x_1,\dots,x_n)$ is $\exists x_{n+1}\, \psi(x_1,\dots,x_n,x_{n+1})$, and $\varphi_{\mathrm{b}}(x_1,\dots,x_n,y_1,\dots,y_k,)$ is $\exists x_{n+1} \in y_k\, \psi_{\mathrm{b}}$. Fix $a \in M$.

Claim 37.17.1. *There is $y_k \in M$ such that*

$$\forall x_1,\dots,x_n \in a\,(\varphi^{(M)}(x_1,\dots,x_n) \Leftrightarrow \exists x_{n+1} \in y_k\, \psi^{(M)}(x_1,\dots,x_{n+1})).$$

Proof. As $\varphi^{(M)}$ is $\exists x_{n+1} \in M\, \psi^{(M)}$, by collection there is a set $z \subseteq M$ such that $\forall x_1,\dots,x_n \in a\, \exists x_{n+1} \in z\, \psi^{(M)}$. By almost universality there is $y_k \in M$ such that $z \subseteq y_k$. This establishes the forward implication; the reverse implication follows from transitivity of M. □

By almost universality there is $a' \in M$ such that $a \cup y_k \subseteq a'$, and by inductive assumption there are $y_1,\dots,y_{k-1} \in M$ such that

$$\forall x_1,\dots,x_{n+1} \in a'\,(\psi^{(M)}(x_1,\dots,x_{n+1}) \Leftrightarrow \psi_{\mathrm{b}}(x_1,\dots,x_{n+1},y_1,\dots,y_{k-1})),$$

therefore for all $x_1,\dots,x_n \in a$

$$\begin{aligned}\varphi^{(M)}(x_1,\dots,x_n) &\Leftrightarrow \exists x_{n+1} \in y_k\, \psi_{\mathrm{b}}(x_1,\dots,x_{n+1},y_1,\dots,y_{k-1})\\ &\Leftrightarrow \varphi_{\mathrm{b}}(x_1,\dots,x_n,y_1,\dots,y_k)\end{aligned}$$

which is what we had to prove. □

37.D. The satisfaction relation in ZF. Recall that a signature τ is a pair $(\langle I,J,K\rangle, \mathrm{ar}_\tau)$ with I,J,K pairwise disjoint sets, and $\mathrm{ar}_\tau\colon I \cup J \to \omega \setminus \{0\}$. A τ-structure is a pair (A,F) where A is a non-empty *set* and F is a function with domain $I \cup J \cup K$ such that

- if $i \in I$ then $F(i) \subseteq {}^{\mathrm{ar}_\tau(i)}A$,

- if $j \in J$ then $F(j) \colon {}^{\mathrm{ar}_\tau(j)}A \to A$,
- if $k \in K$ then $F(k) \in A$.

The (proper) class of all τ-structures is $\mathrm{Str}(\tau)$. The universe $\|\mathcal{A}\|$ of $\mathcal{A} \in \mathrm{Str}(\tau)$ is just the first component of $\mathcal{A} = (A, F)$.

Let

$$\mathscr{F} = \{\langle \tau, \mathcal{A}, \boldsymbol{\varphi}, g \rangle \mid \tau, \mathcal{A} \in \mathrm{Str}(\tau), \boldsymbol{\varphi} \in \mathrm{Fml}(\mathcal{L}), g \colon \mathrm{Fv}(\boldsymbol{\varphi}) \to \|\mathcal{A}\|\},$$

where τ is a signature, and $\mathcal{L} = \mathcal{L}_\tau$. For the sake of readability, let us fix for the time being τ and $\mathcal{A}$, so that the elements of $\mathscr{F}$ can be identified with pairs of the form $(\boldsymbol{\varphi}, g)$ with $g \colon \mathrm{Fv}(\boldsymbol{\varphi}) \to \|\mathcal{A}\|$. Let $\mathscr{F}_{\mathrm{AtFml}}$ be the subclasses obtained by requiring that $\boldsymbol{\varphi}$ be atomic. By Section 31.A.1, if $\boldsymbol{t} \in \mathrm{Term}(\mathcal{L})$ is a term and $g \colon \mathrm{dom}\, g \to \|\mathcal{A}\|$ is a finite function such that $\mathrm{V{\scriptstyle BL}}(\boldsymbol{t}) \subseteq \mathrm{dom}\, g \subseteq \mathrm{Vbl}$, then an element $\boldsymbol{t}^{\mathcal{A}}[g] \in \|\mathcal{A}\|$ is defined by induction on the complexity of $\boldsymbol{t}$. The function $\mathrm{Sat}_{\mathrm{AtFml}} \colon \mathscr{F}_{\mathrm{AtFml}} \to 2$ is defined

- if $\boldsymbol{\varphi} = \boldsymbol{t} \mathrel{\dot{=}} \boldsymbol{s}$ then $\mathrm{Sat}_{\mathrm{AtFml}}(\boldsymbol{\varphi}, g) = 1 \Leftrightarrow \boldsymbol{t}^{\mathcal{A}}[g] = \boldsymbol{s}^{\mathcal{A}}[g]$,
- if $\boldsymbol{\varphi} = \boldsymbol{R}(\boldsymbol{t}_1, \dots, \boldsymbol{t}_n)$ then $\mathrm{Sat}_{\mathrm{AtFml}}(\boldsymbol{\varphi}, g) = 1 \Leftrightarrow \boldsymbol{R}^{\mathcal{A}}(\boldsymbol{t}_1^{\mathcal{A}}[g], \dots, \boldsymbol{t}_n^{\mathcal{A}}[g])$.

Thus $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ if and only if $\mathrm{Sat}_{\mathrm{AtFml}}(\boldsymbol{\varphi}, g) = 1$, for any atomic formula $\boldsymbol{\varphi}$.

Write $\boldsymbol{\varphi}' <^* \boldsymbol{\varphi}$ to say that $\boldsymbol{\varphi}'$ is a sub-formula of $\boldsymbol{\varphi}$. A **satisfaction map** is a class-function S whose domain is a subclass of $\mathscr{F}$ and taking values in $\{0, 1\}$, such that:

(37.2a) $(\boldsymbol{\varphi}, g) \in \mathrm{dom}\, S \wedge g' \in {}^{\mathrm{Fv}(\boldsymbol{\varphi})}\|\mathcal{A}\| \Rightarrow (\boldsymbol{\varphi}, g') \in \mathrm{dom}\, S$

(37.2b) $(\boldsymbol{\varphi}, g) \in \mathrm{dom}\, S \wedge \boldsymbol{\varphi}' <^* \boldsymbol{\varphi} \wedge g' \in {}^{\mathrm{Fv}(\boldsymbol{\varphi}')}\|\mathcal{A}\| \Rightarrow (\boldsymbol{\varphi}', g') \in \mathrm{dom}\, S$

(37.2c) $S \restriction \mathscr{F}_{\mathrm{AtFml}} = \mathrm{Sat}_{\mathrm{AtFml}}$

(37.2d) $(\neg\boldsymbol{\varphi}, g) \in \mathrm{dom}\, S \Rightarrow S(\neg\boldsymbol{\varphi}, g) = 1 - S(\boldsymbol{\varphi}, g)$

(37.2e) $(\boldsymbol{\varphi} \vee \boldsymbol{\psi}, g) \in \mathrm{dom}\, S \Rightarrow S(\boldsymbol{\varphi} \vee \boldsymbol{\psi}, g) = \max(S(\boldsymbol{\varphi}, g), S(\boldsymbol{\psi}, g))$

(37.2f) $(\exists \boldsymbol{x} \boldsymbol{\varphi}, g) \in \mathrm{dom}\, S \Rightarrow S(\exists \boldsymbol{x} \boldsymbol{\varphi}, g) = \sup\{S(\boldsymbol{\varphi}, g') \mid g' \supseteq g\}$.

The class-function $\mathrm{Sat} \colon \mathscr{F} \to 2$ is the largest satisfaction map. It is defined in ZF by recursion using the relation $\lhd$ on $\mathscr{F}$

$$\langle \boldsymbol{\varphi}', g' \rangle \lhd \langle \boldsymbol{\varphi}, g \rangle \Leftrightarrow \boldsymbol{\varphi}' <^* \boldsymbol{\varphi} \wedge g' \restriction \mathrm{Fv}(\boldsymbol{\varphi}) = g.$$

The relation $\lhd$ is well-founded because of $<^*$, and it is left-narrow as $\|\mathcal{A}\|$ is a *set*. Let

$$\mathcal{A} \vDash_g \boldsymbol{\varphi} \Leftrightarrow \mathrm{Sat}(\boldsymbol{\varphi}, g) = 1.$$

As usual, when $\boldsymbol{\varphi}$ is a sentence, we drop the g and write $\mathcal{A} \vDash \boldsymbol{\varphi}$.

We cannot formalize in ZF the notion $\mathcal{A} \vDash_g \boldsymbol{\varphi}$ when $\|\mathcal{A}\|$ is a proper class, unless we put some restrictions on the complexity of $\boldsymbol{\varphi}$, as the next result shows.

Let's introduce a bit of notation. First of all, for notational ease, we focus on the signature for set theory, i.e. having only $\in$ as non-logical symbol. Also let's assume that $\mathcal{A} = \langle \mathrm{V}, \in \rangle$. Let

$$\begin{aligned}
\Sigma_n\text{-}\,\mathrm{Fml} &= \{\boldsymbol{\varphi} \in \mathrm{Fml} \mid \boldsymbol{\varphi} \text{ is } \Sigma_n\} \\
\mathscr{F}_{\Sigma_n} &= \{(\boldsymbol{\varphi}, g) \mid \boldsymbol{\varphi} \in \Sigma_n\text{-}\,\mathrm{Fml} \wedge g \colon \mathrm{Fv}(\boldsymbol{\varphi}) \to \mathrm{V}\} \\
\mathrm{Sat}_{\Sigma_n} &: \mathscr{F}_{\Sigma_n} \to 2, \text{ a satisfaction map} \\
\mathrm{Truth}_{\Sigma_n} &= \{(\boldsymbol{\varphi}, g) \in \mathscr{F}_{\Sigma_n} \mid \mathrm{Sat}_{\Sigma_n}(\boldsymbol{\varphi}, g) = 1\}.
\end{aligned}$$

Similarly we define Π_n-Fml, $\mathscr{F}_{\Pi_n}$, ..., and note that $(\boldsymbol{\varphi}, g) \in \mathrm{Truth}_{\Pi_n} \Leftrightarrow (\boldsymbol{\neg\varphi}, g) \notin \mathrm{Truth}_{\Sigma_n}$.

Theorem 37.18. *Work in* ZF.

(a) *Each* $\mathscr{F}_{\Sigma_n}, \mathscr{F}_{\Pi_n}$ *is* Δ_1^{ZF}*-definable.*

(b) Sat_{Σ_0} *and* $\mathrm{Truth}_{\Sigma_0}$ *are* Δ_1^{ZF}*-definable.*

(c) *For each* $n \geq 1$, $\mathrm{Truth}_{\Sigma_n}$ *is* Σ_n*-definable,* Truth_{Π_n} *is* Π_n*-definable, and* Sat_{Σ_n} *is defined by a disjunction of a* Σ_n *and a* Π_n *formula.*

Proof. (a)

(b)

(c) Note that $(\boldsymbol{\varphi}, g) \in \mathrm{Truth}_{\Sigma_{n+1}}$ if and only if $\boldsymbol{\varphi}$ is of the form $\boldsymbol{\exists x \psi}$ with $\boldsymbol{\psi} \in \Pi_n$-Fml and if $\boldsymbol{x}$ occurs free in $\boldsymbol{\psi}$ then $(\boldsymbol{\psi}, g \cup \{(\boldsymbol{x}, a)\}) \in \mathrm{Truth}_{\Pi_n}$, for some a. In symbols:

$$\begin{aligned}
(\boldsymbol{\varphi}, g) \in \mathrm{Truth}_{\Sigma_{n+1}} \Leftrightarrow \exists a\, \exists \boldsymbol{\psi} \in \Sigma_n\text{-}\,\mathrm{Fml}\, \exists \boldsymbol{x} \in \mathrm{Vbl}\, \big[\boldsymbol{\varphi} = \boldsymbol{\exists x \neg \psi} \wedge \\
\exists g' \big(g \subseteq g' \subseteq g \cup \{(\boldsymbol{x}, a)\} \wedge (\boldsymbol{\psi}, g') \notin \mathrm{Truth}_{\Sigma_n} \big) \big].
\end{aligned}$$

Therefore when $n = 0$ this proves that $\mathrm{Truth}_{\Sigma_1}$ is Σ_1-definable, since $\mathrm{Truth}_{\Sigma_0}$ is Π_1 by part (b), and assuming $\mathrm{Truth}_{\Sigma_n}$ is Σ_n-definable, then Truth_{Π_n} is Π_n-definable, and hence $\mathrm{Truth}_{\Sigma_{n+1}}$ is Σ_{n+1}-definable.

The class-function Sat_{Σ_n} is defined by a disjunction of a Σ_n and a Π_n formula, since

$$\mathrm{Sat}_{\Sigma_n}(\boldsymbol{\varphi}, g) = i \Leftrightarrow \big[(\boldsymbol{\varphi}, g) \in \mathrm{Truth}_{\Sigma_n} \wedge i = 1 \big] \vee \big[(\boldsymbol{\varphi}, g) \notin \mathrm{Truth}_{\Sigma_n} \wedge i = 0 \big].$$

□

37.E. The satisfaction relation in NGB and MK. Working in MK one can give-up the requirement that the structures are sets.

Later

Exercises

Exercise 37.19. Show that $\mathsf{Ext} + \mathsf{Pwr} + \mathsf{Rpl} \vdash \mathsf{Prn}$. [Hint: $\mathscr{P}(\mathscr{P}(\emptyset))$ has exactly two elements]

Exercise 37.20. Let T be Zermelo's set theory Z with the axiom of separation removed, and with the addition of two axioms: $\exists x \forall y (y \notin x)$ asserting the existence of the empty set, and tRpl the axiom-schema of tight replacement. Show that ZF is equivalent to T.

Exercise 37.21. Suppose Ω is either a regular cardinal, orelse $\Omega = \mathrm{Ord}$. Show that Ω ia a transitive inner model of: Ext, Fnd, Prn, Unn, Pwr, Rpl, and AC.

38. Reflection

38.A. The reflection theorem.

Definition 38.1. A **hierarchy** is a sequence of sets $\langle Z_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ which is monotone, that is $\alpha < \beta \Rightarrow Z_\alpha \subseteq Z_\beta$, and continuous at limits, that is $Z_\lambda = \bigcup_{\alpha < \lambda} Z_\alpha$ if λ is limit. If $Z = \bigcup_{\alpha \in \mathrm{Ord}} Z_\alpha$ then we say that $\langle Z_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ is a hierarchy for Z.

Clearly $\langle \mathrm{V}_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ is a hierarchy for V.

Theorem 38.2. *If $\langle Z_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ is a hierarchy for Z, then for all $\varphi_1, \dots, \varphi_n$ there is a definable closed and unbounded class C such that*

$$\mathsf{ZF} \vdash \forall \alpha \in C \, (\varphi_1, \dots, \varphi_n \textit{ are absolute between } Z_\alpha \textit{ and } Z) \, .$$

Formally: given $\zeta(x, y)$ and $\varphi_1, \dots, \varphi_n$, if $\mathsf{ZF} \vdash \forall \alpha \exists ! y \zeta(\alpha, y)$ so that letting Z_α be the unique y satisfying $\zeta(\alpha, y)$, if ZF proves the defining conditions for a hierarchy, then there is a formula χ that defines in ZF a closed unbounded class of ordinals, and

$$\mathsf{ZF} \vdash \forall \alpha \, (\chi(\alpha) \Rightarrow \varphi_1, \dots, \varphi_n \text{ are absolute between } Z_\alpha \text{ and } Z) \, .$$

Proof. By adding sub-formulæ, if needed, we may assume that $\varphi_1, \dots, \varphi_n$ is closed under sub-formulæ.

If φ_i is $\exists x \varphi_j(x, y_1, \dots, y_h)$ let $G_i(y_1, \dots, y_h)$ be the least η such that $\exists x \in Z_\eta \varphi_j^{(Z)}(x, y_1, \dots, y_h)$, if $\exists x \in Z \varphi_j^{(Z)}(x, y_1, \dots, y_h)$, and $G_i(y_1, \dots, y_h) = 0$ otherwise. Let $F_i(\xi) = \sup \{ G_i(\vec{y}) \mid \vec{y} \in Z_\xi \}$. If φ_i is not existential let $F_i(\xi) = 0$. Thus $F_i \colon \mathrm{Ord} \to \mathrm{Ord}$ for $i = 1, \dots, n$. If α is limit and closed under the F_is, then $\varphi_1, \dots, \varphi_n$ are absolute between Z_α and Z by Lemma 37.7.

On the other hand the class of limit closure points of any class-function on the ordinals, is a closed and unbounded class. □

If $\varphi \Leftrightarrow \varphi^{(\mathrm{V}_\beta)}$ we say that V_β reflects φ.

Corollary 38.3. *If* T *extends* ZF *and* $\sigma_1, \dots, \sigma_n$ *are in* T*, then there is a definable class* C *such that* $\mathsf{T} \vdash$*"*C *is closed and unbounded in* Ord*" and* $\mathsf{T} \vdash \forall \alpha \in C \left(\sigma_1^{(\mathrm{V}_\alpha)} \wedge \dots \wedge \sigma_n^{(\mathrm{V}_\alpha)} \right)$.

Lemma 38.4. *The formulæ* $y = \mathscr{P}(x)$ *and* $y = \mathrm{V}_\alpha$ *are absolute between* V_λ *and* V*, with* λ *limit.*

Proof. If $x \in \mathrm{V}_\lambda$ then $x \in \mathrm{V}_\alpha$ for some $\alpha < \lambda$, so $\mathscr{P}(x) \in \mathrm{V}_{\alpha+1} \subseteq \mathrm{V}_\lambda$. Therefore $(y = \mathscr{P}(x))^{(\mathrm{V}_\lambda)} \Leftrightarrow y = \mathscr{P}(x)$.

Note that $y = \mathrm{V}_\alpha$ if and only if

$$\begin{aligned}\mathsf{Ord}(\alpha) \wedge \exists f \, \exists \delta \Big[\mathsf{Ord}(\delta) \wedge \alpha \in \delta \wedge \mathsf{Fn}(f) \wedge \delta = \operatorname{dom}(f) \\ \wedge f(\emptyset) = \emptyset \wedge f(\alpha) = y \wedge \forall \nu \in \delta \, (\nu \text{ limit} \Rightarrow f(\nu) = \textstyle\bigcup_{\xi < \nu} f(\xi)) \\ \wedge \forall \nu \in \delta \, (\mathbf{S}(\nu) \in \delta \Rightarrow f(\mathbf{S}(\nu)) = \mathscr{P}(f(\nu))) \Big].\end{aligned}$$

As $\langle \mathrm{V}_\nu \mid \nu < \alpha \dotplus 1 \rangle \in \mathrm{V}_\lambda$, it follows that $y = \mathrm{V}_\alpha$ is absolute between V_λ and V. □

Theorem 38.5. *If* T *extends* ZF *is finitely axiomatizable, then* T *is inconsistent.*

In other words, no consistent extension of ZF is finitely axiomatizable.

Proof. Suppose T is $\sigma_1, \dots, \sigma_n$ and let β be the least limit ordinal such that V_β reflects $\sigma_1 \wedge \dots \wedge \sigma_n$, that is $\mathrm{V}_\beta \vDash \ulcorner \mathsf{T} \urcorner$ by (37.1). As $\mathsf{T} \vdash \exists \alpha (\mathrm{V}_\alpha \vDash \ulcorner \mathsf{T} \urcorner)$ and by Lemma 38.4, there is a limit $\alpha < \beta$ such that V_α reflects the σ_i, against the minimality of β. □

Theorem 38.6 (ZF)**.** *Let* Z *be a class, let* $X \subseteq Z$ *be a set, and let* $\varphi_1, \dots, \varphi_n$ *be formulæ. Suppose that either*

(a) $|X| \nleq \omega$ *and* AC *holds, or else*

(b) $|X| \leq \omega$ *and* DC *holds.*

Then there is a set A *such that* $X \subseteq A \subseteq Z$*, with* $|A| = \max(|X|, \omega)$ *and each* φ_i *is absolute between* A *and* Z*.*

Proof. We may assume that $\varphi_1, \dots, \varphi_n$ is closed under sub-formulæ. Let $Z_\alpha = Z \cap \mathrm{V}_\alpha$ so that $\langle Z_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ is a hierarchy. Let α be sufficiently large so that $X \subseteq Z_\alpha$ and let $\beta > \alpha$ be such that each φ_i is absolute between

Z_β and Z. Let $\mathcal{B} = \langle Z_\beta; \in, \boldsymbol{c}_x \rangle_{x \in X}$. We will prove that there is $\mathcal{A} \preccurlyeq \mathcal{B}$ such that $X \subseteq A = \|\mathcal{A}\|$ and $|A| \leq \max(|X|, \omega)$.

If (a) holds, apply Theorem 31.15; since X is uncountable then $|A| = \max(|X|, \omega)$.

If (b) holds, apply Theorem 31.19; since we can always enlarge X so that $\omega \precsim X$ we have that $|A| = \omega = \max(|X|, \omega)$.

Thus we have that each φ_i is absolute between A, Z_β, and Z as required. □

Corollary 38.7 (AC). *Let Z be a transitive class and let $\sigma_1, \ldots, \sigma_n$ be sentences. Then for every transitive set $X \subseteq Z$ there is a transitive set $M \supseteq X$ such that $|M| \leq \max(\omega, |X|)$ and $\sigma_i^{(M)} \Leftrightarrow \sigma_i^{(Z)}$ for all $1 \leq i \leq n$.*

Proof. Without loss of generality the axiom of extensionality is one of the σ_i and let A be given by Theorem 38.6, so that $\sigma_j^{(Z)} \Leftrightarrow \sigma_j^{(A)}$: Z is transitive, so extensionality holds in Z, and hence also in A. Let $\boldsymbol{\pi} \colon A \to M$ be the Mostowski collapse. As $\boldsymbol{\pi}(x) = \{\boldsymbol{\pi}(y) \mid y \in x \cap A\}$ and $X \subseteq A$ is transitive, $\boldsymbol{\pi} \restriction X$ is the identity, so $X \subseteq M$. □

If $Z = \mathrm{V}$ and $X = \omega$ we obtain

Corollary 38.8. *If* T *extends* ZFC *and* $\sigma_1, \ldots, \sigma_n$ *are in* T*, then*

$$\mathsf{T} \vdash \exists M \big(\mathsf{Trans}(M) \land |M| \leq \omega \land \langle M, \in \rangle \vDash \ulcorner \textstyle\bigwedge_{i=1}^{n} \sigma_i \urcorner \big).$$

Let $\langle \sigma_n \mid n \in \omega \rangle$ be an enumeration of the axioms of ZFC and let ZFC_n be the theory that has axioms $\{\sigma_i \mid i < n\}$. Every theorem of ZFC is a theorem of ZFC_n, for some n.

For any *fixed* n, the theory ZFC proves that there is a countable transitive $M \vDash \mathsf{ZFC}_n$. If n is large enough, $M \vDash (\omega_1$ exists). Therefore "being uncountable" is *not absolute* for transitive models of any ZFC_n.

38.B. The models H_κ.

Recall from Section 19.A.1 that the transitive closure of a class X is the smallest transitive class Y containing X.

Definition 38.9. For $\alpha \geq \omega$, let

$$\mathrm{H}_\alpha = \{x \mid \mathrm{TC}(x) \text{ is well-orderable, and } |\mathrm{TC}(x)| < \alpha\}.$$

If α is not a cardinal, then $\mathrm{H}_\alpha = \mathrm{H}_{\alpha^+}$, so the definition above is of interest only when α is a *cardinal.* On the other hand this extra generality and the next result shows that $\langle \mathrm{H}_\alpha \mid \alpha \in \mathrm{Ord} \rangle$ is a hierarchy for V.

Lemma 38.10. *For every infinite cardinal κ:*

(a) H_κ *is transitive, and* $\kappa = \mathrm{H}_\kappa \cap \mathrm{Ord}$.

(b) $\forall x \in \mathrm{H}_\kappa\, \forall y \subseteq x\, (y \in \mathrm{H}_\kappa)$.

(c) $\mathrm{H}_\kappa \subseteq \mathrm{V}_\kappa$.

(d) *Assuming* AC, $|\mathrm{H}_\kappa| = 2^{<\kappa}$.

Proof. (a) If $x \in y \in \mathrm{H}_\kappa$, then $\mathrm{TC}(x) \subset \mathrm{TC}(y)$ so $\mathrm{TC}(x)$ is well-orderable and $|\mathrm{TC}(x)| < \kappa$, i.e. $x \in \mathrm{H}_\kappa$. Thus $\mathrm{H}_\kappa \cap \mathrm{Ord}$ is an ordinal, and hence it must be κ.

(b) If $y \subseteq x \in \mathrm{H}_\kappa$, then $\mathrm{TC}(y) \subseteq \mathrm{TC}(x)$ so $|\mathrm{TC}(y)| \leq |\mathrm{TC}(x)| < \kappa$, and hence $y \in \mathrm{H}_\kappa$.

(c) If $\xi < \alpha = \mathrm{rank}(x)$ then $\xi = \mathrm{rank}(z)$ for some $z \in \mathrm{TC}(x)$, so $\alpha = \{\mathrm{rank}(z) \mid z \in \mathrm{TC}(x)\}$. Thus if $x \in \mathrm{H}_\kappa$ then $\mathrm{TC}(x)$ has size $< \kappa$ so $\mathrm{rank}(x) < \kappa$, i.e. $\mathrm{H}_\kappa \subseteq \mathrm{V}_\kappa$.

(d) $\mathscr{P}(\lambda) \subseteq \mathrm{H}_\kappa$ for all $\lambda < \kappa$, so $2^{<\kappa} \leq |\mathrm{H}_\kappa|$. Given $x \in \mathrm{H}_\kappa$, fix a bijection $f_x \colon \mathrm{TC}(\{x\}) \to \lambda_x < \kappa$ and let

$$E_x = \{(\alpha, \beta) \in \lambda_x \times \lambda_x \mid f_x^{-1}(\alpha) \in f_x^{-1}(\beta)\}.$$

Then $\langle \lambda_x, E_x \rangle$ is extensional and well-founded, and $\langle \mathrm{TC}(\{x\}), \in \rangle$ is the unique transitive structure isomorphic to it. As x is the unique $\bar{x} \in \mathrm{TC}(\{x\})$ such that $\forall y (\bar{x} \notin y)$ is true in $\langle \mathrm{TC}(\{x\}), \in \rangle$, then there is a unique $\alpha \in \mathrm{fld}(E_x)$ such that $\neg \exists \beta (\alpha\ E_x\ \beta)$ is true in $\langle \lambda_x, E_x \rangle$. Therefore $\mathrm{TC}(\{x\})$ can be recovered from E_x alone. (This is the point for using $\mathrm{TC}(\{x\})$ rather than $\mathrm{TC}(x)$.) The map $\mathrm{H}_\kappa \to \bigcup\{\mathscr{P}(\lambda \times \lambda) \mid \lambda < \kappa\}$, $x \mapsto E_x$ is injective, and therefore $|\mathrm{H}_\kappa| \leq 2^{<\kappa}$. □

Theorem 38.11. *Let κ be an infinite cardinal.*

(a) H_κ *satisfies all axioms of* ZF *with the possible exception of* Inf, Pwr, *and* Rpl.

(b) *If* $\kappa > \omega$ *then* $\mathrm{H}_\kappa \vDash \ulcorner\mathsf{Inf}\urcorner$.

(c) *If we assume* AC, *then* $\mathrm{H}_\kappa \vDash \ulcorner\mathsf{AC}\urcorner$.

(d) *Assume* AC. *If* $\kappa > \omega$ *is regular, then* $\mathrm{H}_\kappa \vDash \ulcorner\mathsf{Clct}\urcorner$, *and therefore* $\mathrm{H}_\kappa \vDash \ulcorner\mathsf{ZFC} - \mathsf{Pwr}\urcorner$.

Proof. (a) follows from Theorem 19.22 and Lemma 38.10, while (b) is immediate.

(c) It is enough to show that if $\mathcal{A} \in \mathrm{H}_\kappa$ and

(38.1a) $\mathrm{H}_\kappa \vDash \mathcal{A}$ is a family of pairwise disjoint non-empty sets,

then there is $b \in \mathrm{H}_\kappa$ such that

(38.1b) $\mathrm{H}_\kappa \vDash \forall a \in \mathcal{A}\, (b \cap a$ is a singleton).

By transitivity of H_κ it is easy to check that any $\mathcal{A}$ as in (38.1a) is indeed a family of pairwise disjoint non-empty sets, so by AC pick a $b \subseteq \bigcup \mathcal{A}$ which intersects every set in $\mathcal{A}$ in a singleton. As $\bigcup \mathcal{A} \in \mathrm{H}_\kappa$, it follows that $b \in \mathrm{H}_\kappa$, so we are only left to check (38.1b), which we leave to the reader.

(d) Let $a \in \mathrm{H}_\kappa$, and let $R \subseteq \mathrm{H}_\kappa$ be a binary relation with domain a. By choice there is $f \colon a \to \mathrm{H}_\kappa$ such that $f \subseteq R$, and let $b = \operatorname{ran} f \subseteq M$, so that $|b| \leq |a| < \kappa$. Since κ is regular, then $\mathrm{TC}(b) = b \cup \bigcup \{\mathrm{TC}(y) \mid y \in b\}$ has size $< \kappa$, and hence $b \in \mathrm{H}_\kappa$. Therefore H_κ satisfies collection. □

Theorem 38.12 (Lévy)**.** *If $\varphi(x, \vec{z})$ is Σ_1 and $\kappa > \omega$ is an infinite cardinal, then $\forall \vec{z} \in \mathrm{H}_\kappa\, (\exists x\, \varphi \Rightarrow \exists x \in \mathrm{H}_\kappa\, \varphi)$.*

Proof. Suppose first that $\varphi(x, z_1, \dots, z_k)$ is Σ_0. Let $a_1, \dots, a_k \in \mathrm{H}_\kappa$ and let α be such that $a_1, \dots, a_k \in \mathrm{V}_\alpha$ and

$$\exists x \varphi(a_1, \dots, a_k) \Leftrightarrow (\exists x \varphi(a_1, \dots, a_k))^{(\mathrm{V}_\alpha)}.$$

Let $X \preccurlyeq \mathrm{V}_\alpha$ be such that $\mathrm{TC}(\{a_1, \dots, a_k\}) \subseteq X$ and $|\mathrm{TC}(\{a_1, \dots, a_k\})| = |X|$. If M is the transitive collapse of X, then $|M| < \kappa$ so $M \in \mathrm{H}_\kappa$. In particular, there is $b \in M \subseteq \mathrm{H}_\kappa$ such that $M \vDash \varphi(b, a_1, \dots, a_k)$, and by Σ_0-absoluteness $\varphi(b, a_1, \dots, a_k)$.

Suppose now $\varphi(x, z_1, \dots, z_k)$ is $\exists y \psi(y, x, z_1, \dots, z_k)$ with ψ Σ_0. The formula $\chi(u, z_1, \dots, z_k)$ given by $\exists x \in u\, \exists y \in u\, \psi(y, x, z_1, \dots, z_k)$ is Σ_0, and $\exists x \varphi(x, z_1, \dots, z_k) \Leftrightarrow \exists u \chi(u, z_1, \dots, z_k)$. So now we fall into the previous case. □

Exercises

Exercise 38.13. Assume $\mathsf{Con}_{\mathsf{ZF}}$ and suppose $\mathcal{M} = \langle M, E \rangle$ is a model of $\mathsf{ZF} + \neg \mathrm{Con}(\ulcorner \mathsf{ZF} \urcorner)$. With the notation of Example 35.7 show that

(i) $I \nsubseteq n$ for any $n \in \omega$

(ii) $I \cap (\omega^{\mathcal{M}} \setminus \omega)$ is non-empty and has no minimum.

39. Constructibility

39.A. Gödel's operations. In Chapter V we defined the ordered pair, and then we agreed to construe the n-tuple $\langle a_1, \dots, a_n \rangle$ to be the function with domain n that sending i to a_{i+1}. But of course, one could define triples from pairs, quadruples from triples, and so on.

Definition 39.1. The set $(a_1, \dots, a_n)$ is defined as follows: $(a_1) = a_1$, $(a_1, a_2) = \{\{a_1\}, \{a_1, a_2\}\}$ as in (16.4), and if $n \geq 2$ $(a_1, \dots, a_n, a_{n+1}) = ((a_1, \dots, a_n), a_{n+1})$.

Similarly we set $x_1 \times \cdots \times x_n \times x_{n+1} = (x_1 \times \cdots \times x_n) \times x_{n+1}$.

Definition 39.2. A **Gödel operation** is a class function obtained by composing the functions $\mathfrak{F}_1, \dots, \mathfrak{F}_8$ below:

$$\begin{aligned}
\mathfrak{F}_1(x, y) &= \{x, y\} & \mathfrak{F}_5(x, y) &= \bigcup x \\
\mathfrak{F}_2(x, y) &= x \times y & \mathfrak{F}_6(x, y) &= \{(u, v) \in x \times y \mid u \in v\} \\
\mathfrak{F}_3(x, y) &= x \setminus y & \mathfrak{F}_7(x, y) &= \{(u, v, w) \mid (u, w, v) \in x\} \\
\mathfrak{F}_4(x, y) &= \operatorname{dom} x & \mathfrak{F}_8(x, y) &= \{(u, v, w) \mid (v, w, u) \in x\}.
\end{aligned}$$

It is convenient to write the $\mathfrak{F}_i$s as binary operations, although $\mathfrak{F}_4$, $\mathfrak{F}_5$, $\mathfrak{F}_7$, $\mathfrak{F}_8$ are unary operations. Let $\theta_i(x, y, z)$ $(1 \leq i \leq 8)$ be Δ_0-formulæ such that

$$\forall x, y, z\ (\mathfrak{F}_i(x, y) = z \Leftrightarrow \theta_i(x, y, z)).$$

Therefore a class M is closed under the Gödel operations if and only if $\bigwedge_{1 \leq i \leq 8} \forall x, y \in M\, \exists z \in M\, \theta_i(x, y, z)$, so "being closed under the Gödel operations" is a notion that makes sense in ZF, NGB, and MK. Note that if λ is limit, then V_λ is closed under the Gödel operations.

Lemma 39.3. *The following are Gödel operations:*

(a) $(x, y) \mapsto x \cap y$

(b) $x \mapsto \breve{x} = \{(u, v) \mid (v, u) \in x\}$

(c) $(x_1, \dots, x_n) \mapsto E^n_{i,j} \overset{\text{def}}{=} \{(u_1, \dots, u_n) \in x_1 \times \cdots \times x_n \mid u_i \in u_j\}$, *where* $n \geq 2$ *and* $i \neq j$.

Proof. (a) $x \cap y = \mathfrak{F}_3(\mathfrak{F}_3(x, y))$.

(b) $\breve{x} = \operatorname{dom} \mathfrak{F}_8(\mathfrak{F}_8(\mathfrak{F}_7(\mathfrak{F}_8(x \times x))))$.

(c) We proceed by induction on n: $E^2_{1,2} = \mathfrak{F}_6(x_1, x_2)$ and $E^2_{2,1} = \breve{E}^2_{1,2}$ so we are done by part (b).

Suppose the result holds for some $n \geq 2$, towards proving it for $n + 1$. If $i, j \leq n$, then $E^{n+1}_{i,j} = E^n_{i,j} \times x_{n+1}$, so we may assume that $\max(i, j) = n + 1$. By part (b) we may assume that $i \leq n$ and $j = n + 1$. Then

$$E^{n+1}_{i,j} = \begin{cases} x_1 \times \cdots \times x_{n-1} \times \mathfrak{F}_6(x_n, x_{n+1}) & \text{if } i = n, \\ \mathfrak{F}_7(E^n_{i,n} \times x_{n+1}) & \text{if } i < n. \end{cases} \qquad \square$$

Theorem 39.4. *If* $\varphi(v_1, \dots, v_n)$ *is* Δ_0, *then there is a Gödel operation* $\mathfrak{F}$ *such that for all* $x_1, \dots, x_n$,

$$\mathfrak{F}(x_1, \dots, x_n) = \{(u_1, \dots, u_n) \in x_1 \times \cdots \times x_n \mid \varphi(u_1, \dots, u_n)\}.$$

Proof. Without loss of generality we may assume that

- the only logical symbols in φ are $\neg$, $\wedge$, and the restricted $\exists$,
- the symbol $=$ does not occur, since $x = y$ can be rendered by $\forall z \in x\,(z \in y) \wedge \forall z \in y\,(z \in x)$,
- $x \in x$ does not occur, since it can be replaced by $\exists u \in x\,(u = x)$.

If φ is atomic, use part (c) of Lemma 39.3. If φ is $\neg\psi$, and $\mathfrak{F}$ is the Gödel operation for ψ, then

$$\{(u_1,\dots,u_n) \in x_1 \times \cdots \times x_n \mid \varphi(u_1,\dots,u_n)\} = x_1 \times \cdots \times x_n \setminus \mathfrak{F}(x_1,\dots,x_n).$$

If φ is $\psi \wedge \chi$, apply the inductive hypothesis and part (a) of Lemma 39.3. If φ is $\exists u_{n+1}(u_{n+1} \in u_i \wedge \psi)$, then by inductive assumption there is a Gödel operation $\mathfrak{F}$ such that

$$\mathfrak{F}(x_1,\dots,x_{n+1}) = \\ \{(u_1,\dots,u_{n+1}) \in x_1 \times \cdots \times x_{n+1} \mid \psi(u_1,\dots,u_{n+1}) \wedge u_{n+1} \in u_i\}.$$

Then

$$\operatorname{dom} \mathfrak{F}(x_1,\dots,x_n,\textstyle\bigcup x_i) = \{(u_1,\dots,u_n) \in x_1 \times \cdots \times x_n \mid \varphi(u_1,\dots,u_n)\}.$$

□

Corollary 39.5. *If M is a transitive class, closed under the Gödel operations, and $\varphi(v_0, v_1, \dots, v_n)$ is Δ_0, and $x, p_1, \dots, p_n \in M$, then $\{u \in x \mid \varphi(u, p_1, \dots, p_n)\} \in M$.*

Proof. By Theorem 39.4 there is a Gödel operation such that

$$\mathfrak{F}(x, \{p_1\}, \dots, \{p_n\}) = \{(u, p_1, \dots, p_n) \mid u \in x \wedge \varphi(u, p_1, \dots, p_n)\},$$

so

$$\{u \in x \mid \varphi(u, p_1, \dots, p_n)\} = \underbrace{\operatorname{dom}\dots\operatorname{dom}}_{n \text{ times}} \mathfrak{F}(x, \{p_1\}, \dots, \{p_n\}).$$ □

Theorem 39.6 (ZF). *Suppose M is a transitive proper class. Then M is almost universal and closed under the Gödel operations if and only if M is an inner model of* ZF.

Theorem 39.6 is stated informally—the actual statement would be as follows. Suppose $\upsilon(x)$ is a formula such that

$$\mathsf{ZF} \vdash \exists x\, \upsilon(x) \wedge \forall x, y\ (\upsilon(x) \wedge y \in x \Rightarrow \upsilon(y)) \wedge \neg\exists y\, \forall x\, (\upsilon(x) \Rightarrow x \in y),$$

i.e. ZF proves that the class $M \overset{\text{def}}{=} \{x \mid \upsilon(x)\}$ is non-empty, transitive, and proper: if

$$\mathsf{ZF} \vdash \textstyle\bigwedge_{1 \le i \le 8} \forall x, y, z\ (\upsilon(x) \wedge \upsilon(y) \wedge \theta_i(x, y, z) \Rightarrow \upsilon(z)) \\ \wedge \forall x\, (\forall z \in x\, \upsilon(z) \Rightarrow \exists y\ (\upsilon(y) \wedge \forall z \in x\, (z \in y)))$$

i.e. ZF proves that M is closed under the Gödel operations and it is almost universal, then $\mathsf{ZF} \vdash \sigma^{(\upsilon)}$ for every σ axiom of ZF, and conversely.

Proof. Suppose M is closed under the Gödel operations and it is almost universal. By Lemma 37.16 it is enough to check that $\mathsf{Spr}^{(M)}$. Fix $x, p_1, \ldots, p_n \in M$: we must show that $z = \{u \in x \mid \varphi^{(M)}(u, \vec{p})\} \in M$. As M is closed under $\mathfrak{F}_0$, it is closed under singletons, so $\{x, p_1, \ldots, p_n\} \subseteq M$ and by almost universality there is $x, p_1, \ldots, p_n \in a \in M$. By Lemma 37.17 there are $y_1, \ldots, y_k \in M$ such that $\varphi^{(M)}(u, \vec{p}) \Leftrightarrow \varphi_{\mathrm{b}}(u, \vec{p}, \vec{y})$, and since φ_{b} is Δ_0, it is absolute between V and M by Lemma 37.10. Therefore we can apply Corollary 39.5 and argue that $z = \{u \in x \mid \varphi_{\mathrm{b}}(u, \vec{p})\}$ is in M.

Conversely, suppose M is an inner model of ZF. As $\mathsf{ZF} \vdash \forall x, y, z\, (\mathfrak{F}_i(x, y) = z \Leftrightarrow \theta_i(x, y, z))$, then M is closed under the basic Gödel operations. If $x \subseteq M$ is a set, then there is α such that $x \subseteq \mathrm{V}_\alpha \cap M = \mathrm{V}_\alpha^{(M)} \in M$. □

39.B. Intermezzo: NGB is finitely axiomatizable. Recall from Section 17.B that NGB is a theory in a two-sorted language with lower case variables $x, y, z, \ldots$ for sets, and upper case letters $X, Y, Z, \ldots$ for classes, with only one axiom schema, namely the axiom of comprehension restricted to formulæ that are predicative, that is such that all quantifiers range over sets. We now give a finite list Σ of sentences that are provable in NGB, and then argue that the axiom schema of predicative comprehension follows from Σ.

The first four axioms of Σ and NGB are the same:

Sets are classes: $\forall x\, \exists X\, (x = X)$,

Classes belonging to classes are sets: $\forall X\, \forall Y\, (X \in Y \Rightarrow \exists x\, (x = X))$,

Extensionality: $\forall X \forall Y\, (\forall z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y)$,

Pairing: $\forall x \forall y \exists z \forall w\, (w \in z \Leftrightarrow w = x \vee w = y)$.

The next eight axioms of Σ are provable in NGB using predicative comprehension:

Empty set: $\exists x \forall y (y \notin x)$,

Membership: $\exists E \forall x \forall y\, ((x, y) \in E \Leftrightarrow x \in y)$,

Intersection: $\forall X \forall Y \exists Z \forall w\, (w \in Z \Leftrightarrow w \in X \wedge w \in Y)$,

Complementation: $\forall X \exists Y \forall z (z \in X \Leftrightarrow z \notin Y)$,

Domain: $\forall R \exists X \forall x\, (x \in X \Leftrightarrow \exists y ((x, y) \in R))$,

Cartesian product:[3] $\forall X \exists Y \forall x \forall z\, (x \in X \Leftrightarrow (x, z) \in Y)$,

Permutation: $\forall X \exists Y \forall u \forall v \forall w\, [(u, v, w) \in X \Leftrightarrow (w, u, v) \in Y]$,

Exchange: $\forall X \exists Y \forall u \forall v \forall w\, [(u, v, w) \in X \Leftrightarrow (u, w, v) \in Y]$.

The axiom of exchange can be generalized to: for all $n \geq 1$ and every class X we can construct the class

$$Y = \{(v_1, \ldots, v_n, x, v_{n+1}) \mid (v_1, \ldots, v_n, v_{n+1}, x) \in X\}.$$

Extensionality together with the axioms of intersection and of complementation guarantee that, given classes X and Y we can construct the classes

$$\begin{aligned} X^{\complement} &= \{z \mid z \notin X\}, \\ X \cap Y &= \{z \mid z \in X \wedge z \in Y\}, \\ X \cup Y &= (X^{\complement} \cap Y^{\complement})^{\complement} = \{z \mid z \in X \vee z \in Y\}, \end{aligned}$$

while the axiom of domain guarantees the existence of the class

$$\operatorname{dom} X = \{z \mid \exists w\, (z, w) \in X\}.$$

By the axioms of extensionality and empty set there is a unique set $\emptyset$ without elements, and let $\mathrm{V} \stackrel{\text{def}}{=} \emptyset^{\complement}$. Thus $\forall x\, (x \in \mathrm{V})$. By the axiom of cartesian products, for each $n \geq 1$ one can prove the existence of

$$\mathrm{V}^n \stackrel{\text{def}}{=} \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathrm{V}\}$$

the class of all n-tuples $(x_1, \ldots, x_n)$. By the axiom permutation, for every class X there is a class Y such that for all x, y, z we have $(x, y, z) \in X \Leftrightarrow (z, x, y) \in Y$ so $Y \cap \mathrm{V}^3 = \{(z, x, y) \mid (x, y, z) \in X\}$ exists. Similarly, the axiom of exchange proves that the class $\{(x, z, y) \mid (x, y, z) \in X\}$ exists. By repeated applications of the axioms of permutation and exchange one can show that $\{(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \mid (x_1, x_2, x_3) \in X\}$ exists, for each class X and each permutation π of $\{1, 2, 3\}$. In particular

$$\{(x_2, x_1, x_3) \mid (x_1, x_2, x_3) \in X\} \text{ exists for every class } X. \tag{39.1}$$

Proposition 39.7. *The following are provable in* Σ.

(a) $\breve{R} = \{(y, x) \mid (x, y) \in R\}$ *exists for every class* R.

(b) $X \times Y$ *exists for all classes* X, Y.

(c) *For every* n, m *and every class* Y *there exists the class*

$$\{(z_1, \ldots, z_n, y, w_1, \ldots, w_m) \mid y \in Y \wedge z_1, \ldots, z_n, w_1, \ldots, w_m \in \mathrm{V}\}.$$

[3] The axiom of cartesian products asserts the existence of the class $X \times \mathrm{V}$ for any class X, although we have not yet formally defined the general cartesian product $X \times Y$ for arbitrary classes.

(d) *For every n, m, k and every class R there exists the class*

$$\{(z_1, \dots, z_n, x, u_1, \dots, u_k, y, w_1, \dots, w_m) \mid (x, y) \in R \wedge \\ z_1, \dots, z_n, u_1, \dots, u_k, w_1, \dots, w_m \in \mathrm{V}\}\,.$$

Proof. (a) Let R be a class. By the axiom of cartesian products the class $Y = \{(x, y, z) \mid (x, y) \in R\}$ exists, and so does $Z = \{(y, x, z) \mid (x, y, z) \in Y\}$ by (39.1). Therefore $\breve{R} = \operatorname{dom} Z$ exists.

(b) Note that $X \times \mathrm{V}$ exists by the axiom of cartesian products, so $X \times Y = (X \times \mathrm{V}) \cap (Y \times \mathrm{V})\breve{}$.

(c) By the axiom of cartesian products, the class $Y \times \mathrm{V}^n$ exists, and so does $\{((z_1, \dots, z_n), y) \mid y \in Y \wedge z_1, \dots, z_n \in \mathrm{V}\}$ by part (a). The result now follows by m applications of the axiom of cartesian products.

(d) By replacing R with $\breve{\breve{R}}$ if needed, we may assume that R is a relation. By part (c) Y_0 exists, where for $k \geq 0$

$$Y_k \overset{\text{def}}{=} \{(z_1, \dots, z_n, x, u_1, \dots, u_k, y) \mid (x, y) \in R \wedge z_1, \dots, z_n, u_1, \dots, u_k \in \mathrm{V}\}\,.$$

It is enough to show that Y_k exists for any $k \geq 0$, and then apply m many times the axiom of cartesian products. We proceed by induction on k: if Y_k exists for some k, then $Y_k \times \mathrm{V}$ exists by the axiom of cartesian products, so Y_{k+1} exists by the axiom of exchange. □

The next result is very similar to Theorem 39.4.

Theorem 39.8. *Let $\varphi(x_0, \dots, x_{n-1}, Y_0, \dots, Y_{m-1})$ be a predicative formula. Then the class*

$$A_\varphi \overset{\text{def}}{=} \{(x_0, \dots, x_{n-1}) \mid \varphi(x_0, \dots, x_{n-1}, Y_0, \dots, Y_{m-1})\}$$

exists.

Proof. We may assume that $Y_k \in z$ (with $k < m$) is not a sub-formula of φ, since it can be replaced by $\exists y\, (y = Y_k \wedge y \in z)$. Similarly, we may assume that no formula of the form $W \in Z$ or $z \in z$ occurs in φ, since they can be replaced by $\exists w\, (w = W \wedge w \in Z)$ and $\exists w\, (w = z \wedge w \in z)$, where w is a new variable. We may also assume that the equality symbol does not occur in φ, since it can be eliminated by the axiom of extensionality. We prove the result by induction on the complexity of φ.

If φ is atomic, then our assumptions imply that φ is of the form:

(i) $x_i \in Y_k$ with $i < n$ and $k < m$, or

(ii) $x_i \in x_j$ with $i < j < n$, or

(iii) $x_j \in x_i$ with $i < j < n$.

If case (i) holds, then $A_\varphi = \{(x_0, \dots, x_{n-1}) \mid x_i \in Y_k\}$ which exists by Proposition 39.7(c). If case (ii) holds, then $A_\varphi = \{(x_0, \dots, x_{n-1}) \mid x_i \in x_j\}$ is obtained by applying Proposition 39.7(d) to the class $E = \{(x, y) \mid x \in y\}$ which exists by the axiom of membership, while in case (iii) we apply the previous argument to $\breve{E}$ which exists by Proposition 39.7(a). If φ is $\neg\psi$, then $A_\varphi = \mathrm{V}^n \setminus A_\psi$ which exists by inductive assumption and the axiom of complements. If φ is $\psi \wedge \chi$, then $A_\varphi = A_\psi \cap A_\chi$ which exists by inductive assumption and the axiom of intersection. Finally, suppose φ is $\exists x_n\, \psi$. Then

$$A_\psi = \{(x_0, \dots, x_{n-1}, x_n) \mid \psi(x_0, \dots, x_{n-1}, x_n, Y_0, \dots, Y_{m-1})\}$$

exists by inductive assumption, so $A_\varphi = \operatorname{dom}(A_\psi)$ exists by inductive assumption and the axiom of domains. □

Using Theorem 39.8 it is easy to construct new classes such as $\bigcup X$, $\bigcap X$, ..., and combining this with the axiom of domain we obtain the axiom of predicative comprehension.

Corollary 39.9. *For every predicative formula $\varphi(x, y_1, \dots, y_n, Z_1, \dots, Z_m)$ with x free in φ and Y a variable not occurring in φ, the theory Σ proves*

$$\forall y_1, \dots, y_n, Z_1, \dots, Z_m \exists X \forall x (x \in X \Leftrightarrow \varphi(x, y_1, \dots, y_n, Z_1, \dots, Z_m)).$$

We can now complete our list of axioms of Σ by adding the remaining axioms of NGB:

Separation: $\forall x \forall Y \exists z \forall w\, (w \in z \Leftrightarrow w \in x \wedge w \in Y)$, that is: the intersection of a class with a set is a set.

Power-set: $\forall x \exists y \forall z\, (z \in y \Leftrightarrow z \subseteq x)$.

Foundation: $\forall X\, (\exists y\, (y \in X) \Rightarrow \exists y\, (y \in X \wedge \forall z\, (z \notin y \cap X)))$.

Union: $\forall x \exists y \forall z\, (z \in y \Leftrightarrow \exists u\, (u \in x \wedge z \in u))$.

Infinity: $\exists x\, (\emptyset \in x \wedge \forall y\, (y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Replacement: $\forall F \forall a \big[\forall x\, (x \in a \Rightarrow \exists! y\, (x, y) \in F) \Rightarrow \exists b \forall y\, (y \in b \Leftrightarrow \exists x\, (x \in a \wedge (x, y) \in F))\big]$.

39.C. The constructible closure. The main result of this section is that for any set S there is a definable proper class $\mathrm{L}(S)$, called the **constructible closure of** S such that:

- $S \in \mathrm{L}(S)$,
- $\mathrm{L}(S)$ is an inner model of ZF,
- if M is a proper class inner model of ZF such that $S \in M$, then $\mathrm{L}(S) \subseteq M$.

The model $\mathrm{L}(S)$ is first constructed under the additional assumption that $S \neq \emptyset$ is transitive and $S \asymp S$. The constructible closure of S is built by means of a class function $\mathsf{F}\colon S \times \mathrm{Ord} \to \mathrm{V}$ that we define next.

Recall from Section 18.C that $\mathrm{Ord} \times \mathrm{Ord}$ is well-ordered by

$$\begin{aligned}(\beta, \gamma) <_{\mathrm{G}} (\beta', \gamma') \Leftrightarrow \max(\beta, \gamma) < \max(\beta', \gamma') \vee \\ \left[\max(\beta, \gamma) = \max(\beta', \gamma') \wedge (\beta, \gamma) <_{\mathrm{lex}} (\beta', \gamma')\right],\end{aligned}$$

and that if (β, γ) has order-type α in this order, then $\beta, \gamma < \alpha$. Let

$$\mathrm{Ord} \to \mathrm{Ord} \times \mathrm{Ord}, \quad \alpha \mapsto ((\alpha)_0, (\alpha)_1)$$

be the enumerating class-function. Let $\mathsf{D}\colon \mathrm{Ord} \to \mathrm{Ord}$ and $\mathsf{R}\colon \mathrm{Ord} \to 9$ be the operations of dividing-by-9 and taking the remainder, that is

$$\forall \alpha \in \mathrm{Ord}\, (\alpha = 9 \cdot \mathsf{D}(\alpha) \dotplus \mathsf{R}(\alpha))\,. \tag{39.2}$$

If $p\colon S \to S \times S$, $s \mapsto (p_0(s), p_1(s))$ is a bijection, then the class-function

$$\mathsf{F} = \mathsf{F}_{S,p}\colon S \times \mathrm{Ord} \to \mathrm{V}$$

is defined as follows. Let $\mathsf{F}(s, 0) = s$ for all $s \in S$, and for $\alpha > 0$ let $\beta = \mathsf{D}(\alpha) \leq \alpha$ and $0 \leq i = \mathsf{R}(\alpha) < 9$, so that $\alpha = 9 \cdot \beta \dotplus i$, and set

$$\mathsf{F}(s, \alpha) = \begin{cases} \{\mathsf{F}(t, \gamma) \mid t \in S \wedge \gamma < \beta\} & \text{if } i = 0, \\ \mathfrak{F}_i(\mathsf{F}(p_0(s), (\beta)_0), \mathsf{F}(p_1(s), (\beta)_1)) & \text{if } 1 \leq i \leq 8. \end{cases}$$

In other words, at stage $\alpha = 9 \cdot \beta > 0$ we collect the previous values, and at all other stages we apply one of the Gödel operations. Note that when $\alpha > 0$ is divisible by 9, the value of F does not depend on s, so for the sake of readability we write $\mathsf{F}(\alpha) = \{\mathsf{F}(s, \gamma) \mid s \in S \wedge \gamma < \beta\}$.

If $q\colon S \to S \times S$ is another bijection then an easy induction shows that

$$\forall \alpha\, (\mathsf{F}_{S,p}``9 \cdot \alpha = \mathsf{F}_{S,q}``9 \cdot \alpha)\,,$$

and therefore the range of $\mathsf{F}_{S,p}$ depends only on S. Let

$$\mathrm{L}(S) = \operatorname{ran} \mathsf{F}_{S,p}$$

for some/any bijection $p\colon S \to S \times S$.

Theorem 39.10. *For $S \asymp S \times S$ transitive, the class $\mathrm{L}(S)$ is transitive, almost universal, closed under the Gödel functions and such that $S \in \mathrm{L}(S)$.*

Proof. First of all notice that $S = \{\mathsf{F}(s, 0) \mid s \in S\} \subseteq \mathrm{L}(S)$, and that $S = \mathsf{F}(9) \in \mathrm{L}(S)$.

Next we prove that $\mathrm{L}(S)$ is closed under the $\mathfrak{F}_i$s. Let $x_0 = \mathsf{F}(s_0, \beta_0)$ and $x_1 = \mathsf{F}(s_1, \beta_1)$, so let $s \in S$ and $\beta \in \mathrm{Ord}$ be such that $s_j = p_j(s)$ and $\beta_j = (\beta)_j$ for $j = 0, 1$. Then $\mathfrak{F}_i(x_0, x_1) = \mathsf{F}(s, 9 \cdot \beta \dotplus i) \in \mathrm{L}(S)$.

If $\emptyset \neq x \subseteq \mathrm{L}(S)$ is a set, then for all $y \in x$ there is $\alpha_y \in \mathrm{Ord}$ such that $y = \mathsf{F}(s, \alpha_y)$ for some $s \in S$. Then $x \subseteq \mathsf{F}(s, \alpha) \in \mathrm{L}(S)$ where $\alpha > 0$ is of the form $9 \cdot \beta$, and $\beta \geq \sup\{\alpha_y \dotplus 1 \mid y \in x\}$. Therefore $\mathrm{L}(S)$ is almost universal.

Finally we prove that $\mathrm{L}(S)$ is transitive by showing by induction on α that $\forall s \in S\,(\mathrm{TC}(\mathsf{F}(s, \alpha)) \subseteq \mathrm{L}(S))$. If $\alpha = 0$ the result follows from the transitivity of S and from $S \subseteq \mathrm{L}(S)$, so assume $\alpha > 0$ and that the result holds for all $\alpha' < \alpha$. If $\alpha = 9 \cdot \beta$, then $\mathsf{F}(s, \alpha) = \{\mathsf{F}(t, \alpha') \mid \alpha' < \beta \wedge t \in S\} \subseteq \mathrm{L}(S)$; as $\mathrm{TC}(\mathsf{F}(s, \alpha')) \subseteq \mathrm{L}(S)$ by inductive assumption, the result follows. Therefore we may assume that $\alpha = 9 \cdot \beta \dotplus i$ for some $1 \leq i \leq 8$, and thus

$$\mathsf{F}(s, \alpha) = \mathfrak{F}_i(\mathsf{F}(s_0, \beta_0), \mathsf{F}(s_1, \beta_1)),$$

with $s_j = p_j(s)$, $\beta_j = (\beta)_j < \beta \leq \alpha$, and $j \leq 1$. Thus by inductive assumption $\mathrm{TC}(\mathsf{F}(s_j, \beta_j)) \subseteq \mathrm{L}(S)$ for $j \leq 1$.

- If $i = 1$, then $\mathsf{F}(s, \alpha) = \{\mathsf{F}(s_0, \beta_0), \mathsf{F}(s_1, \beta_1)\}$ is a subset of $\mathrm{L}(S)$, so the result follows.
- If $i = 2$, then $\mathsf{F}(s, \alpha) = \mathsf{F}(s_0, \beta_0) \times \mathsf{F}(s_1, \beta_1)$. In order to show that $\mathrm{TC}(\mathsf{F}(s, \alpha)) \subseteq \mathrm{L}(S)$ it is enough to show that

$$(u_0, u_1) \in \mathrm{L}(S) \text{ and } \mathrm{TC}(\{\{u_0\}, \{u_0, u_1\}\}) \subseteq \mathrm{L}(S)$$

for all $u_j \in \mathsf{F}(s_j, \beta_j)$ and $j = 0, 1$. By inductive assumption $\mathrm{TC}(\mathsf{F}(s_j, \beta_j)) \subseteq \mathrm{L}(S)$, and since $u_j \in \mathrm{TC}(\mathsf{F}(s_j, \beta_j))$, and $\mathrm{TC}(u_j) \subseteq \mathrm{TC}(\mathsf{F}(s_j, \beta_j))$, we have that $u_j, \mathrm{TC}(u_j) \in \mathrm{L}(S)$, for $j = 0, 1$. As $\mathrm{L}(S)$ is closed under $\mathfrak{F}_1$, then $(u_0, u_1) \in \mathrm{L}(S)$. Moreover

$$\mathrm{TC}((u_0, u_1)) = \mathrm{TC}(\{\{u_0\}, \{u_0, u_1\}\}) = (u_0, u_1) \cup \{u_0, u_1\} \cup \mathrm{TC}(u_0) \cup \mathrm{TC}(u_1)$$

is contained in $\mathrm{L}(S)$. This completes the proof.
- If $i = 3$, then $\mathsf{F}(s, \alpha) = \mathsf{F}(s_0, \beta_0) \setminus \mathsf{F}(s_1, \beta_1) \subseteq \mathsf{F}(s_0, \beta_0)$. Thus by inductive assumption $\mathrm{TC}(\mathsf{F}(s, \alpha)) \subseteq \mathrm{TC}(\mathsf{F}(s_0, \beta_0)) \subseteq \mathrm{L}(S)$.
- If $i = 4$, then $\mathsf{F}(s, \alpha) = \operatorname{dom} \mathsf{F}(s_0, \beta_0)$. If $u \in \mathsf{F}(s, \alpha)$ then there is v such that $u \in \{u\} \in (u, v) \in \mathsf{F}(s_0, \beta_0)$, so $\{u\} \cup \mathrm{TC}(u) = \mathrm{TC}(\{u\}) \subseteq \mathrm{TC}(\mathsf{F}(s_0, \beta_0)) \subseteq \mathrm{L}(S)$ by inductive assumption. Therefore

$$\mathrm{TC}(\mathsf{F}(s, \alpha)) = \mathsf{F}(s, \alpha) \cup \textstyle\bigcup_{u \in \mathsf{F}(s, \alpha)} \mathrm{TC}(u) \subseteq \mathrm{L}(S).$$
- If $i = 5$, then $\mathsf{F}(s, \alpha) = \bigcup \mathsf{F}(s_0, \beta_0)$, and the result follows easily.
- If $i = 6$, then $\mathsf{F}(s, \alpha) \subseteq \mathsf{F}(s_0, \beta_0) \times \mathsf{F}(s_1, \beta_1)$, so the result holds by the case $i = 2$.
- If $i = 7$, then $\mathsf{F}(s, \alpha) = \{(u, v, w) \mid (u, w, v) \in \mathsf{F}(s_0, \beta_0)\}$. Let $(u, v, w) \in \mathsf{F}(s, \alpha)$. Since $u, v, w \in \mathrm{TC}((u, w, v)) \subseteq \mathrm{TC}(\mathsf{F}(s_0, \beta_0)) \subseteq \mathrm{L}(S)$, then $(u, v, w) \in \mathrm{L}(S)$ by closure under $\mathfrak{F}_1$, and using the inductive assumption $\mathrm{TC}(u), \mathrm{TC}(v), \mathrm{TC}(w) \subseteq \mathrm{L}(S)$. Arguing as above,

$$\mathrm{TC}((u, v, w)) = (u, v, w) \cup \{(u, v), w\} \cup \{u, v\} \cup \mathrm{TC}(u) \cup \mathrm{TC}(v) \cup \mathrm{TC}(w)$$

is contained in $\mathrm{L}(S)$. Therefore

$$\mathrm{TC}(\mathsf{F}(s,\alpha)) = \mathsf{F}(s,\alpha) \cup \bigcup\nolimits_{(u,v,w)\in\mathsf{F}(s,\alpha)} \mathrm{TC}((u,v,w)) \subseteq \mathrm{L}(S).$$

- If $i = 8$, then $\mathsf{F}(s,\alpha) = \{(u,v,w) \mid (v,w,u) \in \mathsf{F}(s_0,\beta_0)\}$, and the argument is similar to the case $i = 7$. □

Corollary 39.11. *Suppose $S \asymp S \times S$ is transitive. Then $\mathrm{L}(S)$ is a proper class inner model of* ZF, *and $\langle \mathsf{F}(9\cdot\beta) \mid \beta \in \mathrm{Ord}\rangle$ is a hierarchy for it.*

Proof. Apply Theorem 39.6. □

The class-function $\mathrm{Ord} \to \mathrm{Ord} \times 9$, $\alpha \mapsto (\mathsf{D}(\alpha), \mathsf{R}(\alpha))$ is Δ_1^{ZF}, so

$$\mathsf{F}_{S,p} \colon S \times \mathrm{Ord} \to \mathrm{V}$$

is defined by a Σ_1 formula, that is

$$\mathsf{F}_{S,p}(s,\alpha) = x \Leftrightarrow \exists f\, \varphi(f,s,\alpha,S,p,x)$$

where φ is Δ_0. Being an operation, this implies that $\mathsf{F}_{S,p}$ is Δ_1^{ZF}-definable, and hence absolute for inner models of ZF. Suppose M is a proper class inner model of ZF such that $S, p \in M$, and $p\colon S \to S\times S$ is a bijection. Since $(p\colon S \to S \times S \text{ is a bijection})^{(M)}$, then $\mathsf{F}_{S,p}(s,\alpha)$ computed in M is the same as $\mathsf{F}_{S,p}(s,\alpha)$ computed in V, so $\mathrm{L}(S)^{(M)} = \mathrm{L}(S)$. If $(S \asymp S\times S)^{\mathrm{L}(S)}$, then the following sentence holds when relativized to $\mathrm{L}(S)$:

$$\forall x\, \exists \alpha\, \exists s \in S\, \exists f\, \varphi(f,s,\alpha,S,p,x).$$

The formula above is abbreviated as $\mathrm{V} = \mathrm{L}(S)$, meaning that the inner model $\mathrm{L}(S)$ thinks that the universe is the constructible closure of S.

Given an arbitrary set S, let $\overline{S}$ be the closure of $\mathrm{TC}(\{S\}) \cup \omega$ under the operations $x \mapsto \{x\}$ and $(x,y) \mapsto x \cup y$. Then $\overline{S}$ is transitive and $\overline{S} \asymp \overline{S} \times \overline{S}$, and $S \in M \Leftrightarrow \overline{S} \in M$ for any inner model M (Exercise 39.30).

Definition 39.12. For S and arbitrary set, let $\mathrm{L}(S)$ be $\mathrm{L}(\overline{S})$ where $\overline{S}$ is as above.

Theorem 39.13. (a) *If M is a proper class inner model of* ZF *such that $S \in M$, then $\mathrm{L}(S) \subseteq M$.*

(b) *In $\mathrm{L}(S)$ the following are true: $\mathrm{V} = \mathrm{L}(S)$, and every set is the surjective image of $S \times \alpha$ for some α, that is*

$$(\forall x\, \exists\alpha\, \exists f\, (f\colon S\times\alpha \twoheadrightarrow x))^{\mathrm{L}(S)}.$$

Moreover, if $(S \text{ is well-orderable})^{(\mathrm{L}(S))}$, then the axiom of global choice AGC *is true in $\mathrm{L}(S)$, that is $\mathsf{AGC}^{(\mathrm{L}(S))}$ holds.*[4]

[4] The axiom AGC is defined on page 378.

Proof. Without loss of generality we may assume that $S \neq \emptyset$ is transitive, and that $p\colon S \to S \times S$ is a bijection. Then part (a) follows from the absoluteness of $\mathsf{F}_{S,p}$.

Now we tackle part (b). The class function $\mathsf{F} : S \times \mathrm{Ord} \to \mathrm{L}(S)$ is surjective, so for all $y \in \mathrm{L}(S)$ there is a least α_y such that $\mathsf{F}(s, \alpha_y) = y$ for some $s \in S$. Therefore for any $x \in \mathrm{L}(S)$ let $\alpha = \sup\{\alpha_y \dotplus 1 \mid y \in x\}$ so that $x \subseteq \mathsf{F}``S \times \alpha$. As $\mathsf{F} \restriction S \times \alpha$ is definable in $\mathrm{L}(S)$, and hence belongs to $\mathrm{L}(S)$, the result follows.

Assume now that S is well-orderable in $\mathrm{L}(S)$. Then $S \times \mathrm{Ord}$ is also well-orderable, and so is $\mathrm{L}(S) = \operatorname{ran} \mathsf{F}$, and hence $\mathsf{AGC}^{(\mathrm{L}(S))}$ holds by Theorem 18.3. □

Part (a) of Theorem 39.13 can be stated as: $\mathrm{L}(S)$ is the smallest proper class inner model M of ZF such that $S \in M$. By Exercise 39.31 the assumption $S \in M$ cannot be weakened to $S \subseteq M$.

Examples 39.14. (a) If $S = \{0\} = 1$ then S and the unique bijection $S \to S \times S$ belong to any inner model of ZF. Therefore $\mathrm{L}(1)$ is the smallest inner model of ZF, and it is commonly denoted as L—see Section 39.D.

(b) If $S = \alpha \geq \omega$ then $S \asymp S \times S$, and since α belongs to any proper class inner model of ZF, then $\mathrm{L}(\alpha) = \mathrm{L}$.

(c) If $S = \mathrm{V}_\alpha$ with $\alpha \geq \omega$, then $S \asymp S \times S$ by Exercise 20.25. As $\mathrm{V}_\alpha \cap \mathrm{L}(\mathrm{V}_\alpha) = \mathrm{V}_\alpha$, then $\mathrm{V}_\alpha \in \mathrm{L}(\mathrm{V}_\alpha)$ and $\mathrm{L}(\mathrm{V}_\alpha)$ is an inner model of $\mathsf{ZF} + \mathrm{V} = \mathrm{L}(\mathrm{V}_\alpha)$.

If $\alpha = \omega$ then $\mathrm{L}(\mathrm{V}_\alpha) = \mathrm{L}$ (Exercise 39.32).

If $\alpha = \omega \dotplus 1$, then $\mathrm{V}_{\omega \dotplus 1} \asymp \mathbb{R}$, and we cannot prove that $\mathrm{V}_{\omega \dotplus 1} \in \mathrm{L}$. It is customary to write $\mathrm{L}(\mathbb{R})$ for $\mathrm{L}(\mathrm{V}_{\omega \dotplus 1})$.

The following comes up naturally: does $\mathsf{AC}^{(\mathrm{L}(\mathbb{R}))}$ hold? Equivalently: is $\mathrm{V}_{\omega \dotplus 1}$ well-orderable in $\mathrm{L}(\mathbb{R})$? The answer is: it depends. If $\mathrm{V} = \mathrm{L}$ is assumed, then $\mathrm{L}(\mathbb{R}) = \mathrm{L}$, so $\mathrm{V}_{\omega \dotplus 1}$ is well-orderable, since every set is. On the other hand, there is no way to construct in ZF a well-order of $\mathrm{V}_{\omega \dotplus 1}$, one that would be absolute enough to trickle-down in $\mathrm{L}(\mathbb{R})$. In fact, working in ZFC and assuming the existence of large enough cardinals, one can prove that $\mathbb{R}$ is not well-orderable in $\mathrm{L}(\mathbb{R})$.

39.D. The constructible universe. The constructible closure of $1 = \{\emptyset\}$, is called the **constructible universe** and it is denoted by L, rather than $\mathrm{L}(1)$. By Theorem 39.13 it is the smallest proper class inner model of ZF, and as $1 \asymp 1 \times 1$ in any inner model, L is an inner model of $\mathsf{ZFC} + \mathrm{V} = \mathrm{L}$. Note that all this yields an interpretation of ZFC in ZF. Summarizing:

Theorem 39.15. *The constructible universe* L *is a transitive proper class such that*

(a) L *is an inner model of* ZFC*, and hence* $\mathsf{Con}_{\mathsf{ZF}} \Rightarrow \mathsf{Con}_{\mathsf{ZFC}}$.

(b) *If M is a proper class inner model of* ZF*, then* $\mathrm{L} \subseteq M$ *and* L *is absolute between M and* V.

The class-function F can be construed as a unary operation on the ordinals:

$$\mathsf{F}(\alpha) = \begin{cases} \operatorname{ran} \mathsf{F} \restriction \alpha & \text{if } \mathsf{R}(\alpha) = 0, \\ \mathfrak{F}_{\mathsf{R}(\alpha)}(\mathsf{F}((\mathsf{D}(\alpha))_0), \mathsf{F}((\mathsf{D}(\alpha))_1)) & \text{otherwise,} \end{cases}$$

where D and R are as in (39.2).

Theorem 39.16. *Assume* $\mathrm{V} = \mathrm{L}$. *If $x \subseteq \kappa$ an infinite cardinal, then there is an $\alpha < \kappa^+$ such that $\mathsf{F}(\alpha) = x$.*

Proof. Let κ be an infinite cardinal, let $x \subseteq \kappa$, and let α be such that $\mathsf{F}(\alpha) = x$. Fix a finite sub-theory T of ZF containing Ext and such that the formula $\psi(\nu, y)$ asserting that $\mathsf{F}(\nu) = y$ is Δ_1^{T}. Let $\lambda > \kappa, \alpha$ be a limit ordinal such that the following formulæ $\bigwedge \mathsf{T}$, $\forall \nu\, \exists y\, (\mathsf{F}(\nu) = y)$, and $\forall y\, \exists \nu\, (\mathsf{F}(\nu) = y)$ are absolute between $\mathsf{F}(\lambda)$ and L. Let M be such that $\kappa \cup \{x\} \subseteq M \prec \mathsf{F}(\lambda)$, and $|M| = \kappa$. If $\boldsymbol{\pi} \colon M \to \overline{M}$ is the transitive collapse, then $\boldsymbol{\pi}$ is an isomorphism, as M satisfies extensionality, and $\boldsymbol{\pi} \restriction \kappa$ is the identity so that $\boldsymbol{\pi}(x) = x \in \overline{M}$. Since T, $\forall \nu\, \exists y\, (\mathsf{F}(\nu) = y)$, and $\forall y\, \exists \nu\, (\mathsf{F}(\nu) = y)$ are true in $\mathsf{F}(\lambda)$, the same can be said of M, and hence of $\overline{M}$. Therefore the operation F is absolute for $\overline{M}$ (as ψ is Δ_1^{T}), $\overline{M}$ is closed under F, and every $y \in \overline{M}$ is of the form $\mathsf{F}(\beta)$ for some $\beta \in \overline{M}$. Thus $x = \mathsf{F}(\gamma) \in \overline{M}$ for some $\gamma \in \overline{M}$. As $\overline{M}$ is transitive and $|\overline{M}| = \kappa$, it follows that $\gamma < \kappa^+$. □

Theorem 39.17. $\mathsf{ZF} \vdash \mathrm{V} = \mathrm{L} \Rightarrow \mathsf{GCH}$. *Therefore* $\mathsf{Con}_{\mathsf{ZF}} \Rightarrow \mathsf{Con}_{\mathsf{ZFC+GCH}}$.

Proof. By Theorem 39.16, if κ is an infinite cardinal, then $\mathscr{P}(\kappa) \subseteq \mathsf{F}``\kappa^+$, and $|\mathsf{F}``\kappa^+| \leq \kappa^+$ so $2^\kappa \leq \kappa^+$. □

Theorems 39.16 and 39.17 can be strengthened: if κ is a cardinal snd $S \subseteq \kappa^+$ then $\left(\forall \lambda \geq \kappa\, (2^\lambda = \lambda^+)\right)^{(\mathrm{L}(S))}$. In particular, if $S \subseteq \omega_1$ then GCH holds in $\mathrm{L}(S)$.

39.D.1. *Absoluteness.* In the preceding pages we have shown in ZF that L is a proper class inner model of $\mathsf{ZFC} + \mathsf{GCH}$. Clearly $\mathrm{L} \subseteq \mathrm{V}$, and we cannot expect to prove in ZF that the inclusion is proper, as this proof would work inside L as well, while we know that people in the constructible universe believe that every set is constructible, that is $\mathrm{V} = \mathrm{L}$. Still one might ask what is the simplest kind of set, if any, that does not belong to L.

Using the results in the preceding pages we have that if M is a transitive inner model of ZF, then:

- If $a \subseteq M$ is finite, then $a \in M$, by closure under the Gödel functions; in particular ${}^{<\omega}M \subseteq M$.
- If $a \in M$ then $\mathscr{P}(a) \cap M \in M$.
- $\mathrm{V}_\alpha \cap M \in M$ for all $\alpha \in \mathrm{Ord}$, and $\mathrm{V}_\omega \in M$. In particular $\mathbb{Z}, \mathbb{Q} \in M$ and $\mathbb{R} \cap M \in M$.

As $\mathbb{Q} \subseteq \mathbb{R} \cap M$ is a dense subgroup of $(\mathbb{R}, +)$, if it is $\mathbf{G}_\delta$ then $\mathbb{R} \cap M = \mathbb{R}$. In fact if $x + (\mathbb{R} \cap M)$ were a coset disjoint from $\mathbb{R} \cap M$ we would have two disjoint $\mathbf{G}_\delta$ subsets of $\mathbb{R}$, against Baire's category theorem.

Going back to the constructible universe, we have that $\mathbb{R}^{(\mathrm{L})} \subseteq \mathbb{R}$. The statement $\mathbb{R}^{(\mathrm{L})} = \mathbb{R}$, that is $\mathbb{R} \subseteq \mathrm{L}$ is consistent; it clearly follows from $\mathrm{V} = \mathrm{L}$, but it also consistent with $\mathrm{V} \neq \mathrm{L}$. On the other hand it is also consistent that $\mathbb{R} \cap \mathrm{L} \neq \mathbb{R}$, that is to say: there are real numbers that are not constructible. For example, each of the following is consistent with ZFC:

- $2^{\aleph_0} > \aleph_1 = \aleph_1^{(\mathrm{L})} = |\mathbb{R}^{(\mathrm{L})}|$,
- $2^{\aleph_0} = \aleph_1 = \aleph_1^{(\mathrm{L})} = |\mathbb{R}^{(\mathrm{L})}|$, and $\mathbb{R}^{(\mathrm{L})} \neq \mathbb{R}$,
- $2^{\aleph_0} \geq \aleph_1$ and $|\aleph_1^{(\mathrm{L})}| = |\mathbb{R}^{(\mathrm{L})}| = \aleph_0$.

Theorem 39.18. $\mathsf{Con}_{\mathsf{T}_1} \Leftrightarrow \mathsf{Con}_{\mathsf{T}_2}$, *where* T_1 *is* $\mathsf{ZF} +$ *"there is a weakly inaccessible cardinal", and* T_2 *is* $\mathsf{ZFC} +$ *"there is a strongly inaccessible cardinal".*

Proof. As T_2 extends T_1, then $\mathsf{Con}_{\mathsf{T}_2} \Rightarrow \mathsf{Con}_{\mathsf{T}_1}$. To prove the reverse implication it is enough to show that L provides an interpretation of T_2 in T_1. The formula $\varphi(\kappa)$ asserting that κ is weakly inaccessible is Π_1^{ZF}, so $\varphi(\kappa) \Rightarrow (\varphi(\kappa))^{(\mathrm{L})}$. Since GCH holds in L, then $\mathsf{ZF} \vdash \forall\kappa\left(\varphi(\kappa) \Rightarrow (\kappa \text{ is strongly inaccessible})^{(\mathrm{L})}\right)$. □

The next result shows that consistency-wise, large cardinals are related to the continuum.

Theorem 39.19. $\mathsf{Con}_{\mathsf{T}_1} \Rightarrow \mathsf{Con}_{\mathsf{T}_2}$, *where* T_1 *is* $\mathsf{ZF} + \mathsf{AC}_\omega(\mathbb{R}) + \omega_1 \not\precsim \mathbb{R}$, *and* T_2 *is* $\mathsf{ZFC} +$ *"there is a strongly inaccessible cardinal".*

Proof. Work in T_1. The cardinal $\kappa = \omega_1$ is regular by $\mathsf{AC}_\omega(\mathbb{R})$, and by downward absoluteness $(\omega < \kappa \text{ is regular})^{(\mathrm{L})}$. Suppose $(\kappa \text{ is a successor cardinal})^{(\mathrm{L})}$; then $(\kappa \precsim \mathscr{P}(\gamma))^{(\mathrm{L})}$ for some $\omega \leq \gamma < \kappa$, and since $\omega \asymp \gamma$, then $\omega_1 = \kappa \precsim \mathscr{P}(\omega) \asymp \mathbb{R}$, a contradiction. Therefore inside L, κ is a limit cardinal, i.e. it is inaccessible. In other words: L is a transitive inner model of T_2. □

Theorem 39.20. *Suppose* σ *is a* $\mathcal{L}_\in$*-statement that is absolute between* V *and* L*, that is* $\mathsf{ZF} \vdash \sigma \Leftrightarrow (\sigma)^{(\mathrm{L})}$. *Then* $\mathsf{ZFC} + \mathrm{V} = \mathrm{L} \vdash \sigma$ *if and only if* $\mathsf{ZF} \vdash \sigma$.

Proof. Suppose there is a proof of σ from $\mathsf{ZFC} + \mathrm{V} = \mathrm{L}$, and work in ZF. As L is an inner model of $\mathsf{ZFC} + \mathrm{V} = \mathrm{L}$, then $\sigma^{(\mathrm{L})}$ holds. Therefore the left-to-right implication holds; the reverse implication is trivial. □

Therefore any Δ_1^{ZF} statement σ proved in ZF with the aid of some consequence of $\mathrm{V} = \mathrm{L}$, like AC of CH, follows from ZF alone. Typical examples of such statements are the results in number theory—for example Fermat's Last Theorem, being a result of ZFC, it is provable in ZF alone.

We close this Section with a result substantiating the remarks of Section 34.A. Note that every effective language $\mathcal{L}$ and every effective theory T belong to L.

Theorem 39.21. *Suppose that T is a theory in a language $\mathcal{L}$, that $\boldsymbol{\sigma}$ is an $\mathcal{L}$-sentence, and that $T, \mathcal{L} \in \mathrm{L}$. If $T \models \boldsymbol{\sigma}$ follows from $\mathsf{ZF} + \mathrm{V} = \mathrm{L}$, then it follows from ZF alone.*

Proof. The language $\mathcal{L}$ is well-orderable, as it belongs to L, and hence the instance of the Completeness Theorem

$$T \models \boldsymbol{\sigma} \Leftrightarrow T \vdash \boldsymbol{\sigma}$$

is provable in ZF. Working inside L we have that $T \models \boldsymbol{\sigma}$ and hence $T \vdash \boldsymbol{\sigma}$, so that

$$\mathsf{ZF} \vdash \left(\exists s \, (s \text{ is a derivation in } \mathcal{L} \text{ of } \boldsymbol{\sigma} \text{ from } T)\right)^{(\mathrm{L})}.$$

As being a derivation is Δ_1^{ZF}, then $\mathsf{ZF} \vdash \exists s \, (s \text{ is a derivation in } \mathcal{L} \text{ of } \boldsymbol{\sigma} \text{ from } T)$ so $T \models \boldsymbol{\sigma}$ is provable in ZF, as required. □

39.E. The constructible hierarchy*. Here is a sleeker approach to the constructible universe. Arguing as in Section 37.D the class

$$\mathscr{F} = \{\langle M, \boldsymbol{\varphi}, g\rangle \mid \mathsf{Trans}(M) \wedge \boldsymbol{\varphi} \wedge g \colon \operatorname{Fv}(\boldsymbol{\varphi}) \to M\}$$

can be shown to be Δ_1^{ZF}, where $\mathrm{Fml} = \mathrm{Fml}(\mathcal{L}_{\in})$ is the set of all (codes for) formulæ of the language of set theory. As $\operatorname{Fv}(\boldsymbol{\varphi})$ is a finite subset of $\mathrm{Vbl} = \{\boldsymbol{v}_n \mid n \in \omega\}$, it is customary to replace the assignment g with the n-tuple of its values. Thus if $\boldsymbol{\varphi}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ and $g(\boldsymbol{x}_i) = a_i$ we write $\langle M, \in\rangle \vDash \boldsymbol{\varphi}[\vec{a}]$ in place of $\langle M, \in\rangle \vDash_g \boldsymbol{\varphi}$. The class

$$\{\langle M, \boldsymbol{\varphi}, \vec{a}\rangle \in \mathscr{F} \mid \langle M, \in\rangle \vDash \boldsymbol{\varphi}[\vec{a}]\}$$

is also Δ_1^{ZF}, and therefore also the operation $M \mapsto \operatorname{Def}(M)$ is Δ_1^{ZF} where $\operatorname{Def}(M)$ is the set of all subsets of M that are definable in $\langle M, \in\rangle$ with parameters in M,

$$\begin{aligned}\operatorname{Def}(M) = \Big\{X \subseteq M \mid \exists \boldsymbol{\varphi}(\boldsymbol{x}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \in \mathrm{Fml}\, \exists b_1, \ldots, b_n \in M \\ \forall a \in M \left(a \in X \Leftrightarrow \langle M, \in\rangle \vDash \boldsymbol{\varphi}[a, \vec{b}]\right)\Big\}.\end{aligned}$$

As the universe of a structure must be a non-empty set, so let's convene that when $M = \emptyset$ then $\mathrm{Def}(M) = \{\emptyset\}$. Also when there is no danger of confusion we will blur the distinction between the structure $\langle M, \in\rangle$ and its underlying universe M.

Definition 39.22. Let $\mathrm{L}_0 = \emptyset$, $\mathrm{L}_{\alpha\dotplus 1} = \mathrm{Def}(\mathrm{L}_\alpha)$, and $\mathrm{L}_\lambda = \bigcup_{\alpha<\lambda} \mathrm{L}_\alpha$, for λ limit.

Proposition 39.23. *For all* $\alpha \in \mathrm{Ord}$

(a) $\mathrm{L}_\alpha \in \mathrm{L}_{\alpha\dotplus 1}$,

(b) L_α *is transitive,*

(c) $\forall \beta \leq \alpha\, (\mathrm{L}_\beta \subseteq \mathrm{L}_\alpha)$.

Proof. (a) L_α is definable (without parameters) in L_α via $\boldsymbol{v}_0 \doteq \boldsymbol{v}_0$.

(b) Suppose L_β is transitive for all $\beta < \alpha$. If α is limit, then the result is immediate; if $\alpha = \beta \dotplus 1$ and $y \in x \in \mathrm{L}_\alpha$ then $y \in x \subseteq \mathrm{L}_\beta$ so $y \in \mathrm{L}_\beta$ and $y \subseteq \mathrm{L}_\beta$. But y is definable in L_β using y as a parameter via the formula $\boldsymbol{v}_0 \in \boldsymbol{v}_1$, that is $y \in \mathrm{Def}(\mathrm{L}_\beta) = \mathrm{L}_\alpha$.

(c) By induction on α. If α is 0 or limit the result is trivial. If $\alpha = \gamma \dotplus 1$ then $\mathrm{L}_\gamma \in \mathrm{L}_\alpha$, so $\mathrm{L}_\gamma \subset \mathrm{L}_\alpha$; so if $\beta \leq \alpha$ then either $\beta = \alpha$ and there is nothing to prove, or $\beta < \alpha$ so either $\beta = \gamma$ and the result follows, or $\beta < \gamma$ and we apply the induction hypothesis and conclude that $\mathrm{L}_\beta \subseteq \mathrm{L}_\gamma$ and therefore $\mathrm{L}_\beta \subseteq \mathrm{L}_\alpha$. □

Proposition 39.24. (a) $\mathsf{ZF} \vdash \forall\alpha(\mathrm{L}_\alpha \subseteq \mathrm{V}_\alpha)$.

(b) $\mathrm{L}_\alpha \cap \mathrm{Ord} = \alpha$,

(c) $\mathrm{L}_n = \mathrm{V}_n$ *for all* $n \in \omega$*, and hence* $\mathrm{L}_\omega = \mathrm{V}_\omega$.

Proof. (a) By induction on α. If $\alpha = 0$ or α is limit, then the result is trivial. Suppose $\mathrm{L}_\alpha \subseteq \mathrm{V}_\alpha$: then $\mathrm{L}_{\alpha+1} = \mathrm{Def}(\mathrm{L}_\alpha) \subseteq \mathscr{P}(\mathrm{L}_\alpha) \subseteq \mathscr{P}(\mathrm{V}_\alpha)$.

(b) By induction on α. If $\alpha = 0$ or α is limit, then the result is trivial. Suppose $\alpha = \mathrm{L}_\alpha \cap \mathrm{Ord}$: then $\alpha = \{a \in \mathrm{L}_\alpha \mid \mathrm{L}_\alpha \vDash \ulcorner \mathsf{Ord}(x) \urcorner[a]\} \in \mathrm{L}_{\alpha\dotplus 1}$. Thus $\{\alpha\} \subseteq \mathrm{L}_{\alpha\dotplus 1}$ and since $\alpha \subseteq \mathrm{L}_{\alpha\dotplus 1}$ then $\alpha\dotplus 1 \subseteq \mathrm{L}_{\alpha\dotplus 1} \cap \mathrm{Ord}$. The other inclusion follows from (a).

(c) If $\mathrm{L}_n = \mathrm{V}_n$ and $a \in \mathrm{V}_{n\dotplus 1}$ then $a = \{a_1, \ldots, a_k\}$ for some $k \in \omega$ so $a = \{x \in \mathrm{L}_n \mid \mathrm{L} \vDash \boldsymbol{\varphi}_k[x, a_i, \ldots, a_k]\} \in \mathrm{L}_{n\dotplus 1}$, where $\boldsymbol{\varphi}_k$ is $\bigvee_{1\leq i\leq k} \boldsymbol{v}_0 \doteq \boldsymbol{v}_i$. □

As $M \mapsto \mathrm{Def}(M)$ is Δ_1^{ZF} and using Proposition 37.13, the class-function $\alpha \mapsto \mathrm{L}_\alpha$ is Δ_1^{ZF}, so it is absolute between V and any inner model M of ZF, and hence $\mathrm{L}_\alpha = (\mathrm{L}_\alpha)^{(\mathrm{L})}$ for all $\alpha \in M$. In particular $\mathrm{L}_\alpha = (\mathrm{L}_\alpha)^{(\mathrm{L})}$ for all α, and hence

$$\textstyle\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha \subseteq \mathrm{L}.$$

The next goal is to show that this inclusion is an equality, and hence obtaining a more transparent definition of the constructible universe. In other words, L is the analogue of V where the operation $x \mapsto \mathscr{P}(x)$ used to construct the hierarchy $\langle \mathrm{V}_\alpha \mid \alpha \in \mathrm{Ord}\rangle$ for V is replaced by the operation $x \mapsto \mathrm{Def}(x)$ yielding the hierarchy $\langle \mathrm{L}_\alpha \mid \alpha \in \mathrm{Ord}\rangle$ for L.

In order to prove that $\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha = \mathrm{L}$, it is enough to show (Theorem 39.26) that $\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$ is a proper class inner model of ZF and then appeal to part (b) of Theorem 39.15. If $y \in \bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$ then $y \in \mathrm{L}_\beta$ for some β, and let $\mathrm{rank}_{\mathrm{L}}(y)$ be the least such β. Clearly $\mathrm{rank}_{\mathrm{L}}(y)$ is always a successor ordinal.

Lemma 39.25. *The class $\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$ is almost universal. In fact*

$$\forall x \subseteq \textstyle\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha \, \exists \beta \, (x \subseteq \mathrm{L}_\beta).$$

Proof. By replacement, for every $x \subseteq \bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$ there is β such that $\forall y \in x\, (\mathrm{rank}_{\mathrm{L}}(y) < \beta)$. □

Theorem 39.26 (ZF)**.** *The class $\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$ is an inner model for ZF.*

Proof. For notational ease we use the acronyms introduced in Section 37 and write L' for $\bigcup_{\alpha\in\mathrm{Ord}} \mathrm{L}_\alpha$.

The class L' is transitive and $\mathrm{Ord} \subseteq \mathrm{L}'$ by Propositions 39.23 and 39.24, so $(\mathsf{Ext} \wedge \mathsf{Fnd} \wedge \mathsf{Inf})^{(\mathrm{L}')}$. For any α, $\mathrm{L}_\alpha \in \mathrm{L}_{\alpha+1} \subseteq \mathrm{L}'$ by Propositions 39.23.

If $a_1, a_2 \in \mathrm{L}'$, let α_1, α_2 such that $a_i \in \mathrm{L}_{\alpha_i}$, so $\{a_1, a_2\} \subseteq \mathrm{L}_\alpha \in \mathrm{L}'$, where $\alpha = \max(\alpha_1, \alpha_2)$. Thus $\mathsf{Prn}^{(\mathrm{L}')}$.

If $a \in \mathrm{L}'$ then $a \in \mathrm{L}_\alpha$ for some α, and as L_α is transitive, it follows that $\bigcup a \subseteq \mathrm{L}_\alpha \in \mathrm{L}'$. Thus $\mathsf{Unn}^{(\mathrm{L}')}$.

Fix $a \in \mathrm{L}'$. As $b = \mathscr{P}(a) \cap \mathrm{L}'$ is a set, then $b \in \mathrm{L}_\beta$ for some β, by Proposition 39.25. Thus $\mathsf{Pwr}^{(\mathrm{L}')}$.

Finally we prove that $\mathsf{tRpl}^{(\mathrm{L}')}$, where tRpl is the axiom-schema of tight replacement introduced on page 591, and hence the axiom-schemata of replacement and separation hold in L' by Exercise 37.20. Consider an instance of tRpl:

$$\forall w_1, \dots, w_n \, \forall z \, (\psi(z, \vec{w}) \Rightarrow \exists u \, \chi(z, u, \vec{w}))$$

where

$$\begin{aligned} \psi(z, \vec{w}) &: \forall x \in z \, \forall y_1, y_2 \, [\varphi(x, y_1, \vec{w}) \wedge \varphi(x, y_2, \vec{w}) \Rightarrow y_1 = y_2] \\ \chi(z, u, \vec{w}) &: \forall y \, (y \in u \Leftrightarrow \exists x \in z \, \varphi(x, y, \vec{w})) \end{aligned}$$

Fix $a, p_1, \dots, p_n \in \mathrm{L}'$ such that $\psi(a, \vec{p})^{(\mathrm{L}')}$ towards proving $\chi(a, b, \vec{p})^{(\mathrm{L}')}$ for some $b \in \mathrm{L}'$. Let α be such that $a, \vec{p} \in \mathrm{L}_\alpha$ and $\forall x \in a \, \forall y \in \mathrm{L}' \, (\varphi(x, y, \vec{p})^{\mathrm{L}'} \Rightarrow c \in \mathrm{L}_\alpha)$. By the reflection principle there are β and γ such that $\alpha < \beta < \gamma$ and ψ and χ are absolute between $\mathrm{L}_\beta, \mathrm{L}_\gamma$ and L'. Then $\psi(a, \vec{p})^{(\mathrm{L}_\beta)}$ and hence

$\mathrm{L}_\beta \vDash \ulcorner \psi(z, \vec{w}) \urcorner [a, \vec{p}]$. Letting $\varphi'(z, y, \vec{w})$ be the formula $\exists x \in z\, \varphi(x, y, \vec{w})$, then

$$b = \{c \in \mathrm{L}_\beta \mid \mathrm{L}_\alpha \vDash \ulcorner \varphi'(z, y, \vec{w}) \urcorner [a, c, \vec{p}]\} \in \mathrm{L}_{\beta+1} \subseteq \mathrm{L}_\gamma,$$

that is $\chi(a, b, \vec{p})^{(\mathrm{L}_\beta)}$. This implies that $\chi(a, b, \vec{p})^{(\mathrm{L}')}$, which is what we had to prove. □

Exercises

Exercise 39.27. Show that if M is closed under the Gödel operations and $(u, v) \in M$, then $u, v \in M$.

Exercise 39.28. Suppose M is closed under the Gödel operations, and let $\boldsymbol{\pi}\colon M \to \overline{M}$ be the transitive collapse. Show that $\forall x, y \in M\, (\boldsymbol{\pi}(\mathfrak{F}_i(x, y)) = \mathfrak{F}_i(\boldsymbol{\pi}(x), \boldsymbol{\pi}(y)))$, for all $i = 1, \ldots, 8$.

Exercise 39.29. Let $M = \{x \in \mathrm{V} \mid \rho(x) < \omega\}$, where $\rho(x) = 0$ if $x \in \mathrm{Ord}$, and $\rho(x) = \sup\{\mathbf{S}(\rho(y)) \mid y \in x\}$ otherwise. Show that:

(i) M is a transitive class, containing the ordinals, closed under the Gödel operations, but not almost universal. In particular, $M \cap \mathrm{L} \neq \mathrm{L}$.

(ii) $M \cap \mathrm{V}_{\omega+\omega}$ is a model of Z. Conclude that Z does not prove the existence of V_ω.

Exercise 39.30. Let M be an inner model of ZF, let S be an arbitrary set, and let $\overline{S}$ be the closure of $\mathrm{TC}(\{S\}) \cup \omega$ under the operations $x \mapsto \{x\}$ and $(x, y) \mapsto x \cup y$. Show that:

(i) $\overline{S}$ is transitive and $S \subseteq \overline{S}$.

(ii) ${}^{<\omega}\overline{S} \subseteq \overline{S}$, and hence $\overline{S} \times \overline{S} \asymp \overline{S}$.

(iii) $S \in M \Leftrightarrow \overline{S} \in M$.

Exercise 39.31. Suppose there is an $x \subseteq \omega$ such that $x \notin \mathrm{L}$, and let $S = \omega \cup \{\{n\} \mid n \in x\}$. Show that:

(i) $S \asymp S \times S$ is transitive,

(ii) $S \subseteq \mathrm{L}$ and $S \notin \mathrm{L}$,

(iii) $\mathrm{L} \neq \mathrm{L}(S)$.

Exercise 39.32. Show that if $S \in \mathrm{L}$, then $\mathrm{L}(S) = \mathrm{L}$.

Exercise 39.33. Assume $\mathsf{DC}(\mathbb{R})$ and show that $\mathsf{DC}^{(\mathrm{L}(\mathbb{R}))}$.

40. Measurable cardinals

Throughout this section we assume AC. Recall that κ is a **real-valued measurable cardinal** if there is a κ-additive, non-singular, probability measure $\mu\colon \mathscr{P}(\kappa) \to [0;1]$ (Definition 26.16). Every real-valued measurable cardinal is weakly inaccessible, and if μ is atomless $\kappa \leq 2^{\aleph_0}$ (Theorems 26.17 and 26.14). If $A \subseteq \kappa$ is an atom for μ, that is to say $\mu(A) > 0$ and $\forall B \subseteq A\, (\mu(B) = 0 \vee \mu(B) = \mu(A))$, then

$$\nu\colon \mathscr{P}(A) \to \{0,1\}, \qquad \nu(B) = \mu(B)/\mu(A)$$

is a κ-additivity, non-singular, non-zero (equivalently: probability) measure. A measure as above is equivalent to the existence of a κ-complete non-principal ultrafilter U on A:

$$\nu(B) = 1 \Leftrightarrow B \in U.$$

By κ-additivity $|A| = \kappa$, so by copying everything on κ we have a κ-complete non-principal ultrafilter on κ.

Definition 40.1. A cardinal $\kappa > \omega$ is **measurable** if there is a κ-complete non-principal ultrafilter on κ.

Theorem 40.2. *Every measurable cardinal is inaccessible.*

Proof. Let κ be measurable and let U be a κ-complete non-principal ultrafilter on $\mathscr{P}(\kappa)$. We know that κ is regular, so it is enough to prove that $2^\lambda < \kappa$ for $\lambda < \kappa$. Towards a contradiction suppose $\kappa \to {}^\lambda 2$, $\xi \mapsto f_\xi$ is injective and $\lambda < \kappa$. For each $\alpha < \lambda$ the sets $Y_{\alpha,0}, Y_{\alpha,1}$ partition ${}^\lambda 2$, where $Y_{\alpha,i} = \{f \in {}^\lambda 2 \mid f(\alpha) = i\}$. As $\{\xi < \kappa \mid f_\xi(\alpha) = 0\}, \{\xi < \kappa \mid f_\xi(\alpha) = 1\}$ partition κ let $i_\alpha \in \{0,1\}$ be such that $X_\alpha = \{\xi < \kappa \mid f_\xi(\alpha) = i_\alpha\} \in U$. By κ-completeness $X = \bigcap_{\alpha<\lambda} X_\alpha \in U$, but $\xi \in X \Rightarrow f_\xi = \langle i_\alpha \mid \alpha < \lambda\rangle$, that is X is a singleton, against the assumption that U is non-principal. □

Summarizing, if κ be a real-valued measurable cardinal and $\mu\colon \mathscr{P}(\kappa) \to [0;1]$ is a non-singular, non-zero measure, then

- either $\kappa \leq 2^{\aleph_0}$ and μ is atomless,
- or else κ is measurable and μ has atoms.

40.A. Measurable cardinals and elementary embeddings. Suppose U is a non-principal ultrafilter on some set $I \neq \emptyset$. We have seen how to construct the ultrapower $\mathcal{M}^I/U$ of any $\mathcal{L}$-structure $\mathcal{M}$. We would like to recast the construction when the *set* $\mathcal{M}$ is replaced by the *class* V and the language $\mathcal{L}_\in$.

Consider the two relations on the proper class V^I

$$f =_U g \Leftrightarrow \{i \in I \mid f(i) = g(i)\} \in U$$
$$f \in_U g \Leftrightarrow \{i \in I \mid f(i) \in g(i)\} \in U.$$

The former is an equivalence relation and its equivalence classes are proper classes, so we resort to Scott's trick seen in Section 20.C and set

$$[\![f]\!]_U = \left\{g \in {}^I\mathrm{V} \mid f =_U g \wedge \operatorname{rank}(g) \text{ minimal}\right\}.$$

The **ultrapower of** V **modulo** U is $\left\langle \mathrm{V}^I/U, \tilde{\in}\right\rangle$, where

$$\mathrm{V}^I/U = \left\{[\![f]\!] \mid f \in \mathrm{V}^I\right\}, \quad \text{and} \quad [\![f]\!] \mathrel{\tilde{\in}} [\![g]\!] \Leftrightarrow f \in_U g.$$

Recall that Łos' Theorem 31.23 for *set-sized* structures—the very same result holds for *class-sized* structures and in particular for the ultrapower of V modulo U, but of course we must state and prove this using relativization rather than satisfaction. If $\varphi(x_1, \dots, x_n)$ is any $\mathcal{L}_\in$-formula and $[\![f_1]\!], \dots, [\![f_n]\!] \in \mathrm{V}^I/U$, then

$$\varphi([\![f_1]\!], \dots, [\![f_n]\!])^{(\mathrm{V}^I/U)} \Leftrightarrow \{i \in I \mid \varphi(f_1(i), \dots, f_n(i))\} \in U$$

where $\varphi([\![f_1]\!], \dots, [\![f_n]\!])^{(\mathrm{V}^I/U)}$ is the relativization of φ to $\left\langle \mathrm{V}^I/U, \tilde{\in}\right\rangle$. Then

$$\forall x_1, \dots, x_n \left(\varphi(x_1, \dots, x_n) \Leftrightarrow \varphi(j(x_1), \dots, j(x_n))^{(\mathrm{V}^I/U)}\right)$$

where $j(x)$ is $[\![\mathbf{c}_x]\!]$ and $\mathbf{c}_x \colon I \to \{x\}$.

Informally speaking, the formula above says that the class-function j is an elementary embedding $j \colon \langle \mathrm{V}, \in\rangle \to \left\langle \mathrm{V}^I/U, \tilde{\in}\right\rangle$. But the notion of *elementarity* was officially defined for the relation $\vDash$, and deals with all infinitely many formulæ in one sweeping stroke. On the other hand, since proper classes are not officially admitted and $\vDash$ is replaced by relativization, we must verify that j respects each φ, so it is not a single sentence, but rather a scheme of sentences. Despite all this the temptation of calling such j an elementary embedding is too strong, so exerting the due care we put forth the following definition-scheme.

Definition 40.3. Let $\langle M, E\rangle$ and $\langle M', E'\rangle$ be inner models of ZF. A class-function $j \colon M \to M'$ is **elementary** if

$$\forall x_1, \dots, x_n \in M \left(\varphi(x_1, \dots, x_n)^{(M)} \Leftrightarrow \varphi(j(x_1), \dots, j(x_n))^{(M')}\right)$$

for all φ. We say that j is **non-trivial** if $j \neq \mathrm{id}_M$, that is $j(x) \neq x$ for some $x \in M$.

Definition 40.4. Let $j \colon N \to M$ be a non-trivial elementary embedding of transitive inner models of ZF. The least ordinal κ such that $j(\kappa) \neq \kappa$ (if it exists) is called the **critical point** of j, denoted by $\operatorname{crit}(j)$.

As j is injective, if $\kappa = \operatorname{crit}(j)$ then $\kappa < j(\kappa)$.

Lemma 40.5. *Suppose $j\colon N \to M$ is an elementary embedding between transitive inner models of* ZF.

(a) *For all $\alpha, \beta \in \mathrm{Ord} \cap N$: $j(\alpha) \in \mathrm{Ord} \cap M$, $\alpha < \beta \Rightarrow j(\alpha) < j(\beta)$ and hence $\alpha \leq j(\alpha)$.*

(b) *If $(\mathrm{rank}(x) = \alpha)^{(N)}$ then $(\mathrm{rank}(j(x)) = j(\alpha))^{(M)}$.*

(c) *If $M \subseteq N$ and j is non-trivial, then $\mathrm{crit}(j)$ exists, and it is $\min\{\mathrm{rank}(x) \mid j(x) \neq x\}$.*

Proof. Part (a) follows from the fact that $\mathsf{Ord}(x)$ and $x \in y$ are Δ_0, while part (b) follows from the fact that the formula $\varphi(x, \alpha)$: "$\mathrm{rank}(x) = \alpha$" is Δ_1^{ZF} and hence absolute for inner models of ZF.

(c) Let $\kappa = \min\{\mathrm{rank}(x) \mid j(x) \neq x\}$. If $\alpha < \kappa$ then $\alpha = j(\alpha)$; we prove that $\kappa \neq j(\kappa)$ and hence $\kappa < j(\kappa)$. Pick x such that $j(x) \neq x$ and $\mathrm{rank}(x) = \kappa$. Then $y \in x \Rightarrow y = j(y) \in j(x)$, so $x \subset j(x)$. Let $y \in j(x) \setminus x$. If, towards a contradiction, $j(\kappa) = \kappa$, then $\mathrm{rank}(y) < \kappa$ and as $y \in M \subseteq N$ then $j(y) = y$. Therefore $y = j(y) \in j(x)$ and hence $y \in x$: a contradiction. □

Proposition 40.6. *If U is ω_1-complete on a set I, then $\tilde{\in}$ is well-founded and left-narrow on V^I/U.*

Proof. Suppose $\tilde{\in}$ is ill-founded, so by DC there is an infinite descending chain $\ldots \tilde{\in} [\![f_2]\!] \tilde{\in} [\![f_1]\!] \tilde{\in} [\![f_0]\!]$. Fix representatives in ${}^I\mathrm{V}$ so that $\cdots \in_U f_2 \in_U f_1 \in_U f_0$. Then $A_n = \{i \in I \mid f_{n+1}(i) \in f_n(i)\} \in U$ and hence $A = \bigcap_n A_n \in U$. As U is proper, $A \neq \emptyset$ so if $i \in A$ we have that $f_{n+1}(i) \in f_n(i)$, a contradiction.

Next we prove left-narrowness. Fix $f\colon I \to \mathrm{V}$. We must show that $\{[\![g]\!] \mid [\![g]\!] \tilde{\in} [\![f]\!]\}$ is a set. If $\{i \in I \mid f(i) = \emptyset\} \in U$ then $X = \emptyset$, so we may assume that $\forall i \in I\, (f(i) \neq \emptyset)$. Let $\nu = \mathrm{rank}(f)$. If $[\![g]\!] \tilde{\in} [\![f]\!]$ then we may choose the representative so that $\forall i \in I\, (g(i) \in f(i))$. Therefore $X \subseteq \{[\![g]\!] \mid g \in {}^I\mathrm{V}_\nu\}$, which is a set. □

If U is ω_1-complete, the structure $\langle \mathrm{V}^I/U, \tilde{\in} \rangle$ is well-founded, left-narrow and extensional, so it is isomorphic to a unique transitive class $\mathrm{Ult}(\mathrm{V}, U)$ via a unique isomorphism $\boldsymbol{\pi}$, the Mostowski collapse. Then

$$i_U\colon \mathrm{V} \to \mathrm{Ult}(\mathrm{V}, U), \qquad i_U(x) = \boldsymbol{\pi}([\![\mathbf{c}_x]\!])$$

is an elementary embedding.

Lemma 40.7. *Suppose κ is a measurable cardinal and U is a κ-complete non-principal ultrafilter on κ.*

(a) $\boldsymbol{\pi}([\![f]\!]) \in \mathrm{Ord} \Leftrightarrow \{\xi \in \kappa \mid f(\xi) \in \mathrm{Ord}\} \in U$.

(b) *If $\beta \in i_U(\alpha)$ then there is $f\colon \kappa \to \alpha$ such that $\beta = \boldsymbol{\pi}([\![f]\!])$.*

(c) *If $\alpha < \kappa$ then $i_U(\alpha) = \alpha$.*

(d) $\mathrm{crit}(i_U) = \kappa$ *and* $i_U(\kappa) < (2^\kappa)^+$.

(e) $\forall \alpha\, (i_U(\mathrm{V}_\alpha) = \mathrm{V}_{i_U(\alpha)})^{\mathrm{Ult}(\mathrm{V},U)}$, *and if* $\alpha < \kappa$ *then* $i_U(\mathrm{V}_\alpha) = \mathrm{V}_\alpha$.

(f) ${}^\kappa\mathrm{Ult}(\mathrm{V},U) \subseteq \mathrm{Ult}(\mathrm{V},U)$ *and* $\mathrm{V}_{\kappa+1} \subseteq \mathrm{Ult}(\mathrm{V},U)$.

(g) $U \notin \mathrm{Ult}(\mathrm{V},U)$ *and* $\mathrm{V}_{\kappa+2} \nsubseteq \mathrm{Ult}(\mathrm{V},U)$.

Proof. (a) follows from Łos theorem applied to the formula $\mathsf{Ord}(x)$.

(b) If $\beta \in i_U(\alpha)$ then $\beta = \boldsymbol{\pi}([\![g]\!])$ with $g \in_U \mathbf{c}_\alpha$, that is $A = \{\xi \in \kappa \mid g(\xi) \in \alpha\} \in U$. Then $f\colon \kappa \to \alpha$

$$f(\xi) = \begin{cases} g(\xi) & \text{if } \xi \in A, \\ 0 & \text{otherwise,} \end{cases}$$

is as required.

(c) If $\nu \in i_U(\alpha)$ then pick $f\colon \kappa \to \alpha$ such that $\nu = \boldsymbol{\pi}([\![f]\!])$. The sets $A_\beta = \{\xi \in \kappa \mid f(\xi) = \beta\}$ are pairwise disjoint, and $\bigcup_{\beta<\alpha} A_\beta = \kappa$, so by κ-completeness there is a unique $\beta < \alpha$ such that $A_\beta \in U$, and hence $\boldsymbol{\pi}([\![f]\!]) = i_U(\beta)$. Therefore $i_U(\alpha) = \{i_U(\beta) \mid \beta < \alpha\}$ and hence $i_U(\alpha) = \alpha$.

(d) Let $d\colon \kappa \to \kappa$ be the identity function. For each $\alpha < \kappa$ the set $\{\xi \in \kappa \mid \alpha < \xi\} = \{\xi \in \kappa \mid \mathbf{c}_\alpha(\xi) < d(\xi)\} \in U$, and since $\forall \xi < \kappa\, (d(\xi) < \mathbf{c}_\kappa(\xi))$ we have that

$$\alpha = i_U(\alpha) < \boldsymbol{\pi}([\![d]\!]) < i_U(\kappa).$$

Therefore $\kappa \leq \boldsymbol{\pi}([\![d]\!]) < i_U(\kappa)$.

If $\alpha < i_U(\kappa)$ then there is $f\colon \kappa \to \kappa$ such that $\boldsymbol{\pi}([\![f]\!]) = \alpha$, and hence $|i_U(\kappa)| \leq 2^\kappa$.

(e) By elementarity of i_U we have that $\varphi(x,\alpha) \Leftrightarrow \varphi(i_U(x), i_U(\alpha))^{(\mathrm{Ult}(\mathrm{V},U))}$ where $\varphi(x,\alpha)$ is $x = \mathrm{V}_\alpha$. Therefore $i_U(\mathrm{V}_\alpha) = \mathrm{V}_{i_U(\alpha)}^{(\mathrm{Ult}(\mathrm{V},U))}$ for all α. As $\kappa = \mathrm{crit}(j)$ then j is the identity on V_κ, so $j(\mathrm{V}_\alpha) = \mathrm{V}_\alpha$ for all $\alpha < \kappa$.

(f) Given $x_\xi \in \mathrm{Ult}(\mathrm{V},U)$ for $\xi < \kappa$ we must find $h \in {}^\kappa\mathrm{V}$ such that $\boldsymbol{\pi}([\![h]\!]) = \langle x_\xi \mid \xi < \kappa \rangle$. Let $f_\xi \in {}^\kappa\mathrm{V}$ be such that $\boldsymbol{\pi}([\![f_\xi]\!]) = x_\xi$. Let $d\colon \kappa \to \kappa$ be such that $\boldsymbol{\pi}([\![d]\!]) = \kappa$. Let $h \in {}^\kappa\mathrm{V}$ be such that

$$h(\alpha)\colon d(\alpha) \to \mathrm{V}, \quad h(\alpha)(\xi) = f_\xi(\alpha).$$

For all $\alpha < \kappa$ we have that $\mathrm{Fn}(h(\alpha)) \wedge \mathrm{dom}(h(\alpha)) = d(\alpha)$, so that $\boldsymbol{\pi}([\![h]\!])$ is a function with domain $\kappa = \boldsymbol{\pi}([\![d]\!])$. Fix $\xi \in \kappa$. As $\boldsymbol{\pi}([\![\mathbf{c}_\xi]\!]) < \boldsymbol{\pi}([\![d]\!]) = \kappa$, the set $A = \{\alpha \in \kappa \mid \mathbf{c}_\xi(\alpha) < d(\alpha)\} \in U$. Then $\forall \alpha \in A\, \bigl(h(\alpha)(\mathbf{c}_\xi(\alpha)) = f_\xi(\alpha)\bigr)$, that is $\boldsymbol{\pi}([\![h]\!])(\xi) = \boldsymbol{\pi}([\![f_\xi]\!]) = x_\xi$, as required.

By part (e) $\mathrm{V}_\kappa \subseteq \mathrm{Ult}(\mathrm{V},U)$. Any non-empty $x \subseteq \mathrm{V}_\kappa$ is of the form $x = \{x_\xi \mid \xi \in \kappa\}$, so it belongs to $\mathrm{Ult}(\mathrm{V},U)$. Therefore $\mathrm{V}_{\kappa+1} = \mathrm{V}_{\kappa+1} \cap \mathrm{Ult}(\mathrm{V},U) \in \mathrm{Ult}(\mathrm{V},U)$.

(g) By part (f) ${}^{\kappa}\kappa \subseteq \mathrm{Ult}(\mathrm{V}, U)$. If $U \in \mathrm{Ult}(\mathrm{V}, U)$ then the map ${}^{\kappa}\kappa \ni f \mapsto \boldsymbol{\pi}(\llbracket f \rrbracket)$ would belong to $\mathrm{Ult}(\mathrm{V}, U)$, so $i_U(\kappa) \leq (2^{\kappa})^{+}$ in $\mathrm{Ult}(\mathrm{V}, U)$, against the fact that $i_U(\kappa)$ is measurable (and hence inaccessible) in $\mathrm{Ult}(\mathrm{V}, U)$. Therefore $U \notin \mathrm{Ult}(\mathrm{V}, U)$, and as $U \in \mathrm{V}_{\kappa \dotplus 2}$ this proves that $\mathrm{V}_{\kappa \dotplus 2} \nsubseteq \mathrm{Ult}(\mathrm{V}, U)$. □

Lemma 40.7 shows that $\mathrm{Ult}(\mathrm{V}, U)$ closely resembles V up to rank $\kappa \dotplus 1$, but it is completely different from that level up.

Theorem 40.8. *Suppose $j \colon \mathrm{V} \to M$ is a non-trivial elementary embedding with M a transitive class. Then* $\mathrm{crit}(j)$ *is a measurable cardinal.*

Proof. By Lemma 40.5 the critical point of j exists and set $\kappa = \mathrm{crit}(j)$. Then $\kappa > \omega$ since every ordinal $\leq \omega$ is definable without parameters, so it is not moved by j. Define $U \subseteq \mathscr{P}(\kappa)$ by

$$X \in U \Leftrightarrow \kappa \in j(X).$$

It is immediate to check that $\kappa \in U$, and that if $X \in U$ and $X \subseteq Y \subseteq \kappa$ then $Y \in U$.

Claim 40.8.1. *The family U is closed under intersections of length $< \kappa$, so that U is a κ-complete filter on κ.*

Proof of Claim. Fix $\gamma < \kappa$ and suppose $X_\alpha \in U$ for all $\alpha \in \gamma$. We must prove that $X = \bigcap_{\alpha < \gamma} X_\alpha \in U$ that is $\kappa \in j(X)$. Let $F \colon \gamma \to \mathscr{P}(\kappa)$ be defined as $F(\alpha) = X_\alpha$. Then $(j(F) \colon j(\gamma) \to \mathscr{P}(j(\kappa)))^{(M)}$, so by absoluteness $j(F) \colon \gamma \to M$ and

$$\forall \alpha < \gamma \, (j(F)(\alpha) = j(F)(j(\alpha)) = j(F(\alpha)) = j(X_\alpha) \subseteq j(\kappa)).$$

Then, since $j(\gamma) = \gamma$

$$j(X) = \textstyle\bigcap_{\alpha < j(\gamma)} j(F)(\alpha) = \bigcap_{\alpha < \gamma} j(X_\alpha)$$

and hence $\kappa \in j(X)$. □

For any $X \subseteq \kappa$, the sets X, $\kappa \setminus X$ partition κ so the sets $j(X)$, $j(\kappa \setminus X) = j(\kappa) \setminus j(X)$ partition $j(\kappa)$. Therefore $\kappa \in j(X) \Leftrightarrow \kappa \notin j(\kappa \setminus X)$. In other words, U is an ultrafilter. Finally, if U were principal, then $\{\alpha\} \in U$ for some $\alpha \in \kappa$. But then $\kappa \in j(\{\alpha\}) = \{j(\alpha)\} = \{\alpha\}$, a contradiction. □

Remark 40.9. The statement of Theorem 40.8 presents two issues: the first is the universal quantification over proper classes (M and j) and the second is the elementarity of the class-function j. Here is an explanation on how this result can be formulated in MK, NGB, and ZF. The universal quantifiers $\forall M \, \forall j$ are not an issue in MK or NGB, while ZF dictates that the result must be construed as a theorem-scheme: "Suppose $\varphi_M(y, \vec{z})$ and $\varphi_j(x, y, \vec{z})$ define a transitive class M and a class-function $j \colon \mathrm{V} \to M$ ...". The elementarity of j is a more delicate issue. Working in MK the satisfaction relation can be formalized also for classes, so the elementarity of j becomes

$$\forall \boldsymbol{\varphi} \in \mathrm{Fml}\, \forall a_1, \dots, a_n \, (\mathrm{V} \vDash \boldsymbol{\varphi}[a_1, \dots, a_n] \Rightarrow M \vDash \boldsymbol{\varphi}[j(a_1), \dots, j(a_n)]).$$

On the other hand this argument does not work in NGB or ZF, so the best approximation of the formula above would be an infinite list of sentences

$$(\sigma_\varphi) \qquad \forall x_1, \dots, x_n \, (\varphi(x_1, \dots, x_n) \Rightarrow \varphi(j(x_1), \dots, j(x_n))^{(M)}),$$

one for each $\varphi(x_1, \dots, x_n)$. Examining the proof of Theorem 40.8 we see that we need to require only *finitely many* σ_φ as hypotheses of the theorem.

Theorem 40.10. *If κ is measurable then $\{\nu < \kappa \mid \nu$ is inaccessible$\}$ has cardinality κ.*

Proof. Any subset of $\kappa \times \kappa$ belongs to $\mathrm{V}_{\kappa+1}$, so any function witnessing that ν is singular, or that $\nu \precsim \mathscr{P}(\lambda)$ belongs to $\mathrm{V}_{\kappa+1}$, for all $\lambda < \nu \leq \kappa$. Therefore for any $\nu \leq \kappa$

$$\nu \text{ is inaccessible} \Leftrightarrow (\nu \text{ is inaccessible})^{(\mathrm{Ult}(\mathrm{V},U))}$$

with U a non-principal κ-complete ultrafilter on κ. In particular, κ is inaccessible in $\mathrm{Ult}(\mathrm{V}, U)$. Let $f \in {}^\kappa\kappa$ be such that $\boldsymbol{\pi}([\![f]\!]) = \kappa$. By Łos $I = \{\xi < \kappa \mid f(\xi) \text{ is inaccessible}\} \in U$.

Claim 40.10.1. $\forall \xi \in I \, \exists \nu \in I \, (\xi < \nu \wedge f(\xi) < f(\nu))$.

Proof. Suppose otherwise, and let $\xi \in I$ such that $f(\nu) \leq f(\xi) < \kappa$ for all $\nu \in I \setminus \xi$. As $I \setminus \xi \in U$ then $\kappa = \boldsymbol{\pi}([\![f]\!]) \leq \boldsymbol{\pi}([\![\mathbf{c}_{f(\xi)}]\!]) = f(\xi) < \kappa$, a contradiction. □

As $I \in U$ then $|I| = \kappa$, and as κ is regular, there is $J \subseteq I$ of size κ such that f is increasing on J. Therefore $f``J \subseteq \{\nu < \kappa \mid \nu \text{ is inaccessible}\}$ and hence $|\{\nu < \kappa \mid \nu \text{ is inaccessible}\}| = \kappa$. □

Theorem 40.11. *If there is a measurable cardinal, then* $\mathrm{V} \neq \mathrm{L}$.

Proof. Suppose U is a κ-complete non-principal ultrafilter on κ, and let $i_U \colon \mathrm{V} \to \mathrm{Ult}(\mathrm{V}, U)$. As $\mathrm{Ult}(\mathrm{V}, U)$ is a transitive, proper class inner model of ZFC, then $\mathrm{L} \subseteq \mathrm{Ult}(\mathrm{V}, U) \subset \mathrm{V}$ by Lemma 40.7, so $\mathrm{V} \neq \mathrm{L}$. □

Theorem 40.11 can be improved to: if there is a measurable cardinal, then $\mathbb{R}^{\mathrm{L}}$ is countable.

It can be shown that a positive answer to Banach's Question 26.13 in Section 26.D is equiconsistent with the existence of measurable cardinals. To be more specific, the following theories are equiconsistent:

(1) ZFC + there is a measure μ extending the Lebesgue measure, with $\operatorname{dom} \mu = \mathscr{P}(\mathbb{R})$.

(2) ZFC + there is a real valued measurable cardinal.

(3) ZFC + there is a measurable cardinal.

41. Boolean valued models

For $\mathbf{B}$ a complete Boolean algebra define the class

$$\mathrm{V}^{(\mathbf{B})} = \bigcup_{\alpha \in \mathrm{Ord}} \mathrm{V}^{(\mathbf{B})}_{\alpha}$$

where $\langle \mathrm{V}^{(\mathbf{B})}_{\alpha} \mid \alpha \in \mathrm{Ord} \rangle$ is defined by recursion by

$$\begin{aligned} \mathrm{V}^{(\mathbf{B})}_{0} &= \emptyset \\ \mathrm{V}^{(\mathbf{B})}_{\alpha+1} &= \{ \underset{\sim}{u} \mid \exists d \subseteq \mathrm{V}^{(\mathbf{B})}_{\alpha} \, (\underset{\sim}{u} \colon d \to \mathbf{B}) \} \\ \mathrm{V}^{(\mathbf{B})}_{\lambda} &= \textstyle\bigcup_{\alpha < \lambda} \mathrm{V}^{(\mathbf{B})}_{\alpha} && \text{when } \lambda \text{ is limit.} \end{aligned}$$

Here, and in what follow, we agree to use letters underscored by a $\sim$ to denote elements of $\mathrm{V}^{(\mathbf{B})}$.

Next we construct two binary functions $M, E \colon \mathrm{V}^{(\mathbf{B})} \times \mathrm{V}^{(\mathbf{B})} \to \mathbf{B}$, one for Membership, the other for Equality. The values $M(\underset{\sim}{u}, \underset{\sim}{v})$ and $E(\underset{\sim}{u}, \underset{\sim}{v})$ should capture truth value of "$\underset{\sim}{u}$ belongs to $\underset{\sim}{v}$" and "$\underset{\sim}{u}$ is equal to $\underset{\sim}{v}$", and for this reason it is customary to write them as

$$[\![\underset{\sim}{u} \in \underset{\sim}{v}]\!] = M(\underset{\sim}{u}, \underset{\sim}{v}) \qquad [\![\underset{\sim}{u} = \underset{\sim}{v}]\!] = E(\underset{\sim}{u}, \underset{\sim}{v}).$$

Once M and E are given, we can define $[\![\varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!]$ for any formula $\varphi(x_1, \dots, x_n)$ and any choice of $\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n \in \mathrm{V}^{(\mathbf{B})}$ by letting

$$\begin{aligned} [\![\neg \varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] &= [\![\varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!]' \\ [\![\varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n) \vee \psi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] &= [\![\varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] \curlyvee [\![\psi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] \\ [\![\exists x_0 \varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] &= \sup \{ [\![\varphi(\underset{\sim}{u}_0, \underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] \mid \underset{\sim}{u}_0 \in \mathrm{V}^{(\mathbf{B})} \}. \end{aligned}$$

For the third clause note that $\{ [\![\varphi(\underset{\sim}{u}_0, \underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!] \mid \underset{\sim}{u}_0 \in \mathrm{V}^{(\mathbf{B})} \}$ is a subset of $\mathbf{B}$, so the supremum exists by completeness of the Boolean algebra. Note that we should really write $[\![\varphi(\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_n)]\!]_{\mathbf{B}}$, but we drop the subscript

To be added later

Indexes

Here are three indexes: **People**, **Concepts**, **Symbols**. In the first index you will find the list of the mathematicians quoted in the text (e.g.: Kurt Gödel), but no theorems or concepts named after them, which instead appear in the second index (e.g.: Theorem|Gödel's First Incompleteness —). The third Index is the list of all major symbols used in the text (for the more usual ones see the Preliminaries).

Concepts

Symbols

People

Bibliography

[AH76] K. Appel and W. Haken. Every planar map is four colorable. *Bull. Amer. Math. Soc.*, 82(5):711–712, 1976.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AMP90] R. Aharoni, E. C. Milner, and K. Prikry. Unfriendly partitions of a graph. *J. Combin. Theory Ser. B*, 50(1):1–10, 1990.

[Bai88] David H. Bailey. The computation of π to $29,360,000$ decimal digits using Borweins' quartically convergent algorithm. *Math. Comp.*, 50(181):283–296, 1988.

[Bel09] John L. Bell. *The axiom of choice*, volume 22 of *Studies in Logic (London)*. College Publications, London, 2009. Mathematical Logic and Foundations.

[Ber12] Clifford Bergman. *Universal algebra*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012. Fundamentals and selected topics.

[Bès01] Alexis Bès. A survey of arithmetical definability. *Bull. Belg. Math. Soc. Simon Stevin*, (suppl.):1–54, 2001. A tribute to Maurice Boffa.

[Bla77] Andreas Blass. A model without ultrafilters. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, 25(4):329–331, 1977.

[Bla79] Andreas Blass. Injectivity, projectivity, and the axiom of choice. *Trans. Amer. Math. Soc.*, 255:31–59, 1979.

[Bla84] Andreas Blass. Existence of bases implies the axiom of choice. In *Axiomatic set theory (Boulder, Colo., 1983)*, volume 31 of *Contemp. Math.*, pages 31–33. Amer. Math. Soc., Providence, RI, 1984.

[Bly05] T. S. Blyth. *Lattices and ordered algebraic structures*. Universitext. Springer-Verlag London, Ltd., London, 2005.

[Boo88] George Boolos. Alphabetical order. *Notre Dame J. Formal Logic*, 29(2):214–215, 1988.

[BPBE11] David Barker-Plummer, Jon Barwise, and John Etchemendy. *Language, Proof and Logic*. CSLI, 2011.

[BS70] K. F. Barth and W. J. Schneider. Entire functions mapping countable dense subsets of the reals onto each other monotonically. *J. London Math. Soc. (2)*, 2:620–626, 1970.

[BS81] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.

[Byr46] L. Byrne. Two brief formulations of Boolean algebra. *Bulletin (New Series) of the American Mathematical Society*, 52(4):269–272, 1946.

[CHR03] Patrick Cégielski, François Heroult, and Denis Richard. On the amplitude of intervals of natural numbers whose every element has a common prime divisor with at least an extremity. *Theoret. Comput. Sci.*, 303(1):53–62, 2003. Logic and complexity in computer science (Créteil, 2001).

[Cie97] Krzysztof Ciesielski. *Set theory for the working mathematician*, volume 39 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997.

[Con78] John B. Conway. *Functions of one complex variable*, volume 11 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1978.

[Coo93] Roger Cooke. Uniqueness of trigonometric series and descriptive set theory, 1870–1985. *Arch. Hist. Exact Sci.*, 45(4):281–334, 1993.

[Cra11] Marcel Crabbé. Cantor-Bernstein's Theorem in a Semiring. *The Mathematical Intelligencer*, 33(3):80, 2011.

[CW00] Neil Calkin and Herbert S. Wilf. Recounting the rationals. *Amer. Math. Monthly*, 107(4):360–363, 2000.

[Dav55] Anne C. Davis. A characterization of complete lattices. *Pacific J. Math.*, 5:311–319, 1955.

[Die05] Reinhard Diestel. *Graph theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 2005.

[Dow89] David L. Dowe. On the existence of sequences of co-prime pairs of integers. *J. Austral. Math. Soc. Ser. A*, 47(1):84–89, 1989.

[DP02] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, New York, second edition, 2002.

[End01] Herbert B. Enderton. *A mathematical introduction to logic*. Harcourt/Academic Press, Burlington, MA, second edition, 2001.

[Eng89] Ryszard Engelking. *General topology*, volume 6 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, second edition, 1989. Translated from the Polish by the author.

[Fef64] Solomon Feferman. *The number systems. Foundations of algebra and analysis*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1964.

[Fol99] Gerald B. Folland. *Real analysis*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1999. Modern techniques and their applications, A Wiley-Interscience Publication.

[Fre03] D. H. Fremlin. *Measure theory. Vol. 2*. Torres Fremlin, Colchester, 2003. Broad foundations, Corrected second printing of the 2001 original.

[Fre04a] D. H. Fremlin. *Measure theory. Vol. 1*. Torres Fremlin, Colchester, 2004. The irreducible minimum, Corrected third printing of the 2000 original.

[Fre04b] D. H. Fremlin. *Measure theory. Vol. 3*. Torres Fremlin, Colchester, 2004. Measure algebras, Corrected second printing of the 2002 original.

[Fre06] D. H. Fremlin. *Measure theory. Vol. 4.* Torres Fremlin, Colchester, 2006. Topological measure spaces. Part I, II, Corrected second printing of the 2003 original.

[Fre08] D. H. Fremlin. *Measure theory. Vol. 5.* Torres Fremlin, Colchester, 2008. Topological measure spaces. Part I, II, Corrected second printing of the 2003 original.

[FW91] Matthew Foreman and Friedrich Wehrung. The Hahn-Banach theorem implies the existence of a non-Lebesgue measurable set. *Fund. Math.*, 138(1):13–19, 1991.

[GH09] Steven Givant and Paul Halmos. *Introduction to Boolean algebras.* Undergraduate Texts in Mathematics. Springer, New York, 2009.

[Gol84] Robert Goldblatt. *Topoi*, volume 98 of *Studies in Logic and the Foundations of Mathematics.* North-Holland Publishing Co., Amsterdam, second edition, 1984. The categorial analysis of logic.

[Gol96] Dorian M. Goldfeld. Beyond the last theorem. *Math Horizons*, 1996.

[Goo91] K. R. Goodearl. *von Neumann regular rings.* Robert E. Krieger Publishing Co. Inc., Malabar, FL, second edition, 1991.

[Grä11] George Grätzer. *Lattice theory: foundation.* Birkhäuser/Springer Basel AG, Basel, 2011.

[GT02] Andrew Granville and Thomas J. Tucker. It's as easy as *abc*. *Notices Amer. Math. Soc.*, 49(10):1224–1231, 2002.

[Guy04] Richard K. Guy. *Unsolved problems in number theory.* Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[H0̈5] Lars Hörmander. *The analysis of linear partial differential operators. II.* Classics in Mathematics. Springer-Verlag, Berlin, 2005. Differential operators with constant coefficients, Reprint of the 1983 original.

[Hen60] Leon Henkin. On mathematical induction. *The American Mathematical Monthly*, 67:323–338, 1960.

[Her06] Horst Herrlich. *Axiom of choice*, volume 1876 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 2006.

[Hod79] Wilfrid Hodges. Krull implies Zorn. *J. London Math. Soc. (2)*, 19(2):285–287, 1979.

[HR98] Paul Howard and Jean E. Rubin. *Consequences of the axiom of choice*, volume 59 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 1998. With 1 IBM-PC floppy disk (3.5 inch; WD).

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[Huu94] Taneli Huuskonen. Constants are definable in rings of analytic functions. *Proc. Amer. Math. Soc.*, 122(3):697–702, 1994.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1990.

[Jac85] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[Jec73] Thomas J. Jech. *The axiom of choice.* North-Holland Publishing Co., Amsterdam, 1973. Studies in Logic and the Foundations of Mathematics, Vol. 75.

[Jec03] Thomas Jech. *Set theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded.

[Joh84] P. T. Johnstone. Almost maximal ideals. *Fund. Math.*, 123(3):197–209, 1984.

[Kap95] Irving Kaplansky. *Fields and rings.* Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1995. Reprint of the second (1972) edition.

[Kec95] Alexander S. Kechris. *Classical Descriptive Set Theory.* Number 156 in Graduate Texts in Mathematics. Springer-Verlag, Heidelberg, New York, 1995.

[Kel55] John L. Kelley. *General Topology.* D. van Nostrand, 1955.

[Koe16] Jochen Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Ann. of Math. (2)*, 183(1):73–93, 2016.

[Kop89] Sabine Koppelberg. *Handbook of Boolean algebras. Vol. 1.* North-Holland Publishing Co., Amsterdam, 1989. Edited by J. Donald Monk and Robert Bonnet.

[Kun83] Kenneth Kunen. *Set theory*, volume 102 of *Studies in Logic and the Foundations of Mathematics.* North-Holland Publishing Co., Amsterdam, 1983. An introduction to independence proofs, Reprint of the 1980 original.

[Lev02] Azriel Levy. *Basic set theory.* Dover Publications Inc., Mineola, NY, 2002. Reprint of the 1979 Springer edition.

[LR84] D. H. Luecking and L. A. Rubel. *Complex analysis.* Universitext. Springer-Verlag, New York, 1984. A functional analysis approach.

[Man03] Zohar Manna. *Mathematical theory of computation.* Dover Publications Inc., Mineola, NY, 2003. Reprint of the 1974 original [McGraw-Hill, New York; MR0400771].

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002. An introduction.

[Maz02] Stefano Mazzanti. Plain bases for classes of primitive recursive functions. *MLQ Math. Log. Q.*, 48(1):93–104, 2002.

[MB89a] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 2.* North-Holland Publishing Co., Amsterdam, 1989.

[MB89b] J. Donald Monk and Robert Bonnet, editors. *Handbook of Boolean algebras. Vol. 3.* North-Holland Publishing Co., Amsterdam, 1989.

[Men70] Elliott Mendelson. *Theory and problems of Boolean algebra and switching circuits.* McGraw-Hill Book Co., New York, 1970. Schaum's Outline Series.

[Men15] Elliott Mendelson. *Introduction to mathematical logic.* Textbooks in Mathematics. CRC Press, Boca Raton, FL, sixth edition, 2015.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1998.

[Mon69] J. Donald Monk. *Introduction to set theory.* McGraw-Hill Book Co., New York, 1969.

[Mon76] J. Donald Monk. *Mathematical logic.* Springer-Verlag, New York-Heidelberg, 1976. Graduate Texts in Mathematics, No. 37.

[Mor65] Anthony P. Morse. *A theory of sets.* Pure and Applied Mathematics, Vol. XVIII. Academic Press, New York, 1965.

[MS96] W. McCune and A. D. Sands. Computer and human reasoning: single implicative axioms for groups and for abelian groups. *Amer. Math. Monthly*, 103(10):888–892, 1996.

[MVF$^+$02] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos. Short single axioms for Boolean algebra. *Journal of Automated Reasoning*, 29(1):1–16, 2002.

[MW96] Angus Macintyre and A. J. Wilkie. On the decidability of the real exponential field. In *Kreiseliana*, pages 441–467. A K Peters, Wellesley, MA, 1996.

[OtR85] A. M. Odlyzko and H. J. J. te Riele. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, 357:138–160, 1985.

[Oxt80] John C. Oxtoby. *Measure and category*, volume 2 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. A survey of the analogies between topological and measure spaces.

[Paw91] Janusz Pawlikowski. The Hahn-Banach theorem implies the Banach-Tarski paradox. *Fund. Math.*, 138(1):21–22, 1991.

[PD11] Alexander Prestel and Charles N. Delzell. *Mathematical Logic and Model Theory*. Springer, 2011.

[PR08] R. Padmanabhan and S. Rudeanu. *Axioms for lattices and Boolean algebras*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008.

[Rav77] Yehuda Rav. Variants of Rado's selection lemma and their applications. *Math. Nachr.*, 79:145–165, 1977.

[Ric85] Denis Richard. Answer to a problem raised by J. Robinson: the arithmetic of positive or negative integers is definable from successor and divisibility ["Definability and decision problems in arithmetic", J. Symbolic Logic **14** (1949), 98–114; MR **11**, 151]. *J. Symbolic Logic*, 50(4):927–935 (1986), 1985.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.

[Rob51] Raphael M. Robinson. Undecidable rings. *Trans. Amer. Math. Soc.*, 70:137–159, 1951.

[Ros03] Haskell P. Rosenthal. The Banach spaces $C(K)$. In *Handbook of the geometry of Banach spaces, Vol. 2*, pages 1547–1602. North-Holland, Amsterdam, 2003.

[RR85] Herman Rubin and Jean E. Rubin. *Equivalents of the axiom of choice. II*, volume 116 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1985.

[Rud91] Walter Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill Inc., New York, second edition, 1991.

[Sag75] Gershon Sageev. An independence result concerning the axiom of choice. *Ann. Math. Logic*, 8:1–184, 1975.

[Sch97] Eric Schechter. *Handbook of analysis and its foundations*. Academic Press Inc., San Diego, CA, 1997.

[Sha03] Igor R. Shafarevich. *Discourses on Algebra*. Springer-Verlag New York Inc., 2003.

[Smo91] Craig Smoryński. *Logical number theory. I*. Universitext. Springer-Verlag, Berlin, 1991. An introduction.

[SR74] Daihachiro Sato and Stuart Rankin. Entire functions mapping countable dense subsets of the reals onto each other monotonically. *Bull. Austral. Math. Soc.*, 10:67–70, 1974.

[Ste66] A. K. Steiner. The lattice of topologies: Structure and complementation. *Trans. Amer. Math. Soc.*, 122:379–398, 1966.

[Tar55] Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific J. Math.*, 5:285–309, 1955.

[Tar68] Alfred Tarski. *Undecidable theories.* In collaboration with Andrzej Mostowski and Raphael M. Robinson. Second printing. Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Co., Amsterdam, 1968.

[Thu82] William P. Thurston. Three-dimensional manifolds, Kleinian groups and hyperbolic geometry. *Bull. Amer. Math. Soc. (N.S.)*, 6(3):357–381, 1982.

[TW16] Grzegorz Tomkowicz and Stan Wagon. *The Banach-Tarski paradox*, volume 163 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, New York, second edition, 2016. With a foreword by Jan Mycielski.

[vdD98] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998.

[Wil96] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.*, 9(4):1051–1094, 1996.

[Woo] Kevin Woods. Presburger arithmetic, rational generating functions, and quasi-polynomials.

[Woo81] Alan Robert Woods. *Some problems in logic and number theory, and their connections*. PhD thesis, Manchester University, 1981.