Il Sistema Assiomatico di Zermelo e Fraenkel

In questo primo capitolo presentiamo il sistema assiomatico di Zermelo–Fraenkel, su cui è basata tutta la matematica moderna. Nel primo paragrafo enunceremo gli assiomi, con qualche commento sul loro significato, e nel secondo discuteremo più in dettaglio l'assioma della scelta e alcune sue importanti conseguenze, come il lemma di Zorn, il principio del buon ordinamento e l'induzione transfinita.

Una discussione completa sul significato degli assiomi in matematica, e in particolare degli assiomi della teoria degli insiemi, si trova in [**Ma**]. Un'altra fonte utile è [**An**], dove si trovano sviluppati in dettaglio molti degli argomenti che qui sono solo accennati.

1. Gli assiomi

Nell'enunciare gli assiomi useremo un linguaggio non completamente formale. Sviluppare in modo strettamente formale l'assiomatica della teoria degli insiemi richiede un lavoro notevole, e per questo rimandiamo a un corso di Istituzioni di Logica Matematica. Scriveremo le formule, quando necessario, utilizzando gli usuali simboli logici. Il sistema assiomatico che descriveremo ha 10 assiomi. L'ultimo di questi è l'assioma della scelta, e ha una posizione un po' particolare rispetto agli altri. Di solito il sistema formato dai primi nove viene detto ZF, e quello con tutti e dieci ZFC (e cioè $\mathsf{ZF} + \mathsf{C}$, dove C = choice, scelta in inglese)

Nella teoria degli insiemi vi è un solo tipo di oggetto primitivo, l'*insieme* e una sola relazione fra insiemi, l'*appartenenza.* Per dire che un insieme appartiene ad un altro si scrive

$$x \in y$$

che si legge "x appartiene ad y" oppure "x è un elemento di y". Di solito, siamo abituati a distinguere fra "insiemi" ed "elementi", ma in effetti basta un solo concetto primitivo. Il primo assioma dice che un insieme è determinato unicamente dalla collezione dei suoi elementi e non da altre informazioni, come per esempio l'ordine dei suoi elementi.

ZF 1. Assioma dell'estensione. *Due insiemi x e y sono uguali se e solo se ogni elemento dell'insieme x è un elemento dell'insieme y e ogni elemento dell'insieme y è un elemento dell'insieme x.*

In simboli

$$\forall x \forall y \quad x = y \iff [\forall z \quad z \in x \iff z \in y] \tag{1}$$

Se ogni elemento di x è un elemento di y scriviamo $x \subseteq y$ e leggiamo "x è un sottoinsieme di y".

ZF 2. Assioma dell'insieme vuoto. *Esiste un insieme che non contiene elementi.*

In simboli

$$\exists z \, \forall x \quad x \notin z \tag{2}$$

Dall'assioma di estensione segue che l'insieme vuoto è unico, e si indica con il simbolo $\emptyset$. Osserviamo anche che $\emptyset \subseteq x$ per ogni insieme x.

Tutti i rimanenti assiomi garantiscono l'esistenza di insiemi aventi opportune proprietà o risultanti da appropriate costruzioni.

ZF 3. Assioma della coppia. *Per ogni due insiemi x e y esiste un insieme z i cui elementi sono solo x e y.*

In simboli

$$\forall x \forall y \, \exists z : \quad \forall w \; w \in z \iff [w = x \vee w = y] \tag{3}$$

Questo insieme si denota con $z = \{x, y\}$. Osserviamo che x e y non sono necessariamente distinti, e si ha allora $z = \{x, x\} = \{x\}$. Dunque, dato un insieme x, l'assioma della coppia afferma, in particolare, l'esistenza di un insieme $\{x\}$ che ha come unico elemento x. È importante ricordarsi che $x \neq \{x\}$. In particolare, $x \in \{x\}$, ma dimostreremo che $x \notin x$. In effetti, uno degli scopi dell'assiomatica di Zermelo–Fraenkel è di escludere l'affermazione $x \in x$, poiché da questa si possino derivare delle contraddizioni (paradosso di Russell).

A partire dall'esistenza della coppia, si può definire la *coppia ordinata* di due insiemi $\langle x, y \rangle$ ponendo, per definizione

$$\langle x, y \rangle = \{x, \{x, y\}\}.$$

Lo scopo di questa definizione è avere

$$\langle x, y \rangle = \langle u, v \rangle \iff x = u \wedge y = v,$$

cosa che si verifica facilmente usando gli assiomi che abbiamo già. La nozione di coppia ordinata sarà utile per definire le corrispondenze fra insiemi e le funzioni.

ZF 4. Assioma dell'unione. *Per ogni insieme x esiste un insieme y tale che l'insieme z è un elemento di y se e solo se z è elemento di un elemento di x.*

In simboli

$$\forall x \, \exists y : \quad \forall z \; z \in y \iff [\exists w : z \in w \wedge w \in x] \tag{4}$$

L'insieme y è l'unione di tutti gli elementi di tutti gli elementi di x, e si scrive

$$y = \bigcup x.$$

La notazione non è quella che siamo abituati ad usare: per esempio, $\bigcup\{x_1, x_2\}$ di solito si scrive $x_1 \bigcup x_2$, l'unione $\bigcup\{x_1, x_2, \dots, x_n\}$ di solito si scrive $\bigcup_{i=1}^{n} x_i$, e così via.

ZF 5. Assioma dell'insieme potenza. *Per ogni insieme x esiste un insieme y tale che gli elementi di y siano tutti e soli i sottoinsiemi di x.*

In simboli

$$\forall x\, \exists y : \quad \forall z\; z \in y \iff z \subseteq x \tag{5}$$

Naturalmente, y è l'insieme delle parti di x, (o *insieme potenza*, in inglese *power set*) e useremo la notazione $y = \mathcal{P}(x)$.

Quali insiemi possiamo costruire a partire dagli assiomi che abbiamo? L'assioma dell'insieme vuoto garantisce che c'è almeno un insieme, $\emptyset$, e usando l'assioma della coppia, dell'unione e dell'insieme potenza possiamo costruire la sequenza di insiemi:

$$\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\},\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$$

ottenuta "collezionando" via via gli insiemi già costruiti. Si vede subito che ogni insieme che si ottiene in questo modo ha un numero *finito* di elementi. Se vogliamo parlare di insiemi infiniti dobbiamo avere un assioma apposito. Definiamo la nozione di "seguente": se x è un insieme, l'insieme seguente è $x' = x \cup \{x\}$. Per esempio,

$$\emptyset' = \emptyset \cup \{\emptyset\} = \{\emptyset\}, \quad \emptyset'' = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$$

ZF 6. Assioma dell'infinito. *Esiste un insieme x che ha $\emptyset$ come elemento e per ogni $y \in x$ anche $y' \in x$.*

In simboli

$$\exists x : \quad \emptyset \in x \wedge [\forall y\; y \in x \implies y' \in x] \tag{6}$$

È immediato riconoscere in questo assioma la base del principio di induzione e la costruzione stessa dell'insieme dei numeri naturali. L'assioma dell'infinito afferma che i numeri naturali formano un insieme e si possono considerare come una "infinità conclusa", e cioè possono essere considerati tutti contemporaneamente, e non solo uno dopo l'altro.

Notiamo però che, per l'assioma dell'insieme potenza, esiste l'insieme delle parti di questo insieme infinito, e Cantor scoprì che questa nuova infinità è maggiore di quella iniziale, e così via. Dunque, l'esistenza di un solo insieme infinito implica l'esistenza di infiniti insiemi infiniti, tutti di cardinalità maggiore uno dell'altro.

Ora che abbiamo moltissimi insiemi, grandi quanto vogliamo, possiamo costruire altri insiemi come "sottoinsiemi" di insiemi già dati. Si tratta di stabilire se riusciamo a individuare solo alcuni fra i sottoinsiemi di un insieme, e non ottenerli tutti contemporaneamente come ci permette l'assioma dell'insieme potenza.

ZF 7. Assioma del sottoinsieme. *Per ogni insieme x e per ogni proprietà P di un insieme, esiste un insieme y tale che $z \in y$ se e solo se $z \in x$ e z gode della proprietà P.*

In simboli

$$\forall x\, \forall P\, \exists y : \quad \forall z\; z \in y \iff z \in x \wedge P(z) \tag{7}$$

Di solito si scrive $y = \{z \in x \mid P(z)\}$. Questo assioma viene anche chiamato *assioma di comprensione* o *assioma di separazione*.

Nella formulazione di questo assioma è evidente l'incertezza di significato dell'espressione "proprietà di insiemi". Formulare con precisione questo significato è molto difficile nel linguaggio naturale che stiamo usando; diciamo solo che una proprietà è espressa mediante una "frase" che contiene solo simboli per rappresentare insiemi e le parole (o i simboli corrispondenti) "non", "e", "oppure", "se ... allora ...", "per ogni", "esiste", "uguale", "essere elemento", loro sinonimi, e che è costruita "regolarmente". Proprio dire cosa è una frase costruita regolarmente è la difficoltà maggiore e necessita l'introduzione di un linguaggio formale e la nozione di correttezza sintattica. Rimandiamo a [**An**] per una trattazione più completa.

Piuttosto che tentare di definire con precisione "proprietà", vediamone almeno alcune, che corrispondono a costruzioni ben note. Se $P(u)$ è la proprietà $u \in v$, allora per ogni insieme x l'assioma del sottoinsieme garantisce l'esistenza dell'intersezione $y = x \cap v$. Se $P(u)$ è la proprietà $u \notin v$, allora si ha il complemento $y = x \setminus v$.

Osserviamo infine che l'assioma del sottoinsieme è in realtà uno "schema di assiomi", e cioè abbiamo un assioma per ogni proprietà P. Dunque ZF contiene infiniti assiomi e non solo 10, come avevamo affermato al'inizio della discussione. In virtù del teorema di incompletezza di Gödel (vedi, per esempio, [**NaNe**]), questo non è un difetto grave. Anche i due prossimi assiomi sono schemi di assiomi.

In matematica le funzioni hanno un ruolo importante, e il prossimo assioma dice, intuitivamente, che l'immagine di un insieme è un insieme. Per enunciare con precisione l'assioma, ricordiamo la definizione di *prodotto cartesiano* di insiemi e cioè l'insieme delle coppie ordinate il cui primo elemento appartiene a x e il secondo a y. Osserviamo che se $u \in x$ e $v \in y$, allora $\{u, v\} \in \mathcal{P}(x \cup y)$ e $\langle u, v\rangle = \{u, \{u, v\}\} \in \mathcal{P}(\mathcal{P}(x \cup y))$. Il prodotto cartesiano $x \times y$ è definito da

$$x \times y = \{z \in \mathcal{P}(\mathcal{P}(x \cup y)) \mid \exists u \in x \, \exists v \in y : z = \langle u, v\rangle\}$$

e dagli assiomi dell'insieme potenza e del sottoinsieme si ha che è un insieme. Ricordiamo che una *relazione binaria* fra gli insiemi x e y è un sottoinsieme di $x \times y$, e una *funzione* da x a y è una relazione binaria $f \subseteq x \times y$ tale che per ogni $u \in x$ esiste un unico $v \in y$ tale che $\langle u, v\rangle \in f$.

ZF 8. Assioma del rimpiazzamento. *Sia P una proprietà di coppie ordinate di insiemi tale che per tutti gli elementi x di un certo insieme u e per tutti gli insiemi y e z se le coppie $\langle x, y\rangle$ e $\langle x, z\rangle$ godono di P, allora $y = z$. Allora esiste un insieme v tale che $y \in v$ se e solo se esiste $x \in u$ tale che la coppia $\langle x, y\rangle$ gode della proprietà P*

In simboli

$$(8) \quad \forall u \, \forall P \quad [\forall x \in u \; \forall y \forall z \; P(\langle x, y\rangle) \wedge P(\langle x, z\rangle) \implies y = z] \implies \\ [\exists v \, \forall t \quad t \in v \iff \exists s \in u \; P(\langle s, t\rangle)]$$

Dopo aver letto con cura l'enunciato, capiamo che l'ipotesi è che P definisce una funzione sull'insieme u (in realtà, P può essere una proprietà un po' più generale di una funzione, ma ristretta a u definisce essenzialmente una funzione) e la conclusione garantita dall'assioma è che esiste un insieme v che è l'immagine della funzione.

L'assioma del sottoinsieme garantisce l'esistenza di un insieme per ogni proprietà, e cioè per ogni formula "sintatticamente corretta", ma solo come sottoinsieme di un insieme già dato. Ci si può chiedere se si possa ampliare questo assioma, e cioè se data una proprietà P si possa postulare l'esistenza di un insieme formato da tutti gli insiemi che soddisfano P. Questa era l'idea originale di Cantor e Frege (e cioè "insieme = proprietà"), ma il paradosso di Russell mise presto in evidenza che non è sufficiente che la frase che definisce P sia corretta grammaticalmente. Ci devono essere delle restrizioni semantiche, e cioè di significato. Il paradosso di Russell nasce dall'affermazione che

$$V = \{x \mid x \notin x\}$$

sia un insieme. Allora $V \in V \implies V \notin V$ e anche $V \notin V \implies V \in V$, una contraddizione. Una possibile soluzione a questo dilemma è impedire che $V \in V$ sia vero.

ZF 9. Assioma della fondazione. *Sia P una proprietà degli insiemi, e supponiamo che esista un insieme y che gode di P. Allora esiste un insieme x che gode di P e tale che ogni suo elemento non gode di P.*

In simboli

$$\forall P \quad [\exists y\, P(y)] \implies [\exists x\ P(x) \wedge \forall z\ P(z) \implies z \notin x] \tag{9}$$

Lemma 1.1. *Per ogni insieme x,*

$$x \notin x.$$

Dimostrazione. Sia $P(u)$ la proprietà $u \in u$. Se esiste un insieme y tale che $P(y)$, e cioè $y \in y$, per l'assioma della fondazione esiste un altro insieme x tale che

(i) $x \in x$,
(ii) $\forall z \in x, \quad z \notin z$

Dalla (i) $x \in x$, e quindi dalla (ii) si ha che $x \notin x$ e dunque una contraddizione. Dunque non può esistere nessun insieme y tale che $y \in y$ e questa è la tesi. □

Dunque

$$V = \{x \mid x \notin x\}$$

è la totalità di tutti gli insiemi dell'universo di Zermelo–Frankel, ma V non è un insieme, altrimenti dovrebbe essere $V \in V$, impossibile per gli insiemi di ZF. In questo modo si evita il paradosso di Russell. Nulla vieta che ci siano altri paradossi meno immediati e non ancora scoperti, ma per ora (in poco più di cento anni) non ne sono stati trovati.

L'ultimo assioma è il celebre assioma della scelta:

ZF 10. Assioma della scelta. *Per ogni insieme x non vuoto esiste una funzione f che ad ogni sottoinsieme non vuoto di x assegna un suo elemento.*

In simboli

$$\forall x \quad [x \neq \emptyset] \implies \exists f : \mathcal{P}(x) \setminus \emptyset \to x \ \wedge\ [\forall y\ y \subseteq x \wedge y \neq \emptyset \implies f(y) \in y] \tag{10}$$

L'assioma della scelta viene spesso abbreviato AC (Axiom of Choice), specialmente nei libri in inglese.

AC afferma la possibilità di scegliere un elemento da ogni sottoinsieme di un insieme dato, e di poter fare tutte queste scelte simultaneamente. È evidente che se l'insieme x è finito, non c'è bisogno dell'assioma della scelta per l'esistenza della funzione f. Dunque AC è un'affermazione vera nel caso finito che vogliamo valga anche nel caso infinito. È appena il caso di notare che vi sono molte dimostrazioni matematiche che richiedono questo assioma, e molte di queste erano considerate valide anche prima che Zermelo usasse questa forma nella sua famosa dimostrazione del principio del buon ordinamento nel 1904. Nel prossimo paragrafo vedremo alcune conseguenze di questo assioma, di uso corrente nelle dimostrazioni matematiche.

Gödel, nel 1940, ha dimostrato che AC è *consistente* con gli altri assiomi usuali della teoria degli insiemi, nella formulazione di Zermelo–Fraenkel, e cioè non si può dimostrare la negazione di AC in ZF. Paul Cohen, nel 1963 ha dimostrato che AC è *indipendente* dagli altri assiomi, e cioè non può essere dimostrato in ZF.

Dunque accettare o meno AC è una questione di scelta (il gioco di parole è voluto). La matematica contemporanea ha accettato AC e lo considera un assioma indispensabile. Vi è una corrente in Matematica, detta Costruttivismo, che non accetta AC e considera corrette solo dimostrazioni di esistenza in cui sia possibile "costruire" esplicitamente l'oggetto di cui si afferma l'esistenza. Molti teoremi della matematica contemporanea (e anche della matematica dell'Ottocento) sono fuori dalla portata dei metodi costruttivi, per esempio il teorema di Weierstrass sull'esistenza di massimi e minini di funzioni continue.

Per una interessante discussione sull'assioma della scelta, condotta da Emil Borel, Henri Lebesgue, Jacques Hadamard e Robert Baire nel 1905, vedere [**Lettres**]. Proprio la controversia che si sviluppò sulla dimostrazione di Zermelo del principio del buon ordinamento portò quest'ultimo alle ricerche sui fondamenti della teoria degli insiemi che culminarono nella formulazione del sistema assiomatico che abbiamo appena descritto.

2. Conseguenze dell'assioma della scelta

Vedremo, in questo paragrafo, alcuni enunciati equivalenti all'assioma della scelta in ZF. Questo vuol dire che, assumendo solo gli assiomi ZF 1–9 si può dimostrare che AC vale se e solo se vale uno di questi enunciati. Dunque accettare AC o uno di questi come assioma è logicamente equivalente, ma può essere psicologicamente differente. E in effetti, forse è proprio AC ad essere il più intuitivamente "vero".

Non riporteremo le dimostrazioni. In [**An**] e in [**Dev**] Capitolo II.9 le dimostrazioni di equivalenza sono basate sulla teoria dei numeri ordinali, mentre in [**vdW**], Volume I, Capitolo 9 vi sono delle dimostrazioni dirette dei teoremi seguenti sulla base di AC.

Molte delle riformulazioni dell'assioma della scelta riguardano gli insiemi ordinati, e abbiamo perciò bisogno di ricordare alcune definizioni. Sia X un insieme.

Definizione 2.1. Una relazione $\leq$ su X si dice un *ordine* se è riflessiva, antisimmetrica e transitiva, e cioè

(1) $a \leq a$ per ogni $a \in X$;
(2) $a \leq b$ e $b \leq a \implies a = b$;
(3) $a \leq b$ e $b \leq c \implies a \leq c$.

Se per ogni coppia di elementi $a, b \in X$ vale una delle $a \leq b$ oppure $b \leq a$, allora l'ordine è detto *totale* e X è detto *linearmente ordinato* (o *totalmente ordinato*), altrimenti l'ordine è detto *parziale*. La relazione $a \leq b$ si legge *a precede b* oppure *a è minore o uguale a b*. C'è anche un simbolo di "minore stretto" con il significato solito, e cioè $a < b$ se e solo se $a \leq b$ e $a \neq b$.

Esempi ben noti sono l'ordinamento dei numeri naturali, interi, razionali e reali. Questi ordini sono totali. Un esempio di ordinamento parziale è quello dato dall'inclusione fra i sottoinsiemi di un insieme Z definito da $A \leq B$ se e solo se $A \subseteq B$.

Se X è ordinato, un elemento $a \in X$ si dice *minimo* se per ogni $b \in X$, $a \leq b$, e analogamente per il *massimo*. È chiaro che il minimo (massimo) se esiste, è unico.

Definizione 2.2. Un insieme X si dice *bene ordinato* se ogni sottoinsieme di X ha un minimo.

Per esempio $\mathbb{N}$, con l'ordinamento solito, è bene ordinato. $\mathbb{Z}$ non è bene ordinato, ma può essere bene ordinato da un altro ordinamento, per esempio

$$0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3, \ldots$$

oppure

$$1,\ 2,\ 3, \ldots;\quad 0,\ -1,\ -2,\ -3, \ldots$$

in cui ogni positivo precede tutti i negativi.

L'insieme dei razionali $\mathbb{Q}$ non è bene ordinato dall'ordinamento solito, ma poiché è numerabile può essere bene ordinato usando una corrispondenza biunivoca con $\mathbb{N}$ e trasportando l'ordine. Dunque tutti gli insiemi numerabili possono essere bene ordinati (e anche quelli finiti, naturalmente).

L'insieme $\mathbb{R}$ dei numeri reali non è bene ordinato dall'ordinamento solito, e non è nemmeno numerabile. Esiste su $\mathbb{R}$ un buon ordinamento? La risposta non è ovvia, e costruire esplicitamente un buon ordinamento risulta a prima vista molto difficile.

Principio del Buon Ordinamento. *Ogni insieme X può essere bene ordinato.*

Fu proprio nel dimostrare questo teorema che Zermelo usò in modo esplicito AC (che non era ancora un assioma), dando così inizio alla discussione sulla sua verità o necessità di essere accettato. A questo proposito, i commenti di Lebesgue nella terza lettera in [**Lettres**] sono ancora oggi molto interessanti.

Definizione 2.3. Sia M un sottoinsieme di un insieme parzialmente ordinato X. Se per ogni $x \in M$ si ha $x \leq s$, allora s si dice un *maggiorante* di M. Se esiste un maggiorante m di M tale che $m \leq s$ per ogni maggiorante s di M, allora m è unico, e viene detto *estremo superiore* di M.

L'enunciato originale del lemma di Zorn riguarda l'ordinamento dei sottoinsiemi di un insieme. Sia dunque X un insieme e ordiniamo (parzialmente) l'insieme delle parti $\mathcal{P}(X)$ con l'inclusione. Un sottoinsieme C di $\mathcal{P}(X)$ totalmente ordinato si dice una *catena*. Un sottoinsieme A di $\mathcal{P}(X)$ si dice *chiuso* se per ogni catena, contiene anche l'unione della catena. Un elemento di A si dice *massimale* se non è contenuto in nessun altro elemento di A. Possiamo definire questi concetti per qualunque ordine: se M è un qualunque insieme parzialmente ordinato, un sottoinsieme è una *catena* se è totalmente ordinato, è *chiuso* se con ogni catena contiene anche l'estremo superiore della catena e un elemento $x \in M$ è *massimale* se per ogni $y \in M$, $x \leq y \implies x = y$.

Lemma di Zorn. *Ogni sottoinsieme chiuso A di M contiene almeno un elemento massimale.*

Una catena K di M si dice *massimale* se per ogni $x \in M$, se $x \notin K$ allora l'insieme $K \cup \{x\}$ non è più una catena.

Principio di Massimalità di Hausdorff. *Ogni catena di un insieme ordinato può essere estesa ad una catena massimale.*

Questi due enunciati, molto simili tra loro, sono spesso usati nelle dimostrazioni. Entrambi sono equivalenti ad AC.

Molti sono i teoremi che richiedono AC per la loro dimostrazione. Ecco qualche esempio (alcuni sono addirittura equivalenti ad AC, come il teorema di Tychonoff):

(1) *L'unione di una infinità numerabile di insiemi numerabili è ancora numerabile.*
(2) *Ogni anello commutativo con unità ha un ideale massimale.*
(3) *Ogni spazio vettoriale ha una base.*
(4) *Ogni sottogruppo di un gruppo abeliano libero è libero.*
(5) *Ogni campo ammette una chiusura algebrica.*
(6) *Il prodotto di (infiniti) spazi compatti è compatto.* (Teorema di Tychonoff)
(7) *In uno spazio di Banach B, ogni funzionale lineare limitato definito su un sottospazio si estende a un funzionale lineare limitato con la stessa norma su tutto B.* (Teorema di Hahn–Banach)

Purtroppo, AC ha anche conseguenze "negative". Vi sono alcuni teoremi dimostrabili usando (e a volte addirittura equivalenti a) AC che forse non vorremmo avere. Di questi, il più famoso è noto come "Paradosso di Banach–Tarski"

Paradosso di Banach–Tarski. *Sia $B = \{(x, y, z) \in \mathbb{R}^3 \mid x^2+y^2+z^2 \leq 1\}$ la palla unitaria dello spazio euclideo. Allora esiste una partizione $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ di B e $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m$ isometrie di $\mathbb{R}^3$ tali che $\{\sigma_1(X_1), \ldots, \sigma_n(X_n)\}$ e $\{\tau_1(Y_1), \ldots, \tau_m(Y_m)\}$ sono partizioni di B.*

In altre parole: è possibile suddividere B in un numero finito di pezzi che opportunamente traslati e ruotati formano due copie di B e cioè, *mediante isometrie è possibile duplicare la sfera.*

Un'altra ben nota conseguenza di AC è l'esistenza di insiemi non misurabili secondo Lebesgue, e anzi l'impossibilità di avere una misura invariante per traslazioni e definita per tutti i sottoinsiemi della retta reale che estenda il concetto di "lunghezza di un intervallo".

Evidentemente le conseguenze "buone" sono superiori a quelle "cattive", nondimeno AC ha sempre suscitato un po' di imbarazzo fra i matematici. Molti pensano che non li riguardi, che nella matematica "vera" queste cose non capitano, che non si fa uso di enunciati esoterici come AC. Messi di fronte al fatto che senza AC non ci sarebbero molti teoremi di analisi elementare, come l'esistenza di massimi e minimi per funzioni continue, essi reagiscono accettandolo allora come fatto evidente, di cui non si deve discutere. Quando poi però devono accettare che è possibile avere un buon ordinamento sull'insieme dei numeri reali (e quindi, si potrebbero fare dimostrazioni per induzione usando questo ordinamento, se solo sapessimo qual è . . . , vedi ancora la lettera di Lebesgue in [**Lettres**]), allora cambiano discorso, dicendo che è "roba da logici".

Questo atteggiamento non è sorprendente. Un matematico è tutto sommato un essere umano, e la coerenza non è il primo tratto che associamo al carattere umano. Inoltre, nonostante affermazioni altisonanti sulla verità "assoluta" ed "eterna" della matematica, la matematica è un'attività compiuta da esseri umani in collaborazione, e ci sono aspetti psicologici e sociologici che giocano un ruolo non solo su cosa è "interessante" ma anche su cosa è "vero". La discussione su AC è uno di questi aspetti.

Come possiamo concludere? Cosa pensiamo dei vari enunciati che abbiamo visto? Una battuta, che cattura abbastanza bene l'aspetto psicologico, può aiutare:

> *. . . l'assioma della scelta è sicuramente vero, il principio del buon ordinamento è sicuramente falso, e per quanto riguarda il lemma di Zorn, chi può dirlo?*

Bibliografia

[An] A. Andretta, *Elementi di Logica Matematica.* Dispense del corso disponibili su Moodle per il corso di Logica del terzo anno

[Lettres] R. Baire, E. Borel, J. Hadamard, H. Lebesgue, *Bull. Soc. Math. France*, **33**, (1905), pp. 261–273, ripubblicato in traduzione inglese in G. H. Moore, *Zermelo's axiom of choice : its origins, development, and influence*, Springer–Verlag, 1982, pp. 311–320

[Dev] K. J. Devlin, *The Joy of Sets: Fundamentals of Contemporary Set Theory.*, Springer–Verlag, 1993

[Hu] T. W. Hungerford, *Algebra*, Springer–Verlag, 1974

[Ma] Y. I. Manin, "Assioma/Postulato", in Enciclopedia Einaudi, volume 1, Einaudi 1977

[NaNe] E. Nagel, J. R. Newman, *La prova di Gödel*, Boringhieri, 1974

[vdW] B. L. van der Waerden, *Algebra*, (settima ed., 2 volumi), Frederick Ungar Publishing Co., 1970