ISBN 88-7171-005-3

9 788871 710051

93B.6588 PROCESI"ELEM.TEORIA DI GALOIS (DB)

Distribuzione esclusiva Zanichelli Editore S.p.A.

Al pubblico L. 16 500•••

Claudio Procesi

ELEMENTI DI TEORIA DI GALOIS

a cura di Silvana Abeasis

DECIBEL

ZANICHELLI

Claudio Procesi

ELEMENTI
DI
TEORIA DI GALOIS

a cura di Silvana Abeasis

Decibel editrice di Giorgio Villella
via del Santo 30, 35123 Padova
telefono (049) 8756956

Distribuzione esclusiva
Zanichelli editore, via Irnerio 34, 40126 Bologna
telefono (051) 293111, telex 521587 Zaned I,
fax (051) 249782, 293224

Prima edizione
dicembre 1977; questa è la seconda stampa corretta

Ristampe

1	2	3	4	5	6	7	8	9	10
1997		1998		1999		2000		2001	2002
2003		2004		2005		2006		2007	2008

Stampato
a Bologna dalla Grafica Ragno, via Piemonte 12, Tolara di Sotto - Ozzano Emilia

Claudio Procesi

ELEMENTI DI TEORIA DI GALOIS

a cura di Silvana Abeasis

DECIBEL

ZANICHELLI

Questo quaderno è il risultato di una riorganizzazione fatta da Silvana Abeasis di appunti di corsi da me tenuti in varie università.

Il suo contenuto e i prerequisiti necessari sono esposti nella introduzione.

Il quaderno può essere usato, in parte o completamente, per vari scopi: un corso di Algebra II, ovvero di Matematiche complementari, ovvero come spunto di studio per tesi nell'indirizzo didattico del corso di laurea in matematica.

INDICE

INTRODUZIONE

La teoria di Galois è una parte matematica che ha sempre esercitato un grande fascino per svariati validi motivi a cui vogliamo accennare.

Innanzi tutto essa è una teoria di grande eleganza e semplicità, ma allo stesso tempo contiene tutti gli ingredienti tipici del pensiero algebrico astratto.

D'altra parte essa mostra come, con l'introduzione di opportuni invarianti (grado di una estensione, gruppo di Galois di una equazione, ecc.) si possano discutere problemi classici quali la possibilità o meno di costruire un poligono regolare con riga e compasso e la risolubilità o meno di una equazione algebrica tramite estrazione di radicali; problemi questi che sembrerebbero altrimenti inattaccabili con metodi geometrici. Per una discussione approfondita delle costruzioni con riga e compasso si confronti il volume raccolto da F. Enriques, *Questioni riguardanti le matematiche elementari*, volume II, Zanichelli, 1914. In esso sono contenute molte informazioni, anche di carattere storico, sui metodi geometrici usati per l'analisi di tali problemi dai greci ai nostri giorni (costruzioni esplicite con riga e compasso, ovvero con altre curve meccaniche, costruzioni approssimate, ecc.).

La teoria di Galois fornisce una prima idea del metodo, tipico dell'algebra, di associare a problemi di varia natura invarianti numerici e algebrici che traducano totalmente o almeno parzialmente le proprietà degli oggetti che si vogliono studiare.

Infine la teoria di Galois è stata il punto di partenza di numerose ricerche in teoria dei numeri ed in geometria algebrica, alle quali purtroppo non potremo neppure accennare in queste note. Per una logica continuazione degli argomenti qui svolti si consiglia il lettore di consultare per esempio, per la teoria dei numeri, S. Lang, *Algebraic number theory*, Addison-Wesley, 1970, dove potrà trovare anche ulteriori riferimenti bibliografici; per quanto riguarda gli aspetti geometrici e in particolare la teoria dei rivestimenti delle superficie di Riemann si veda per esempio Ahlfors-Sario, *Riemann surfaces*, Princeton University Press, 1960, che contiene un'ampia bibliografia della letteratura classica.

La teoria di Galois ha ormai circa 150 anni di età ed in questo periodo è stata sottoposta a svariati cambiamenti sia di contenuto che di presentazione, a seconda dei quesiti e delle idee dominanti. È difficile ora presentarla sotto una veste realmente nuova e non è certo questo lo scopo di questi appunti. Una ottima presentazione, nello stile della matematica del secolo scorso, si può trovare nel libro di C. Bianchi, *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, Enrico Spoerri, Pisa 1899. In questo testo sono contenuti anche teoremi relativi ai gruppi dei poliedri regolari, i quali sono molto utili per passare allo studio geometrico della teoria stessa, cioè la monodromia, ecc. Per una esposizione più dettagliata si veda anche F. Klein, *The icosahedron*, Dover Publications, S 314.

Noi qui ci siamo limitati a fornire degli appunti in italiano il più possibile autosufficienti e brevi, indirizzati a studenti di un secondo o terzo anno di matematica. In essi si sviluppa la teoria di Galois per i campi numerici, Parte I, in modo da arrivare rapidamente al cuore dei problemi e dei metodi, senza appesantire fin dall'inizio la trattazione, né con complicazioni di carattere logico-insiemistico relative alla costruzione della chiusura algebrica di un campo dato, né con i fenomeni dell'inseparabilità specifici alla caratteristica $p>0$.

Nella Parte II si sviluppa la teoria astratta in caratteristica qualunque: questo comporta necessariamente alcune ripetizioni del materiale sviluppato nella Parte I, insieme ad uno sforzo richiesto al lettore di convincersi nel caso generale della validità, senza alcuna modifica, di alcune dimostrazioni fornite precedentemente.

A parte questa scelta dell'organizzatore del materiale, l'approccio seguito è sostanzialmente quello di E. Artin basato sulla nozione di isomorfismo. Si è cercato d'altra parte di mettere di volta in volta in luce anche il punto di vista classico, basato sulla considerazione diretta delle equazioni e delle loro radici. In particolare si veda l'esposizione fatta dei metodi effettivi che riassume concisamente l'approccio classico della teoria stessa.

I requisiti per la lettura di queste note sono ridotti alla conoscenza di un minimo di definizioni di algebra e di algebra lineare fornita dai corsi del primo anno. Solo nel §1, Parte II, si fa riferimento all'assioma della scelta e al metodo delle costruzioni transfinite per il quale si può confrontare per esempio N. Bourbaki: *Theorie des ensembles*. Per il lettore interessato ad ampliare gli argomenti esposti in queste note si consiglia di consultare ad esempio i testi seguenti:

E. Artin, *Galois Theory,* II edition, Notre Dame Mathematical Lectures, Number 2.

L. Bianchi, *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, E. Spoerri, Pisa 1899.

N. Bourbaki, *Algébre*, §4 e 5.

A. Capelli, *Istituzioni di analisi algebrica*, B. Pellerano, Napoli 1902.

I.N. Herstein, *Topics in algebra*, Blaisdell Publishing Co.

N. Jacobson, *Lectures in abstract algebra*, Van Nostrand, 1964.

C. Jordan, *Traité des substitutions ed des équations algébriques*, 1870.

Tschebotarëw, *Grundzüge der Galois'schen theorie*, Groningen 1950.

Weber, *Lehrbuch der Algebra*, 1896.

Terminiamo con un'ultima osservazione: in tempi recenti la teoria di Galois è stata sviluppata in forma più astratta per anelli commutativi e schemi. Si confronti A. Grothendieck, *Seminaire de Geometrie algebrique*, I.H.E.S., 1960-61.

PARTE I LA TEORIA DI GALOIS DEI CAMPI NUMERICI

§ 1 IL CAMPO DEI NUMERI COMPLESSI: TEOREMA FONDAMENTALE DELL'ALGEBRA

Sia $\mathbb{C}$ l'insieme dei numeri complessi. In esso sono definite le operazioni di somma, prodotto, differenza e divisione per un numero non nullo; queste operazioni verificano alcune proprietà formali che non elencheremo e che permettono di affermare che $\mathbb{C}$ è un campo. Tutto ciò appartiene all'algebra elementare e lo supporremo pertanto noto.

Ricordiamo che la proprietà algebrica fondamentale del campo $\mathbb{C}$ dei complessi è la possibilità, senza eccezioni, di risolvere una equazione algebrica. Abbiamo infatti il seguente:

TEOREMA FONDAMENTALE DELL'ALGEBRA 1.1 *Se* $f(x)=\sum_{i=0}^{n} a_i x^i$ *è un polinomio a coefficienti* $a_i \in \mathbb{C}$ *e di grado effettivo* $n>0$, *allora esiste un* $\alpha \in \mathbb{C}$ *tale che* $f(\alpha)=0$.

Dal teorema precedente discende poi il seguente:

COROLLARIO 1.2 *Esistono* n *numeri* $\alpha_1,\dots,\alpha_n$ *tali che* $f(x)=a_n \prod_{i=1}^{n}(x-\alpha_i)$.

Il teorema fondamentale dell'algebra si può dimostrare in varie maniere; una dimostrazione rapida, ma poggiata sulla teoria delle funzioni olomorfe, è la seguente:

Dimostrazione I) $f(x)$ è una funzione olomorfa della variabile x. Se fosse $f(\alpha)\neq 0$ per ogni $\alpha\in\mathbb{C}$, la funzione $\frac{1}{f(x)}$ sarebbe una funzione olomorfa sull'intero piano della variabile complessa, (cioè una funzione intera); ora è facile verificare che $\lim_{x\to\infty}\frac{1}{f(x)}=0$. Ne segue allora, per il teorema di Liouville, che $\frac{1}{f(x)}$ è costante; questa è una contraddizione perchè abbiamo supposto che il grado n di $f(x)$ è positivo $\square$.

Se vogliamo evitare l'uso del teorema di Liouville (ma essenzialmente ridimostrarlo in questo caso particolare) possiamo procedere in modo elementare come segue:

Dimostrazione II) Sia $f(x)=a_0+a_1x+\dots+a_nx^n$; supporremo $f(0)=a_0\neq 0$, poichè se fosse $a_0=0$ il teorema sarebbe provato con $\alpha=0$. Per ogni valore non nullo di x possiamo scrivere:

$$f(x)=a_nx^n\left(1+\frac{a_{n-1}}{a_n}\frac{1}{x}+\dots+\frac{a_1}{a_n}\frac{1}{x^{n-1}}\right)$$

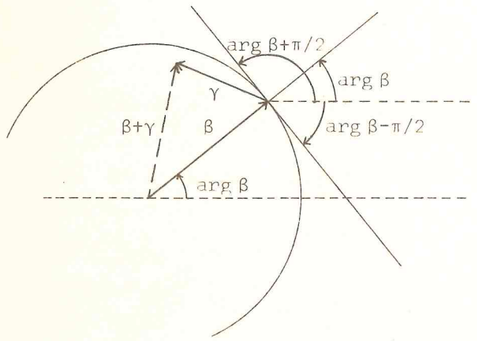
e quindi passando ai moduli si ha:

$$|f(x)|=|a_n||x|^n\left|1+\frac{a_{n-1}}{a_n}\frac{1}{x}+\dots+\frac{a_1}{a_n}\frac{1}{x^{n-1}}\right|.$$

Da questa formula segue che $\lim_{x\to\infty}|f(x)|=+\infty$ e quindi è possibile determinare un numero positivo r per il quale valga: $|f(x)|>|a_0|>0$ per ogni x, con $|x|\geq r$. Questa relazio

ne intanto ci dice che le eventuali radici del polinomio $f(x)$ devono essere all'interno del disco $|x| \leq r$. Tale disco è d'altra parte un insieme compatto (chiuso e limitato) e quindi, per il teorema di Weierstrass sulle funzioni continue, esiste un punto x_0 in cui la funzione $f(x)$ assume il valore minimo. Un tale punto x_0 è necessariamente interno al disco $|x| \leq r$ visto che $f(0) = a_0$ ed $f(x) > a_0$ sulla frontiera $|x| = r$. Ci proponiamo ora di provare che x_0 è una radice di $f(x)$. Cambiando le coordinate possiamo assumere che $x_0 = 0$ e quindi che $|f(x)|$ assume il valore minimo in 0. Vogliamo quindi provare che $f(0) = 0$.

Supponiamo per assurdo che $f(0) = \beta \neq 0$. Nelle nuove coordinate, e con le ipotesi fatte, il polinomio $f(x)$ si può scrivere nella forma $f(x) = \beta + x^i\,(c_0 + c_1 x + \ldots + c_h x^h)$, $c_0 \neq 0$, $|f(0)| = |\beta|$ valore minimo in $|x| \leq r$.

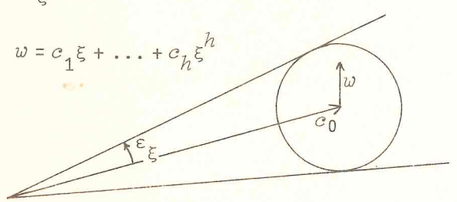


D'altra parte se si prende un numero complesso γ, con $|\gamma|$ abbastanza piccolo e l'argomento di γ non compreso fra arg $\beta-\pi/2$ e arg $\beta+\pi/2$, si ha certamente $|\beta + \gamma| < |\beta|$.

Pertanto otterremo una contraddizione non appena avremo fatto vedere che si può trovare un numero ξ tale che $\xi^i(c_0 + c_1\xi + \ldots + c_h\xi^h)$ ha le proprietà richieste per γ (modulo sufficientemente piccolo ed argomento etc..). In tal caso infatti si avrebbe $|f(\xi)| = |\beta + \gamma| < |\beta|$ contro l'ipotesi che $|\beta|$ sia il valore minimo. Ora il modulo del numero $\xi^i(c_0 + c_1\xi + \ldots + c_h\xi^h)$ può rendersi piccolo quanto si vuole, basta prendere numeri ξ con modulo convenientemente piccolo, e questa condizione non pone alcuna restrizione sull'argomento di ξ il quale può essere fissato in modo arbitrario. Ora, poichè $c_0 \neq 0$, se $|\xi|$ è molto piccolo e quindi anche $|c_1\xi + \ldots + c_h\xi^h|$ è molto piccolo, si avrà che:

$$\arg\,(c_0 + c_1\xi + \ldots + c_h\xi^h) = \arg\, c_0 + \varepsilon_\xi$$

con ε_ξ piccolo a piacere (se $|\xi|$ è piccolo). Questo risulta chiaro dalla figura quì a lato. Pertanto è facile determinare ξ in modo tale che $|\xi|$ sia molto piccolo e arg $|\xi^i(c_0 + c_1\xi + \ldots + c_h\xi^h)| = i$ arg ξ + +arg $c_0 + \varepsilon_\xi$ non sia compreso fra arg $\beta-\pi/2$ e arg $\beta+\pi/2$. Questo termina la dimostrazione.



NOTA STORICA 1.3 La teoria dei numeri complessi ha iniziato il suo sviluppo nel Cinquecento, motivata dallo studio delle equazioni di terzo grado. Le equazioni di secondo grado certamente conducono allo studio di radici quadrate di numeri negativi, ma tali equazioni corrispondono a problemi geometrici, meccanici etc. che non ammettono soluzioni. Le equazioni cubiche forniscono invece un esempio di problemi a carattere geometrico (e quindi possibili) per i quali la soluzione reale è data da numeri espressi mediante radici quadrate di numeri negativi. Un tale esempio è fornito dall'equazione $x^3 - 15x - 4 = 0$ che fu studiata da R.Bombelli (secolo XVI); se si applica la formula data nel §16 si ottiene:

$$x = \sqrt[3]{+2+\sqrt[2]{4-125}} + \sqrt[3]{+2-\sqrt[2]{4-125}} = \sqrt[3]{+2+\sqrt[2]{-121}} + \sqrt[3]{+2-\sqrt[2]{-121}} =$$

$$= \sqrt[3]{2+11i} + \sqrt[3]{2-11i} = 2 + i + 2 - i = 4$$

Lo sviluppo della teoria dei numeri complessi, iniziata e sviluppata dal Bombelli, fu poi proseguita da G.Wallis (1616 - 1703) da A.De Moivre (1667 - 1754) che completò la teoria delle operazioni elementari sui numeri complessi.

L'interpretazione geometrica dei numeri complessi fu sviluppata solo successivamente da C.Wessel (1745-1818), G.R.Argand (1768-1822), Gauss (1777-1855) e Cauchy (1789-1857). Per una panoramica più completa dello sviluppo di tale teoria rinviamo per esempio a "Questioni riguardanti le Matematiche elementari" F.Enriques volume I pagina 495 e seguenti.

Rinviamo allo stesso volume (pagina 547 e seguenti) chi voglia conoscere come si sia pervenuti ad intuire, enunciare e dimostrare il teorema fondamentale dell'algebra. Citiamo soltanto il fatto che dimostrazioni non completamente rigorose furono fornite da Eulero (1707-1783) e da D'Alambert (1717-1783), e che il teorema fu completamente dimostrato da Gauss nel 1799.

§ 2 CAMPI DI NUMERI

DEFINIZIONE 2.1 Un insieme $K \subseteq \mathbb{C}$ si dice un *campo di numeri* se:

1) K ha almeno un elemento diverso dallo 0

2) Se $\alpha, \beta \in K$ si ha $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta \in K$, e se $\beta \neq 0$ anche $\alpha/\beta \in K$.

Osservazione 2.2. Queste condizioni non sono indipendenti, sono infatti sovrabbondanti, ma questo non ci interessa particolarmente. In parole povere si può dire che K è un campo di numeri quando operando sugli elementi di K con le quattro operazioni

(operazioni razionali) otteniamo ancora elementi di K.

Osservazione 2.3 Con la 2.1 abbiamo semplicemente definito un sottocampo del campo $\mathbb{C}$ dei complessi. In tutto quanto segue si potrebbe sostituire $\mathbb{C}$ con un campo qualunque di caratteristica 0 e soddisfacente il teorema fondamentale dell'algebra.

Esempi $\mathbb{C}$, $\mathbb{R}$ (insieme dei numeri reali), $\mathbb{Q}$ (insieme dei numeri razionali) sono campi di numeri.

PROPOSIZIONE 2.4 *Se K è un campo di numeri allora $K \supset \mathbb{Q}$.*

Dimostrazione Sia $a \in K$ un elemento non nullo (certamente esistente per l'ipotesi 1)). Allora $1 = a/a \in K$ per l'ipotesi 2), e così anche $2 = 1 + 1$, $3 = 1 + 2$ ecc, cioè ogni numero naturale è in K. Facendo la differenza di due numeri naturali, e sempre usando la ipotesi 2), vediamo che ogni numero intero relativo è in K. Operando poi con la divisione sugli interi otteniamo tutti i numeri razionali, che sono ancora in K, sempre per l'ipotesi 2). ▽

DEFINIZIONE 2.5 Se $E \supset F$ sono due campi, diremo che E è una *estensione* di F.

Usando questa definizione possiamo esprimere in modo diverso il contenuto della proposizione 2.4; essa infatti dice esattamente che ogni campo di numeri è estensione del campo razionale.

ESERCIZI 2.6

1) Sia q un numero razionale fissato ed α una radice quadrata di q, cioè tale che $\alpha^2 = q$. Verificare che l'insieme $\mathbb{Q}(\alpha) = \{a + \alpha b \mid a,b \in \mathbb{Q}\}$ è un campo di numeri.

2) Sia β una radice cubica di un numero razionale fissato q ($\beta^3 = q$). Verificare che l'insieme $\mathbb{Q}(\beta) = \{a + \beta b + \beta^2 c \mid a,b,c \in \mathbb{Q}\}$ è un campo di numeri. (Tutte le verifiche sono banali tranne per la divisione, cfr. proposizione 4.8).

§ 3 NUMERI ALGEBRICI E TRASCENDENTI

DEFINIZIONE 3.1 a) Se K è un campo di numeri e $\alpha \in \mathbb{C}$, diremo che α è *algebrico su K* se esiste un polinomio non nullo $f(x) = \sum_{i=0}^{n} a_i x^i$, con coefficienti $a_i \in K$, tale che $f(\alpha) = 0$.

b) Se α non è algebrico su K diremo che è *trascendente su K*.
c) Se il campo K è il campo dei razionali $\mathbb{Q}$, diremo semplicemente che α è *algebrico* oppure *trascendente* (senza dire su $\mathbb{Q}$).
d) Se $E \supset K$ è un'estensione di campi di numeri, diremo che E è *algebrico* su K (ovvero che l'*estensione* è *algebrica*) se ogni elemento $\alpha \in E$ è algebrico su K.

Esempi 3.2 a) Se $\alpha \in K$ allora α è algebrico su K. Verifica infatti il polinomio $x - \alpha$ (i coefficienti 1, $-\alpha$ sono in K). In particolare ogni numero $\alpha \in \mathbb{C}$ è algebrico sui complessi. Osserviamo quindi che l'essere un numero $\alpha \in \mathbb{C}$ algebrico o trascendente dipende dal campo numerico K in cui lo si studia.
b) Se α è una radice n-esima di un numero $\beta \in K$ allora α è algebrico su K. Verifica infatti il polinomio $x^n - \beta$.
c) Ogni numero complesso è algebrico sul campo $\mathbb{R}$ dei numeri reali. Infatti sia $\alpha = a + ib$ un numero complesso, $a,b \in \mathbb{R}$, esso soddisfa il polinomio

$$[x - (a + ib)][x - (a - ib)] = x^2 - 2ax + a^2 + b^2$$

che è a coefficienti reali.
d) Il numero $\alpha = \sqrt{2} + \sqrt[3]{5}$ è algebrico. Infatti $\alpha - \sqrt{2} = \sqrt[3]{5}$, da cui $(\alpha - \sqrt{2})^3 = 5$, cioè $\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} = 5$, $\alpha^3 + 6\alpha - 5 = \sqrt{2}(3\alpha^2 + 2)$, $(\alpha^3 + 6\alpha - 5)^2 = 2(3\alpha^2 + 2)^2$. Dall'ultima espressione scritta, sviluppando, si deduce che α verifica il polinomio (a coefficienti razionali) $x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$.

Osservazione 3.3 L'esempio d) suggerisce un modo semplice per costruire numeri algebrici. Sono certamente algebrici per esempio i numeri $\sqrt{7} - \sqrt{3}$, $\sqrt[5]{4} + 2$, $\sqrt[2]{2} + \sqrt[3]{3} + \sqrt[4]{4}$ etc. E' altrettanto semplice costruire numeri trascendenti? O meglio ancora, esistono numeri trascendenti, reali o complessi? La risposta è affermativa, come è ben noto, ma le dimostrazioni non hanno il carattere elementare che ci siamo proposti in queste note. Ci limiteremo pertanto ad una breve nota storica che riassuma le tappe principali che hanno dato origine alla teoria dei numeri trascendenti.

NOTA STORICA 3.4 Un primo passo fondamentale per lo sviluppo della teoria dei numeri trascendenti si ha nel 1844 con una memoria di Liouville, nella quale è descritto essenzialmente un procedimento per costruire una vasta classe di numeri che non sodisfa ad alcuna equazione algebrica a coefficienti razionali (e quindi interi).
Nel 1873 apparve la memoria di Hermite "Sur la function exponentielle", nella quale egli dimostra la trascendenza del numero e, la base dei logaritmi naturali (l'irrazionalità del numero e era stata provata molto tempo prima nel 1744, da Eulero!). In que

sto lavoro sono introdotti nuovi metodi, generalizzando i quali Lindemann riuscì, circa una diecina di anni dopo, a provare la trascendenza del numero π, ed a risolvere il problema posto dai Greci della quadratura del cerchio. Questo problema classico consisteva nel costruire, facendo uso solo della riga e del compasso, un quadrato avente area pari a quella del cerchio di raggio unitario. Bastava quindi saper costruire, in un piano e con assegnata unità di misura, due punti distanti tra loro $\sqrt{\pi}$. Poichè le costruzioni lecite erano solo quelle ottenibili con riga e compasso, i punti dovevano ottenersi come intersezioni di rette e circonferenze e quindi le loro coordinate, in un riferimento cartesiano opportuno, erano soluzioni di equazioni algebriche (cfr.§7). Ecco perchè la trascendenza di π implica l'impossibilità della quadratura del cerchio. Successivamente le idee di Hermite e Lindemann furono semplificate da Weierstrass, Hilbert, Hurwitz e Gordan verso la fine del secolo. Una dimostrazione della trascendenza di e e π secondo le idee degli ultimi autori citati può trovarsi nel libro di Alan Baker: "Trascendental Number theory" Cambridge University Press, 1975.

Nel 1900, al congresso internazionale di Matematica a Parigi, Hilbert pose il seguente problema (il settimo della famosa lista): il logaritmo (supposto irrazionale) di un numero algebrico rispetto ad una base algebrica è algebrico o trascendente? O equivalentemente: α^{β} è trascendente per ogni numero irrazionale algebrico β e per ogni numero algebrico $\alpha \neq 0,1$?

Questo problema fu risolto da Gelfond e Schneider nel 1934. Ulteriori generalizzazioni si sono poi ottenute in data più recente (vedere A.Baker, testo citato).

ESERCIZIO 3.5 Determinare quali dei seguenti numeri sono algebrici (rispettivamente trascendenti):

$$\frac{1}{\sqrt[3]{\sqrt{2}+1}};\ \sqrt{\pi};\ \frac{\pi}{\sqrt{2}+3};\ \sqrt{2}+\sqrt{3}+\sqrt{5};\ e^2+e+1.$$

§ 4 CAMPO GENERATO DA UN INSIEME DI NUMERI: ESTENSIONI SEMPLICI

Sia $S \subset \mathbb{C}$ un insieme di numeri, per semplicità supponiamo che sia un insieme finito $S = \{s_1, s_2, \ldots, s_k\}$, e sia K un campo di numeri. L'insieme $K \cup S$ non sarà in generale un campo.

Esercizio 0) Se S è finito allora $K \cup S$ è un campo se e solo se $S \subset K$.

Se $S \not\subset K$ operando sugli elementi di K e di S con le quattro operazioni genereremo dei

nuovi numeri per i quali ci proponiamo di trovare una scrittura uniforme. Se sugli elementi di K e di S operiamo con la somma ed il prodotto, i numeri ottenuti potranno essere scritti nella forma

$$(1)\quad \sum a_{n_1 \ldots n_k} s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k} \quad \text{con} \quad a_{n_1 \ldots n_k} \in K$$

Se ora operiamo con somma e prodotto su due o più elementi del tipo (1), chiaramente otteniamo elementi dello stesso tipo. Passiamo quindi ad operare con l'altra operazione: la divisione. I numeri che si ottengono si possono scrivere nella forma:

$$(2)\quad \frac{\sum a_{n_1 \ldots n_k} s_1^{n_1} \ldots s_k^{n_k}}{\sum b_{m_1 \ldots m_k} s_1^{m_1} \ldots s_k^{m_k}},\ a_{n_1 \ldots n_k},\ b_{m_1 \ldots m_k} \in K.$$

Se eseguiamo somme, differenze, prodotti e divisioni su due o più elementi del tipo (2) otterremo sempre numeri rappresentabili sotto la forma (2) e quindi non genereremo nuovi numeri. L'insieme:

$$K(S) = \left\{ \frac{\sum a_{n_1 \ldots n_k} s_1^{n_1} \ldots s_k^{n_k}}{\sum b_{m_1 \ldots m_k} s_1^{m_1} \ldots s_k^{m_k}},\ a_{n_1 \ldots n_k}\ \ b_{m_1 \ldots m_k} \in K \right\}.$$

è quindi un campo di numeri che contiene sia K che S.

Inoltre, se W è un campo di numeri tale che $K \subset W$, $S \subset W$, allora W deve contenere tutti i numeri ottenibili da K ed S operando con le quattro operazioni, (W è chiuso rispetto a queste operazioni). Segue che $W \supset K(S)$.

Possiamo riassumere quanto fino ad ora detto con la:

PROPOSIZIONE 4.1 *$K(S)$ è un campo contenente K ed S. Fra tutti i campi W contenenti K ed S, $K(S)$ è il minimo, cioè $K(S) \subset W$.*

DEFINIZIONE 4.2 Il campo $K(S)$ si chiama *campo generato da S su K*, ovvero $K(S)$ è *l'estensione di K tramite gli elementi di S*, ($K \subset K(S)$).

Un caso di particolare importanza si ha quando l'insieme S è costituito da un solo elemento: $S = \{s\}$. In questo caso l'estensione di K tramite l'elemento s si indica con $K(s)$.

DEFINIZIONE 4.3 Un'estensione $K \subset K(s)$ si chiama *estensione semplice*.

I numeri di una estensione semplice $K(s)$ si possono tutti scrivere nella forma (caso particolare della 2)):

$$(3)\ \frac{\sum a_i s^i}{\sum b_j s^j},\ a_i, b_j \in K\ .$$

Ci proponiamo di studiare una estensione semplice $K(s)$ a seconda che il numero s sia algebrico o trascendente su K. Di fatto si hanno due situazioni distinte e di conseguenza una caratterizzazione dei numeri algebrici e trascententi su K.

PROPOSIZIONE 4.4 *s è trascendente su K se e solo se l'espressione* (3) *di ogni elemento di $K(s)$ è unica.*

Dimostrazione Prima di dare la dimostrazione chiariamo il significato dell'enunciato.
Dire che l'espressione $\sum a_i s^i / \sum b_j s^j$ per un elemento di $K(s)$ è unica significa che se il medesimo elemento si può anche scrivere come $\sum c_t s^t / \sum r_h s^h$, allora i polinomi (formali) $(\sum a_i x^i)(\sum r_h x^h)$ e $(\sum b_j x^j)(\sum c_t x^t)$ sono uguali.
La dimostrazione è praticamente immediata. Supponiamo infatti s algebrico su K e sia $\sum a_i x^i$ il polinomio (non nullo) per il quale $\sum a_i s^i = 0$. Allora per l'elemento $0 \in K(s)$ si possono dare due espressioni del tipo (3): 0 e $\sum a_i s^i$; e risulta $0 \neq \sum a_i x^i$. Viceversa se vi è un numero di $K(s)$ che non si esprime univocamente, per il quale cioè si abbia simultaneamente

$$\frac{\sum a_i s^i}{\sum b_j s^j} = \frac{\sum c_t s^t}{\sum r_h s^h}; \quad (\sum a_i x^i)(\sum r_h x^h) \neq (\sum b_j x^j)(\sum c_t x^t),$$

allora il polinomio

$$f(x) = (\sum a_i x^i)(\sum r_h x^h) - (\sum b_j x^j)(\sum c_t x^t)$$

è non nullo e $f(s) = 0$. Il numero s è quindi algebrico su K. ▽△

D'ora in poi ci occuperemo delle estensioni semplici $K(s)$, con s algebrico su K. Una tale estensione la chiameremo anche *estensione algebrica semplice*, il motivo apparirà chiaro dopo aver visto l'esempio 6.9 ed il corollario 6.13.
Abbiamo appena visto che gli elementi di $K(s)$ non si possono scrivere in modo unico nella forma $\sum a_i s^i / \sum b_j s^j$. Vogliamo cercare di scoprire una qualche *forma standard* per questi elementi. Per questo ci serve qualche informazione suppletiva e una digressione sui polinomi.

Ricordiamo che il *simbolo* $K[x]$ denota l'insieme dei *polinomi* in x a coefficienti in K; tali polinomi si possono sommare e moltiplicare fra loro e quindi (facendo le opportune verifiche) $K[x]$ è un *anello* commutativo.
Ricordiamo inoltre che per un anello commutativo A si introduce la nozione di *ideale* nella maniera seguente: $I \subset A$ è un ideale di A se verifica le seguenti proprietà:

(i) Se $i_1, i_2 \in I$ allora $i_1 + i_2 \in I$.
(ii) Se $i \in I$, $a \in A$ allora $ai \in I$.

In particolare per gli ideali dell'anello dei polinomi $K[x]$ sussiste la seguente caratterizzazione.

PROPOSIZIONE 4.5 *Se $I \subset K[x]$ è un ideale, allora esiste un polinomio $f(x)$ tale che:*

$$I = \{g(x)f(x) \mid g(x) \in K[x]\} = (f(x))$$

Dimostrazione Se $I = \{0\}$ è l'ideale nullo, allora $I = (0)$; altrimenti vi è un polinomio non nullo in I e sia $f(x) \in I$ uno di essi e di grado minimo. Proviamo che $I = (f(x))$. Dalla proprietà (ii) degli ideali segue subito che $(f(x)) \subset I$. Viceversa se $h(x) \in I$, eseguiamo la divisione con resto $h(x) = q(x) \cdot f(x) + r(x)$, ove $r(x)$ è nullo oppure ha grado strettamente inferiore a quello del divisore $f(x)$. Scrivendo $r(x) = h(x) - q(x)f(x)$ e sfruttando le (i) e (ii) segue che $r(x) \in I$. Poichè $f(x)$ ha grado minimo per i polinomi non nulli di I, deve necessariamente essere $r(x) = 0$, cioè $h(x) = q(x)f(x)$, $h(x) \in (f(x))$ ▽△

La proposizione appena dimostrata può essere precisata ulteriormente. Essenzialmente la domanda che ci poniamo è la seguente: dato un ideale $I \neq (0)$, è individuato univocamente il polinomio $f(x) \in I$ tale che $I = (f(x))$? La risposta è certamente no, visto che se $a \in K$ è un numero non nullo, $(af(x)) = (f(x))$ (la verifica è immediata!).

Esercizio 1) $(f(x)) = (g(x))$ se e solo se $g(x) = af(x)$ con $a \in K$.

Esercizio 2) Dato un ideale $I \neq (0)$ esiste un unico polinomio *monico* (cioè con coefficiente direttivo uguale ad 1) tale che $I = (f(x))$.

Ad un numero s algebrico su K si può associare un ideale, denotato con I_s, e definito da:

$$I_s = \{g(x) \in K[x] \mid g(s) = 0\}$$

il quale contiene polinomi non nulli proprio perchè s è algebrico. Le proprietà (i) e (ii) degli ideali sono di verifica immediata.
Facendo uso dell'esercizio 2) si ha che $I_s = (f(x))$ per un ben determinato polinomio monico $f(x)$, il quale si chiama il *polinomio minimo* di s su K. Il suo grado si chiama *grado del numero algebrico* s su K.

PROPOSIZIONE 4.6 *Il polinomio minimo $f(x)$ di un elemento s, algebrico su K, è irriducibile. Viceversa se $f(x)$ è monico e irriducibile su K allora esso è il polinomio*

minimo per ciascuna delle sue radici.

Dimostrazione Se $f(x)$ è riducibile e quindi $f(x) = h(x)k(x)$, con $h(x)$ e $k(x)$ di grado strettamente minore di quello di $f(x)$, allora $0 = f(s) = h(s)k(s)$ e quindi o $h(s) = 0$ oppure $k(s) = 0$. Questo è assurdo perchè si è supposto che $f(x)$ abbia grado minimo rispetto ai polinomi che sono annullati da s.
Viceversa se $f(x)$ è irriducibile ed s è una sua radice, cioè $f(s) = 0$, si ha $f(x) \in I_s$. Proviamo che $I_s = (f(x))$. Infatti $I_s = (h(x))$ per qualche polinomio $h(x)$ non costante (per la proposizione 4.5), e quindi $f(x)$ è un multiplo di $h(x)$, ma poichè è irriducibile per ipotesi $f(x)$ differisce da $h(x)$ per una costante moltiplicativa non nulla $a \in K$. Per l'esercizio 1) si ha $(h(x)) = (f(x)) = I_s$ ▽

Continuiamo con la "digressione sui polinomi".

DEFINIZIONE 4.7 Dati due polinomi $f(x)$, $g(x) \in K[x]$ si dice che un polinomio $h(x) \in K[x]$ è un loro *massimo comune divisore* se $h(x)$ divide $f(x)$ e $g(x)$ e se $h(x)$ è multiplo di ogni divisore comune di $f(x)$ e $g(x)$.

In tal caso si scrive: $h(x) = (f(x), g(x))$.

E' immediato verificare che due massimi comun divisori di $f(x)$ e $g(x)$ devono differire solo per una costante moltiplicativa non nulla $a \in K$.

PROPOSIZIONE 4.8 *Dati due polinomi $f(x)$, $g(x) \in K[x]$ esiste sempre un loro massimo comun divisore $h(x)$. Esistono inoltre polinomi $p_0(x)$ e $t_0(x)$ per i quali si abbia:*

$$h(x) = p_0(x)f(x) + t_0(x)g(x)$$

Dimostrazione Si considera l'insieme:

$$I = \{p(x)f(x) + t(x)g(x) \mid p(x), t(x) \in K[x]\}.$$

Esso è un ideale di $K[x]$, come si verifica immediatamente. Pertanto, per la proposizione 4.5, $I = (h(x))$ per qualche polinomio $h(x)$. I polinomi $f(x)$ e $g(x)$ appartengono all'ideale I, infatti:

$$f(x) = 1 \cdot f(x) + 0 \cdot g(x) \quad ; \quad g(x) = 0 \cdot f(x) + 1 \cdot g(x)$$

e quindi sono multipli di $h(x)$, cioè $h(x)$ è un divisore sia di $f(x)$ che di $g(x)$. D'altra parte ogni altro divisore $k(x)$ sia di $f(x)$ che di $g(x)$ divide necessariamente $h(x)$, visto che, essendo $h(x) \in I$, esso può scriversi $h(x) = p_0(x)f(x) + t_0(x)g(x)$ per opportuni polinomi $p_0(x)$ e $t_0(x)$ ▽

La proposizione precedente prova l'esistenza di un massimo comun divisore. Per il calcolo esplicito si ricorre al seguente:

METODO DELLE DIVISIONI SUCCESSIVE DI EUCLIDE 4.9 Si operino le seguenti divisioni:

$$f(x) = q_1(x)g(x) + r_1(x)$$
$$g(x) = q_2(x)r_1(x) + r_2(x)$$
$$r_1(x) = q_3(x)r_2(x) + r_3(x)$$
$$\vdots$$
$$r_k(x) = q_{k+2}(x)r_{k+1}(x) + r_{k+2}(x)$$
$$\vdots$$
$$r_{j-1}(x) = q_{j+1}(x)r_j(x) + r_{j+1}(x), \text{ con } r_j(x) \neq 0,\ r_{j+1}(x) = 0$$

Allora $r_j(x)$ è il massimo comun divisore di $f(x)$ e $g(x)$.

Dimostrazione Osserviamo innanzitutto che le divisioni da effettuare successivamente sono in numero finito; ci si ferma quando si arriva al primo resto $r_{j+1}(x) = 0$, e questo deve necessariamente verificarsi visto che i gradi dei resti $r_1(x)$, $r_2(x)$,... vanno strettamente decrescendo.
Per dimostrare la tesi basta provare che:

a) $f(x)$ e $g(x)$ sono multipli di $r_j(x)$

b) $r_j(x) = p_0(x)f(x) + t_0(x)g(x)$ per opportuni polinomi $p_0(x)$ e $t_0(x)$.

a) Si può dimostrare per induzione nel modo seguente: posto di aver dimostrato che $r_{k+2}(x)$ ed $r_{k+1}(x)$ sono multipli di $r_j(x)$ anche $r_k(x) = q_{k+2}(x)r_{k+1}(x) + r_{k+2}(x)$ è esso stesso multiplo di $r_j(x)$.
Se poniamo convenzionalmente:

$$g(x) = r_0(x) \quad \text{e} \quad f(x) = r_{-1}(x)$$

la stessa formula per $k = 0,1$ mostra, alla fine dell'induzione, che $f(x)$ e $g(x)$ sono multipli di $r_j(x)$.
Il primo passo per l'induzione è d'altra parte ovvio.
b) Si può dimostrare anch'esso per induzione ma andando in senso opposto. Infatti se supponiamo $r_k(x)$ ed $r_{k+1}(x)$ della forma desiderata, cioè:

$$r_k(x) = p(x)f(x) + t(x)g(x);\ r_{k+1}(x) = p'(x)f(x) + t'(x)g(x)$$

allora anche $r_{k+2}(x) = r_k(x) - q_{k+2}(x)r_{k+1}(x)$ è della stessa forma.
Anche qui il primo passo dell'induzione è evidente. ▽

Osservazione 4.10 Il lettore deve convincersi, anche facendo esercizi concreti, che il metodo 4.9 fornisce un procedimento costruttivo per trovare, dati due polinomi $f(x)$

e $g(x)$, prima di tutto il loro massimo comun divisore $h(x)$ ed in secondo luogo due polinomi $p_0(x)$ e $t_0(x)$ per i quali si abbia $h(x) = p_0(x)f(x) + t_0(x)g(x)$.

Esercizi sul massimo comun divisore Determinare il massimo comun divisore $h(x)$ ed i polinomi $p_0(x)$ e $t_0(x)$ per le seguenti coppie di polinomi

$f(x) = 3x^3 + 2x - 5$ $\qquad$ $g(x) = x^2 + 3x - 1$

$f(x) = x^4 - 2x^3 + x^2 - 2x$ $\qquad$ $g(x) = x^3 - 2x^2 + x - 2$

$f(x) = x^3 + x^2 - x - 1$ $\qquad$ $g(x) = x^4 + 2x^3 + 2x^2 + 2x + 1$

NOTA STORICA 4.11 Il metodo esposto per la ricerca del massimo comun divisore di due polinomi ricalca l'analogo procedimento nel caso dei numeri interi.
L'esistenza del massimo comun divisore di due interi è provata all'inizio del Libro VII degli Elementi di Euclide e va sotto il nome di "algoritmo euclideo"; esso fu il punto di partenza per i contributi veramente notevoli che i Greci dettero nel campo dell'Aritmetica (proprietà dei numeri primi, esistenza del minimo comune multiplo, esistenza di infiniti primi).
Non si trova traccia invece del metodo delle divisioni successive per i polinomi, prima del XVI° secolo; e questo principalmente, pare, per la difficoltà a sviluppare in modo generale la teoria della divisibilità fra polinomi prima di aver avuto per questi ultimi delle notazioni coerenti. Sembra che il primo che utilizzi essenzialmente la notazione degli esponenti per le potenze della variabile e che tenti quindi di estendere l'algoritmo euclideo ai polinomi, sia S.Stevin, nel suo "Les Oeuvres mathématiques..." Ed.A.Girard, Leyda, 1634, vol.I.
In ogni caso l'estensione della nozione di divisibilità (e problemi connessi) dall'anello degli interi ad altri anelli si sviluppa a partire dalla seconda metà del XVIII° secolo, con i lavori di Eulero (1770), Lagrange, Gauss, Kummer e finalmente Dedekind e Kroneker i quali creano a questo scopo la teoria degli ideali.

Riprendiamo lo studio di una estensione semplice $K \subseteq K(s)$. Consideriamo l'insieme $K[s] = \{\sum a_i s^i \mid a_i \in K\}$ cioè l'insieme di tutte le espressioni polinomiali in s a coefficienti in K. $K[s]$ è chiuso rispetto alla somma, differenza e moltiplicazione ma non necessariamente rispetto alla divisione. Gli elementi dell'estensione semplice $K(s)$ si ottengono operando con la divisione sugli elementi di $K[s]$ e $K[s]$ è chiuso rispetto alla divisione se e solo se $K[s] = K(s)$.
In ogni caso si ha $K \subseteq K[s] \subseteq K(s)$.

TEOREMA 4.12 1) $K[s] = K(s)$ *se e solo se* s *è algebrico su* K.

2) *Se* s *è algebrico su* K *ogni elemento di* $K(s)$ *si può scrivere in modo unico come polinomio in* s *a coefficienti in* K *e di grado inferiore al grado del polinomio minimo di* s *su* K.

Dimostrazione Se $s = 0$ allora $K = K[s] = K(s)$ ed il teorema è evidente. Possiamo quindi assumere $s \neq 0$.
1) Supponiamo che sia $K[s] = K(s)$; $1/s \in K(s)$ quindi $1/s \in K[s]$ e si può scrivere nella forma $1/s = \sum_{i=0}^{m} a_i s^i$, per opportuni $a_i \in K$; segue che $\sum_{i=0}^{m} a_i s^{i+1} - 1 = 0$. Il polinomio $\sum_{i=0}^{m} a_i x^{i+1} - 1$ è non nullo ed è annullato da s. Il numero s è quindi algebrico su K.
Viceversa supponiamo s algebrico su K e sia $f(x)$ il suo polinomio minimo. Dobbiamo mostrare che un elemento qualunque di $K(s)$, e quindi della forma $\sum a_i s^i / \sum b_j s^j = g(s)/h(s)$, è effettivamente già in $K[s]$.
Poichè $h(s) \neq 0$, (altrimenti $g(s)/h(s)$ non ha senso), il polinomio $h(x)$ non è un multiplo di $f(x)$. Sia $l(x)$ un massimo comun divisore di $f(x)$ ed $h(x)$. Poichè $l(x)$ divide $f(x)$ e quest'ultimo è irriducibile (cfr. proposizione 4.6) segue che $l(x)$ (a meno di un fattore costante) deve essere o $f(x)$ oppure il polinomio costante 1.
Non può aversi $l(x) = f(x)$, perchè $l(x)$ divide $h(x)$, ma $f(x)$ non divide $h(x)$. Pertanto deve aversi $h(x) = 1$. Dalla proposizione 4.8 segue quindi che esistono due polinomi $p(x)$ e $t(x)$ per i quali si ha:

$$l(x) = 1 = p(x)f(x) + t(x)h(x).$$

Calcolando l'espressione trovata in s si ha: $1 = t(s)h(s)$ (essendo $f(s) = 0$); quindi $1/h(s) = t(s)$ e sostituendo:

$$\frac{g(s)}{h(s)} = g(s) \cdot t(s) \in K[s].$$

2) Sia $f(x)$ il polinomio minimo di s e supponiamo che il suo grado sia n. Con 1) si è provato che ogni elemento di $K(s)$ si può scrivere come un polinomio in s; ci proponiamo ora di far vedere che si può scegliere di grado minore di n ed in modo unico. Sia dunque $u(x) \in K[x]$ un polinomio e $u(s) \in K[s]$ l'elemento corrispondente. Eseguiamo la divisione $u(x) = q(x)f(x) + r(x)$, ove il grado del resto $r(x)$ è minore di n e calcoliamo l'espressione in s. Si ha $u(s) = r(s)$. Si è quindi trovato un polinomio di grado minore di n che esprime l'elemento $u(s)$. Questa espressione è unica perchè se $u(s) = v(s)$ ed i gradi di $u(x)$ e $v(x)$ sono entrambi minore di n allora $u(s) - v(s) = 0$ e quindi il polinomio $u(x) - v(x)$ è un multiplo di $f(x)$. Poichè il grado di $u(x) - v(x)$ è minore di n deve essere $u(x) - v(x) = 0$, cioè $u(x) = v(x)$ ∎

ESERCIZI 4.13

1) Sia K un campo numerico ed $a \in \mathbb{C}$. Dimostrare che a è algebrico su $K(b)$ per i seguenti valori di b:

$$b = a^3 + 3a - 1; \quad b = \frac{a^3 - 3a + 2}{a - 3}.$$

2) Sia $K \in \mathbb{C}$ un campo, $h(x)$ una funzione razionale non costante su K ed $a \in \mathbb{C}$ un numero su cui $h(x)$ è definito. Provare che i numeri a ed $h(a)$ sono o entrambi algebrici o entrambi trascendenti su K.

3) Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Trovare un elemento $a \in K$ tale che $K = \mathbb{Q}(a)$.
Quali sono gli elementi $b \in K$ tali che $b^2 \in \mathbb{Q}$?

4) Razionalizzare le seguenti frazioni:

$$\frac{1}{\sqrt{2} + \sqrt{3}}; \quad \frac{1}{\sqrt[3]{2} + 1}; \quad \frac{1}{\alpha^2 - \alpha + 1},$$

dove α è radice del polinomio $x^4 - 2x + 2$.

5) Razionalizzare la frazione $1/\pi^3 + \sqrt[2]{\sqrt{\pi} + 3}$ nel campo $\mathbb{Q}(\pi, \sqrt[2]{\sqrt{\pi} + 3})$.

§ 5 IL CRITERIO DI IRRIDUCIBILITA' DI EISENSTEIN

Vogliamo dare ora un criterio che ci permetterà, almeno in qualche caso, di decidere se un dato polinomio è irriducibile.
Premettiamo alcuni lemmi che enunceremo e dimostreremo solo nel caso in cui l'anello base è l'anello degli interi $\mathbb{Z}$. Il lettore che conosca la definizione di anello a fattorizzazione unica si renderà facilmente conto che gli enunciati e le dimostrazioni valgono senza alcuna modifica quando l'anello dei coefficienti sia tale.

SIMBOLI 5.1 $\mathbb{Z}[x]$ denota l'anello dei polinomi a coefficienti interi;
$\mathbb{Q}[x]$ denota l'anello dei polinomi a coefficienti razionali.

DEFINIZIONE 5.2 Sia $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$ un polinomio non nullo. Si chiama *contenuto* di $f(x)$, e si scrive $c(f)$, il massimo comun divisore dei coefficienti a_i. Se $c(f) = 1$ si dice che $f(x)$ è *primitivo*.

PROPRIETA' 5.3 1) $f(x) = c(f)f'(x)$, $f'(x)$ polinomio primitivo

2) $c(af) = ac(f)$, a intero non nullo.

Dimostrazione 1) Sia $f(x) = \sum a_i x^i$, dalla definizione 5.2 segue che $a_i = c(f)a_i'$ ed il massimo comun divisore degli a_i' è 1. Posto $f'(x) = \sum a_i' x^i$ si ha la 1).
2) Sia a un intero non nullo; $af(x) = \sum aa_i x^i$. Il massimo comun divisore dei numeri aa_i è $ac(f)$, pertanto si ha la 2) ▽

LEMMA 5.4 (di Gauss) $c(f \cdot g) = c(f)c(g)$, *cioè il contenuto del prodotto di due polinomi $f(x)$ e $g(x)$ è uguale al prodotto dei contenuti.*

Dimostrazione Usando la 1) della proprietà 5.3 sia per $f(x)$ che per $g(x)$ si ha: $f(x)g(x) = c(f)c(g)f'(x)g'(x)$. Basta quindi provare che il prodotto dei due polinomi primitivi $f'(x)$ e $g'(x)$ è primitivo, cioè, se p è un numero primo qualunque, basta far vedere che p non divide tutti i coefficienti di $f'(x)g'(x)$. Sia dunque

$$f'(x) = a_0' x^m + a_1' x^{m-1} + \ldots + a_m'; \quad g'(x) = b_0' x^n + b_1' x^{n-1} + \ldots + b_n'$$

Dato che i due polinomi scritti sono primitivi, il primo p non divide né tutti gli a_k' né tutti i b_h'. Sia quindi a_i', rispettivamente b_j', il primo degli a_k' (rispettivamente b_h') che non è diviso da p e guardiamo al coefficiente c_{i+j} di x^{i+j} nel prodotto $f'(x)g'(x)$; $c_{i+j} = a_i'b_j' + (\sum_{\substack{s+t=i+j \\ s \neq i, t \neq j}} a_s'b_t')$. Ciascun addendo che figura entro parentesi è divisibile per p; infatti se $s < i$ p divide a_s' e quindi il prodotto $a_s'b_t'$; se $s > i$ allora $t < j$ e p divide il prodotto $a_s'b_t'$ in quanto divide b_t'. Il coefficiente c_{i+j} non è divisibile per p in quanto somma di un termine divisibile per p e di uno, $a_i'b_j'$, non divisibile per p ▽

TEOREMA 5.5 *Se il polinomio $f(x) \in \mathbb{Z}[x]$ si può fattorizzare in $\mathbb{Q}[x]$, allora questi due polinomi possono essere scelti a coefficienti interi.*

Dimostrazione Supponiamo $f(x) = u(x)v(x)$, $u(x)$, $v(x) \in Q[x]$. Sia a (rispettivamente b) un multiplo dei denominatori dei coefficienti di $u(x)$ (rispettivamente di $v(x)$); si ha $abf(x) = abu(x)v(x) = (au(x))(bv(x))$ ed i polinomi $u'(x) = au(x)$ e $v'(x) = bv(x)$ sono entrambi a coefficienti interi. Dalla $abf(x) = u'(x)v'(x)$, passando ai contenuti e tenendo conto della 2) proposizione 5.3 e del lemma 5.4, si ha $abc(f) = c(u')c(v')$. Usando la 1) proposizione 5.3 si ha $u'(x) = c(u')u''(x)$, $v'(x) = c(v')v''(x)$ con $u''(x)$ e $v''(x)$ polinomi primitivi. Sostituendo si ottiene $f(x) = c(f)u''(x)v''(x)$. Ora $u''(x)$, $v''(x) \in \mathbb{Z}[x]$ e $c(f) \in \mathbb{Z}$, quindi il teorema è dimostrato. ▽

TEOREMA (CRITERIO DI IRRIDUCIBILITA' DI EISENSTEIN) 5.6 *Sia* $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots$

$\dots + a_n$ *un polinomio a coefficienti interi. Se esiste un primo* p *tale che* $p \mid a_1, p \mid a_2 \dots$ $\dots\ p \mid a_n$ *ma* $p^2 \nmid a_n$, *allora* $f(x)$ *è irriducibile come polinomio in* $\mathbb{Q}[x]$.

Dimostrazione Se $f(x)$ fosse riducibile, per il teorema 5.5, i due polinomi che lo fattorizzano potrebbero essere scelti a coefficienti interi e quindi della forma:

$$x^m + b_1 x^{m-1} + \dots + b_m;\ x^k + c_1 x^{k-1} + \dots + c_k;\ m,k < n.$$

Dobbiamo quindi provare che è assurda l'uguaglianza $(x_m + b_1 x^{m-1} + \dots + b_m) \cdot (x^k + c_1 x^{k-1} + \dots + c_k) = x^n + a_1 x^{n-1} + \dots + a_n$, nell'ipotesi che esista il primo p soddisfacente alle condizioni date nell'enunciato. Per i coefficienti del polinomio $f(x)$ si hanno le relazioni

$$a_n = b_m c_k;\ a_{n-1} = b_m c_{k-1} + b_{m-1} c_k;\ a_{n-2} = b_m c_{k-2} + b_{m-1} c_{k-1} + b_{m-2} c_k; \dots$$

Poichè $p \mid a_n$ e $p^2 \nmid a_n$ si dovrà avere per esempio che $p \mid c_k$ e $p \nmid b_m$ (oppure il caso simmetrico: $p \mid b_m$, $p \nmid c_k$). Supponiamo di essere in questo caso. Poichè $p \mid a_{n-1}$, $p \mid b_{m-1}\ c_k$ e $p \nmid b_m$ segue che $p \mid c_{k-1}$. Procedendo nello stesso modo si ottiene che $p \mid c_{k-2}$, $p \mid c_{k-3}$,... etc., finchè si arriva al coefficiente a_{n-k} di x^k:

$$a_{n-k} = b_m c_0 + b_{m-1} c_1 + \dots + b_{m-k} c_k,\ c_0 = 1$$

Dato che $k < n$, e quindi $n - k \geq 1$, $p \mid a_{n-k}$; si è già provato che $p \mid c_k, \dots, p \mid c_1$, segue quindi che $p \mid c_0 = 1$. La contraddizione dimostra il teorema □

ESERCIZI 5.7

1) Provare che il polinomio $x^n \pm p$, p primo, è irriducibile.

2) Provare che il polinomio $x^{p-1} + x^{p-2} + x^{p-3} + \dots + x + 1$, p primo, è irriducibile. (Non possiamo applicare direttamente il criterio di Eisenstein a questo polinomio, conviene fare il seguente cambiamento di variabile $x = y + 1$. Si verifichi che il nuovo polinomio in y soddisfa le condizioni di 5.6 etc.).

3) Si considerino i seguenti polinomi monici:

$f(g)$, $g(x) \in \mathbb{Q}[x]$; $h(x) \in \mathbb{Z}[x]$;

Provare che se $h(x) = f(x) \cdot g(x)$, allora $f(x)$ e $g(x)$ sono a coefficienti interi.

§ 6 SPAZI VETTORIALI; DIMENSIONE; ESTENSIONI ALGEBRICHE

In questo paragrafo richiameremo alcune generalità sugli spazi vettoriali, e ci metteremo in ipotesi molto restrittive, per semplificare la trattazione. Le nozioni di spazio vettoriale, dimensione etc., possono darsi in modo astratto, noi ci limiteremo ai sottospazi dei complessi.

DEFINIZIONE 6.1 Sia K un campo di numeri e $V \subset \mathbb{C}$ un insieme non vuoto; diremo che V è uno *spazio vettoriale* su K se dati comunque $v, w \in V, h, k \in K$ si ha $hv + kw \in V$.

DEFINIZIONE 6.2 Siano $v_1, v_2, \dots, v_s \in V$, V spazio vettoriale su K, e $h_1, \dots, h_s \in K$; l'elemento $h_1 v_1 + \dots + h_s v_s \in V$ si chiama *combinazione lineare* degli elementi v_i a coefficienti h_i.

DEFINIZIONE 6.3 1) Un sistema di elementi $v_1, \dots, v_s \in V$ si dice un *sistema di generatori* (ovvero si dice che i v_i *generano* V) se ogni elemento di V è combinazione lineare dei v_i a coefficienti in K.
2) Un sistema di elementi $v_1, \dots, v_s \in V$ si dice *linearmente indipendente* se due combinazioni lineari dei v_i con coefficienti diversi danno luogo ad elementi diversi di V. (Equivalentemente: una combinazione lineare dei v_i è 0 se e solo se i coefficienti sono tutti 0).
3) Un sistema di elementi $v_1, \dots, v_s \in V$ è una *base* di V se è un sistema di generatori linearmente indipendenti.

Osservazione 6.4 Abbiamo dato per semplicità le definizioni 6.2 e 6.3 solo per sistemi finiti di elementi; ma naturalmente, con semplici modifiche, esse si possono estendere a sistemi infiniti.

Enunciamo ora, senza darne la dimostrazione, il seguente fondamentale:

TEOREMA 6.5 *Sia* $V \subset \mathbb{C}$ *uno spazio vettoriale su* K.
a) *Se* $v_1, \dots, v_s \in V$ *sono generatori da essi possiamo estrarre una base* $v_{i_1}, \dots, v_{i_k}$.
b) *Se* $v_1, \dots, v_s$ *e* $w_1, \dots, w_k$, *sono due basi per* V *allora* $s = k$.
c) *Se* $v_1, \dots, v_s$ *sono linearmente indipendenti e* $v_1, \dots, v_s, v_{s+1}, \dots, v_{s+t}$ *generano* V, *allora si possono estrarre elementi* $v_{s+i_1}, \dots, v_{s+i_k}$ *tali che* $v_1, \dots, v_s, v_{s+i_1}, \dots, v_{s+i_k}$ *sono una base.*

Abbiamo enunciato separatamente a) e c) ma il lettore osserverà facilmente che a) è un caso particolare di c). Quindi se V possiede un numero finito di generatori allora possiede una base finita. Inoltre due diverse basi hanno lo stesso numero di elementi. Si pone quindi

la seguente:

DEFINIZIONE 6.6 Se V ammette una base (finita) si chiama *dimensione di V su K*, e si scrive $\dim_K V$, il numero di elementi di una qualunque sua base.
Se V non ha una base finita diremo che $\dim_K V$ è *infinita*.

Esempio 6.7 Se $K \subseteq E$ sono campi di numeri, allora E è uno spazio vettoriale su K.

DEFINIZIONE 6.8 Data l'estensione $K \subseteq E$ si chiama *grado dell'estensione*, e si scrive $[E : K]$, la dimensione di E come spazio vettoriale su K.

Esempio 6.9 Sia $K \subseteq K(a)$ una estensione algebrica semplice e sia n il grado del polinomio minimo di a su K. Possiamo reinterpretare il teorema 4.12, 2) nel modo seguente: il sistema $1,a,a^2,\ldots,a^{n-1}$ è una base di $K(a)$ su K e quindi in particolare $[K(a) : K] = n$. Cioè il grado di una estensione algebrica semplice è uguale al grado del polinomio minimo dell'elemento algebrico mediante il quale si fa l'estensione.

Consideriamo l'estensione $K \subseteq E$ e sia V uno spazio vettoriale su E. Chiaramente V è anche uno spazio vettoriale su K. Vogliamo vedere se ci sono relazioni tra $\dim_K V$, $\dim_E V$ e $[E : K]$.

TEOREMA 6.10 $\dim_E V$ *e* $[E : K]$ *sono finite se e solo se* $\dim_K V$ *è finita. In questo caso si ha:*

$$\dim_K V = [E : K] \dim_E V.$$

Dimostrazione Supponiamo che $\dim_K V = s$ sia finita e sia $v_1,\ldots,v_s \in V$ una base di V su K. Dato che $K \subseteq E$ si ha certamente che i v_i generano linearmente V su E; segue dal teorema 6.5 a) che $\dim_E V \leq s$ e quindi V ha dimensione finita su E. Se $v \in V$, $v \neq 0$, l'insieme $Ev = \{\alpha v \mid \alpha \in E\}$ è uno spazio vettoriale su K e risulta $\dim_K Ev = [E : K]$; poichè inoltre $Ev \subset V$ si ha anche $\dim_K Ev \leq \dim_K V$; quindi $[E : K]$ è finita.
Viceversa sia $v_1,\ldots,v_s$ una base di V su E e sia $a_1,\ldots,a_t$ una base di E su K. Proviamo che il sistema:

$$a_1v_1,\ldots,a_tv_1,a_1v_2,\ldots,a_tv_2,\ldots,a_1v_s,\ldots,a_tv_s$$

è una base di V su K. Sia $w \in V$ un elemento qualunque, esso si scrive $w = \sum_i \alpha_i v_i$, $\alpha_i \in E$, nella base $\{v_i\}$; inoltre $\alpha_i = \sum_j k_{ij}a_j$, $k_{ij} \in K$, nella base $\{a_j\}$, dunque $w = \sum_{i,j} k_{ij}(a_jv_i)$ da cui segue che gli elementi a_jv_i sono un sistema di generatori di V su K. Resta da provare che sono linearmente indipendenti. Infatti se $\sum_{i,j} h_{ij}a_jv_i = 0$, $h_{ij} \in K$, posto $\beta_i = \sum_j h_{ij}a_j$, si ha che $\beta_i \in E$ e $\sum_i \beta_i v_i = 0$. Poichè i v_i sono linearmente indipendenti deve aversi $\beta_i = 0$ per ogni i. Da questo deduciamo $\sum_j h_{ij}a_j = 0$ e per l'indipendenza degli a_j deduciamo che $h_{ij} = 0$ per ogni i e per ogni j.
La relazione sulle dimensioni è ora ovvia, visto che abbiamo scritto una base esplicita di

V su K ed il teorema è completamente dimostrato. ▽△

Osservazione 6.11 La relazione $\dim_K V = [E : K] \dim_E V$ è valida più in generale, senza assumere che i numeri in questione siano finiti, ma interpretando la dimensione come numero cardinale; la dimostrazione è esattamente la stessa.

COROLLARIO 6.12 *Se* $K \subseteq E \subseteq F$ *sono campi allora* $[F : K] = [F : E][E : K]$

COROLLARIO 6.13 *Se* $E \supseteq K$ *è un'estensione di campi e se* $[E : K]$ *è un numero finito allora:*
1) *ogni elemento* $a \in E$ *è algebrico su* K.
2) *Il grado del polinomio minimo di* a *su* K *divide* $[E : K]$.

Dimostrazione 1) Sia $a \in E$; gli elementi $1,a,a^2,a^3,\ldots,a^n \in E$ non possono essere linearmente indipendenti su K, per ogni n, perchè $\dim_K E = [E : K]$ è finita; quindi per un qualche n deve sussistere una relazione del tipo $\sum_{i=0}^{n} \alpha_i a^i = 0$, ove gli $\alpha_i \in K$ non sono tutti nulli. Questo prova che a è algebrico su K.

2) Poichè E è un campo si ha: $K \subseteq K(a) \subseteq E$, da cui $[E : K] = [K(a) : K][E : K(a)]$ (corollario 6.12). Quindi $[K(a) : K]$ divide $[E : K]$; d'altra parte $[K(a) : K]$ è proprio il grado del polinomio minimo di a su K (esempio 6.9).

Siamo ora in grado di motivare il fatto di aver chiamato *estensione algebrica semplice* la estensione $K \subseteq K(s)$ di K tramite l'elemento s algebrico su K. Infatti dall'esempio 6.9 segue che $[K(s) : K]$ è finito e quindi il corollario ora provato ci dice che ogni elemento di $K(s)$ è algebrico su K. Pertanto l'estensione $K \subseteq K(s)$ è algebrica nel senso della definizione 3.1 d).

Osservazione 6.14 Sia $K \subseteq E$ un'estensione di campi e sia a un numero (non necessariamente in E) algebrico su K. Ovviamente a è anche algebrico su E, visto che ogni polinomio a coefficienti in K è in particolare un polinomio a coefficienti in E. Il polinomio minimo dello elemento a su K è irriducibile in $K[x]$ ma non è affatto detto che sia irriducibile come polinomio in $E[x]$. In generale il polinomio minimo di a su E è un divisore del polinomio minimo di a su K. Quindi il grado di a su E è minore o uguale al grado di a su K.
Un esempio banale di quanto affermato è il seguente: se $a \in E$, $a \notin K$ il polinomio minimo $f(x) \in K[x]$ di a su K non è di grado 1 (altrimenti $a \in K$!). Considerato come polinomio in $E[x]$ esso è divisibile per il polinomio $x - a$ che è il polinomio minimo di a su E.
Un'altro esempio per illustrare la situazione è il seguente. Consideriamo il polinomio $x^4 - 2$, che è irriducibile sui razionali (criterio di Eisenstein 5.6), e pertanto è il polinomio minimo su $\mathbb{Q}$ di ciascuna delle sue radici: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$, (cfr. proposizione 4.6). Consideriamo l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$; il polinomio $x^4 - 2$ si fattorizza in $\mathbb{Q}(\sqrt[4]{2})$ nel modo seguente: $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt[2]{2})$ (verificare che $x^2 + \sqrt[2]{2}$ è a coefficienti in $\mathbb{Q}(\sqrt[4]{2})$ ed è ivi irriducibile!)

Concludendo, se consideriamo l'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ e l'elemento $a = i\sqrt[4]{2} (\notin \mathbb{Q}(\sqrt[4]{2}))$, esso è algebrico su $\mathbb{Q}$ ed ha come polinomio minimo $x^4 - 2 \in \mathbb{Q}[x]$ il quale è irriducibile in $\mathbb{Q}$ ma si fattorizza in $\mathbb{Q}(\sqrt[4]{2})$. Il polinomio minimo di a su $\mathbb{Q}(\sqrt[4]{2})$ è $x^2 + \sqrt{2}$.

PROPOSIZIONE 6.15 *Se K è un campo ed $a_1,\dots,a_s$ sono numeri algebrici su K, allora l'estensione $K \subseteq K(a_1,\dots,a_s) = E$ di K tramite gli elementi a_i è di dimensione finita. Se indichiamo con n_i il grado del polinomio minimo di a_i su K, si ha:*

$$[E : K] \leq n_1 n_2 \dots n_s.$$

Dimostrazione Consideriamo la catena di estensioni semplici:

$$K \subseteq K(a_1) \subseteq K(a_1)(a_2) \subseteq \dots \subseteq K(a_1)(a_2)(a_3)\dots(a_s) = K(a_1,\dots,a_s).$$

Ciascuna delle estensioni semplici $K(a_1)(a_2)\dots(a_{i-1})(a_i)$ è algebrica in quanto l'elemento a_i è algebrico su $K(a_1)(a_2)\dots(a_{i-1})$ ed il grado del suo polinomio minimo su questo campo è minore o uguale al grado del polinomio minimo su K (cfr. osservazione 6.14). Quindi risulta:

$$[K(a_1)(a_2)\dots(a_{i-1})(a_i) : K(a_1)(a_2)\dots(a_{i-1})] \leq n_i$$

Applicando ripetutamente la formula del corollario 6.12 si ha

$$[K(a_1,\dots,a_s) : K] \leq n_1 n_2 \dots n_s \quad \nabla\Delta$$

La proposizione 6.15 può essere invertita nel senso che:

PROPOSIZIONE 6.16 *Se $K \subseteq E$ è un'estensione di campi di dimensione finita allora si possono trovare elementi $a_1,\dots,a_s \in E$ tali che $E = K(a_1,\dots,a_s)$.*

Dimostrazione Basta prendere elementi che generino linearmente E come spazio vettoriale su K, questi stessi a maggior ragione generano E come campo $\nabla\Delta$
Naturalmente la condizione per gli elementi $a_1,\dots,a_s$ di generare E come estensione (cfr. 4.2) è molto più debole della condizione di generare E linearmente. Infatti nel primo caso ciò che si richiede è che ogni elemento di E si scriva come funzione razionale in $a_1,\dots,a_s$ (polinomio se $K \subseteq E$ è algebrico), mentre nel secondo caso si richiede che ogni elemento di E si esprima come combinazione lineare di $a_1,\dots,a_s$, cioè con un polinomio di primo grado. Vedremo in seguito (proposizione 9.4) che in effetti esiste un elemento $a \in E$ tale che $E = K(a)$.

COROLLARIO 6.17 i) *Se $K \subseteq E$ e $E \subseteq F$ sono estensioni algebriche allora $K \subseteq F$ è un'estensione algebrica.*
ii) *Se $K \subseteq E$ è un'estensione e $\overline{K} = \{a \in E \mid a$ è algebrico su $K\}$ allora $\overline{K}$ è un campo. In particolare l'insieme di tutti i numeri algebrici è un campo.*

Dimostrazione i) Sia $a \in F$; poichè a è algebrico su E si ha $\sum_{i=0}^{m} \alpha_i a^i = 0$ per opportuni $\alpha_i \in E$ e non tutti nulli. Sia $\widetilde{E} = K(\alpha_1,\dots,\alpha_m)$; poichè gli α_i sono algebrici su K si ha che

$\dim_K \widetilde{E}$ è finita, (cfr. 6.15). Il polinomio $\sum_{i=0}^{m} \alpha_i x^i$ è a coefficienti in $\widetilde{E}$ e quindi a è algebrico su $\widetilde{E}$; ne segue (sempre per 6.15) che $\dim_{\widetilde{E}} \widetilde{E}(a)$ è finita. Per le dimensioni delle seguenti estensioni: $K \subseteq \widetilde{E} \subseteq \widetilde{E}(a)$ si ha la relazione $[\widetilde{E}(a) : K] = [\widetilde{E}(a) : \widetilde{E}][\widetilde{E} : K]$ e quindi $[\widetilde{E}(a) : K]$ è finita. Il corollario 6.13, 1) permette di concludere allora che a è algebrico su K.
ii) Siano $a,b \in \overline{K}$, allora il campo $K(a,b)$ è di dimensione finita su K (cfr.6.15). Segue, sempre dal corollario 6.13, che gli elementi $a+b$, $a-b$, ab, $a/b \in K(a,b)$ sono algebrici su K e quindi che appartengono a $\overline{K}$ $\nabla\Delta$

DEFINIZIONE 6.18 Sia K un campo di numeri, si chiama *chiusura algebrica* di K in $\mathbb{C}$ l'insieme $\overline{K} = \{a \in \mathbb{C} \mid a$ è algebrico su $K\}$.

ESERCIZI 6.19

1) Sia K un campo di numeri e $\overline{K}$ la sua chiusura algebrica su $\mathbb{C}$. Dimostrare che:
   1) Se $a \in \mathbb{C}$ è algebrico su $\overline{K}$ allora $a \in \overline{K}$
   2) Se $f(x) \in \overline{K}[x]$ è un polinomio, allora $f(x)$ si spezza su $\overline{K}$ in fattori lineari.

2) Sia a algebrico su K ed E un'estensione di K. Dimostrare che nei due casi seguenti il polinomio minimo di a su K è anche polinomio minimo su E:
   α) $[E : K]$ è primo con il grado di a su K
   β) $E = K(s)$ con s trascendente.

3) Si consideri l'estensione $E = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Determinare il grado dell'estensione su $\mathbb{Q}$ e quali sono gli elementi di grado 2.

§ 7 COSTRUZIONI EUCLIDEE E NUMERI EUCLIDEI

Vogliamo applicare la teoria fino ad ora sviluppata per risolvere alcuni problemi classici dell'antichità, per dimostrare cioè l'impossibilità di effettuare alcune costruzioni facendo uso solo della riga e del compasso. Dobbiamo pertanto dare una definizione di "costruzione con riga e compasso" sufficientemente precisa da permetterci di operare con essa e che nello stesso tempo sia la traduzione formale di ciò che tutti intuitivamente intendiamo.

Il dato iniziale è un sistema di riferimento nel piano che per noi può consistere semplicemente nell'assegnare un segmento unità, cioè due punti 0,U (come si vedrà nell'esempio 7.2).

DEFINIZIONE 7.1 Una *costruzione euclidea (con riga e compasso)* è una successione $K_1, K_2, \dots, K_i, \dots, K_n$, dove K_i $(i = 1,2,\dots,n)$ è un punto o una retta o una circonferenza, ed

in modo tale che siano verificate le seguenti proprietà:

1) Se K_i è una retta, allora K_i deve essere la retta per due punti distinti K_s e K_t già costruiti (cioè $s,t<i$).

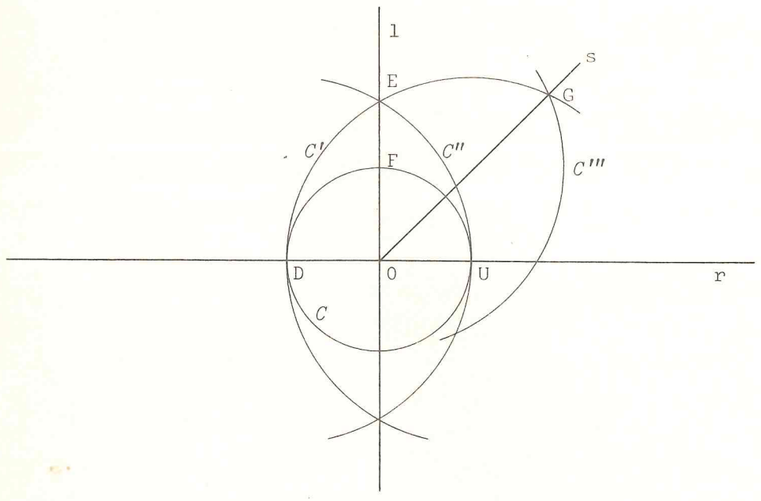
2) Se K_i è una circonferenza allora deve essere la circonferenza di centro K_s e raggio il segmento di estremi K_u,K_t, dove K_s,K_u,K_t sono punti già costruiti (cioè $s,u,t<i$).

3) Se K_i è un punto si possono presentare tre eventualità: I) $K_i=0$ oppure $K_i=U$ (i punti dati inizialmente); II) K_i deve essere il punto di intersezione di due rette distinte K_s e K_t già costruite ($s,t<i$); III) K_i deve essere uno dei due punti di intersezione di due circonferenze o di una circonferenza e di una retta, K_s,K_t, già costruite (cioè $s,t<i$).

Cerchiamo di renderci conto su esempi che la definizione ha senso e che dà una traduzione formale di ciò che intendiamo per costruzione euclidea.

Esempi 7.2 1) Un sistema di assi cartesiani di origine O, unità di misura OU è ottenibile con una costruzione euclidea.

La successione per la prima costruzione è: O,U,r,C,D,C',C'',E,l, dove r è la retta per i punti O ed U; C è la circonferenza di centro O e raggio OU; D è l'ulteriore punto di intersezione di C ed r; C' è la circonferenza di centro U e raggio DU; C'' è la circonferenza di centro D e raggio DU; E è uno dei due punti di intersezione di C' e C'', l è la retta per i punti E ed O.



2) La bisettrice di un quadrante è ottenibile con una costruzione euclidea. Per costruire la bisettrice di $U\hat{O}E$ si continua la costruzione precedente con ...,l,F,C''',G,s, dove F è uno dei punti di intersezione di C ed l, quello appartenente al segmento OE, C''' è la circonferenza di centro F e raggio DU; G è un punto di intersezione fra C''' e C'; s la retta per OG.

Si vede bene in questo esempio come ogni passo della costruzione sia fatto tramite i precedenti, secondo la ricetta data nella definizione.

3) La parallela per un punto ad una retta data è costruibile con riga e compasso. (Si può ottenere con due perpendicolari!).

4) Dati due segmenti di lunghezza rispettivamente a e b si possono costruire con riga e compasso segmenti di lunghezza $a+b$, $a-b$, a^{-1} etc. (si usi 3) ed il teorema di Talete!).

DEFINIZIONE 7.3 1) Un *punto* P del piano si dice *euclideo* se compare in una costruzione euclidea.

2) Un *numero complesso* $a+ib$ si dice *euclideo* se il punto $P\equiv(a,b)$ di coordinate a e b (nel sistema di assi associato ai punti O,U inizialmente dati) è un punto euclideo.

TEOREMA 7.4 *Un numero complesso* α *è euclideo se e solo se esiste una successione di campi* $\mathbb{Q}=E_0\subseteq E_1\subseteq\ldots\subseteq E_m$ *tale che*

1) $\alpha\in E_m$

2) $[E_{j+1}:E_j]\leq 2$ *per* $j=0,1,\ldots,m-1$.

Dimostrazione Supponiamo che il numero $\alpha=a+ib$ sia euclideo ed indichiamo con $K_1,K_2,\ldots,K_n=P\equiv(a,b)$ una costruzione euclidea per il punto $P\equiv(a,b)$ associato ad α.

Si tratta ora di costruire una successione di campi $E_0=\mathbb{Q}\subseteq E_1\subseteq\ldots\subseteq E_{n+1}$ soddisfacenti le condizioni 1) e 2). Procederemo per induzione. Supponiamo di aver già costruito il campo E_j e facciamo vedere come da esso si costruisce il campo E_{j+1}. Consideriamo l'elemento K_{j+1} della costruzione di $P\equiv(a,b)$: se K_{j+1} è una retta oppure una circonferenza poniamo $E_{j+1}=E_j$; se K_{j+1} è un punto di coordinate (c,d), poniamo $E_{j+1}=E_j(c,d)$ (l'estensione di E_j con i numeri c e d). Da ultimo poniamo $E_{n+1}=E_n(i)$ (estensione del campo E_n con l'unità immaginaria i). Poichè $K_n=P\equiv(a,b)$, la costruzione data implica che $a,b\in E_n=E_{n-1}(a,b)$; inoltre $i\in E_{n+1}$ quindi $\alpha=a+ib\in E_{n+1}$ e la condizione 1) è provata.

Per far vedere che $[E_{j+1}:E_j]\leq 2$, per ogni j, procederemo ancora per induzione. Proviamo innanzi tutto che se K_j è una retta oppure una circonferenza allora la sua equazione cartesiana può essere scelta con coefficienti in E_j. Sia per esempio K_j la retta per i due punti K_s e K_t, $s,t<j$. Le coordinate di K_s e K_t sono nel campo E_j; per scrivere l'equazione di K_j si deve operare razionalmente sulle coordinate dei punti K_s e K_t, secondo la ben nota formula della geometria analitica, e quindi tale equazione ha coefficienti in E_j. Analogamente se K_j è la circonferenza di centro il punto K_s e raggio il segmento di estremi K_u, K_t ($s,u,t<j$) una sua equazione si ottiene operando razionalmente sulle coordinate dei punti K_s,K_u,K_t che sono in E_j. Passiamo ora alle dimostrazioni di 2). Per l'estensione $E_n\subseteq E_{n+1}=E_n(i)$ si ha $[E_{n+1}:E_n]=2$ visto che $i^2+1=0$.

Se K_j è una retta oppure una circonferenza, allora $E_j=E_{j-1}$ e quindi $[E_j:E_{j-1}]=1$.

Se K_j è un punto allora si hanno tre casi. I) K_j è il punto di intersezione di due rette K_s,K_t ($s,t<j$). Da quanto visto precedentemente le equazioni di K_s e K_t sono a coefficienti

in E_j pertanto le coordinate di K_j, che si ottengono risolvendo un sistema di due equazioni di primo grado, si esprimono razionalmente tramite i coefficienti delle equazioni di K_s e K_t; le coordinate di K_j sono dunque in E_j e quindi $E_{j+1} = E_j$, da cui ancora $[E_{j+1} : E_j] = 1$

II) K_j è uno dei punti di intersezione della retta K_s e della circonferenza K_t, $s,t < j$, di equazioni rispettivamente:

$$K_s: ax + by + c = 0; \quad K_t: x^2 + y^2 + dx + ey + f = 0, \quad \text{con } a,b,c,d,e,f \in E_j$$

per l'ossevazione che abbiamo preliminarmente fatto.

Le coordinate di K_j si ottengono dalla risoluzione del sistema delle due equazioni scritte; se per esempio $a \neq 0$ (analogamente si fa se $b \neq 0$) sostituendo la $x = -(b/a)y - c/a$ nella equazione della circonferenza si perviene ad una equazione di secondo grado in y, del tipo $y^2 + ly + m = 0$, a coefficienti in E_j (le cui soluzioni forniscono le ordinate dei due punti di intersezione di K_s e K_t, uno dei quali è K_j). L'equazione $y^2 + ly + m = 0$ è risolubile in E_j se e solo se il corrispondente polinomio è riducibile su E_j; in questa eventualità ancora $E_{j+1} = E_j$. Altrimenti le radici $y_1 = (-l + \sqrt{l^2 - 4m})/2$, $y_2 = (-l - \sqrt{l^2 - 4m})/2$ sono nel campo $E_j(\sqrt{l^2 - 4m})$ il quale è un'estensione quadratica di E_j. E' subito visto d'altra parte che $E_{j+1} = E_j(\sqrt{l^2 - 4m})$; infatti, posto che il punto K_j corrisponda all'ordinata y_1, la sua ascissa $x_1 = -(b/a)y_1 - c/a$ appartiene, come y_1, al campo $E_j(\sqrt{l^2 - 4m})$, e chiaramente $E_{j+1} = E_j(x_1, y_1) = E_j(\sqrt{l^2 - 4m})$.

III) K_j è uno dei punti di intersezione delle circonferenze K_s, K_t, $s,t < j$. Il ragionamento è ora del tutto analogo al caso II), in quanto dal sistema:

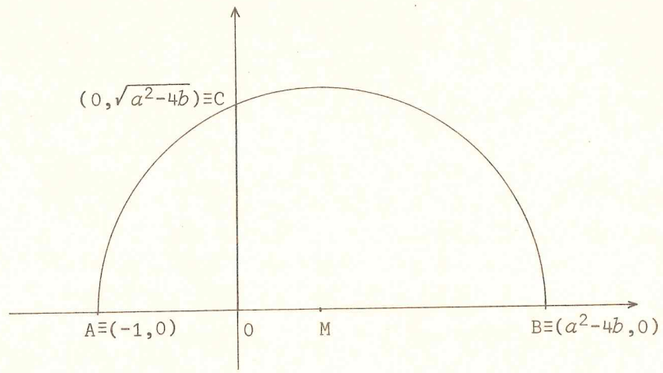
$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases} \qquad a,b,c,d,e,f \in E_j$$

si deduce subito il sistema equivalente

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ (a-d)x + (b-e)y + c - f = 0. \end{cases}$$

Per completare la dimostrazione del teorema, dobbiamo far vedere che se $\alpha \in E_m \supseteq E_{m-1} \supseteq \ldots \supseteq E_0 = \mathbb{Q}$ ed $[E_{j+1} : E_j] \leqslant 2$ allora α è euclideo. Se $\alpha \in \mathbb{Q}$, è ben noto che la costruzione di un punto sull'asse OU e con ascissa razionale si può eseguire con riga e compasso. Procediamo allora per induzione; supponiamo di avere mostrato come si costruiscono i punti sull'asse OU aventi per ascissa i numeri $\beta \in E_j$ e passiamo a costruire i punti che hanno ascissa $\gamma \in E_{j+1}$. Poichè $[E_{j+1} : E_j] \leqslant 2$ segue che γ è algebrico su E_j di grado 1 o 2 (cfr. corollario 6.13). Se il grado di γ è 1, allora $\gamma \in E_j$ e si sa già costruire. Se il grado di γ è 2, esso verifica un'equazione del tipo $x^2 + ax + b = 0$, $a,b \in E_j$. Limitiamoci per brevità al caso in cui γ, a, b sono tutti reali, gli altri casi si riducono infatti facilmente a questo e li lasciamo per esercizio. Si ha $\gamma = (-a \pm \sqrt{a^2 - 4b})/2$, $a^2 - 4b > 0$ (se $a^2 - 4b = 0$ allora $\alpha \in E_j$). Costruiamo allora con riga e compasso un segmento di lunghezza $a^2 - 4b$ (si sa fare visto che

$a^2 - 4b \in E_j$), e successivamente usiamo la ben nota costruzione, che diamo in figura, per ottenere il segmento OC di lunghezza $\sqrt{a^2 - 4b}$.



Da questo si costruisce facilmente il punto P sull'asse OU avente per ascissa γ. Il teorema è ora completamente dimostrato. ∇Δ

Un importante corollario del teorema 7.4 è il seguente:

COROLLARIO 7.5 *Se $\alpha \in \mathbb{C}$ è euclideo, allora α è un numero algebrico di grado 2^k, per un opportuno naturale k.*

Dimostrazione Tenendo conto della formula data in 6.12 si ha per la successione di campi $\mathbb{Q} = E_0 \subseteq \ldots \subseteq E_m$ determinata da α (teorema 7.4), $[E_m : \mathbb{Q}] = 2^s$ per un s opportuno. Per il corollario 6.13 si ha che $\alpha \in E_m$ è algebrico ed il suo grado divide 2^s, cioè è della forma 2^k. ∇Δ

Passiamo a dare alcune applicazioni del corollario 7.5.

APPLICAZIONI 1) *Impossibilità di rettificare la circonferenza con riga e compasso.* Il problema si riduce a rettificare la circonferenza di raggio 1 e quindi a costruire un segmento di lunghezza 2π (ovvero π). Se una tale costruzione esistesse, per 7.6 seguirebbe che π è un numero algebrico (di grado 2^k). La trascendenza di π (cfr. nota storica 3.4) implica che tale costruzione è impossibile.

2) *Impossibilità di duplicare il cubo con riga e compasso.* Il problema è il seguente: dare una costruzione con riga e compasso del lato di un cubo che abbia volume doppio di quello di un cubo assegnato. Naturalmente si può assumere che il cubo assegnato abbia lato unitario, quindi il lato del cubo di volume 2 è $\sqrt[3]{2}$. Ma $\sqrt[3]{2}$ è un numero algebrico di grado 3, e 3 non è una potenza di 2, pertanto, sempre dal corollario 7.5, segue che non si può costruire con riga e compasso un segmento di lunghezza $\sqrt[3]{2}$.

3) *Impossibilità di costruire con riga e compasso i poligoni regolari con 7, 9, 11, 13 lati.*

Discussione generale del problema. Ci proponiamo qui di discutere il seguente:

PROBLEMA 7.6 Per quali numeri interi n è possibile costruire con riga e compasso il poligono regolare di n lati?

Questo problema è detto *problema della ciclotomia*, dal greco *kýklos* 'cerchio' e *tomḗ* 'taglio'.

Consideriamo nel piano la circonferenza di centro O e raggio OU e simultaneamente identifichiamo, tramite il riferimento assegnato, i punti del piano con i numeri complessi. Supponiamo che la circonferenza sia divisa in n parti uguali, e a partire dal punto $U \equiv (1,0)$. I punti di divisione che sono anche i vertici del poligono regolare con n lati, hanno per argomento: $0, 2\pi/n, 2\cdot 2\pi/n, 3\cdot 2\pi/n, \ldots, (n-1)2\pi/n$; essi si rappresentano come numeri complessi nella forma: $\cos(k\,2\pi/n) + i \operatorname{sen}(k\,2\pi/n)$ $k = 0,1,\ldots,n-1$. Indichiamo con $\varepsilon = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$; per la ben nota formula si ha che $\varepsilon^k = \cos(k\,2\pi/n) + i \operatorname{sen}(k\,2\pi/n)$. I vertici del poligono regolare di n lati si scrivono quindi, sotto forma complessa, con le potenze $\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{n-1}, \varepsilon^n = 1$, e la possibilità di costruire con riga e compasso un tale poligono è equivalente al fatto che il numero ε sia euclideo.
Il numero ε e le sue potenze ε^k $(k = 0,\ldots,n-1)$ sono soluzioni dell'equazione $x^n - 1 = 0$ (infatti $(\varepsilon^k)^n = (\varepsilon^n)^k = 1$) e sono radici distinte, quindi $x^n - 1 = \prod_{i=1}^{n} (x - \varepsilon^i)$. In particolare ε è un numero algebrico. Per quali numeri n il numero $\varepsilon = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$ è anche euclideo? Il corollario 7.5 ci riconduce a studiare il grado e quindi il polinomio minimo.
Il numero n si scrive in modo unico, mediante la fattorizzazione in numeri primi, come $n = p_1^{k_1} \cdot p_2^{k_2} \ldots p_r^{k_r}$ (p_i primo).
Cominciamo a discutere il problema nel caso $n = p^k$, con p primo; vedremo in seguito (osservazione 7.11 e corollario 7.12) come da questo si deduce il caso generale.

Caso $n = p^k$, con p numero primo. Il polinomio $x^n - 1 = x^{p^k} - 1$ è riducibile e si fattorizza in:

$$x^{p^k} - 1 = (x^{p^{k-1}} - 1)\left[(x^{p^{k-1}})^{p-1} + (x^{p^{k-1}})^{p-2} + \ldots + (x^{p^{k-1}}) + 1\right] = (x^{p^{k-1}} - 1)\,\varphi_{p^k}(x)$$

ove $\varphi_{p^k}(x)$ denota il secondo fattore (tra parentesi quadre).
Proviamo che ε è radice di $\varphi_{p^k}(x)$. Infatti $\varepsilon^{p^{k-1}} = \cos(p^{k-1}\,2\pi/p^k) + i \operatorname{sen}(p^{k-1}\,2\pi/p^k) = \cos 2\pi/p + i \operatorname{sen} 2\pi/p \neq 1$, quindi da $0 = \varepsilon^{p^k} - 1 = (\varepsilon^{p^{k-1}} - 1)\varphi_{p^k}(\varepsilon)$ si ha $\varphi_{p^k}(\varepsilon) = 0$.
Proviamo ora che $\varphi_{p^k}(x)$ è irriducibile sui razionali. Poichè non possiamo fare direttamente uso del criterio di Eisenstein, eseguiamo il cambiamento di variabili $x = y + 1$, ottenendo il polinomio $g(y) = \varphi_{p^k}(y+1) = [(y+1)^{p^{k-1}}]^{p-1} + [(y+1)^{p^{k-1}}]^{p-2} + \ldots + [(y+1)^{p^{k-1}}] + 1 =$

$$= y^{(p-1)p^{k-1}} + \sum_{i<(p-1)p^{k-1}} a_i y^i .$$

Se $g(y)$ è irriducibile tale è anche $\varphi_{p^k}(x)$. L'idea è quindi di verificare le condizioni del criterio di Eisenstein sul polinomio $g(y)$. A tal scopo premettiamo il seguente:

LEMMA 7.7 *Sia p un primo, s un naturale e si consideri la potenza:* $(x_1 + \ldots + x_m)p^s$. *Nell'espansione tutti i coefficienti dei monomi nelle x_j sono divisibili per p tranne quelli degli* $(x_i)p^s$ *che valgono* 1. (Rinviamo la dimostrazione alla fine del paragrafo, per non perdere troppo il filo del discorso).

Sostituiamo, nell'espressione $(x^{p^k} - 1) = (x^{p^{k-1}} - 1)\varphi_{p^k}(x)$, $x = y+1$; si ha: $(y+1)^{p^k} - 1 = [(y-1)^{p^{k-1}} - 1]g(y)$. Facendo uso del lemma 7.7 possiamo scrivere:

$$(y+1)^{p^k} - 1 = y^{p^k} + ph(y); \qquad (y+1)^{p^{k-1}} - 1 = y^{p^{k-1}} + pl(y)$$

con $h(y)$ ed $l(y)$ polinomi a coefficienti interi. Sostituendo si ottiene:

$$(y^{p^k} + ph(y)) = (y^{p^{k-1}} + pl(y))g(y)$$

cioè

$$y^{p^k} = y^{p^{k-1}} g(y) + pr(y), \text{ ove si è posto } r(y) = l(y)g(y) - h(y).$$

Sostituendo in quest'ultima relazione l'espressione di $g(y)$ si ricava: $\sum_{i<(p-1)p^{k-1}} a_i y^i = -pr(y)$, da cui si deduce che tutti i coefficienti a_i del polinomio $g(y)$ (escluso il coefficiente direttore) sono divisibili per p. Per poter applicare il criterio di Eisenstein si deve ancora provare che il termine costante non è divisibile per p^2. Calcoliamo esplicitamente tale termine costante che risulta uguale a $g(0)$:

$$g(0) = [(0+1)^{p^{k-1}}]^{p-1} + [(0+1)^{p^{k-1}}]^{p-2} + \ldots + [(0+1)^{p^{k-1}}] + 1 = p$$

Il polinomio $g(y)$ è pertanto irriducibile.
Concludendo: il polinomio $\varphi_{p^k}(x)$ è il polinomio minimo (su $\mathbb{Q}$) del numero $\varepsilon = \cos 2\pi/p^k + i \operatorname{sen} 2\pi/p^k$ e quindi:

COROLLARIO 7.8 $\varepsilon = \cos 2\pi/p^k + i \operatorname{sen} 2\pi/p^k$ *è un numero algebrico di grado* $(p-1)p^{k-1}$.

Proviamo ora il seguente:

COROLLARIO 7.9 *Se* $\varepsilon = \cos 2\pi/p^k + i \operatorname{sen} 2\pi/p^k$ *è euclideo allora o* $p = 2$ *oppure se* $p \neq 2$ *si deve avere* $k = 1$ *e p deve essere un primo della forma* $p = 2^{2^m} + 1$.

Dimostrazione Se ε è euclideo, il suo grado deve essere una potenza di due (cfr. corollario 7.5), cioè $(p-1)p^{k-1} = 2^t$, con t opportuno. Se $p \neq 2$ allora si deve avere $k-1 = 0$, cioè $k = 1$; inoltre $p-1 = 2^t$ da cui $p = 2^t + 1$. Scriviamo il naturale t nella forma $t = 2^m l$, con l dispari, si ha: $p = 2^{2^m l} + 1$. Poniamo per comodità di notazione, $2^{2^m} = a$ ed

osserviamo che $a^l + 1$, per l dispari, si fattorizza: $a^l + 1 = (a+1)(a^{l-1} - a^{l-2} + \ldots + 1)$. Perchè $a^l + 1$ sia un primo si deve avere o $a = 0$ oppure $l = 1$. Nel nostro caso a non è nullo e quindi $l = 1$. Segue quindi che $p = 2^{2^m} + 1$. ∇Δ

Osservazione 7.10 I numeri della forma $2^{2^m} + 1$ si chiamano numeri di Fermat, dal nome di colui che per primo li introdusse. Essi non sono necessariamente numeri primi. Per $m = 0,1,2,3,4$ si hanno rispettivamente i numeri: 3, 5, 17, 257, 65537 e sono primi.
Nel 1732 Eulero dimostrò che per $m = 5$ non si ottiene un primo, infatti $2^{2^5} + 1 = 641 \times 6700417$.
E' stato dimostrato in seguito che per:

$m = 6,7,8,9,11,12,18,23,36,38,73$

i numeri corrispondenti non sono primi.
Non è attualmente noto né se esistano infiniti numeri di Fermat primi, né se i numeri di Fermat che non sono primi siano essi infiniti.

Osservazione 7.11 Sia $n = hk$, con h e k primi fra loro. Se si possono costruire con riga e compasso i poligoni con h e k lati allora si può costruire con riga e compasso anche il poligono di n lati.
Dimostrazione Sia $\varepsilon_h = \cos 2\pi/h + i \operatorname{sen} 2\pi/h$, $\varepsilon_k = \cos 2\pi/k + i \operatorname{sen} 2\pi/k$ e siano a e b due interi tali che $ak + bh = 1$ (essendo h e k primi fra loro tali interi esistono e si possono trovare facendo uso del metodo di Euclide delle divisioni successive). I numeri

$$\varepsilon_h^a = \cos a\, 2\pi/h + i \operatorname{sen} a\, 2\pi/h; \quad \varepsilon_k^b = \cos b\, 2\pi/k + i \operatorname{sen} b\, 2\pi/k$$

si possono costruire con riga e compasso a partire da ε_h ed ε_k; pertanto il prodotto $\varepsilon_h^a \cdot \varepsilon_k^b$ si può costruire anch'esso con riga e compasso.
Dal calcolo: $\varepsilon_h^a \cdot \varepsilon_k^b = \cos(a/h + b/k)\, 2\pi + i \operatorname{sen}(a/h + b/k)\, 2\pi = \cos 2\pi/h + i \operatorname{sen} 2\pi/h = \varepsilon_h$ segue la tesi. ∇Δ
Il corollario 7.9 e l'osservazione 7.11 permettono immediatamente di dedurre una condizione necessaria affinchè la risposta al problema 7.6 sia affermativa, nel caso generale di $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $p_1, p_2, \ldots, p_r$ primi. La riassumiamo nel seguente:

COROLLARIO 7.12 *Se un poligono di n lati è costruibile con riga e compasso allora tutti i primi dispari della fattorizzazione di n devono essere primi della forma* $2^{2^k} + 1$ *e devono apparire con esponente* 1 *(nella fattorizzazione medesima).*

Segue subito, tenuto conto dell'osservazione 7.10, che non si possono costruire con riga e compasso i poligoni di 7, 9, 11, 13 lati.

Osservazione 7.13 La condizione enunciata è anche sufficiente (fu dimostrata da Gauss nei suoi lavori sulla ciclotomia). Noi la proveremo come conseguenza della teoria di Galois che svilupperemo in seguito (cfr. §11, pagina 42).

Prima di concludere questo paragrafo diamo la dimostrazione del lemma 7.7.

Dimostrazione (di 7.7) Procediamo per doppia induzione su s ed m.
a) Sia $s = 1$ ed $m = 2$, siamo cioè nel caso:

$$(x_1 + x_2)^p = \sum_{h=0}^{p} \binom{p}{h} x_1^h x_2^{p-h} = x_1^p + \sum_{h=1}^{p-1} \binom{p}{h} x_1^h x_2^{p-h} + x_2^p.$$

Il numero $\binom{p}{h} = (p(p-1)!)/(h!(p-h)!)$ è un intero, quindi i fattori primi del denominatore devono tutti cancellarsi con fattori primi del numeratore. Per $1 \leq h \leq p-1$ si ha $h < p$, $p-h < p$ e poichè p è primo segue $p \nmid h!$ e $p \nmid (p-h)!$.
Il denominatore $h!(p-h)!$ deve quindi cancellarsi con fattori di $(p-1)!$ e $((p-1)!)/(h!(p-h)!)$ è un intero. Pertanto $p \mid \binom{p}{h}$ ed in questo caso il lemma è provato.
b) Usiamo ora l'induzione su m, e per $s = 1$:

$$(x_1 + x_2 + \ldots + x_m)^p = [(x_1 + x_2 + \ldots + x_{m-1}) + x_m]^p = (x_1 + x_2 + \ldots + x_{m-1})^p + x_m^p + \text{termini con}$$

coefficiente multiplo di p (questo per quanto provato in a)). Per induzione $(x_1 + x_2 + \ldots + x_{m-1})^p = x_1^p + \ldots + x_{m-1}^p$ + termini con coefficiente multiplo di p, e quindi il lemma è provato per $s = 1$ ed m qualunque.
c) Usiamo infine l'induzione su s.

$$(x_1 + x_2 + \ldots + x_m)^{p^s} = [(x_1 + x_2 + \ldots + x_m)^{p^{s-1}}]^p = [x_1^{p^{s-1}} + x_2^{p^{s-1}} + \ldots + x_m^{p^{s-1}} + \sum a_i]^p$$

ove si sono indicati con a_i i monomi dell'espansione di $(x_1 + x_2 + \ldots + x_m)^{p^{s-1}}$ che contengono almeno due fra gli $x_1, \ldots, x_m$, fra loro distinti.

$$[x_1^{p^{s-1}} + x_2^{p^{s-1}} + \ldots + x_m^{p^{s-1}} + \sum a_i]^p = x_1^{p^s} + x_2^{p^s} + \ldots + x_m^{p^s} + \sum a_i^p + \text{termini con coefficiente}$$

multiplo di p (questo segue da quanto provato in b)). Per l'ipotesi induttiva su s, i coefficienti dei termini a_i sono tutti divisibili per p, quindi lo stesso vale per i coefficienti di $(a_i)^p$ ed il lemma è completamente provato. ∇Δ

ESERCIZI 7.13 (Costruzioni con riga e compasso)

1) Dato un angolo costruirne la bisettrice.

2) Costruire i poligoni regolari con 3,4,5,6 lati.

3) Costruire il poligono regolare di 15 lati.

4) Dato il tetraedro (piramide a facce triangoli equilateri) di volume 1, è possibile costruire con riga e compasso il suo lato?

5) Data un'ellisse di semiassi a e b, costruire i fuochi.

6) E' possibile costruire un quadrato di area pari a quella dell'ellisse di semiassi a e b, con a e b razionali?

Per ulteriori esercizi sulle costruzioni si consiglia il testo di F.Enriques-U.Amaldi: *Elementi di Geometria* ad uso delle scuole secondarie, Parte II - Edizione Zanichelli Bologna, 1956, pagine 113-128.

§ 8 ISOMORFISMI

DEFINIZIONE 8.1 Sia E un campo (di numeri). Una funzione $\sigma : E \to \mathbb{C}$, definita su E ed a valori complessi si dice un *isomorfismo* se:

i) $\sigma(a+b) = \sigma(a) + \sigma(b)$; $a,b \in E$

ii) $\sigma(a \cdot b) = \sigma(a)\sigma(b)$; $a,b \in E$

iii) $\sigma(a)$, al variare di a in E, non assume solo il valore nullo.

Dalla definizione 8.1 discendono subito alcune proprietà elementari sugli isomorfismi:

PROPRIETA' 8.2 Sia $\sigma : E \to \mathbb{C}$ un isomorfismo, allora:

1) $\sigma(1) = 1$

2) Se $a \neq 0$ allora $\sigma(a) \neq 0$ e $\sigma(a^{-1}) = \sigma(a)^{-1}$

3) $\sigma(0) = 0$ e $\sigma(-a) = -\sigma(a)$

4) Se $a \neq b$ allora $\sigma(a) \neq \sigma(b)$

Dimostrazione 1) Sia $a \in E$ un elemento tale che $\sigma(a) \neq 0$ si ha $\sigma(a) = \sigma(a \cdot 1) = \sigma(a)\sigma(1)$; da cui, moltiplicando per $\sigma(a)^{-1}$ si ottiene $1 = \sigma(1)$.

2) $1 = \sigma(1) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1})$ da cui $\sigma(a^{-1}) = \sigma(a)^{-1}$ e quindi anche $\sigma(a) \neq 0$.

3) $\sigma(0) = \sigma(0+0) = \sigma(0) + \sigma(0)$, sottraendo $\sigma(0)$ si ha $0 = \sigma(0)$. Inoltre $0 = \sigma(0) = \sigma(a-a) = \sigma(a) + \sigma(-a)$, da cui $\sigma(-a) = -\sigma(a)$.

4) Se $a \neq b$ allora $a - b \neq 0$ e $\sigma(a-b) = \sigma(a) - \sigma(b) \neq 0$. ▽

Esempi 8.3 1) $E = \mathbb{C}$, $\sigma : \mathbb{C} \to \mathbb{C}$ l'applicazione di coniugio che associa ad ogni complesso a il suo coniugato $\overline{a}$.

2) $E = \mathbb{Q}(\sqrt{m})$, m numero razionale non quadrato, $\sigma : E \to \mathbb{C}$ definita da $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$.

In seguito ci sarà utile la seguente:

PROPOSIZIONE 8.4 *Sia $\sigma : E \to \mathbb{C}$ un isomorfismo e sia $\overline{\sigma} : E[x] \to \mathbb{C}[x]$ la trasformazione definita da $\overline{\sigma}(\sum a_i x^i) = \sum \sigma(a_i) x^i$. Si ha: $\overline{\sigma}(f+g) = \overline{\sigma}(f) + \overline{\sigma}(g)$ e $\overline{\sigma}(fg) = \overline{\sigma}(f)\overline{\sigma}(g)$, $f,g \in E[x]$.*

Dimostrazione Segue immediatamente dalle proprietà degli isomorfismi e dalla definizione di somma e di prodotto per gli anelli di polinomi. ▽

Sia $\sigma : E \to \mathbb{C}$ un isomorfismo e supponiamo che il campo E sia un'estensione di K: $K \subseteq E$. Possiamo allora restringere l'applicazione σ a K: $\sigma|_K = \varphi : K \to \mathbb{C}$; evidentemente la restrizione φ è un isomorfismo. Si pone quindi la seguente

DEFINIZIONE 8.5 Si dice che $\sigma : E \to \mathbb{C}$ *estende* l'isomorfismo $\varphi : K \to \mathbb{C}$ se E è un'estensione di K e $\sigma|_K = \varphi$.

Osservazione 8.6 Poichè ogni campo di numeri E è un'estensione dei razionali (cfr. proposizione 2.4), possiamo chiederci: se $\sigma : E \to \mathbb{C}$ è un isomorfismo, qual'è la sua restrizione a $\mathbb{Q}$? Sappiamo già che $\sigma(0) = 0$ e $\sigma(1) = 1$, da cui segue $\sigma(2) = \sigma(1+1) = \sigma(1) + \sigma(1) = 2$; $\sigma(3) = \sigma(2+1) = 3$; ..., e quindi $\sigma(m) = m$ per ogni intero naturale. La 3) delle proprietà 8.2 ci permette di dire che $\sigma(m) = m$ per ogni intero relativo. La 2) ci permette di dire che $\sigma(p/q) = p/q$, p,q interi, $q \neq 0$; infatti $\sigma(p/q) = \sigma(pq^{-1}) = \sigma(p)\sigma(q)^{-1} = pq^{-1}$. In definitiva σ ristretta ai razionali è l'identità. Ossia σ estende l'identità di $\mathbb{Q}$, ove per identità di $\mathbb{Q}$ si intende l'applicazione $\mathbb{Q} \to \mathbb{C}$ che associa ad ogni razionale il numero stesso come elemento di $\mathbb{C}$. Più in generale se K è un campo di numeri (e quindi $K \subseteq \mathbb{C}$) si chiama *identità di K* l'isomorfismo $1_K : K \to \mathbb{C}$ che associa ad ogni $a \in K$ l'elemento stesso ($\in \mathbb{C}$).

DEFINIZIONE 8.7 Sia $K \subseteq E$ un'estensione. Si dice che l'isomorfismo $\sigma : E \to \mathbb{C}$ è un *isomorfismo di E su K*, ovvero un K-isomorfismo se la restrizione di σ a K è l'identità di K.

Da quanto abbiamo appena visto si ha che ogni isomorfismo $\sigma : E \to \mathbb{C}$ è un isomorfismo su $\mathbb{Q}$. Quest'espressione è effettivamente piuttosto ambigua dato che la si può confondere con il concetto di *applicazione su*, cioè surjettiva, con la quale però non ha nulla a che vedere.

PROPOSIZIONE 8.8 *Se E è un campo e σ e τ sono due suoi isomorfismi, allora l'insieme $K = \{a \in E \mid \sigma(a) = \tau(a)\}$ è un campo. In particolare $E^\sigma = \{a \in E \mid \sigma(a) = 1_E(a) = a\}$ è un campo.*

Dimostrazione Si hanno le seguenti verifiche immediate: se $a,b \in E$ $\sigma(a-b) = \sigma(a) - \sigma(b) = \tau(a) - \tau(b) = \tau(a-b)$; $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = \tau(a)\tau(b)^{-1} = \tau(ab^{-1})$. Segue che $a-b$, $ab^{-1} \in K$, il che è sufficiente a concludere che K è un campo. ▽

La proposizione 8.8 si estende subito a più di due isomorfismi.

Osservazione 8.9 Se K è un campo e σ è un isomorfismo allora $\sigma(K) = \{\sigma(a) \mid a \in K\}$ è un campo. La verifica è immediata.

PROPOSIZIONE 8.10 *Se $E \supseteq K$ è un'estensione e se $\sigma : E \to \mathbb{C}$ è un isomorfismo allora $\sigma(E) \supseteq \sigma(K)$ è una estenzione. Inoltre se $[E : K] = n$ allora $[\sigma(E) : \sigma(K)] = n$.*

Dimostrazione La prima affermazione è ovvia per l'osservazione 8.9. Sia $v_1,\dots,v_n$ una base di E come spazio vettoriale su K, proviamo che $\sigma(v_1),\dots,\sigma(v_n)$ è una base di $\sigma(E)$ su $\sigma(K)$. Un qualunque elemento di $\sigma(E)$ è della forma $\sigma(a)$ con $a\in E$; scritto $a=\sum k_i v_i$, $k_i\in K$, si ha che $\sigma(a)=\sum \sigma(k_i)\sigma(v_i)$. Inoltre quest'espressione è unica poichè $\sigma(a)=\sum \sigma(h_i)\sigma(v_i)$, $h_i\in K$ allora $\sigma(\sum k_i v_i)=\sigma(\sum h_i v_i)$, da cui $\sum k_i v_i=\sum h_i v_i$ e quindi $k_i=h_i$, perchè i v_i sono una base di E su K. □

Per gli isomorfismi vale il seguente fondamentale

TEOREMA 8.11 *Sia $K\subseteq E$ un'estensione, con $[E:K]=n$, e sia $\varphi: K\to\mathbb{C}$ un'isomorfismo. Esistono allora esattamente n isomorfismi distinti $\alpha_1,\alpha_2,\dots,\alpha_n : E\to\mathbb{C}$ che estendono φ.*

Dimostrazione Ci proponiamo di dimostrare il teorema per induzione a partire dalla seguente osservazione. Un'estensione finita $K\subset E$ si può sempre ottenere per successive estensioni algebriche semplici, cioè esiste una catena di campi $K=K_0\subseteq K_1\subseteq\dots\subseteq K_n=E$, con $K_i=K_{i-1}(a_i)$, $a_i\in E$, $i=1,\dots,n$. Basta infatti, per esempio, assumere che $a_1,\dots,a_n$ siano una base di E su K (cfr. proposizione 6.16). Gli elementi a_i sono tutti algebrici su K (corollario 6.13) e quindi a_i è algebrico su $K(a_{i-1})$. L'induzione che vogliamo usare è basata su 1°) Siano $K\subseteq F\subseteq E$ tre campi. Se il teorema è vero per $K\subseteq F$ e per $F\subseteq E$ allora è vero per $K\subseteq E$.

2°) Se $K\subseteq K(a)$ è un'estensione algebrica semplice allora il teorema è vero (base dell'induzione).

Chiaramente dall'osservazione fatta segue per induzione che il teorema è vero per ogni estensione finita, non appena avremo provato 1°) e 2°). La dimostrazione di 1°) è piuttosto formale. Sia $m=[F:K]$ e $k=[E:F]$. Allora $[E:K]=m\cdot k$ (cfr. 6.12). Se $\varphi: K\to\mathbb{C}$ è un isomorfismo e se il teorema è vero per $K\subseteq F$, φ si estende esattamente in m modi: $\sigma_1,\dots,\sigma_m : F\to\mathbb{C}$. Consideriamo ora l'isomorfismo $\sigma_i : F\to\mathbb{C}$ $(i=1,\dots,m)$; se il teorema è vero per $F\subseteq E$ allora σ_i si estende esattamente in k modi: $\sigma_{i1},\sigma_{i2},\dots,\sigma_{ik} : E\to\mathbb{C}$. Al variare di i otteniamo $m\cdot k=n$ isomorfismi di E che estendono φ. Verifichiamo infine che questi sono tutti e soli i possibili modi di estendere φ. Supponiamo che $\psi: E\to\mathbb{C}$ sia un isomorfismo che estende φ e indichiamo con γ la restrizione di ψ ad F; γ estende φ ad F e quindi deve essere uno dei $\sigma_1,\dots,\sigma_m$ (perchè il teorema è supposto vero per $K\subseteq F$), quindi $\gamma=\sigma_j$ per un j opportuno. Dovendo ψ estendere $\gamma=\sigma_j$ deve essere uno dei σ_{jk}. Passiamo a dimostrare 2°). Sia a algebrico su K e sia $f(x)=\sum_{i=0}^{n} k_i x^i$ il suo polinomio minimo (di grado n). Ricordiamo che gli elementi di $K(a)$ si scrivono in modo unico nella forma $\sum_{j=0}^{n-1} h_j a^j$, $h_j\in K$ (cfr. 2) del teorema 4.10), e che $[K(a):K]=n$ (cfr. esempio 6.9).

Osserviamo che, se $\sigma: K(a)\to\mathbb{C}$ estende $\varphi: K(a)\to\mathbb{C}$, allora: per ogni elemento $\sum_{j=0}^{n-1} h_j a^j\in K(a)$ risulta $\sigma(\sum_{j=0}^{n-1} h_j a^j)=\sum_{j=0}^{n-1}\sigma(h_j)\sigma(a)^j=\sum_{j=0}^{n-1}\varphi(h_j)\sigma(a)^j$ e quindi l'isomorfismo σ è determinato

dalla formula scritta, non appena sia noto il valore $\sigma(a)$. D'altra parte $\sigma(a)$ deve essere una delle radici del polinomio $\overline{f}(x)=\sum_{i=0}^{n}\varphi(k_i)x^i$, in quanto $0=\sigma(0)=\sigma(\sum_{i=0}^{n} k_i a^i)=$
$=\sum_{i=0}^{n}\sigma(k_i)\sigma(a)^i=\sum_{i=0}^{n}\varphi(k_i)\sigma(a)^i$.

La 2°) resterà provata non appena si sia fatto vedere che

i) Data comunque una radice α del polinomio $\overline{f}(x)$, l'applicazione $\sigma: K(a)\to\mathbb{C}$ che associa all'elemento $\sum_{j=0}^{n-1} h_j a^i$ l'elemento $\sum_{j=0}^{n-1}\varphi(h_j)\alpha^i$ è un isomorfismo ed un'estensione di φ.

ii) Il polinomio $\overline{f}(x)=\sum_{i=0}^{n}\varphi(k_i)x^i$ ammette n radici distinte.

Per provare i) occorre fare le seguenti verifiche: $\sigma(u+v)=\sigma(u)+\sigma(v)$; $\sigma(u\cdot v)=\sigma(u)\sigma(v)$. La prima è ovvia. Per la seconda siano:

$$u=\sum_{j=0}^{n-1} h_j a^j=h(a)\quad;\quad h(x)=\sum_{j=0}^{n-1} h_j x^j\in K[x]$$
$$v=\sum_{j=0}^{n-1} t_j a^j=t(a)\quad;\quad t(x)=\sum_{j=0}^{n-1} t_j x^j\in K[x]$$

La rappresentazione canonica di $u\cdot v$ è data da $u\cdot v=\sum_{j=0}^{n-1} r_j a^j=r(a)$, dove $r(x)$ è il resto della divisione del polinomio $h(x)\cdot t(x)$ per il polinomio minimo di a, $f(x)$; vale quindi l'identità $h(x)t(x)=f(x)q(x)+r(x)$. Dalla proposizione 8.4 si vede che questa identità fra polinomi si conserva se sostituiamo ai coefficienti, che sono tutti in K, i coefficienti stessi trasformati per φ. Vale quindi l'identità $\overline{h}(x)\overline{t}(x)=\overline{f}(x)\overline{q}(x)+\overline{r}(x)$, dove si è indicato con soprassegno il trasformato del polinomio mediante φ. Sostituendo α ad x si ottiene $\overline{h}(\alpha)\overline{t}(\alpha)=\overline{f}(\alpha)\overline{q}(\alpha)+\overline{r}(\alpha)=\overline{r}(\alpha)$ e quindi la tesi visto che $\overline{h}(\alpha)=\sigma(u)$, $\overline{t}(\alpha)=\sigma(v)$, $\overline{r}(\alpha)=\sigma(u\cdot v)$ (per la definizione stessa di σ) ed $\overline{f}(\alpha)=0$. La verifica poi che σ estende φ è banale.

Per la ii) osserviamo innazi tutto che il polinomio $\overline{f}(x)=\sum_{i=0}^{n}\varphi(k_i)x^i$ è irriducibile. Infatti, se così non fosse, dovrebbe essere:

$$\sum_{i=0}^{n}\varphi(k_i)x^i=(\sum_{j=0}^{s}\varphi(m_j)x^j)(\sum_{r=0}^{t}\varphi(n_r)x^r),\ \text{con } s,t<n.$$

Poichè φ è un isomorfismo, risulterebbe $f(x)=\sum k_i x^i=(\sum m_j x^j)(\sum n_r x^r)$ e questo è assurdo in quanto $f(x)$ è irriducibile su K. Le radici di $\overline{f}(x)$ sono tutte distinte in quanto sussiste il seguente lemma, che dimostreremo fra breve.

LEMMA 8.12 *Se $g(x)\in K[x]$ è un polinomio irriducibile sul campo K allora tutte le radici di $g(x)$ sono distinte.*

Il teorema 8.11 è pertanto completamente provato. □

Per poter dare la dimostrazione di 8.12 dobbiamo premettere alcune definizioni e lemmi.

DEFINIZIONE 8.13 Se $g(x) = \sum_{i=0}^{k} m_i x^i \in K[x]$ chiamiamo *derivata* di $g(x)$ il polinomio $g'(x) = \sum_{i=1}^{m} i m_i x^{i-1}$. (Questa è naturalmente l'usuale derivata dell'analisi).

Vale, come è ben noto, la formula di derivazione del prodotto $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

LEMMA 8.14 *Le radici multiple di un polinomio $g(x)$ sono tutte radici del polinomio $g'(x)$ e quindi del massimo comun divisore di $g(x)$ e $g'(x)$.*

Dimostrazione Supponiamo $g(x) = (x-\alpha)^k h(x)$, $k > 1$. Derivando si ha: $g'(x) = k(x-\alpha)^{k-1}h(x) + (x-\alpha)^k h'(x)$, da cui $g'(x) = (x-\alpha)^{k-1} l(x)$, $k - 1 > 0$ e questo prova che α è radice di $g'(x)$. D'altra parte $(x-\alpha)^{k-1}$ divide sia $g(x)$ che $g'(x)$ e quindi divide il loro massimo comun divisore. □

Il discorso usato per provare il lemma 8.14 è fatto essenzialmente per i polinomi a coefficienti complessi, ed il massimo comun divisore è da intendersi in questo senso; a noi interessa qualcosa di diverso; poichè se $g(x) \in K[x]$ anche $g'(x) \in K[x]$, vorremmo considerare il loro massimo comun divisore come polinomi di $K|x|$. Fortunatamente sussiste il seguente:

LEMMA 8.15 *Siano $f(x), g(x) \in K[x]$ e sia $K \subseteq E$ un'estensione. Il massimo comun divisore di $f(x)$, $g(x)$ come polinomi a coefficienti in K è uguale al massimo comun divisore di $f(x)$ e $g(x)$ come polinomi a coefficienti in E. In altre parole il massimo comun divisore non dipende dal campo.*

Dimostrazione Il massimo comun divisore si ottiene tramite il metodo delle divisioni successive (cfr.4.9), metodo che non fa intervenire il campo E ma solo K, e quindi dà un risultato indipendente dall'estensione $E \supseteq K$. □

Siamo ora in grado di provare il lemma 8.12.

Dimostrazione di 8.12 Se $g(x) \in K[x]$ è irriducibile sul campo K esso non ha radici multiple. Infatti se $g(x)$ avesse radici multiple queste sarebbero anche radici del massimo comun divisore $h(x) \in K[x]$ di $g(x)$ e $g'(x)$. Segue che $h(x)$ è di grado almeno 1 e divide $g(x)$. Ma $g(x)$ è irriducibile su K e quindi $h(x) = g(x)$. Poichè $h(x) = g(x)$ divide $g'(x)$ si perviene ad un assurdo: infatti il polinomio $g'(x)$ ha grado inferiore a $g(x)$ ed è *non nullo* (interviene qui il fatto che lavoriamo su un campo di caratteristica 0, i complessi). □

Osservazione 8.16 Il ragionamento fatto per provare 8.12 non funziona in caratteristica $p \neq 0$ poichè in tal caso può aversi $g'(x)$ polinomio nullo, essendo $g(x)$ un polinomio non costante. Un'analisi di questo fenomeno dà luogo alla teoria più generale sulle estensioni separabili per le quali la teoria fino ad ora sviluppata continua a valere.

Osservazione 8.17 Sia $K \subset K[a] = E$ un'estensione algebrica semplice e sia $f(x)$ il polinomio

minimo di a su K. Nel corso della dimostrazione del teorema 8.11, abbiamo visto in particolare come le radici di $f(x)$ siano in corrispondenza biunivoca canonica con gli isomorfismi di E su K. Quindi per lo studio di questa estensione, e quindi dell'equazione $f(x) = 0$, possiamo prendere di mira uno dei due seguenti oggetti: radici o isomorfismi. Il passaggio dalla considerazione delle radici a quello degli isomorfismi è tipico dell'algebra astratta e possiede il seguente vantaggio fondamentale: gli isomorfismi di E su K dipendono *solo* dall'*estensione* e non dal particolare elemento a per cui $E = K(a)$. Vi sono infiniti elementi $a \in E$ di questo tipo ed i loro polinomi minimi sono essi stessi infiniti. Un'analisi di tutti questi polinomi è molto più complessa che non un'analisi globale dell'estensione $E \supseteq K$ fatta tramite gli isomorfismi di E su K.

Per sviluppare la teoria di Galois prenderemo pertanto il punto di vista degli isomorfismi, anche se questo non è il punto di vista con cui è stata originariamente costruita la teoria stessa (cfr. i paragrafi 17, 18, 19).

Per finire questa discussione diamo un ultimo corollario

COROLLARIO 8.18 *Sia $K \subseteq E$ un'estensione di grado finito n; $a \in E$; m il grado di a su K; $f(x)$ il polinomio minimo di a su K; $a = a_1, a_2, a_3, \ldots, a_m$ le m radici di $f(x)$; $\sigma_1, \sigma_2, \ldots, \sigma_n$ gli n isomorfismi di E su K. Allora, gli elementi $\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)$ sono esattamente le radici $a_1, a_2, \ldots, a_m$, ciascuna contata n/m volte.*

Dimostrazione Sappiamo che $m|n$ (cfr.2) dal corollario 6.13); sappiamo inoltre che gli isomorfismi $\sigma_1, \ldots, \sigma_n$ estendono gli isomorfismi $\varphi_1, \ldots, \varphi_m$ di $K(a)$ su K ed ogni φ_i è esteso esattamente da n/m fra i σ_i (cfr. la dimostrazione di 1°) nel corso della dimostrazione del teorema 8.11). Per quanto osservato in 8.17 i φ_i corrispondono biunivocamente alle radici di $f(x)$ quindi, pur di scegliere gli indici coerentemente, possiamo assumere che $\varphi_i(a) = a_i$; da ciò segue che $\sigma(a) = a_i$ per gli n/m isomorfismi σ che estendono φ_i. □

ESERCIZI 8.19

1) Sia $K = E(s)$, con s trascendente. Determinare gli automorfismi di E su K (*suggerimento:* considerare le trasfromazioni $s \rightsquigarrow as + b \,/\, cs + d$).

2) Sia $E = K(s_1, s_2, \ldots, s_m)$ e supponiamo che l'estensione E non sia algebrica su K. Provare che esistono infiniti K-isomorfismi di E (*suggerimento*: procedere come nel teorema 8.11).

3) Usando 8.18 si determini per ciascuna delle seguenti estensioni un elemento che le generi:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}); \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{5}); \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}).$$

§ 9 LA CORRISPONDENZA DI GALOIS

Passiamo ora alle applicazioni del teorema 8.11.
Sia $K \subseteq E$ un'estensione finita di grado $[E:K] = n$; sappiamo che gli isomorfismi di E che estendono l'identità di K sono un insieme finito con n elementi.

Notazione 9.1 $\mathcal{J}(E/K)$ denota l'insieme degli isomorfismi di E su K.

Se consideriamo un campo intermedio F, cioè $K \subset F \subset E$, l'insieme $\mathcal{J}(E/F)$ è chiaramente un sottoinsieme di $\mathcal{J}(E/K)$ in quanto ogni isomorfismo di E che estenda l'identità su F è in particolare un'estensione dell'identità su K. Abbiamo quindi una corrispondenza che associa ad ogni campo intermedio F un sottoinsieme di $\mathcal{J}(E/K) : F \rightsquigarrow \mathcal{J}(E/F)$. Viceversa sia $T = \{t_1, \ldots, t_s\} \subset \mathcal{J}(E/K)$, ad esso possiamo associare un campo intermedio definito da: $E^T = \{e \subseteq E \mid t_i(e) = e \ \forall\, t_i \in T\}$ (la verifica che E^T è un campo e che $K \subseteq E^T \subseteq E$ è immediata). Abbiamo quindi un'altra corrispondenza che associa ad ogni sottoinsieme $T \subset \mathcal{J}(E/K)$ un campo intermedio: $T \rightsquigarrow E^T$. Le due corrispondenze sono legate dalle seguenti *relazioni*:
1) $T \subseteq \mathcal{J}(E/E^T)$, 2) $F = E^{\mathcal{J}(E/F)}$.
La 1) è immediata conseguenza della definizione di E^T.
Per la 2) si ha intanto l'inclusione ovvia $F \subseteq E^{\mathcal{J}(E/F)}$. Per provare l'uguaglianza ragioniamo così: prima di tutto $[E:F] = |\mathcal{J}(E/F)|$ (cfr.8.11) ($|T|$ indica il numero degli elementi dell'insieme finito T). Inoltre esistono almeno $|\mathcal{J}(E/F)|$ isomorfismi distinti di E su $E^{\mathcal{J}(E/F)}$, esattamente gli isomorfismi di $\mathcal{J}(E/F)$. Quindi $[E : E^{\mathcal{J}(E/F)}] \geq |\mathcal{J}(E/F)| = [E,F]$ (cfr. teorema 8.11). D'altra parte $[E:F] = [E : E^{\mathcal{J}(E/F)}]\,[E^{\mathcal{J}(E/F)} : F]$, e quindi si deve necessariamente avere $[E^{\mathcal{J}(E/F)} : F] = 1$, cioè $E^{\mathcal{J}(E/F)} = F$. ▽△
La relazione 2) ci dice che, se ad un campo intermedio F associamo il sottoinsieme corrispondente $\mathcal{J}(E/F)$ e a questo sottoinsieme associamo il campo intermedio $E^{\mathcal{J}(E/F)}$ otteniamo il campo di partenza.
Quanto detto fino ad ora si può riassumere nella:

PROPOSIZIONE 9.2 *La corrispondenza $F \rightsquigarrow \mathcal{J}(E/F)$ è una corrispondenza biunivoca fra i campi intermedi $K \subseteq F \subseteq E$ e particolari sottoinsiemi dell'insieme $\mathcal{J}(E/K)$.*

COROLLARIO 9.3 *Esiste solo un numero finito di campi intermedi F fra K ed E.*

Dimostrazione Basta osservare che il numero dei sottoinsiemi di un insieme finito è finito. ▽△
Una bella applicazione di questo corollario è la seguente:

PROPOSIZIONE 9.4 *Ogni estensione di dimensione finita è un'estensione semplice.*

Dimostrazione Per la proposizione 6.16, ogni estensione $K \subseteq E$ di dimensione finita è finitamente generata, cioè $E = K(a_1, \ldots, a_s)$, con $a_i \in E$ algebrici su K (cfr.6.13). Cerchiamo ora di ridurre ad 1 il numero dei generatori. Basta dimostrare allora che un'estensione generata da due elementi è semplice e il risultato segue per induzione.

Sia $E = K(a,b)$, a,b algebrici su K. Per ogni intero h consideriamo il campo $E_h = K(a + hb)$. Ogni E_h è un'estensione semplice intermedia fra K ed E. Poichè vi è solo un numero finito di campi intermedi, per almeno due interi distinti h e k deve aversi $E_h = E_k$. In particolare $a + kb \in K(a+hb)$ e quindi $(a+kb) - (a-hb) = b(k-h) \in K(a+hb)$, da cui si ricava $b = b(k-h)/k-h \in K(a+hb)$, inoltre $a = (a+kb) - kb \in K(a+hb)$. In definitiva, poichè $a,b \in K(a+hb)$, si ha che $K(a,b) \subseteq K(a+hb)$, ma $K(a+hb) \subseteq K(a,b)$ e quindi $a+hb$ genera $K(a,b)$. ▽△

§ 10 ESTENSIONI GALOISSIANE

Consideriamo la proposizione 9.2 e poniamo la seguente domanda: quali sono i possibili sottoinsiemi di $\mathcal{J}(E/K)$ che vengono a corrispondere ai campi intermedi? Il sottoinsieme ridotto al solo elemento $1_E = \mathcal{J}(E/E)$ è il corrispondente del campo intermedio E; tutto l'insieme $\mathcal{J}(E/K)$ è il corrispondente di K. Vi sono a priori molte restrizioni perchè un sottoinsieme $T \subset \mathcal{J}(E/K)$ sia della forma $\mathcal{J}(E/F)$, per esempio il numero degli elementi di un tale sottoinsieme deve dividere il numero degli elementi dell'insieme (cfr. 6.12). Una risposta assolutamente soddisfacente la otterremo per quelle particolari estensioni che si chiamano Galoissiane e che passiamo a definire.

DEFINIZIONE 10.1 Un'estensione $K \subseteq E$ si dice *Galoissiana* se per ogni $\varphi \in \mathcal{J}(E/K)$ si ha $\varphi(E) \subseteq E$.

Osservazione 10.2 Sia $\varphi \in \mathcal{J}(E/K)$ tale che $\varphi(E) \subseteq E$. Inoltre $\varphi(K) = K$ perchè φ estende l'identità di K; quindi, per la proposizione 8.10, si ha $[\varphi(E) : K] = [E : K]$, da cui segue che $\varphi(E) = E$, cioè φ è un *automorfismo* di E su K.

Gli automorfismi, come è ben noto, si possono comporre ed invertire, ottenendo come risultato ancora un automorfismo. Poniamo quindi la seguente:

DEFINIZIONE 10.3 Si chiama *gruppo di Galois* dell'estensione $E \supseteq K$ il gruppo degli automorfismi di E su K. Tale gruppo si denota con $G(E/K)$.
In generale $G(E/K) \subseteq \mathcal{J}(E/K)$; dire che l'estensione è Galoissiana significa dire che $G(E/K) = \mathcal{J}(E/K)$.

Osservazione 10.4 Se $K \subseteq F \subseteq E$ è chiaro dalla definizione che, se $K \subseteq E$ è Galoissiana tale

è anche $F \subseteq E$ e che $G(E/F)$ è un sottogruppo di $G(E/K)$.

Attenzione Se $K \subseteq F \subseteq E$ e se $K \subseteq F$ e $F \subseteq E$ sono Galoissiane *non* è vero in generale che $K \subseteq E$ sia essa stessa Galoissiana, come vedremo nell'esercizio 15.13.

Sia $f(x) \in K[x]$ un polinomio ed $\alpha_1,\ldots,\alpha_n$ tutte le sue radici distinte:

DEFINIZIONE 10.5 L'estensione $E = K(\alpha_1,\ldots,\alpha_n)$ ottenuta aggiungendo a K le radici di $f(x)$ si chiama *campo di decomposizione* di $f(x)$. Il suo gruppo di Galois si chiama *gruppo di Galois* del polinomio $f(x)$ su K.

TEOREMA 10.6 1) *Il campo di decomposizione* $E = K(\alpha_1,\ldots,\alpha_n)$ *è un'estensione Galoissiana di* K.
2) *Ogni automorfismo di* E *su* K *permuta fra loro le radici* $\alpha_1,\ldots,\alpha_n$.
3) $G(E/K)$ *è isomorfo al gruppo di permutazioni da esso indotto su* $\alpha_1,\ldots,\alpha_n$.
4) *Se* $f(x)$ *è irriducibile su* K, $G(E/K)$ *opera transitivamente sulle radici.*

Dimostrazione Ricordiamo un fatto già più volte utilizzato: sia $E \supseteq K$ un'estensione, $a \in E$ un suo elemento e $g(x) \in K[x]$ un polinomio tale che $g(a) = 0$. Per ogni isomorfismo $\sigma : E \to \mathbb{C}$ di E su K si ha: $0 = \sigma(g(a)) = g(\sigma(a))$, ovvero σ trasforma una radice a di $g(x)$ in un'altra radice.
In particolare, se σ è un K-isomorfismo di $E = K(\alpha_1,\ldots,\alpha_n)$ esso deve necessariamente permutare fra loro le radici $\alpha_1,\ldots,\alpha_n$ di $f(x)$; pertanto trasforma E in sé stesso. Questo prova 1) e 2).
Per provare 3) basta verificare che un K-automorfismo σ che induca la permutazione identica fra gli elementi $\alpha_1,\ldots,\alpha_n$ è necessariamente l'identità di E. Ma questo è banale poichè ogni elemento di E è esprimibile come funzione razionale negli α_i a coefficienti in K.
4) Ricordiamo che un gruppo G di permutazioni su X opera transitivamente se dati comunque due elementi $a,b \in K$ esiste un $g \in G$ tale che $ga = b$. Se $f(x)$ è irriducibile esso è il polinomio minimo di ciascuna delle sue radici. Date comunque due radici α_i e α_j esiste un K-isomorfismo $K(\alpha_i) \to \mathbb{C}$ che trasforma α_i in α_j (cfr. teorema 8.11, punto i) della dimostrazione). Tale isomorfismo si estende ad un automorfismo di $K(\alpha_1,\ldots,\alpha_n)$, per la 8.11 ed il punto 1) di questo teorema. Questo prova la transitività. ▽△

Osservazione 10.7 In generale, se G è un gruppo di permutazioni che opera sull'insieme X, possiamo decomporre X nelle sue orbite, cioè le classi rispetto alla seguente equivalenza: a equivalente a b se e solo se esiste $g \in G$ con $ga = b$.
Nel caso esaminato nel teorema precedente decomponiamo l'insieme $\{\alpha_1,\ldots,\alpha_n\}$ nelle sue orbite rispetto all'azione di $G(E/K)$. Se $\beta_1,\ldots,\beta_k$ è una tale orbita, formiamo il polinomio $\prod_{i=1,\ldots,k}(x - \beta_i)$. I polinomi ottenuti in tale modo sono esattamente i fattori irriducibili e distinti di $f(x)$ su K.

Si lascia da provare la precedente osservazione come esercizio per il lettore.
Il teorema 10.6 ammette come inversa la seguente:

PROPOSIZIONE 10.8 *Se* $K \subseteq E$ *è un'estensione Galoissiana, esiste un polinomio irriducibile* $f(x) \in K[x]$ *con radici* $\alpha_1,\ldots,\alpha_n$ *tale che* $E = K(\alpha_1,\ldots,\alpha_n)$.

Dimostrazione Sappiamo che $E = K(a)$, per un opportuno elemento a (cfr. 9.4); sia $f(x)$ il polinomio minimo di a su K, e siano $a = \alpha_1,\alpha_2,\ldots,\alpha_n$ le sue radici. Per il teorema 8.11 esistono n K-isomorfismi $\sigma_i : E = K(\alpha_1) \to K(\alpha_i)$ per cui $\sigma_i(\alpha_1) = \alpha_i$. Poichè l'estensione $K \subseteq E$ è di Galois si avrà $\sigma_i(E) = E$ e quindi $\alpha_i \in E$, $i = 1,\ldots,n$, ovvero $E = K(\alpha_1,\ldots,\alpha_n)$. ▽△

Osservazione 10.9 La proposizione precedente fornisce una presentazione esplicita della estensione Galoissiana E come campo di decomposizione di un polinomio, e precisamente si è scelto un polinomio di grado n uguale al grado dell'estensione. In questo caso si è ottenuto $E = K(a) = K(\alpha_i) = K(\alpha_1,\ldots,\alpha_n)$, $i = 1,\ldots,n$. In generale E si può ottenere come campo di decomposizione di un polinomio di grado inferiore al grado dell'estensione; si confronti per esempio l'analisi fatta in 6.14 per il polinomio $x^4 - 2$. In questo caso $K(\alpha_1,\ldots,\alpha_n) \neq K(\alpha_i)$ per ogni i.
Come conseguenza del teorema sulla corrispondenza di Galois (cfr. esercizio 10.12) si potranno trovare dei criteri per la generazione di E, in particolare per determinare il grado minimo di un polinomio di cui E sia campo di decomposizione.

Osservazione 10.10 Il teorema 10.6 e la proposizione 10.8 ci dicono che estensioni Galoissiane e campi di decomposizione di polinomi sono sostanzialmente la stessa cosa. Però la considerazione di un'estensione è da un punto di vista algebrico più semplice, in quanto intrinseca. In altre parole, una estensione Galoissiana è campo di decomposizione di infiniti polinomi e studiare la struttura di uno particolare di essi può essere più complesso che studiare la struttura dell'estensione, (cfr. osservazione 8.17).

Riprendiamo ora il problema che ci siamo proposti all'inizio di questo paragrafo: data l'estensione $K \subseteq E$, quali sono i sottoinsiemi di $\mathcal{I}(E/K)$ che vengono a corrispondere ai campi intermedi? Per le estensioni Galoissiane la risposta è data dal seguente:

TEOREMA 10.11 (Corrispondenza di Galois) *Sia* $K \subseteq E$ *un'estensione Galoissiana. Allora:*
1) *La corrispondenza* $F \rightsquigarrow G(E/F)$, *che associa ad ogni campo intermedio* $K \subseteq F \subseteq E$ *il gruppo* $G(E/F)$ *degli automorfismi di* E *su* F, *pone in corrispondenza biunivoca l'insieme dei campi intermedi fra* E *e* K *con l'insieme dei sottogruppi di* $G(E/K)$.
2) *Dato il campo intermedio* F, $K \subseteq F \subseteq E$, $K \subseteq F$ *è Galoissiana se e solo se* $G(E/F)$ *è un sottogruppo normale di* $G(E/K)$. *In questo caso ogni automorfismo di* E *su* K *induce un automorfi-*

smo di F su K e si ottiene così un epimorfismo:

$$G(E/K) \to G(F/K) \to 1$$

con nucleo $G(E/F)$; cioè $G(F/K) \simeq G(E/K) \,/\, G(E/F)$.

3) *Per un campo intermedio F, più generalmente, i K-isomorfismi di F in $\mathbb{C}$ corrispondono alle classi laterali destre di $G(E/F)$ in $G(E/K)$.*

Dimostrazione 1) Per l'osservazione 10.4 sappiamo che $F \subseteq E$ è Galoissiana e quindi $\mathcal{G}(E/F) = G(E/F)$. La relazione 2) provata prima della proposizione 9.2 ci dice che $E^{G(E/F)} = F$. Si tratta quindi di far vedere che se $H \subseteq G(E/K)$ è un sottogruppo, si ha: $G(E/E^H) = H$.
Chiaramente $G(E/E^H) \supseteq H$ e l'ordine di $G(E/E^H)$ è uguale a $[E : E^H]$. Basta quindi dimostrare che $[E : E^H] \leq m$, dove m indica l'ordine di H.
A tal scopo osserviamo che $E = K(a)$ (cfr.9.4) e quindi a maggior ragione $E = E^H(a)$, pertanto basta provare che l'elemento a soddisfa un polinomio di grado m ed a coefficienti in E^H.
Consideriamo il seguente polinomio:

$$f(x) = (x - h_1(a))(x - h_2(a))\ldots(x - h_m(a))$$

ove $1 = h_1, h_2, \ldots, h_m$ sono gli elementi (automorfismi) del sottogruppo H. Poichè $h_1(a) = a$, a è una radice di $f(x)$, ed $f(x)$ ha il grado voluto. Resta solo da provare che i coefficienti di $f(x)$ sono in E^H. Infatti, se applichiamo un automorfismo $h_j \in H$ ai coefficienti di $f(x)$ otteniamo il polinomio $(x - h_j h_1(a))(x - h_j h_2(a))\ldots(x - h_j h_m(a))$ il quale è ancora $f(x)$, visto che $h_j h_1, h_j h_2, \ldots, h_j h_m$ non è altro che una permutazione di $h_1, h_2, \ldots, h_m$. (H è un gruppo). Questo dimostra completamente 1).
2) Supponiamo di avere $K \subseteq F \subseteq E$. Provare che $G(E/F)$ è normale in $G(E/K)$ se e solo se $K \subseteq F$ è Galoissiana equivale a far vedere che, $\varphi G(E/F)\varphi^{-1} = G(E/F)$ per ogni $\varphi \in G(E/K)$, se e solo se $K \subseteq F$ è Galoissiana. A tal scopo consideriamo il campo $\varphi(F) \subseteq E$ e cerchiamo di determinare il sottogruppo $G(E/\varphi(F))$. $\psi \in G(E/\varphi(F))$ se e solo se $\psi\varphi(f) = \varphi(f)$ per ogni $f \in F$, cioè se e solo se $\varphi^{-1}\psi\varphi(f) = f$ per ogni $f \in F$, e, equivalentemente, $\varphi^{-1}\psi\varphi \in G(E/F)$, $\psi \in \varphi G(E/F)\varphi^{-1}$.
In definitiva abbiamo così provato che $G(E/\varphi(F)) = \varphi G(E/F)\varphi^{-1}$.
D'altra parte $K \subseteq F$ è Galoissiana se e solo se ogni isomorfismo di F su K trasforma F in sé. Poichè ogni isomorfismo di F su K si può estendere ad un isomorfismo di E su K, l'affermazione ora fatta è equivalente al fatto che $\varphi(F) = F$ per ogni $\varphi \in G(E/K)$. Poichè si è già visto in 1) che vi è corrispondenza biunivoca fra sottogruppi e campi intermedi, questo equivale al fatto che $G(E/\varphi(F)) = G(E/F)$ per ogni $\varphi \in G(E/K)$. Poichè abbiamo visto che $G(E/\varphi(F)) = \varphi G(E/F)\varphi^{-1}$, resta provata la prima affermazione di 2). Sempre nelle stesse ipotesi, poichè ogni automorfismo $\varphi \in G(E/K)$ induce un K-isomorfismo di F, con $\varphi(F) = F$, si ha un'applicazione: $G(E/K) \to G(F/K)$ che associa ad ogni $\varphi \in G(E/K)$ la sua restrizione ad F. E' chiaro dalle definizioni che quest'applicazione è un omomorfismo fra gruppi e che è suriettiva, visto

che ogni automorfismo di F su K si estende ad un automorfismo di E. Il nucleo consiste esattamente di quegli automorfismi di E che danno l'identità su F, cioè il nucleo è $G(E/F)$. La 2) è così completamente provata.
3) Più generalmente se il campo intermedio F non è necessariamente di Galois, possiamo solo dire che ogni automorfismo di E su K dà luogo, per restrizione, ad un isomorfismo di F su K e viceversa ogni K-isomorfismo di F si può estendere ad un K-isomorfismo (di fatto a un K-automorfismo) di E; naturalmente i K-isomorfismi di F non formano un gruppo.
Due elementi $\varphi, \psi \in G(E/K)$ danno luogo allo stesso K-isomorfismo di F se e solo se $\varphi(f) = \psi(f)$ per ogni $f \in F$, cioè $\psi^{-1}\varphi(f) = f$ per ogni $f \in F$, ovvero $\psi^{-1}\varphi \in G(E/F)$ e quindi $\varphi \in \psi G(E/F)$. Concludendo φ e ψ stanno nella stessa classe laterale destra di $G(E/K)$ rispetto al sottogruppo $G(E/F)$.
Un momento di riflessione permetterà di convincersi che in questo modo abbiamo stabilito una corrispondenza biunivoca fra le classi laterali destre di $G(E/F)$ in $G(E/K)$ e i K-isomorfismi di F. ▽△

ESERCIZI 10.12

1) Sia $K \subseteq E$ un'estensione Galoissiana con gruppo di Galois $G = G(E/K)$. Sia $a \in E$ un elemento ed $f(x)$ il suo polinomio minimo su K. Sia infine H il sottogruppo di G che lascia fisso a. Provare che il campo di decomposizione di $f(x)$ è contenuto in E e corrisponde al sottogruppo M di G caratterizzato dalla seguente proprietà: M è il massimo sottogruppo normale di G contenuto in H.

2) Dedurre a partire dall'esercizio 1) una condizione sufficiente affinchè il campo di decomposizione di $f(x)$ coincida con E.
Si provi a considerare la validità di tale condizione nel caso di gruppi noti al lettore, per esempio G gruppo abeliano, G il gruppo simmetrico su n elementi, G un gruppo di simmetrie.

3) Determinare il gruppo di Galois (su $\mathbb{Q}$) delle seguenti equazioni:

$$x^4 - 2 \quad ; \quad x^5 - 3 \quad ; \quad x^3 - x + 10$$

(*suggerimento*: per l'ultimo polinomio si osservi che la coniugazione fra numeri complessi induce un automorfismo non banale del suo campo di decomposizione).

4) Si considerino i campi di decomposizione per le equazioni dell'esercizio 3). Determinare i campi intermedi e per ciascuno di essi un elemento generante.

5) Determinare il gruppo di Galois di $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ ed un elemento generante l'estensione. Quali sono le estensioni quadratiche di $\mathbb{Q}$ contenute in E?

§ 11 ESTENSIONI CICLOTOMICHE

In questo paragrafo vogliamo discutere un caso speciale del teorema 10.11 sulla corrispondenza di Galois da cui dedurremo la condizione sufficiente, annunciata in 7.13, perchè un poligono di n lati sia costruibile con riga e compasso.

Consideriamo il polinomio $x^n - 1$; posto $\varepsilon = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$, abbiamo visto che $1 = \varepsilon^n, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ sono le n radici distinte di $x^n - 1$ (cfr. applicazione 3) del §7).

Vogliamo studiare l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\varepsilon)$, (*estensione ciclotomica*). La prima osservazione che possiamo fare è che $\mathbb{Q}(\varepsilon)$ è il campo di decomposizione del polinomio $x^n - 1$ su $\mathbb{Q}$, in quanto $\varepsilon^i \in \mathbb{Q}(\varepsilon)$ per ogni intero i, e pertanto l'estensione ciclotomica è Galoissiana. Vogliamo determinarne il gruppo di Galois.

Ci proponiamo innanzitutto di determinare il polinomio minimo di ε su $\mathbb{Q}$. Ciò è stato fatto (cfr. 7.8) nel caso in cui n è potenza di un primo. Determiniamolo ora nel caso generale.

Per ogni divisore d di n consideriamo l'insieme I delle radici primitive d-esime dell'unità ed il polinomio $\prod_{\alpha \in I}(x - \alpha) = \Phi_d(x)$. Poichè ogni radice n-ma dell'unità è radice primitiva d-ma, per un qualche numero d che sia divisore di n, e viceversa, si avrà:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

In particolare osserviamo che $\Phi_n(x) = \prod_{\substack{(k,n)=1 \\ k<n}} (x - \varepsilon^k)$. Infatti l'ordine m di una radice ε^k si determina facilmente nel modo seguente: sia q il massimo comun divisore fra k ed n, provare che $m = n/q$. Pertanto il grado di $\Phi_n(x)$ è $\varphi(n)$ (ove φ denota la funzione di Eulero, di cui ricordiamo l'espressione: se $n = p_1^{k_1} \ldots p_s^{k_s}$ è la decomposizione in primi di n, $\varphi(n) = (p_1 - 1)p_1^{k_1 - 1} \ldots (p_s - 1)p_s^{k_s - 1}$).

Il polinomio $\Phi_n(x)$ viene chiamato n-mo *polinomio ciclotomico*.

PROPOSIZIONE 11.1 1) *Il polinomio $\Phi_n(x)$ è un polinomio monico a coefficienti interi.*
2) *$\Phi_n(x)$ è irriducibile su $\mathbb{Q}$ e pertanto è il polinomio minimo di ε.*

Dimostrazione 1) Procediamo per induzione su n. Consideriamo la formula

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$$

Per l'ipotesi induttiva il polinomio $\prod_{\substack{d|n \\ d<n}} \Phi_d$ è un polinomio monico a coefficienti interi, e pertanto lo stesso è vero per $\Phi_n(x)$ in quanto quoziente di polinomi monici a coefficienti interi.

2) Supponiamo $\Phi_n(x) = f(x)g(x)$, ove $f(x)$ è il polinomio minimo di ε. La tesi sarà provata non appena avremo fatto vedere che ogni radice n-ma primitiva dell'unità annulla $f(x)$, in

quanto in questo caso $g(x)$ è necessariamente costante. Poichè tali radici sono della forma ε^k con k primo con n basterà provare (per induzione su k) la seguente affermazione: sia η radice primitiva n-ma ed $f(\eta) = 0$ e sia p un primo che non divide n; allora $f(\eta^p) = 0$. Supponiamo per assurdo $f(\eta^p) \neq 0$, si avrà allora necessariamente $g(\eta^p) = 0$. Consideriamo il polinomio $h(x) = g(x^p)$. Poichè $h(\eta) = 0$ $h(x)$ è un multiplo di $f(x)$, polinomio minimo di η: $g(x^p) = q(x)f(x)$. Poichè i polinomi sono a coefficienti interi possiamo considerare questa ultima uguaglianza nell'anello $\mathbb{Z}/_{(p)}[x]$ dei polinomi a coefficienti interi modulo p. Ma in tale anello si ha $\overline{g}(x^p) = (\overline{g}(x))^p$ (cfr. lemma 7.7); da cui $(\overline{g}(x))^p = \overline{q}(x)\overline{f}(x)$, pertanto ogni fattore irriducibile $\psi(x)$ di $\overline{f}(x)$ divide $\overline{g}(x)$. Da $\overline{\Phi}_n(x) = \overline{f}(x)\overline{g}(x)$ segue che $(\psi(x))^2$ divide $\overline{\Phi}_n(x)$ e quindi anche $x^n - \overline{1} = \overline{\Phi}_n(x) \prod_{\substack{d|n \\ d<n}} \overline{\Phi}_d(x)$. Otterremo una contraddizione non appena avremo provato che il polinomio $x^n - \overline{1}$ non ha radici multiple in caratteristica p, con p primo con n.

Le radici multiple di un polinomio sono quelle comuni anche alla sua derivata. La derivata di $x^n - \overline{1}$ è nx^{n-1} cioè un polinomio che ha come sole radici lo zero (poichè $n \not\equiv 0 \bmod p$) e lo zero non è radice di $x^n - \overline{1}$ □

Prima di calcolare il gruppo di Galois dell'estensione ciclotomica, ricordiamo che in $\mathbb{Z}/_{(n)}$ la classe $\overline{k}$ di un intero k è invertibile se e solo se $(k,n) = 1$. Denoteremo con $(\mathbb{Z}/_{(n)})^*$ il gruppo di tali elementi.

TEOREMA 11.2 *Il gruppo $G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ è isomorfo a $(\mathbb{Z}/_{(n)})^*$.*

Dimostrazione Sia $\sigma \in G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$; σ permuta le radici di $\Phi_n(x)$, onde $\sigma(\varepsilon) = \varepsilon^i$, con $(i,n) = 1$, $i < n$. Consideriamo l'applicazione $\lambda : G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \to (\mathbb{Z}/_{(n)})^*$ che associa a σ la classe di i modulo n. Proviamo che λ è un isomorfismo di gruppi.

Poichè i due gruppi hanno lo stesso numero di elementi basta provare che λ è un omomorfismo iniettivo. Se $\sigma, \tau \in G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$, e $\sigma(\varepsilon) = \varepsilon^i$, $\tau(\varepsilon) = \varepsilon^j$, si ha $\tau\sigma(\varepsilon) = \tau(\varepsilon^i) = (\tau(\varepsilon))^i = \varepsilon^{ij}$. Pertanto λ è un omomorfismo. Inoltre λ è iniettivo poichè se $\sigma(\varepsilon) = \varepsilon$ σ è necessariamente l'identità su $\mathbb{Q}(\varepsilon)$. □

Osserviamo in particolare che il gruppo di Galois di un'estensione ciclotomica è abeliano e pertanto ogni campo intermedio è Galoissiano su $\mathbb{Q}$ con gruppo di Galois abeliano. L'inversa di questa affermazione è anch'essa vera e forma il contenuto di un famoso teorema dovuto a Kronecker, di cui non possiamo dare la dimostrazione, in quanto essa richiederebbe una conoscenza vasta della teoria degli interi algebrici (cfr. S.Lang, *Algebraic numbers*)

TEOREMA (Kronecker) *Se $\mathbb{Q} \in E$ è un'estensione di Galois con gruppo di Galois commutativo allora $E \subseteq \mathbb{Q}(\varepsilon)$ per una estensione ciclotomica opportuna.*

Siamo ora finalmente in grado di dare la risposta definita al problema 7.6:

TEOREMA 11.3 *Condizione necessaria e sufficiente affinchè un poligono di n lati sia costruibile con riga e compasso è che i primi dispari che compaiono nella fattorizzazione dell'intero n abbiano tutti esponente uno e siano primi di Fermat.*

Dimostrazione La condizione necessaria è stata vista nel §7. Dimostriamo quindi la condizione sufficiente, la quale, per quanto visto nell'Applicazione 3) del §7 all'inizio, e osservazione 7.11 è equivalente a provare che è possibile costruire con riga e compasso una radice primitiva dell'unità con p primo della forma $2^{2^k}+1$. A tale scopo dobbiamo verificare le condizioni del teorema 7.4. Pertanto è sufficiente mostrare che esiste una successione di sottogruppi $G_0 = G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{1\}$ con $(G_i : G_{i+1}) = 2$, visto che dal teorema 10.11, posto $K_i = (\mathbb{Q}(\varepsilon))^{G_i}$, si avrà $\mathbb{Q}(\varepsilon) = K_m \supseteq K_{m-1} \supseteq \ldots \supseteq \mathbb{Q} = K_0$ e $[K_i : K_{i-1}] = 2$. Poichè G_0 è abeliano di ordine 2^m, il teorema segue dal seguente lemma di teoria dei gruppi:

LEMMA 11.4 *Se G è un gruppo abeliano finito esiste una catena di sottogruppi $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = \{0\}$ con G_i / G_{i+1} ciclico di ordine primo (ovviamente tale primo divide l'ordine di G).*

Dimostrazione Sia $G_1 \subseteq G$ un sottogruppo proprio massimale di G. Poichè G è abeliano G_1 è normale e G/G_1 è un gruppo privo di sottogruppi propri, pertanto è generato da ciascuno dei suoi elementi non nulli, e quindi ciclico. Il suo ordine è primo, ancora perchè è privo di sottogruppi propri. Si procede ora su G_1 e così via. ▽△

ESERCIZI 11.5

1) Sia G un gruppo di ordine p^m con p primo. Dimostrare che esiste una successione di sottogruppi

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{0\}$$

tale che G_i è normale in G_{i-1} di indice p.

2) Dimostrare che un numero algebrico α è euclideo se e solo se il grado del campo di decomposizione del suo polinomio minimo è una potenza di 2.

3) Calcolare il polinomio $\Phi_{10}(x)$ e il gruppo di Galois di $\mathbb{Q}(\varepsilon)$ con ε radice primitiva decima dell'unità; studiare algebricamente il decagono regolare.

Prima di svolgere l'esercizio n.3 sarà conveniente leggere il seguente esempio, che si riferisce al caso $n = 5$.

Esempio 11.6 La radice primitiva quinta dell'unità, ε, soddisfa il polinomio $x^4 + x^3 + x^2 + x + 1 = 0$.

Il gruppo di Galois dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\varepsilon)$ è isomorfo a $(\mathbb{Z}/_{(5)})^*$. Tale gruppo è ciclico di ordine 4 ed è generato dalla classe $\bar{2}$; infatti si ha: $\bar{2}, \bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{3}$, $\bar{2}^4 = \bar{1}$. La classe $\bar{4} = -\bar{1}$ genera un sottogruppo $H = \{\bar{1}, -\bar{1}\}$ con due elementi. La radice ε è pertanto quadratica su $\mathbb{Q}(\varepsilon)^H$ ed il suo polinomio minimo è dato (secondo quanto descritto nel teorema 10.11) da:

$$(x - \varepsilon)(x - \varepsilon^{-1}) = x^2 - (\varepsilon + \varepsilon^{-1})x + 1$$

Per costruzione $\varepsilon + \varepsilon^{-1} \in \mathbb{Q}(\varepsilon)$ ed è quadratico su $\mathbb{Q}$.

Ora l'automorfismo non identico di $\mathbb{Q}(\varepsilon)$ è indotto dall'automorfismo di $\mathbb{Q}(\varepsilon)$ associato a $\bar{2}$ (ed anche a $\bar{3}$, visto che $\bar{2}$ e $\bar{3}$ sono nella stessa classe laterale di $H = (\bar{4}, \bar{1})$ (cfr.10.11); pertanto $\varepsilon + \varepsilon^{-1}$ soddisfa su $\mathbb{Q}$ il polinomio:

$$\left[x - (\varepsilon + \varepsilon^{-1})\right]\left[x - (\varepsilon^2 + \varepsilon^{-2})\right] = x^2 - (\varepsilon + \varepsilon^{-1} + \varepsilon^2 + \varepsilon^{-2})x + (\varepsilon^3 + \varepsilon^{-1} + \varepsilon + \varepsilon^{-3}).$$

Poichè

$$\varepsilon + \varepsilon^{-1} + \varepsilon^2 + \varepsilon^{-2} = \varepsilon + \varepsilon^4 + \varepsilon^2 + \varepsilon^3 = -1\ ,$$
$$\varepsilon^3 + \varepsilon^{-1} + \varepsilon + \varepsilon^{-3} = \varepsilon^3 + \varepsilon^4 + \varepsilon + \varepsilon^2 = -1$$

segue che $\varepsilon + \varepsilon^{-1}$ è radice di $x^2 - x - 1$, ovvero è uno dei due numeri $(1 \pm \sqrt{5})/2$

Se abbiamo scelto $\varepsilon = \cos 2\pi/5 + i \operatorname{sen} 2\pi/5$ si ha $\varepsilon^{-1} = \bar{\varepsilon} = \cos 2\pi/5 - i \operatorname{sen} 2\pi/5$ da cui $\varepsilon + \varepsilon^{-1} = 2 \cos 2\pi/5 > 0$ e pertanto $\varepsilon + \varepsilon^{-1} = (1 + \sqrt{5})/2$.

Se avessimo invece scelto come radice primitiva $\cos 4\pi/5 + i \operatorname{sen} 4\pi/5$ avremmo avuto $\varepsilon + \varepsilon^{-1} = (1 - \sqrt{5})/2$.

Conludendo, abbiamo trovato che ε soddisfa il polinomio $x^2 - \left(\frac{1+\sqrt{5}}{2}\right)x + 1$, da cui segue:

$$\varepsilon = 1/2\left(\frac{1+\sqrt{5}}{2} \pm \sqrt{\frac{6+2\sqrt{5}}{4} - 4}\right).$$

Si vede poi facilmente, guardando ai segni, che $\varepsilon = 1/2\left(\frac{1+\sqrt{5}}{2} + i\sqrt{4 - \frac{6+2\sqrt{5}}{4}}\right)$.

§ 12 COMPOSTO DI DUE CAMPI

Consideriamo i seguenti problemi:

I) Dato un polinomio $f(x) \in K[x]$ ed un'estensione $K \subseteq E$, che relazione c'è fra il gruppo di Galois di $f(x)$ su K e quello su E?

II) Dati due polinomi $f(x)$, $g(x) \in K[x]$ che relazione c'è fra i gruppi di Galois dei polinomi $f(x)$, $g(x)$ e $f(x)g(x)$?

Possiamo rendere più intrinseci i due problemi posti introducendo il concetto di *composto*

di due estensioni.

Siano $E \subseteq H$, $E \subseteq K$ due estensioni di campi di numeri.

Consideriamo l'insieme: $HK = \{\sum h_i k_i \mid h_i \in H, k_i \in K\}$. Esso è un anello in quanto somme e prodotti di elementi in HK sono ancora in HK.

PROPOSIZIONE 12.1 1) *Se una delle due estensioni, $E \subseteq H$, $E \subseteq K$, è finita allora HK è un campo.*

2) *Se le due estensioni sono entrambe finite allora l'estensione $E \subseteq HK$ è finita e risulta* $[HK : E] \leq [H : E][K : E]$.

Dimostrazione 1) Sia per esempio $[H : E] = h < \infty$ e sia $v_1, \ldots, v_h$ una base di H su E.

Poichè $h_i = \sum_j \alpha_{ij} v_j$ con $\alpha_{ij} \in E$ per ogni $h_i \in H$, si ha anche $\sum_i h_i k_i = \sum_i \alpha_{ij} v_j k_i = \sum_i (\alpha_{ij} k_i) v_j$ con $\alpha_{ij} k_i \in K$ e questo prova che i v_j sono un sistema di generatori lineari di HK su K; per tanto $\dim_K HK < \infty$.

Usiamo ora il seguente lemma, di cui daremo la dimostrazione dopo aver completato la proposizione in esame.

LEMMA 12.2 *Sia A un anello di numeri; $B \subseteq A$ un campo; $\dim_B A < \infty$ (A è chiaramente uno spazio vettoriale su B). Allora A è un campo.*

Il punto 1) è pertanto concluso.

2) Innanzitutto si ha $[HK : E] = [HK : K][K : E]$ e pertanto l'estensione $E \subseteq HK$ è finita.

D'altra parte, posto $h_i = \sum_j \alpha_{ij} v_j$, $k_i = \sum_s \beta_{is} w_s$ (w_s base di K su E), risulta:

$$\sum_i h_i k_i = \sum_i \Big(\sum_{j,s} \alpha_{ij} v_j \beta_{is} w_s\Big) = \sum_{j,s} \Big(\sum_i \alpha_{ij} \beta_{is}\Big) v_j w_s$$

e questo prova che i $v_j w_s$ sono un sistema di generatori lineare di HK su E, cioè $[HK : E] \leq [H : E][K : E]$. ▽△

Dimostrazione (Lemma 12.2) Sia $a \in A$, $a \neq 0$. $B[a] \subset A$ poichè A è un anello. Poichè $\dim_B B[a] \leq \dim_B A < \infty$, l'elemento a è algebrico su B, pertanto $a^{-1} \in B[a] \subseteq A$. Questo prova che A è un campo. ▽△

Esercizio 12.3 Affinchè HK sia un campo è sufficiente che sia verificata la seguente condizione: ogni elemento di H è algebrico su K (o simmetricamente, ogni elemento di K è algebrico su H).

DEFINIZIONE 12.4 Date le estensioni $E \subseteq H$, $E \subseteq K$, se HK è un campo, esso prende il nome di *composto* fra H e K.

L'operazione di composto si può fare anche per più campi $E \subseteq H_1, E \subseteq H_2, \ldots, E \subseteq H_n$ e verrà

denotato con $H_1 H_2 \ldots H_n$; se $E \subseteq H_i$ sono tutte estensioni finite allora sicuramente $H_1 H_2 \ldots H_n$ è un campo e $[H_1 \ldots H_n : E] \leq \prod_i [H_i : E]$.

In particolare è interessante il caso di cui tratta il seguente teorema:

TEOREMA 12.5 *Sia $K \subseteq E$ un'estensione finita di grado n e siano $\sigma_1, \ldots, \sigma_n$ gli n K-isomorfismi di E. Allora:*

1) *L'estensione $K \subseteq \sigma_1(E)\sigma_2(E)\ldots\sigma_n(E) = E'$ è Galoissiana.*

2) *Se $K \subseteq E \subseteq F$ sono estensioni e $K \subseteq F$ è Galoissiana allora $E' \subseteq F$.*

3) *Il gruppo di Galois di $K \subseteq E'$ è isomorfo in modo canonico ad un gruppo di permutazioni transitivo su n elementi.*

Dimostrazione 1) Se $\varphi : E' \to \mathbb{C}$ è un K-isomorfismo si ha che $\varphi|_{\sigma_i(E)}$ è un K-isomorfismo, e $E \xrightarrow{\sigma_i} \sigma_i(E) \xrightarrow{\varphi} C$ è un K-isomorfismo; quindi $\varphi\sigma_i = \sigma_j$ per un opportuno j, e $\varphi\sigma_i(E) = \sigma_j(E) \subseteq E'$.

Poichè E' è il composto dei $\sigma_i(E)$ si ha $\varphi(E') \subseteq E'$ e $K \subseteq E'$ è Galoissiana.

2) Siano $K \subseteq E \subseteq F$ estensioni. Ogni $\sigma_i : E \to \mathbb{C}$ si può estendere ad un K-isomorfismo $\psi_i : F \to \mathbb{C}$; essendo $K \subseteq F$ Galoissiana segue che $\psi_i(F) \subseteq F$. A maggior ragione $\sigma_i(E) \subseteq F$ e quindi $E' \subseteq F$.

3) Abbiamo visto che $\varphi\sigma_i = \sigma_j$, per ogni $\varphi \in G(E'/K)$, così abbiamo che ogni φ induce una permutazione sui σ_i.

Se $\varphi\sigma_i = \psi\sigma_i$ per ogni i, si deve avere $\varphi = \psi$ visto che E' è generato dai campi $\sigma_i E$. Quindi $G(E'/K)$ è isomorfo al gruppo di permutazioni che induce sui σ_i.

Tale gruppo è transitivo poichè σ_i e σ_j si estendono entrambi ad automorfismi φ_i e φ_j e quindi $\varphi_j \varphi_i^{-1} \sigma_i = \sigma_j$. ▽△

Osservazione 12.6 Consideriamo l'estensione finita di grado n, $K \subseteq K(a) = E$, sia $f(x)$ il polinomio minimo di a su K e siano $a = \alpha_1, \alpha_2, \ldots, \alpha_n$ le sue radici. Indicati con $\sigma_i : E \to \mathbb{C}$ gli isomorfismi definiti da $\sigma_i(\alpha) = \alpha_i$, si ha $\sigma_i(E) = K(\alpha_i)$ ed il composto $E' = \sigma_1(E)\sigma_2(E)\ldots\sigma_n(E)$ non è altro che il campo di decomposizione $K(\alpha_1, \ldots, \alpha_n)$ del polinomio $f(x)$.

La rappresentazione del gruppo di Galois $G(E'/K)$ come gruppo di permutazioni sui σ_i corrisponde esattamente alla rappresentazione del gruppo di Galois di $f(x)$ come gruppo di permutazioni sulle radici, (cfr. teorema 10.6).

Sia $f(x) \in K[x]$, $\alpha_1, \ldots, \alpha_s$ le sue radici e $K \subseteq E$ una estensione. In base a quanto fino ad ora visto, risultano evidenti le due seguenti proposizioni:

PROPOSIZIONE 12.7 *Il campo di decomposizione di $f(x)$ su E è il composto di E con il campo di decomposizione di $f(x)$ su K: $E(\alpha_1, \ldots, \alpha_s) = E \cdot K(\alpha_1, \ldots, \alpha_s)$.*

PROPOSIZIONE 12.8 *Siano $f(x), g(x) \in K[x]$ due polinomi di radici, rispettivamente, $\alpha_1, \ldots \alpha_s$; $\beta_1, \ldots, \beta_k$. Il campo di decomposizione del prodotto $f(x)g(x)$ è il composto dei campi di decomposizione dei due fattori $f(x)$ e $g(x)$.*

La nozione di composto viene così messa in relazione con i problemi elencati all'inizio del paragrafo. La risposta viene invece fornita dal seguente:

TEOREMA 12.9 *Sia $K \subseteq E$ un'estensione Galoissiana e $K \subseteq F$ un'estensione. Allora:*
i) *$F \subseteq EF$ è un'estensione Galoissiana e $G(EF/F)$ è isomorfo ad un sottogruppo di $G(E/K)$.*
ii) *Se anche $K \subseteq F$ è Galoissiana allora $K \subseteq EF$ è Galoissiana e $G(EF/K)$ è isomorfo ad un sottogruppo H di $G(E/K) \times G(F/K)$.*
Inoltre le due proiezioni $H \to G(E/K)$, $H \to G(F/K)$ sono suriettive.

Dimostrazione i) Sia $\varphi: EF \to \mathbb{C}$ un F-isomorfismo. La restrizione $\varphi|_E : E \to \mathbb{C}$ è un K-isomorfismo ($K \subseteq F$), e dal fatto che $K \subseteq E$ è Galoissiana segue $\varphi|_E : E \to E$. Per ogni elemento $\sum e_i f_i \in EF$ si ha: $\varphi(\sum e_i f_i) = \sum \varphi(e_i) f_i \in EF$; cioè $F \subseteq EF$ è di Galois. D'altra parte l'applicazione che associa ad ogni $\varphi \in G(EF/F)$ la sua restrizione $\varphi|_E \in G(E/K)$ è chiaramente un omomorfismo. Esso è iniettivo perchè se $\varphi|_E = 1_E$ allora $\varphi(\sum e_i f_i) = \sum \varphi|_E(e_i) f_i = \sum e_i f_i$, e $\varphi = 1_{EF}$.
ii) Siano $K \subseteq E$ e $K \subseteq F$ entrambe Galoissiane.
Per ogni K-isomorfismo $\varphi: EF \to \mathbb{C}$, $\varphi_1 = \varphi|_E$, $\varphi_2 = \varphi|_F$ sono K-automorfismi e quindi $\varphi_1(E) = E$, $\varphi_2(F) = F$. $\varphi(\sum e_i f_i) = \sum \varphi_1(e_i)\varphi_2(f_i) \in EF$, quindi $K \subseteq EF$ è Galoissiana.
L'applicazione $G(EF/K) \to G(E/K) \times G(F/K)$ definita da $\varphi \rightsquigarrow (\varphi_1, \varphi_2)$ è chiaramente un omomorfismo iniettivo. Inoltre, dato che ogni K-isomorfismo $E \to \mathbb{C}$ si estende ad un isomorfismo $EF \to \mathbb{C}$ (cfr. 8.11), si ha che la proiezione $H \to G(E/K)$ è sopra. ▽△
Il teorema 12.9 può essere immediatamente letto in termini di polinomi e campi di decomposizione. Invitiamo il lettore a farlo.

COROLLARIO 12.10 i) *Se i gruppi di Galois di due estensioni $K \subseteq E$, $K \subseteq F$ sono commutativi tale è anche il gruppo di Galois di $K \subseteq EF$.*
ii) *Se $[E : K]$ e $[F : K]$ sono primi fra loro allora $[EF : K] = [E : K][F : K]$ e $G(EF/K) \simeq G(E/K) \times G(F/K)$.*

Dimostrazione i) è immediato.
ii) Sia H il sottogruppo di $G(E/K) \times G(F/K)$ isomorfo a $G(EF/K)$. Poichè le proiezioni di H sui due fattori sono suriettive si deve avere:

$o(G(E/K)) \mid o(H)$, $o(G(F/K)) \mid o(H)$, ($o(H) =$ ordine di H, etc.)

quindi $[E : K] \mid o(H)$, $[F : K] \mid o(H)$, e $[E : K][F : K] \mid o(H)$ visto che $[E : K]$ e $[F : K]$ sono primi fra loro. Ora $H \subseteq G(E/K) \times G(F/K)$, quindi $o(H) = [E : K][F : K]$ e la tesi è provata. ▽△

Osservazione 12.11 Tutto quanto abbiamo detto per due estensioni si può ripetere per più di due estensioni; come il lettore si convincerà facilmente.

§ 13 L'EQUAZIONE $x^m - b = 0$

Sia K un campo di numeri, $b \in K$ ed m un numero naturale. Vogliamo studiare l'equazione $x^m - b = 0$. Se a è una sua soluzione, le altre sono date da: $\varepsilon a, \varepsilon^2 a, \ldots, \varepsilon^{m-1} a$, dove $\varepsilon = \cos 2\pi/m + i \operatorname{sen} 2\pi/m$ è una radice primitiva m-esima dell'unità.
Vogliamo quindi studiare l'estensione $K(a, \varepsilon a, \varepsilon^2 a, \ldots, \varepsilon^{m-1} a)$.
Poniamoci innanzitutto nel caso in cui $\varepsilon \in K$.

TEOREMA 13.1 *Sia $\varepsilon \in K$ una radice m-esima primitiva dell'unità. Un'estensione $K \subseteq E$ è Galoissiana con gruppo $G(E/K)$ ciclico di ordine un divisore di m se e solo se $E = K(a)$ con $a^m \in K$, (cioè si ottiene da K estraendo un radicale m-esimo di un numero di K).*

Dimostrazione Supponiamo $E = K(a)$, con $a^m = b \in K$. Poichè per ipotesi $\varepsilon \in K$, $\varepsilon^i a \in K(a)$ per ogni i; $K(a)$ si ottiene allora da K aggiungendo tutte le radici del polinomio $x^m - b = 0$ e quindi $K \subseteq K(a)$ è Galoissiana (cfr.1) del teorema 10.6). Calcoliamone il gruppo di Galois. Se $\sigma \in G(K(a)/K)$, allora $\sigma(a)$ deve essere una delle radici $\varepsilon^i a$ di $x^m - b$, quindi $\sigma(a)/a$ è una delle radici m-esime dell'unità, viceversa σ è individuato dalla sua azione su a e quindi da $\sigma(a)/a$. Si è così trovata un'applicazione iniettiva $G(K(a)/K) \to \Gamma_m$ ove $\Gamma_m = \{1, \varepsilon, \ldots, \varepsilon^{m-1}\}$ è il gruppo (ciclico) delle radici m-esime dell'unità. Se proviamo che essa è un omomorfismo avremo che $G(K(a)/K)$ è isomorfo ad un sottogruppo di Γ_m e quindi è ciclico di ordine un divisore di m. Siano dunque $\sigma, \gamma \in G(K(a)/K)$, dobbiamo verificare che $\sigma\gamma(a)/a = \sigma(a)/a \ \gamma(a)/a$. In effetti $\gamma(a)/a \in K$, quindi $\sigma(\gamma(a)/a) = \sigma\gamma(a)/\sigma(a) = \gamma(a)/a$ da cui l'uguaglianza desiderata. Abbiamo così concluso la prima parte del teorema.
Il viceversa non potremo completarlo qui, perchè ci servono alcune nozioni generali che svilupperemo nel prossimo paragrafo. Procediamo per ora fino al punto in cui gli strumenti di cui già siamo in possesso ce lo consentono.
Sia $K \subseteq E$ Galoissiana con gruppo di Galois $\{1, \sigma, \ldots, \sigma^{n-1}\}$ ciclico di ordine $n \mid m$. Le radici n-esime dell'unità $1, \eta, \eta^2, \ldots, \eta^{n-1}$ sono in K in quanto potenze di ε. Per ogni elemento $b \in E$ sia $a = b + \eta\sigma(b) + \eta^2\sigma^2(b) + \ldots + \eta^{n-1}\sigma^{n-1}(b) = \sum_{i=0}^{n-1} \eta^i \sigma^i(b)$, (tale a prende il nome di *risolvente di Lagrange di b*).
Si ha: $\sigma(a) = \sum_{i=0}^{n-1} \eta^i \sigma^{i+1}(b) = 1/\eta \ a$, $\sigma^i(a) = 1/\eta^i \ a$. Se $a \neq 0$ gli elementi a, $\sigma(a) = 1/\eta \ a$, $\sigma^2(a) = 1/\eta^2 \ a, \ldots, \sigma^{n-1}(a) = 1/\eta^{n-1} \ a$ sono tutti distinti e quindi $[K(a) : K] = n$, cioè $K(a) = E$. Inoltre $a^n \ K$; infatti $\sigma(a^n) = \sigma(a)^n = 1/\eta^n \ a^n = a^n$ cioè a^n è invariante rispetto a σ e quindi rispetto a tutte le potenze di σ che costituiscono l'intero gruppo di Galois di E su K.
Il teorema è dimostrato se riusciamo a trovare un $b \in K$ tale che la corrispondente risolvente di Lagrange a sia non nulla. E' precisamente questo che vedremo come conseguenza del corollario 14.7. ▽△

Ritorniamo ora allo studio dell'estensione $K \subseteq K\ (a, \varepsilon a, \varepsilon^2 a, \ldots, \varepsilon^{m-1} a)$ che ci siamo proposti all'inizio del paragrafo. La radice ε in generale non appartiene a K. In ogni caso abbiamo però la catena di estensioni $K \subseteq K(\varepsilon) \subseteq K(a, \varepsilon a, \ldots, \varepsilon^{m-1} a) = F$, visto che $\varepsilon = \varepsilon a / a \in F$. Tenuto conto che $F = K(\varepsilon)(a)$, $\varepsilon \in K(\varepsilon)$ e $a^m = b \in K(\varepsilon)$, per il teorema 13.1 abbiamo che l'estensione $K(\varepsilon) \subseteq F$ è Galoissiana e $G(F/K(\varepsilon))$ è ciclico di ordine un divisore di m. D'altra parte $K \subseteq K(\varepsilon)$ è Galoissiana con gruppo di Galois commutativo (Teorema 11.2), e risulta

$$G(K(\varepsilon)/K) \simeq \frac{G(F/K)}{G(F/K(\varepsilon))}$$

In conclusione si ha il seguente:

COROLLARIO 13.2 *$G(F/K)$ ha un sottogruppo normale ciclico con quoziente un gruppo abeliano.*

§ 14 TRACCIA, NORMA E DISCRIMINANTE

Sia $K \subseteq E$ un'estensione finita, $n = [E : K]$, $\sigma_1, \sigma_2, \ldots, \sigma_n$ gli n isomorfismi di E su K.

DEFINIZIONE 14.1 Per ogni polinomio $f(x) \in E[x]$ consideriamo il polinomio:

$$N_{E/K}(f(x)) = \prod_{i=1}^{n} \sigma_i f(x).$$

1) $N_{E/K}(f(x))$ prende il nome di *norma del polinomio* $f(x)$ nell'estensione $K \subseteq E$.

2) Se $f(x) = x - a$, $N_{E/K}(x - a)$ si chiama *polinomio caratteristico* di a in $K \subseteq E$; la sua espressione esplicita è data da:

$$N_{E/K}(x - a) = x^n - (\sum \sigma_i(a))x^{n-1} + (\sum_{i<j} \sigma_i(a)\sigma_j(a))x^{n-2} + \ldots + (-1)^n \sigma_1(a)\sigma_2(a)\ldots\sigma_n(a).$$

3) La quantità $\mathrm{Tr}_{E/K}(a) = \sum_i \sigma_i(a)$ si chiama *traccia* di a nell'estensione $K \subseteq E$.

La quantità $N_{E/K}(a) = \prod_i \sigma_i(a)$ si chiama *norma* di a nell'estensione $K \subseteq E$.

La proprietà fondamentale di questa operazione di passaggio alla norma, che la rende utile, è data dal seguente:

TEOREMA 14.2 i) $N_{E/K}(f(x)g(x)) = N_{E/K}(f(x)) \cdot N_{E/K}(g(x))$

ii) $N_{E/K}(f(x)) \in K[x]$

iii) *Se $K \subseteq E \subseteq F$ sono estensioni finite allora*

$$N_{F/K}(f(x)) = N_{E/K}(N_{F/K}(f(x))).$$

Dimostrazione i) è evidente dalla definizione.

ii) Sia $F = \sigma_1(E)\sigma_2(E)\ldots\sigma_n(E)$ il composto dei campi $\sigma_i(E)$. Poichè $\sigma_i(E) \subset F$ si ha che $\sigma_i f(x) \in F[x]$ e quindi $N_{E/K}(f(x)) \in F[x]$. Per provare che tale polinomio è di fatto a coefficienti in K basta provare che esso è mutato in sé da qualunque K-isomorfismo $\varphi: F \to \mathbb{C}$.

Ora $\varphi\sigma_1, \varphi\sigma_2, \ldots, \varphi\sigma_n$ sono K-isomorfismi di E, e sono distinti quindi $\varphi\sigma_1 = \sigma_{i_1}, \ldots, \varphi\sigma_n = \sigma_{i_n}$ per una opportuna permutazione $i_1, \ldots, i_n$ degli indici. Ne segue che:

$$\varphi N_{E/K}(f(x)) = \varphi \prod_h \sigma_h f(x) = \prod_h \varphi\sigma_h f(x) = \prod_h \sigma_{i_h} f(x) = N_{E/K}(f(x)) \ .$$

iii) Siano: $[E : K] = n$; $[F : E] = m$; G una estensione Galoissiana di K contenente F; ψ_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$, degli automorfismi di G che ristretti ad F danno tutti i K-isomorfismi di F. Supponiamo inoltre di aver numerato i ψ_{ij} in modo tale che, per j fissato, le restrizioni di ψ_{ij} ad F siano tutte le estensioni di uno stesso isomorfismo dato σ_j di E. In particolare le ψ_{i1} estendono la σ_1 che è l'identità di E e quindi danno, ristretti ad F, tutti gli E-isomorfismi di F.

Si ha: $N_{F/K}(f(x)) = \prod_{ij} \psi_{ij} f(x)$; $N_{F/E}(f(x)) = \prod_i \psi_{i1} f(x)$; $N_{E/K}(N_{F/E}(f(x))) = \prod_j \sigma_j(N_{F/E}(f(x))) =$

$$= \prod_j \psi_{1j}(\prod_i \psi_{i1} f(x)) = \prod_{i,j} \psi_{1j}\psi_{i1} f(x).$$

Consideriamo gli automorfismi $\psi_{1j}\psi_{i1}$ di G; affermiamo che essi, ristretti ad F, danno tutti i K-isomorfismi di F; e questo prova il teorema. Basta allora verificare che $\psi_{1j}\psi_{i1}$, ristretti ad F, per coppie di indici i, j distinte, sono distinti. Ora ψ_{i1} è l'identità su E, quindi $\psi_{1j}\psi_{i1}$ è una delle estensioni di σ_j e $\psi_{1j}\psi_{i1} \neq \psi_{1j}\psi_{h1}$ su F se $i \neq h$. ▽△

COROLLARIO 14.3 *Siano $K \subseteq E \subseteq F$ estensioni finite.*
Se $a \in F$ allora:

$$\mathrm{Tr}_{F/K}(a) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{F/E}(a)) \quad ; \quad N_{F/K}(a) = N_{E/K}(N_{F/E}(a))$$

Dimostrazione Basta prendere $f(x) = x - a$ e calcolare i coefficienti desiderati. ▽△

Il polinomio caratteristico di un elemento a di una estensione $K \subseteq E$ finita è in strettissima relazione con il suo polinomio minimo; sussiste infatti il seguente:

TEOREMA 14.4 i) *Se $E = K(a)$ allora $N_{E/K}(x - a)$ è il polinomio minimo di a su K.*
ii) *Se $a \in K \subseteq E$ allora $N_{E/K}(x - a) = (x - a)^n$, ove $n = [E : K]$*
iii) *Se $K \subseteq K(a) \subseteq E$ allora $N_{E/K}(x - a) = (f(x))^s$, dove $f(x)$ è il polinomio minimo di a su K ed $s = [E : K(a)]$.*

Dimostrazione i) Sia $n = [E : K]$ e $\sigma_1, \ldots, \sigma_n$ gli n K-isomorfismi di E. Il polinomio minimo di a su K ha n radici $a = a_1, a_2, \ldots, a_n$, ove le radici sono state numerate in modo che $\sigma_i(a) = a_i$. Quindi $f(x) = \prod_{i=1}^{n} (x - a_i) = \prod_{i=1}^{n} (x - \sigma_i(a)) = N_{E/K}(x - a)$.

ii) Se $a \in K$, $\sigma_i(a) = a$ e quindi $\prod_{i=1}^{n} (x - \sigma_i(a)) = (x - a)^n$.

iii) Si ottiene da i) e ii) con il seguente calcolo:

$$N_{E/K}(x - a) = N_{K(a)/K}(N_{E/K(a)}(x - a)) = N_{K(a)/K}((x - a)^s) = (N_{K(a)/K}(x - a))^s = (f(x))^s. \ \text{▽△}$$

Siano: $K \subseteq E$ un'estensione di grado n; $\sigma_1,\dots,\sigma_n$ gli n K-isomorfismi di E; $a_1,\dots,a_n$ una base di E come spazio vettoriale su K. Consideriamo la matrice $(\sigma_i(a_j))$:

DEFINIZIONE 14.5 $\Delta = \det(\sigma_i(a_j))$ si chiama *discriminante della base* $a_1,\dots,a_n$.

PROPOSIZIONE 14.6 i) $\Delta^2 = \det(\mathrm{Tr}_{E/K}(a_i a_j)) \in K$
ii) $\Delta \neq 0$.

Dimostrazione i) Sia $A = (\sigma_i(a_j))$; calcoliamo $A\,{}^tA = (c_{ij})$. Si ha $c_{ij} = \sum_k \sigma_k(a_i)\sigma_k(a_j) = \sum_k \sigma_k(a_i a_j) = \mathrm{Tr}(a_i a_j)$.
Ne segue che $\Delta^2 = \det A^t \times \det A = \det(\mathrm{Tr}(a_i a_j))$. Inoltre $\Delta^2 \in K$, visto che $\mathrm{Tr}(a_i a_j) \in K$.
ii) Per provare che $\Delta \neq 0$, basta verificare che la matrice $(\mathrm{Tr}(a_i a_j))$ è non singolare. A tal scopo consideriamo la forma bilineare $\mathrm{Tr} : E \times E \to K$ definita da $(a,b) \rightsquigarrow \mathrm{Tr}(ab)$, $a,b \in E$. Essa è non degenere perchè se $a \neq 0$ $(a,a^{-1}) \rightsquigarrow \mathrm{Tr}(aa^{-1}) = \mathrm{Tr}(1) = n$. Ne segue che $\det(\mathrm{Tr}(a_i a_j)) \neq 0$. ▽△

COROLLARIO 14.7 *Siano* $\alpha_1,\dots,\alpha_n$ *numeri complessi;* $K \subseteq E$ *un'estensione finita di grado* n*;* $\sigma_1,\dots,\sigma_n$ *gli* n K*-isomorfismi di* E *su* K*. Esiste allora un* $b \in E$ *tale che* $\sum \alpha_i \sigma_i(b) \neq 0$.

Dimostrazione Se così non fosse si avrebbe $\sum \alpha_i \sigma_i(a_j) = 0$, per ogni j, ove $a_1,\dots,a_n$ è una base di E su K. Ne seguirebbe $\Delta = 0$, mentre abbiamo provato che $\Delta \neq 0$. ▽△

Osservazione 14.8 Il corollario precedente permette di completare la dimostrazione del teorema 13.1. In quel caso $G(E/K) = \{1,\sigma,\dots,\sigma^{n-1}\}$, e, con riferimento ai numeri complessi $1, \eta, \eta^2,\dots,\eta^{n-1}$, il corollario ora provato ci permette di affermare che esiste un $b \in E$ per il quale la corrispondente risolvente di Lagrange $a = \sum \eta^i \sigma^i(b) \neq 0$.

§ 15 RISOLUBILITA' DI UN'EQUAZIONE PER RADICALI: IL TEOREMA DI ABEL-RUFFINI

In questo paragrafo vogliamo dare risposta al problema, di cui abbiamo parlato nell'introduzione, sulla risolubilità per radicali di un'equazione $f(x) = 0$, ove $f(x) \in K[x]$.
Prima di tutto, cosa vuol dire esattamente risolvere l'equazione algebrica $f(x) = 0$ per radicali? Poniamo le seguenti definizioni:

DEFINIZIONE 15.1 Diremo che $f(x) = 0$, $f(x) \in K[x]$, è *risolubile per radicali* a partire da K se esiste una successione di campi $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_m$ tali che $K_{i+1} = K_i(a_i)$ con $a_i^{n_i} \in K_i$, (n_i numero naturale), ed inoltre K_m contiene tutte le radici del polinomio $f(x)$.

La condizione posta richiede quindi che il campo K_{i+1} si ottenga da K_i aggiungendo una radice di un elemento di K_i.
Una condizione necessaria e sufficiente perchè l'equazione $f(x) = 0$, $f(x) \in K[x]$, sia risolubile per radicali è fornita dal teorema di Abel-Ruffini.
Per poter dare una formulazione semplice a tale teorema, conviene innanzi tutto introdurre la nozione di *gruppo risolubile*.

DEFINIZIONE 15.2 Un gruppo G si dice *risolubile* se esiste una catena di sottogruppi $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = 1$ tali che G_{i+1} è normale in G_i ed i quozienti G_i/G_{i+1} sono commutativi.

TEOREMA 15.3 (di Abel-Ruffini) *L'equazione* $f(x) = 0$, $f(x) \in K[x]$, *è risolubile per radicali se e solo se il gruppo di Galois del polinomio* $f(x)$ *è risolubile.*

Per poter dare la dimostrazione abbiamo bisogno di alcune proprietà di gruppi risolubili.

PROPRIETA' 15.4 (dei gruppi risolubili) i) Se G è risolubile allora ogni sottogruppo $H \subseteq G$ è risolubile.
ii) Sia G un gruppo ed $H \subseteq G$ un sottogruppo normale, allora G è risolubile se e solo se H e G/H sono risolubili.
iii) Se G è risolubile esiste una successione di sottogruppi $G = G_0' \supseteq G_1' \supseteq \dots \supseteq G_m' = 1$ per i quali sono verificate le condizioni della 15.3 ed inoltre G_i'/G_{i+1}' è ciclico.

Dimostrazione i) Sia $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = 1$ una catena di sottogruppi verificanti la proprietà di 15.2. Posto $H_i = H \cap G_i$ si ha: $H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_m = 1$; inoltre

$$H_i/H_{i+1} = \frac{H \cap G_i}{H \cap G_{i+1}} \simeq \frac{(H \cap G_i)}{G_{i+1}} \subseteq G_i/G_{i+1}$$

questo prova che H_i/H_{i+1} è un gruppo abeliano, e quindi anche che H_{i+1} è normale in H_i.
ii) Se G è risolubile ed $H \subseteq G$ è un sottogruppo normale, per i) H è risolubile e ci resta da provare che anche G/H è risolubile. Posto $\Gamma_i = G_i H/H$ si ha:

$$G/H \supseteq \Gamma_1 \supseteq \Gamma_2 \supseteq \dots \supseteq \Gamma_m = 1$$

ed inoltre

$$\frac{\Gamma_i}{\Gamma_{i+1}} = \frac{G_i H}{G_{i+1} H} \simeq \frac{G_i}{G_{i+1} H \cap G_i} \simeq \frac{G_i/G_{i+1}}{(G_{i+1} H \cap G_i)/G_{i+1}},$$

quindi Γ_i/Γ_{i+1}, come quoziente del gruppo abeliano G_i/G_{i+1} è esso stesso un gruppo abeliano.
Viceversa se H e G/H sono risolubili, sia $G/H = \Gamma_0 \supseteq \Gamma_1 \supseteq \dots \supseteq \Gamma_k = 1$ una catena che dà la risolubilità di G/H e consideriamo la catena $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_k = H$ di sottogruppi di G per cui $\Gamma_i = G_i/H$. Poichè H è risolubile esiste una catena $H = G_k \supseteq G_{k-1} \supseteq \dots \supseteq G_m = 1$ di sottogrup-

pi ciascuno normale nel precedente e con quozienti successivi abeliani. La catena $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k \supseteq \ldots \supseteq G_m = 1$ verifica le condizioni di 15.2, visto che G_i/G_{i+1} è un gruppo commutativo se $i \geq k$ per la risolubilità di H, e $G_i/G_{i+1} \simeq \Gamma_i/\Gamma_{i+1}$ è un gruppo commutativo per $i < k$ per la risolubilità di G/H.

iii) Sia $G \supseteq G_1 \supseteq \ldots \supseteq G_m = 1$ una catena che dà la risolubilità di G. Fra G_{i+1} e G_i possiamo introdurre nuovi sottogruppi $G_i = G_{i,0} \supseteq G_{i,1} \supseteq G_{i,2} \supseteq \ldots \supseteq G_{i+1}$ in modo che $G_{i,h}$ sia un sottogruppo normale massimale di $G_{i,h-1}$. Ora i quozienti $G_{i,h-1}/G_{i,h}$ sono abeliani e privi di sottogruppi propri e quindi sono gruppi ciclici aventi ciascuno come ordine un numero primo. ▽△

LEMMA 15.5 *Sia $K \subseteq E$ un'estensione Galoissiana e sia ε una radice primitiva m-esima dell'unità. Risulta allora:*

1) *L'estensione $K(\varepsilon) \subseteq E(\varepsilon)$ è Galoissiana e $G(E(\varepsilon)/K(\varepsilon))$ è un sottogruppo di $G(E/K)$.*

2) *$G(E/K)$ è risolubile se e solo se $G(E(\varepsilon)/K(\varepsilon))$ è risolubile.*

Dimostrazione 1) Basta tener conto della i) di 12.9 con riferimento alle estensioni $K \subset E$, $K \subseteq K(\varepsilon)$ (il composto di E e $K(\varepsilon)$ è $E(\varepsilon)$).

2) Consideriamo le estensioni $K \subseteq K(\varepsilon) \subseteq E(\varepsilon)$ e $K \subseteq E \subseteq E(\varepsilon)$; per la ii) del teorema 10.11 di corrispondenza di Galois abbiamo che:

a) $G(K(\varepsilon)/K) \simeq \dfrac{(G(E)/K)}{G(E(\varepsilon)/K(\varepsilon))}$; b) $G(E/K) \simeq \dfrac{G(E(\varepsilon)/K)}{G(E(\varepsilon)/E)}$

Osserviamo che i gruppi $G(K(\varepsilon)/K)$ e $G(E(\varepsilon)/E)$ sono risolubili in quanto abeliani. Infatti, tenuto conto del teorema 11.2, basta applicare la i) di 12.9 ai seguenti campi:

$$\begin{array}{ccc} Q \subseteq Q(\varepsilon) & & Q \subseteq Q(\varepsilon) \\ \cap & ; & \cap \\ K \subseteq K(\varepsilon) & & E \subseteq E(\varepsilon) \end{array}$$

da b) si ha allora che, se $G(E/K)$ è risolubile, allora anche $G(E(\varepsilon)/K)$ è risolubile (cfr. ii) della proposizione 15.4) e quindi $G(E(\varepsilon)/K(\varepsilon))$ è risolubile (cfr. i) di 15.4). Viceversa, se $G(E(\varepsilon)/K(\varepsilon))$ è risolubile, da a) segue che $G(E(\varepsilon)/K)$ è risolubile, e quindi $G(E/K)$ è risolubile. ▽△

Siamo ora in grado di dare la dimostrazione del teorema di Abel-Ruffini:

Dimostrazione 15.3 Sia E il campo di decomposizione del polinomio $f(x)$. Supponiamo che $G(E/K)$ sia un gruppo risolubile, e sia $m = o(G(E/K))$ il suo ordine. Detta ε una radice primitiva m-esima dell'unità, abbiamo che il gruppo $\Gamma = G(E(\varepsilon)/K(\varepsilon))$ è risolubile ed è un sottogruppo di $G(E/K)$ (lemma 15.5). Sia $\Gamma \supseteq \Gamma_1 \supseteq \ldots \supseteq \Gamma_n = \{1\}$ una catena di sottogruppi che dà la risolubilità di Γ e tale che Γ_i/Γ_{i+1} sia un gruppo ciclico di ordine m_i (cfr. iii) di

15.4); ovviamente m_i divide m.

Indichiamo con $E(\varepsilon) = E_n \supseteq E_{n-1} \supseteq \ldots \supseteq E_0 = K(\varepsilon)$ la catena di sottocampi intermedi corrispondenti ai sottogruppi Γ_i. Dal teorema di corrispondenza di Galois risulta che le estensioni $E_{i+1} \supseteq E_i$ sono Galoissiane con gruppo di Galois Γ_i/Γ_{i+1}; poichè $m_i \mid m$ ed E_i contiene tutte le radici m-esime dell'unità si ha che $E_{i+1} = E_i(a_i)$ con $a_i^{m_i} \in E_i$ e la successione di campi $K \subseteq K(\varepsilon) \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_n = E(\varepsilon)$ dà luogo alla risolubilità per radicali dell'equazione $f(x) = 0$.

Viceversa supponiamo che l'equazione $f(x) = 0$ sia risolubile per radicali. Allora abbiamo una successione di campi $K \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_s$, con $K_{i+1} = K_i(a_i)$ e $a_i^{m_i} \in K_i$, ed inoltre il campo E ottenuto da K aggiungendo le radici di $f(x)$ è tale che $E \subseteq K_s$. Sia m un multiplo di tutti gli m_i ed ε una radice primitiva m-esima dell'unità. Poniamo $K_i' = K_i(\varepsilon)$, $K' = K(\varepsilon)$, $E' = E(\varepsilon)$. Abbiamo la catena di estensioni $K' \subseteq K_1' \subseteq \ldots \subseteq K_s'$ ed ancora $K_{i+1}' = K_i'(a_i)$ con $a_i^{m_i} \in K_i'$, $E' \subseteq K_s'$. Osserviamo quindi che per provare che $G(E/K)$ è risolubile basta provare che $G(E'/K')$ è risolubile (lemma 15.5). A tal scopo consideriamo le estensioni $K' \subseteq E' \subseteq K_s'$ ed osserviamo che, se supponiamo che $K' \subseteq K_s'$ sia Galoissiana, allora $G(E'/K')$ è un quoziente di $G(K_s'/K')$ ed è sufficiente provare che quest'ultimo gruppo è risolubile.

Supponiamo quindi per il momento che $K' \subseteq K_s'$ sia Galoissiana e proviamo la risolubilità del gruppo $G(K_s'/K')$.

Dall'ipotesi fatta segue che le estensioni $K_i' \subseteq K_s'$ sono Galoissiane, d'altra parte l'estensione $K_i' \subseteq K_{i+1}'$ è anch'essa Galoissiana visto che $K_{i+1}' = K_i'(a_i)$ con $a_i^{m_i} \in K_i'$ e inoltre K_i' contiene tutte le radici m_i-esime dell'unità (visto che contiene tutte le radici m-esime ed $m_i \mid m$). Indicato con $\Gamma_i = G(K_s'/K_i')$, dal teorema di corrispondenza di Galois, relativamente alle estensioni $K_i' \subseteq K_{i+1}' \subseteq K_s'$, e dal teorema 13.1 segue che Γ_{i+1} è un sottogruppo normale di Γ_i e che $\Gamma_{i+1}/\Gamma_i \simeq G(K_{i+1}'/K_i')$, ove quest'ultimo gruppo è ciclico. Questo prova la risolubilità di $G(K_s'/K')$. Naturalmente non vi è alcuna ragione per cui l'estensione $K' \subset K_s'$ debba essere di Galois. E' facile modificare, eventualmente allungandola, la catena di partenza in modo tale che tutte le condizioni siano preservate e con il campo finale Galoissiano su K'. A tal scopo indichiamo con $\sigma_1, \ldots, \sigma_t$ gli isomorfismi di K_s' su K' e consideriamo la catena di campi:

$$K_{s+1}' \subseteq K_{s+2}' \subseteq \ldots \subseteq K_{2s}' \subseteq K_{2s+1}' \subseteq \ldots \subseteq K_{2s+1}' \subseteq \ldots \subseteq K_{ts+s}' = \widetilde{K}$$

ottenuti ponendo $K_{hs+i+1}' = K_{hs+i}'(\sigma_h(a_i))$ per $i < s$; più esplicitamente, poniamo

$$K_{hs+i+1}' = K_s'(\sigma_1(a_0))(\sigma_1(a_1))\ldots(\sigma_1(a_{s-1}))(\sigma_2(a_0))(\sigma_2(a_1))\ldots(\sigma_2(a_{s-1}))\ldots(\sigma_h(a_0))\ldots(\sigma_h(a_i))$$

Il campo $\widetilde{K}$ si ottiene evidentemente estraendo successivi radicali di indice uno degli m_i. Vogliamo ora provare che $\widetilde{K}$ è di Galois su K'. Infatti se $\psi : K \to \mathbb{C}$ è un isomorfismo su K' consideriamo uno dei $\sigma_i(a_j)$; poichè $a_j \in K_s'$ e $\sigma_i : K_s' \to \mathbb{C}$, per la costruzione stessa di $\widetilde{K}$

manda K'_s in $\widetilde{K}$, segue che la composizione $K'_s \xrightarrow{\sigma_i} \widetilde{K} \xrightarrow{\psi} \mathbb{C}$ dà luogo ad un K'-isomorfismo di K'_s, e quindi deve aversi $\psi\sigma_i(a_j) = \sigma_k(a_j) \in \widetilde{K}$ per un k opportuno. Segue che ψ permuta i generatori $\sigma_i(a_j)$ di $\widetilde{K}$ su K' e pertanto $K' \subseteq \widetilde{K}$ è di Galois.

Nell'ultima parte di questo paragrafo ci proponiamo di far vedere, come conseguenza del teorema 15.3, i seguenti fatti:

I) *Un'equazione $f(x) = 0$, $f(x) \in K[x]$, di grado $n \leqslant 4$ è sempre risolubile per radicali.*
II) *In generale, le equazioni di grado $n \leqslant 5$ non sono risolubili per radicali.*

Ricordiamo che il gruppo di Galois G di un polinomio $f(x)$ è isomorfo ad un gruppo di permutazioni sulle n radici di $f(x)$ (teorema 10.6), pertanto dovremo studiare la risolubilità o meno del gruppo $\mathcal{S}_n$ di tutte le sostituzioni su n lettere.
Cominciamo col richiamare alcuni fatti elementari sulle sostituzioni.
Siano $\{1,2,3,\ldots,n\}$ gli elementi su cui operano le sostituzioni di $\mathcal{S}_n$, e siano $a_1,\ldots,a_k$ k di tali elementi.
Il simbolo $(a_1 a_2 \ldots a_k)$ indica la permutazione di $\mathcal{S}_n$ (*ciclo* di ordine k) che manda a_i in a_{i+1} per $i < k$, a_k in a_1, e lascia fissi gli altri elementi.
Data una permutazione qualunque $\sigma \in \mathcal{S}_n$, σ si può decomporre come prodotto di cicli operanti su sottoinsiemi disgiunti di $\{1,\ldots,n\}$.
Infatti si considera per esempio l'elemento 1; se $\sigma(1) = 1$ si passa ad un altro elemento. Se $\sigma(1) \neq 1$, si considerano $\sigma(\sigma(1)) = \sigma^2(1), \sigma^3(1), \ldots, \sigma^h(1), \ldots$, per un qualche $k \leqslant n$ dovrà aversi $\sigma^k(1) = 1$ poichè non si può ritrovare uno dei $\sigma^i(1)$, $i < k$, prima di aver trovato 1; si chiude allora il ciclo $(1, \sigma(1), \ldots, \sigma^{k-1}(1))$. σ opera sugli elementi che non figurano nel ciclo già scritto permutandoli fra di loro e si ricomincia con lo stesso procedimento.

Esempio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 7 & 1 & 3 & 6 \end{pmatrix} = (1\ 2\ 5)(3\ 4\ 7\ 6)$$

Se $\sigma, \psi \in \mathcal{S}_n$ e se σ lascia fissi gli elementi che ψ muove, allora $\sigma\psi = \psi\sigma$.
In particolare nella decomposizione di σ in prodotto di cicli su sottoinsiemi disgiunti di $\{1,\ldots,n\}$, i cicli sono permutabili fra loro.

Esempio

$(1\ 2\ 5)(3\ 4\ 7\ 6) = (3\ 4\ 7\ 6)(1\ 2\ 5)$.

Di conseguenza, se $\sigma \in \mathcal{S}_n$, la sua potenza k-ma σ^k è prodotto delle potenze k-me dei singoli cicli della decomposizione di σ e quindi l'ordine di σ è il minimo comune multiplo degli ordini dei cicli della sua decomposizione (nell'esempio sopra citato l'ordine di σ è 12).

Consideriamo n indeterminate $x_1, x_2, \ldots, x_n$ ed il polinomio $\varphi(x) = \prod_{i>j} (x_i - x_j)$. Se $\sigma \in \mathcal{S}_n$, poniamo $\varphi^\sigma(x) = \prod_{i>j} (x_{\sigma(i)} - x_{\sigma(j)})$. E' chiaro che $\varphi^\sigma(x) = \varepsilon^\sigma \varphi(x)$ ove ε^σ vale +1 o -1. ε^σ è per definizione il *segno della permutazione* σ. Si verifica subito che $\varepsilon^{\sigma\psi} = \varepsilon^\sigma \cdot \varepsilon^\psi$ e quindi l'applicazione che associa a σ il suo segno ε^σ è un omomorfismo dal gruppo $\mathcal{S}_n$ al gruppo moltiplicativo $\{+1,-1\}$.

DEFINIZIONE 15.6 Il nucleo dell'omomorfismo $\mathcal{S}_n \longrightarrow \{+1,-1\}$ si chiama *gruppo alterno* su n elementi e si indica con A_n.
Gli elementi $\sigma \in A_n$ si chiamano *permutazioni pari*, e per essi $\varepsilon^\sigma = +1$. Gli elementi $\sigma \in \mathcal{S}_n$ con $\varepsilon^\sigma = -1$ si chiamano *permutazioni dispari*.

E' chiaro che una trasposizione $(a\ b)$ è una permutazione dispari.
Un ciclo $(a_1 \ldots a_k)$ è una permutazione pari o dispari a seconda che k sia dispari o pari, come si vede facilmente per induzione, tenuto conto che $(a_2 a_1)(a_1 a_2 \ldots a_k) = (a_2 a_3 \ldots a_k)$, e quindi che il segno del ciclo di ordine $k-1$ $(a_2 a_3 \ldots a_k)$ è diverso dal segno del ciclo di ordine k $(a_1 a_2 \ldots a_k)$.

PROPOSIZIONE 15.7 *Sia $\sigma \in \mathcal{S}_n$ una permutazione qualunque e sia $\gamma \in \mathcal{S}_n$ decomposta in cicli*

$$\gamma = (a_1 \ldots a_k)(b_1 \ldots b_h)\ldots(c_1 \ldots c_t) \qquad k + h + \ldots + t = n$$

allora $\sigma\gamma\sigma^{-1} = (\sigma(a_1)\ldots\sigma(a_k))(\sigma(b_1)\ldots\sigma(b_h))\ldots(\sigma(c_1)\ldots\sigma(c_t))$.

Dimostrazione Se $\gamma = \gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_s$, ove i γ_i sono cicli, allora $\sigma\gamma\sigma^{-1} = \sigma(\gamma_1\gamma_2\ldots\gamma_s)\sigma^{-1} = (\sigma\gamma_1\sigma^{-1})(\sigma\gamma_2\sigma^{-1})\ldots(\sigma\gamma_s\sigma^{-1})$ e quindi basta verificare l'asserto per un solo ciclo $\gamma = (a_1 \ldots a_k)$.
Consideriamo allora $\sigma(a_1 \ldots a_k)\sigma^{-1}$; prendiamo un elemento c fra gli elementi di $\{1,\ldots,n\}$ su cui le sostituzioni operano. Se $\sigma^{-1}(c)$ non è uno degli elementi $a_1,\ldots,a_k$ allora $\gamma\sigma^{-1}(c) = \sigma^{-1}(c)$ e quindi $\sigma\gamma\sigma^{-1}(c) = c$. Se invece $\sigma^{-1}(c) = a_i$, cioè $c = \sigma(a_i)$ allora $\gamma\sigma^{-1}(c) = a_{i+1} \pmod k$ e $\sigma\gamma\sigma^{-1}(c) = \sigma(a_{i+1})$, quindi $\sigma\gamma\sigma^{-1} = (\sigma(a_1)\ldots\sigma(a_k))$.
E' facile vedere, da questo, che due permutazioni in $\mathcal{S}_n$ sono coniugate se e solo se sono decomposte in cicli dello stesso tipo.

LEMMA 15.8 *A_n è generato dai cicli di ordine 3.*

Dimostrazione Sia $\sigma \in A_n$, poichè σ è una permutazione pari essa opera almeno su tre elementi; sia a uno di essi, $b = \sigma(a) \neq a$, e $c \neq a,b$. Allora la permutazione $\gamma = (bac)\sigma$ opera su meno elementi che σ (lascia fisso a e non permuta gli elementi lasciati fissi da σ); per induzione γ è prodotto di cicli di ordine 3 e quindi la tesi. ▽△

LEMMA 15.9 *Se $n \geqslant 5$ allora due cicli di ordine 3 sono coniugati in A_n.*

Dimostrazione Siano (abc) e (efg) due cicli di ordine 3. Consideriamo una qualunque permutazione σ della forma

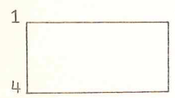
$$\sigma = \begin{pmatrix} a & b & c & \dots \\ e & f & g & \dots \end{pmatrix}$$

e completata in modo arbitrario. Risulta $(efg) = \sigma(abc)\sigma^{-1}$. Si tratta quindi di provare che per $n \geq 5$ la σ può essere scelta in modo tale da essere una permutazione pari. E infatti, se $\sigma = \begin{pmatrix} abc & hk \dots \\ efg & lm \dots \end{pmatrix}$ è dispari, scambiando l'azione di σ in due posti diversi da abc, si ottiene la permutazione pari $\sigma' = \begin{pmatrix} abc & hk \dots \\ efg & ml \dots \end{pmatrix}$ ed ancora $(efg) = \sigma'(abc)\sigma'^{-1}$.

DEFINIZIONE 15.10 Un gruppo G si dice *semplice* se non possiede sottogruppi normali diversi da $\{1\}$ e G.

TEOREMA 15.11 *Il gruppo alterno A_n è risolubile per $n \leq 4$ ed è semplice per $n \geq 5$.*

Dimostrazione Per $n = 1$ tutto è banale. Per $n = 2$, $A_2 = \{1\}$ ed è ancora banale, (si è indicato con 1 la permutazione identica).
Per $n = 3$ il gruppo A_3 consiste delle tre seguenti permutazioni: 1, (1 2 3), (1 3 2) ed è quindi un gruppo ciclico con 3 elementi, esso è quindi risolubile in quanto abeliano.
Per $n = 4$ consideriamo il gruppo commutativo V_4 delle simmetrie di un rettangolo:



$$V_4 \equiv \{1,(12)(34),(13)(24),(14)(23)\}$$

Esso è un sottogruppo di A_4 ed è normale in $\mathcal{S}_4$ in quanto se coniughiamo un elemento di V_4 otteniamo ancora un elemento dello stesso tipo (per la 15.7).
Ora A_4 ha dodici elementi, quindi il quoziente A_4/V_4 ha ordine 3 e pertanto è abeliano.
Passiamo infine al caso $n \geq 5$. Sia $H \subseteq A_n$ un sottogruppo normale ed $H \neq \{1\}$; dobbiamo allora provare che $H = A_n$. Di fatto basta verificare che H contiene un ciclo di ordine 3, in quanto in tal caso per i lemmi 15.8 e 15.9, esso coincide con H.
Sia $\sigma \in H$, $\sigma \neq 1$; se σ è un ciclo di ordine 3 il teorema è provato.
Supponiamo che σ contenga un ciclo di lunghezza almeno 5, sia esso $(a_1a_2a_3a_4a_5)$, e consideriamo la permutazione:

$$\sigma' = (a_1a_2)(a_3a_4)\sigma(a_1a_2)(a_3a_4) = (a_2a_1a_4a_3a_5\dots)(\dots)\dots(\dots) \ .$$

La permutazione σ' è coniugata di σ tramite l'elemento $(12)(34) \in A_n$, pertanto $\sigma' \in H$ e $\sigma'\sigma \in H$; ora $\sigma'\sigma(a_2) = a_5$ quindi $\sigma'\sigma \neq 1$ e opera su meno elementi visto che $\sigma'\sigma(a_1) = a_1$ e $\sigma'\sigma(a_3) = a_3$.
Procedendo quindi per induzione ed il procedimento appena indicato si può sostituire σ con

un altro elemento di H tale che nella sua decomposizione in cicli figurino solo cicli di lunghezza ≤ 4.
Supponiamo di esserci ridotti già a questo caso ed indichiamo sempre con σ un ciclo siffatto. Per esso si possono presentare le seguenti quattro eventualità:
1) σ è prodotto di cicli tutti di lunghezza 3.
2) σ è prodotto di cicli tutti di lunghezza 2.
3) σ è prodotto di cicli alcuni di lunghezza 3 ed altri di lunghezza 2 e 4.
4) σ è prodotto di cicli alcuni di lunghezza 2 ed altri di lunghezza 4.
I casi 3) e 4) si riconducono ad 1) e 2) nel seguente modo. Nel caso 3) basta sostituire σ con $\sigma^4 \neq 1$ che è prodotto solo di cicli di lunghezza 3. Nel caso 4) basta sostituire σ con $\sigma^2 \neq 1$ che è prodotto di cicli tutti di lunghezza 2.
Restano quindi da esaminare i casi 1) e 2). Nel caso 1) σ è della forma $\sigma = (abc)(efg)\dots$ $\dots(\dots)$; posto $\sigma' = (ab)(ce)\sigma(ab)(ce) = (bae)(cfg)\dots$ risulta $\sigma' \in H$ e quindi $\sigma'\sigma \in H$, ove $\sigma'\sigma$ è della forma $\sigma'\sigma = (bfceg)\dots$. Passando quindi da σ alla permutazione $\sigma'\sigma$ si sostituisce il prodotto di due cicli di lunghezza 3 con uno di lunghezza 5, e quindi usando quanto visto per i cicli di lunghezza ≥ 5, e procedendo per induzione, si ottiene un ciclo di lunghezza 3 e il teorema è in questo caso provato.
Nel caso 2) σ è della forma $\sigma = (ab)(cd)(ef)\dots(\dots)$. Posto $\sigma' = (abc)\sigma(abc)^{-1}$, $\sigma', \sigma\sigma' \in H$ e $\sigma\sigma' = (ac)(bd)$. Per ipotesi $n \geq 5$ pertanto vi è un elemento e diverso da a,b,c,d. Coniugando $(ac)(bd)$ con (ace) si ha la permutazione $(ce)(bd) \in H$, finalmente $(ac)(bd)\ (ce)(bd) = (ace) \in H$.
Nel caso 2) σ è della forma $\sigma = (ab)(cd)(ef)\dots(\dots)$.
Quindi H contiene un ciclo di ordine 3 ed il teorema è completamente provato. ∎
Come conseguenza immediata del teorema 15.11 risulta che un'equazione di grado ≤ 4 è sempre risolubile per radicali.
Per terminare la discussione sulla non risolubilità per radicali in generale delle equazioni algebriche di grado $n \geq 5$ basterà far vedere che per ogni numero primo $p \geq 5$ esiste un'equazione algebrica di grado p (a coefficienti razionali) il cui gruppo di Galois (su $\mathbb{Q}$) è $\mathcal{S}_p$. Infatti $\mathcal{S}_p$ non è risolubile per $p \geq 5$, visto che contiene il sottogruppo A_p semplice e non commutativo (e quindi non risolubile).
Premettiamo il seguente:

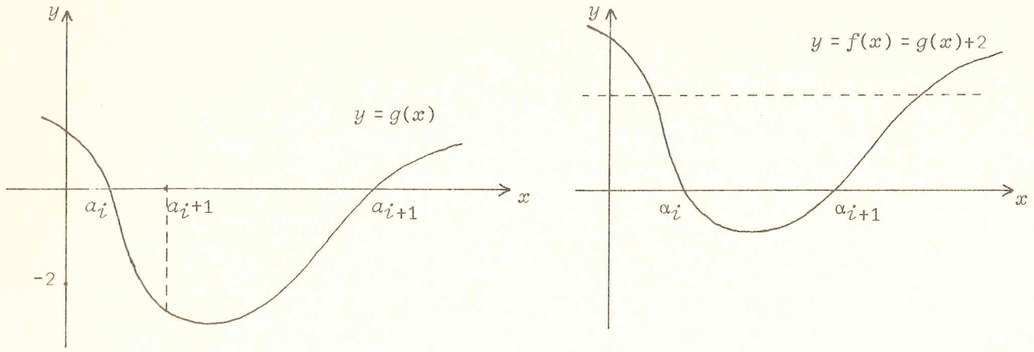
LEMMA 15.12 *Dato un numero primo $p \geq 5$, si può costruire un polinomio irriducibile di grado p a coefficienti razionali con solo due radici complesse.*

Dimostrazione Siano $c > 0, a_1, a_2, \dots, a_k$ $(k > 1)$ dei numeri pari e tali che $a_1 < a_2 < \dots < a_k$, e $\sum a_i = 0$. Consideriamo il polinomio:

$$f(x) = (x^2 + c)(x - a_1)(x - a_2)\dots(x - a_k) + 2.$$

E' facile verificare che $f(x)$ soddisfa il criterio di Eisenstein ed è quindi irriducibile.

Consideriamo ora il polinomio $g(x) = (x^2 + c)(x - a_1)\dots(x - a_k)$ ed il suo grafico:



tenuto conto che $a_i < a_i + 1 < a_{i+1}$ e calcolato il valore $g(a_i + 1)$, si vede che i valori minimi assunti da $g(x)$ sono tutti minori di -2 ($k > 1$). Quindi il polinomio $f(x) = g(x) + 2$ conserva almeno le k radici reali ottenute traslando il grafico di $g(x)$ della quantità -2. Se in tale traslazione $f(x)$ acquistasse un'altra radice reale, tutte le sue radici sarebbero reali. Espandiamo il polinomio $f(x)$:

$$f(x) = x^{k+2} + (c + \sum_{i<j} a_i a_j)x^k + \dots .$$

Se $\alpha_1, \alpha_2, \dots, \alpha_{2k}$ sono le radici di $f(x)$ allora

$$\sum \alpha_i = 0 \ , \quad \sum_{i<j} \alpha_i \alpha_j = c + \sum_{i<j} a_i a_j$$

e quindi

$$\sum_{i<j} \alpha_i \alpha_j = \frac{1}{2}\left[(\sum \alpha_i)^2 - \sum \alpha_i^2\right] = -\frac{1}{2}(\sum \alpha_i^2)$$

Se tutte le radici α_i sono reali $\sum_{i<j} \alpha_i \alpha_j$ risulta negativo, quindi se si sceglie c abbastanza grande, in modo che $c + \sum_{i<j} a_i a_j = \sum_{i<j} \alpha_i \alpha_j$ sia positivo, il polinomio $f(x)$ dovrà avere una e quindi esattamente due radici complesse. ▽△

PROPOSIZIONE 15.13 *Per ogni primo $p \geq 5$ esiste un polinomio a coefficienti razionali il cui gruppo di Galois (su $\mathbb{Q}$) è il gruppo $\mathcal{S}_p$.*

Dimostrazione Sia $f(x)$ un polinomio irriducibile di grado p a coefficienti in $\mathbb{Q}$ e con due sole radici complesse (Lemma 15.12), e sia α una sua radice. Si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. Indicato con $E \supseteq \mathbb{Q}$ il campo di decomposizione di $f(x)$, risulta che p divide $[E : \mathbb{Q}]$.
Sia $G = G(E/\mathbb{Q})$, si ha: $G \subseteq \mathcal{S}_p$ e $p \mid o(G)$ ($o(G)$ = ordine di G) ne segue che G contiene un elemento di ordine p (poichè p è primo), quindi G contiene un ciclo σ di ordine p.
D'altra parte l'automorfismo di coniugazione dei numeri complessi induce un automorfismo di E che permuta fra di loro le due radici complesse e lascia fisse le altre radici, esso

è pertanto una trasposizione, e possiamo assumere sia $\tau = (12)$. Poichè per un qualche $i < p$ risulta $\sigma^i(1) = 2$, e σ^i è ancora un ciclo di lunghezza p, (p è primo), con una scelta conveniente dei simboli, potremo sempre supporre che G contenga il ciclo $\mu = (12\dots p)$.
Siamo ora in grado di provare che ogni trasposizione è in G. Infatti:

$$\mu\tau\mu^{-1} = (23);\ \mu^2\tau\mu^{-2} = (34);\dots\mu^{i-1}\tau\mu^{-(i-1)} = (i\ i+1)$$

Segue che le trasposizioni della forma $(i\ i+1)$ sono in G. D'altra parte

$$(23)(12)(23) = (13);\ (34)(13)(34) = (14);\dots(i\ i+1)(1i)(i\ i+1) = (1\ i+1)$$

e $(1\ j)(1\ i)(1\ j) = (i\ j) \in G$.
Segue che $G = \mathcal{S}_p$.
E' possibile dimostrare che esistono polinomi a coefficienti razionali che ammettono come gruppo di Galois il gruppo $\mathcal{S}_n$ ed A_n per ogni intero n. Questo è conseguenza del seguente teorema di Hilbert:

TEOREMA DI IRRIDUCIBILITA' *Dato un polinomio $f(x_1,\dots,x_n)$ in n variabili, a coefficienti razionali, irriducibile, è possibile attribuire alle variabili $x_2,\dots,x_n$ valori razionali $a_2,\dots,a_n$ in infiniti modi ottenendo $f(x_1,a_2,\dots,a_n)$ irriducibile (come polinomio nella sola x_1).*

Per la dimostrazione cfr.D.Hilbert: *Gesammelte Abhandlungen*. Volume II, pagina 264.

Oltre a questo teorema di Hilbert è noto che ogni gruppo risolubile è ottenibile come gruppo di Galois sui razionali (Šafarevich) ma non è noto se ogni gruppo finito sia ottenibile (cfr. Math.Reviews, Volume 16-1955 - pagine 571-572).

ESERCIZIO 15.14 Sia $E \supseteq K$ di Galois con gruppo S_4 e $\tau = (12)(34)$. Provare che $E^\tau \supseteq E^{V_4}$ e $E^{V_4} \supseteq K$ sono di Galois, ma $E^\tau \supseteq K$ non è di Galois.

§ 16 LE EQUAZIONI DI 3° E 4° GRADO

La teoria di Galois esposta nei paragrafi precedenti, oltre a dare la risposta generale al problema della risolubilità di un'equazione algebrica per radicali, è anche utile per il calcolo esplicito delle formule di risoluzione per le equazioni di terzo e quarto grado.

L'EQUAZIONE CUBICA 16.1 Sia (1) $x^3 + ax^2 + bx + c$ l'equazione di terzo grado.
Con la sostituzione $x = y - a/3$ si ottiene l'equazione (2) $y^3 + py + q = 0$

ove si è posto $p = b - a^2/3$, $q = c - ba/3 + 2a^2/27$.
Risolvere la seconda equazione è chiaramente equivalente a risolvere la prima.
Siano $\alpha_1, \alpha_2, \alpha_3$ le tre radici di (2). Risulta

$$(y - \alpha_1)(y - \alpha_2)(y - \alpha_3) = y^3 + py + q$$

da cui $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = p$, $-\alpha_1\alpha_2\alpha_3 = q$.
Sia K un campo contenente p, q e le radici cubiche dell'unità e sia $E = K(\alpha_1\alpha_2\alpha_3) \supseteq K$. Il gruppo di Galois $G(E/K)$ è un gruppo di permutazioni sugli elementi $(\alpha_1, \alpha_2, \alpha_3)$. Supponiamo che $G(E/K)$ sia l'intero gruppo $\mathcal{S}_3$. Sia $F \subseteq E$ il campo intermedio associato al sottogruppo $A_3 \subset \mathcal{S}_3$ delle permutazioni di classe pari (cfr. teorema 10.11). Poichè l'estensione $F \subseteq E$ è di Galois ciclica, essa si ottiene da F aggiungendo una radice cubica (F contiene le radici cubiche di 1, cfr. teorema 13.1).
Formiamo la risolvente di Lagrange di α_1 (cfr. dimostrazione del teorema 13.1). Indicate con $1, \eta, \eta^2$ le tre radici cubiche dell'unità, se fissiamo come generatore di A_3 l'automorfismo che permuta ciclicamente $(\alpha_1\alpha_2\alpha_3)$ si ottiene:

$$\gamma = \alpha_1 + \eta\alpha_2 + \eta^2\alpha_3 .$$

Se si fissa l'automorfismo $(\alpha_1\alpha_3\alpha_2)$ si ottiene:

$$\bar{\gamma} = \alpha_1 + \eta\alpha_3 + \eta^2\alpha_2 .$$

In ogni caso si ha:

$$\gamma^3 = (\alpha_1 + \eta\alpha_2 + \eta^2\alpha_3)^3 \in F; \quad \bar{\gamma}^3 = (\alpha_1 + \eta\alpha_3 + \eta^2\alpha_2)^3 \in F$$

Ora il campo F è quadratico su K; le permutazioni pari danno luogo all'automorfismo identico di F, le permutazioni dispari, per esempio la trasposizione $(\alpha_2\alpha_3)$, danno luogo all'altro possibile K-automorfismo (cfr.2) del teorema di Corrispondenza di Galois).
Poichè il trasformato di γ^3 tramite l'automorfismo non identico di F è $\bar{\gamma}^3$, l'equazione di γ^3 su K è:

$$(x - \gamma^3)(x - \bar{\gamma}^3) = x^2 - (\gamma^3 + \bar{\gamma}^3)x + \gamma^3\bar{\gamma}^3 .$$

Posto $\lambda = \gamma^3 + \bar{\gamma}^3 \in K$, $\mu = \gamma^3\bar{\gamma}^3 \in K$, risolvendo l'equazione di secondo grado si ha:

$$\begin{cases} \alpha_1 + \eta\alpha_2 + \eta^2\alpha_3 = \sqrt[3]{\dfrac{\lambda + \sqrt{\lambda^2 - 4\mu}}{2}} = Q \\ \alpha_1 + \eta\alpha_3 + \eta^2\alpha_2 = \sqrt[3]{\dfrac{\lambda - \sqrt{\lambda^2 - 4\mu}}{2}} = P \\ \alpha_1 + \alpha_2 + \alpha_3 = 0 \end{cases}$$

da cui si ricava:

$$\alpha_1 = \frac{1}{3}(P + Q); \quad \alpha_2 = \frac{1}{3}(P\eta + Q\eta^2); \quad \alpha_3 = \frac{1}{3}(Q\eta + P\eta^2).$$

Per determinare λ e μ in funzione dei coefficienti p e q dell'equazione 2) ricordiamo che:

$$-\alpha_1\alpha_2\alpha_3 = q, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$$

da cui, sostituendo i valori di α_i in funzione di P e Q e tenendo conto che $1 + \eta + \eta^2 = 0$, si ha:

$$-q = \alpha_1\alpha_2\alpha_3 = \frac{1}{27}(P^3 + Q^3) = \frac{\lambda}{27}$$

$$p = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -\frac{PQ}{3} = \sqrt[3]{\mu/3}$$

da cui si ricava infine:

$$\alpha_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{2} + \frac{p^3}{27}}}$$

etc.
Una derivazione elementare di questa formula, che qui abbiamo illustrata facendo uso della teoria generale, è la seguente. Essa si basa sull'identità,

$$(a + b)^3 - 3ab(a + b) - a^3 - b^3 = 0$$

Quindi se è possibile trovare due numeri a e b tali che $-3ab = p$, $-a^3 - b^3 = q$, allora il numero $a + b$ è soluzione dell'equazione $y^3 + py + q = 0$.
Le due condizioni scritte sono equivalenti a

$$a^3b^3 = -\frac{p^3}{27}, \quad a^3 + b^3 = -q$$

quindi a^3 e b^3 sono le radici dell'equazione:

$$x^2 + qx - \frac{p^3}{27} = 0$$

Le formule risolutive dell'equazione di secondo grado forniscono il risultato voluto.

L'EQUAZIONE DI QUARTO GRADO 16.2 Osserviamo innanzitutto che l'equazione generale di quarto grado $x^4 + ax^3 + bx^2 + cx + d = 0$, può sempre ridursi mediante una sostituzione, alla forma:

$$(3) \quad x^4 + mx^2 + nx + t = 0$$

La soluzione di tale equazione si basa sulla seguente identità (che il lettore può facilmente verificare):

$$(a + b + c)^4 - 2(a^2 + b^2 + c^2)(a + b + c)^2 - 8abc(a + b + c) + (a^2 + b^2 + c^2)^2 - 4(a^2b^2 + a^2c^2 + b^2c^2) = 0$$

Quindi se si riescono a trovare tre numeri a, b, c tali che $-2(a^2 + b^2 + c^2) = m$; $-8abc = n$; $(a^2 + b^2 + c^2)^2 - 4(a^2b^2 + b^2c^2 + a^2c^2) = t$ allora $a + b + c$ è soluzione dell'equazione (3).
Le condizioni scritte per i numeri a, b, c sono equivalenti alle:

$$a^2 + b^2 + c^2 = -\frac{m}{2}$$

$$a^2b^2c^2 = \frac{m^2}{64}$$

$$a^2b^2 + b^2c^2 + a^2c^2 = \frac{m^2}{16} - \frac{t}{4}$$

I numeri a^2, b^2, c^2 sono soluzioni dell'equazione cubica

$$z^3 + \frac{m}{2} z^2 + (\frac{m^2}{16} - \frac{t}{4})z - \frac{n^2}{64} = 0$$

e sono quindi forniti dalle formule per l'equazione cubica.
Da essi si passa ai numeri a, b, c e si ottengono formule per l'equazione di quarto grado.
Queste formule sono ottenute facendo uso di un artificio al quale si può dare una giustificazione facendo uso della teoria di Galois.
Infatti sia K un campo contenente m, n, t e le radici cubiche dell'unità e sia E il campo ottenuto da K aggiungendo le quattro radici $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ dell'equazione (3). Supponiamo che il gruppo di Galois $G(E/K) = \mathcal{S}_4$. Sia V_4 il sottogruppo di $\mathcal{S}_4$ introdotto all'inizio del teorema 15.11, cioè il sottogruppo delle simmetrie di un rettangolo, e sia $F = E^{V_4}$ il campo intermedio ad esso associato.
E si ottiene da F aggiungendo due radici quadrate di elementi di F. Infatti considerati gli automorfismi $\tau = (12)(34)$, $\sigma = (13)(24)$, le estensioni:

$$E^\tau = E^{\{1,\tau\}} \supseteq F, \quad E^\sigma = E^{\{1,\sigma\}} \supseteq F$$

si ottengono da F estraendo una radice quadrata (cfr. teorema 13.1). Anche $E^{\sigma\tau}$ si ottiene nello stesso modo.
Sia dunque $E^\sigma = F(\alpha)$, $\alpha^2 \in F$; $E^\tau = F(\beta)$, $\beta^2 \in F$. Si può scegliere β in modo tale che $\beta = \psi(\alpha)$ con ψ una permutazione che coniuga σ e τ. Si ha $\sigma(\alpha) = \alpha$, $\sigma(\beta) = -\beta$.
Una base di E su F è data da $1, \alpha, \beta, \alpha\beta$. Per le radici $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ dell'equazione (3) si ha:

$$\alpha_2 = \tau(\alpha_1); \quad \alpha_3 = \sigma(\alpha_1), \quad \alpha_4 = \sigma\tau(\alpha_1).$$

Poichè $\alpha_i \in E$ possiamo scrivere:

$$\alpha_1 = f_1 + f_2 + f_3\beta + f_4\alpha\beta \qquad f_i \in E$$

Posto $a = f_2\alpha$, $b = f_3\beta$, $c = f_4\alpha\beta$ si ha:

$$\begin{aligned} \alpha_1 &= f_1 + a + b + c \\ \tau(\alpha_1) = \alpha_2 &= f_1 - a + b - c \\ \sigma(\alpha_1) = \alpha_3 &= f_1 + a - b - c \\ \alpha\tau(\alpha_1) = \alpha_4 &= f_1 - a - b + c \end{aligned}$$

Sommando si ricava $0 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4f_1$, per cui risulta:

$$\alpha_1 = a + b + c; \quad \alpha_2 = -a + b - c; \quad \alpha_3 = a - b - c; \quad \alpha_4 = -a - b + c$$

L'equazione (3) si scrive allora:

$$\begin{aligned} x^4 + mx^2 + nx + t &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) = \\ &= \left[x - (a + b + c)\right]\left[x - (-a + b - c)\right]\left[x - (a - b - c)\right]\left[x - (-a - b + c)\right] = \\ &= x^4 - 2(a^2 + b^2 + c^2)x^2 + abcx + (a^2 + b^2 + c^2)^2 - 4(a^2b^2 + a^2c^2 + b^2c^2) \end{aligned}$$

Questo giustifica a posteriori l'artificio usato.
In effetti la teoria svolta implica che $G(F/K) \simeq \mathcal{S}_4/D_4$, ma tale gruppo è isomorfo ad $\mathcal{S}_3$ e tale isomorfismo è ottenuto proprio considerando l'azione di $\mathcal{S}_4$ sui tre elementi a^2, b^2, c^2. Pertanto essendo i tre elementi a^2, b^2, c^2 coniugati fra loro da $\mathcal{S}_3$ potevamo a priori dedurre che sono le radici di un polinomio cubico $(x - a^2)(x - b^2)(x - c^2)$ a coefficienti in K e che F è il campo di decomposizione di tale polinomio cubico.
Il passaggio da $\mathcal{S}_4$ ad $\mathcal{S}_3 \simeq \mathcal{S}_4/D_4$ è quindi equivalente alla riduzione di una equazione di 4° grado ad una cubica.

§ 17 FUNZIONI SIMMETRICHE, SIMMETRICHE ELEMENTARI E DI NEWTON

Sia A un anello commutativo (per esempio $A = \mathbb{Z}$). Consideriamo $n + 1$ variabili: $x_1, x_2, \ldots, x_n, y$ e formiamo il polinomio:

$$\prod_{i=1}^{n} (y - x_i) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - \sigma_3 y^{n-3} + \ldots + (-1)^n \sigma_n$$

ove si è posto:

$$\sigma_1 = \sum_{i=1}^{n} x_i; \quad \sigma_2 = \sum_{i<j} x_i x_j; \ldots; \sigma_k = \sum_{i_1 < i_2 < \ldots < i_k} x_{i_1} x_{i_2} \ldots x_{i_k}; \quad \sigma_n = x_1 x_2 \ldots x_n.$$

Le funzioni $\sigma_1, \sigma_2, \ldots, \sigma_n$ delle variabili $x_1, x_2, \ldots, x_n$ sono funzioni simmetriche nel senso della seguente:

DEFINIZIONE 17.1 Un polinomio $f(x_1, \ldots, x_n)$ si dice *simmetrico* (nelle x_i) se $f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = f(x_1, x_2, \ldots, x_n)$ per ogni permutazione τ degli indici $1, 2, \ldots, n$.

L'importanza delle funzioni $\sigma_1, \sigma_2, \ldots, \sigma_n$, dette anche *funzioni simmetriche elementari* risiede nei due seguenti fatti:

FATTO I Data un'equazione algebrica:

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - a_3 x^{n-3} + \ldots + (-1)^n a_n = 0$$

e dette $\alpha_1, \alpha_2, \ldots, \alpha_n$ le sue radici, si ha:

$$a_i = \sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

FATTO II Ogni funzione simmetrica nelle $x_1, \ldots, x_n$ si esprime polinomialmente nelle σ_i.
In particolare ogni espressione simmetrica nelle radici di un fissato polinomio $f(x)$ è calcolabile come polinomio nei coefficienti di $f(x)$, e quindi è nel campo in cui sono tali coefficienti.

Il primo fatto citato è evidente; il secondo è un teorema notevole su cui Lagrange fondava la teoria delle equazioni algebriche.

Prima di dare la dimostrazione di questo teorema forniamo un esempio.

Una semplice classe di funzioni simmetriche è data dalle *funzioni di Newton:*

$$\psi_k = \sum_{i=1}^{n} x_i^k$$

Come si esprimono le ψ_k tramite le $\sigma_1,\sigma_2,\ldots,\sigma_n$?

Usiamo, a tal scopo, il calcolo formale con le serie.

Sia $f(y) = \prod_{i=1}^{n} (yx_i + 1) = y^n\sigma_n + y^{n-1}\sigma_{n-1} + \ldots + y\sigma_1 + 1$

Calcoliamone la derivata logaritmica in y:

$$\frac{d}{dy} \log f(y) = \frac{f'(y)}{f(y)} .$$

La derivata logaritmica ha due notevoli proprietà:

1) Trasforma prodotti in somme, cioè $(f(y)g(y))' / f(y)g(y) = f'(y)/f(y) + g'(y)/g(y)$;

2) E'un'operazione puramente algebrica.

Nel nostro caso avremo:

$$\frac{d}{dy} \log \prod_{i=1}^{n} (yx_i + 1) = \sum_{i=1}^{n} \frac{x_i}{yx_i + 1} = \sum_{i=1}^{n} x_i \Big(\sum_{m=0}^{\infty} (-yx_i)^m\Big) = \sum_{m=0}^{\infty} \psi_{m+1}(-y)^m .$$

D'altra parte si ha anche

$$\frac{d}{dy} \log f(y) = \frac{n\sigma_n y^{n-1} + (n-1)\sigma_{n-1}y^{n-2} + \ldots + \sigma_1}{\sigma_n y^n + \sigma_{n-1}y^{n-1} + \ldots + \sigma_1 y + 1}$$

Quindi, uguagliando le due espressioni e moltiplicando, si ottiene

$$\left[\sum_{m=0}^{\infty} \psi_{m+1}(-y^m)\right]\left[1 + \sigma_1 y + \ldots + \sigma_n y^n\right] = \sigma_1 + 2\sigma_2 y + \ldots + n\sigma_n y^{n-1}$$

Da questa uguaglianza se ne ottengono infinite, paragonando i coefficienti di y^t, per ogni t:

$$\begin{aligned}
\psi_1 &= \sigma_1 \\
-\psi_2 + \psi_1\sigma_1 &= 2\sigma_2 \\
\psi_3 - \psi_2\sigma_1 + \psi_1\sigma_2 &= 3\sigma_3 \\
-\psi_4 + \psi_3\sigma_1 - \psi_2\sigma_2 + \psi_1\sigma_3 &= 4\sigma_4 \\
&\vdots \\
(-1)^{n-1}\left[\psi_{n-1} - \psi_{n-2}\sigma_1 + \ldots + \psi_1\sigma_{n-1}\right] &= n\sigma_n
\end{aligned}$$

e per $m > n$

$$\psi_m - \psi_{m-1}\sigma_1 + \psi_{m-2}\sigma_2 - \ldots \pm \psi_{m-n}\sigma_n = 0$$

Da questa tabella si vedono tre cose:

i) come calcolare ricorsivamente le funzioni di Newton ψ_i a partire dalle funzioni simmetriche elementari $\sigma_1,\ldots,\sigma_n$,

ii) come calcolare ricorsivamente le σ_i a partire dalle ψ_i $(i = 1,\ldots,n)$, *purchè* i numeri $2,3,\ldots,n$ siano invertibili nell'anello A dei coefficienti considerati.

iii) In particolare, se $2,3,\ldots,n$ sono invertibili, come calcolare le ψ_i per $i > n$, in termini delle $\psi_1,\ldots,\psi_n$.

Torniamo ora al teorema fondamentale delle funzioni simmetriche:

TEOREMA 17.2 *Ogni polinomio $p(x_1,\ldots,x_n)$ simmetrico nelle $x_1,\ldots,x_n$ si può esprimere in modo unico come polinomio nelle funzioni simmetriche elementari $\sigma_1,\ldots,\sigma_n$.*

Dimostrazione Procederemo per induzione su n e sul grado di $p(x_1,\ldots,x_n)$, dando al tempo stesso un metodo costruttivo.

Indichiamo con $\bar\sigma_1,\bar\sigma_2,\ldots,\bar\sigma_{n-1}$ le funzioni simmetriche elementari nelle $x_1,x_2,\ldots,x_{n-1}$ e notiamo le semplici relazioni ricorsive:

$$\sigma_1 = \bar\sigma_1 + x_n;\ \sigma_2 = \bar\sigma_2 + x_n\bar\sigma_1;\ \ldots;\sigma_k = \sigma_k + x_n\sigma_{k-1};\ \sigma_n = x_n\sigma_{n-1}$$

Il polinomio simmetrico $p(x_1,\ldots,x_n)$ può scriversi nella forma $p(x_1,\ldots,x_n) = \sum f_i(x_1,\ldots,x_{n-1})x_n^i$, ove i polinomi $f_i(x_1,\ldots,x_{n-1})$ sono simmetrici nelle $x_1,\ldots,x_{n-1}$ e quindi, per induzione, si possono esprimere come polinomi nelle $\bar\sigma_1,\bar\sigma_2,\ldots,\bar\sigma_{n-1}$. Usando le espressioni ricorsive per le σ_i possiamo scrivere il polinomio $p(x_1,\ldots,x_n)$ come polinomio nelle $\sigma_1,\sigma_2,\ldots,\sigma_n,x_n$:

$$p = \sum g_i(\sigma_1,\sigma_2,\ldots,\sigma_n)x_n^i .$$

Si noti che in tutti i passi effettuati il grado dell'espressione non cambia; possiamo assumere pertanto che il grado di $g_i(\sigma_1,\sigma_2,\ldots,\sigma_n)x_n^i$ sia al più il grado del polinomio p.

Ora $p - g_0(\sigma_1,\ldots,\sigma_n) = x_n\tilde p$, ove si è indicato con $\tilde p$ un polinomio nelle $\sigma_1,\ldots,\sigma_n,x_n$. Segue che x_n divide il polinomio $\bar p = p - g_0(\sigma_1,\ldots,\sigma_n)$.

Dalla simmetria di p e di $g_0(\sigma_1,\ldots,\sigma_n)$ segue che x_i divide $\bar p$ per ogni i e quindi $\bar p = (x_1\ldots x_n)\bar{\bar p} = \sigma_n\bar{\bar p}$.

Il polinomio $\bar{\bar p}$ è ancora simmetrico e di grado inferiore al grado di p. Procedendo per induzione su $\bar{\bar p}$ otteniamo il teorema.

L'unicità è molto semplice e la lasciamo al lettore. ▽△

Esempio Il determinante di Vandermonde. Si consideri il determinante (di Vandermonde)

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = V(x_1,\dots,x_n).$$

PROPOSIZIONE 17.3 $V(x_1,\dots,x_n) = \prod_{i>j} (x_i - x_j)$.

Dimostrazione La proposizione è evidente per $n = 2$. Procederemo per induzione e daremo due diverse dimostrazioni, entrambe elementari.

I Dimostrazione Sottraiamo all'i-esima riga la prima:

$$V(x_1,\dots,x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 0 & x_2-x_1 & x_2^2-x_1^2 & \dots & x_2^{n-1}-x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & x_n-x_1 & x_n^2-x_1^2 & \dots & x_n^{n-1}-x_1^{n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} x_2-x_1 & (x_2-x_1)(x_2+x_1) & (x_2-x_1)(x_2^2+x_1x_2+x_2^2) & \dots & (x_2-x_2)(x_2^{n-2}+x_1x_2^{n-3}+\dots) \\ x_3-x_1 & (x_3-x_1)(x_3+x_1) & \cdot & \cdots & \cdot \\ \vdots & \vdots & \vdots & & \vdots \\ x_n-x_1 & (x_n-x_1)(x_n+x_1) & \cdot & \cdots & \cdot \end{vmatrix} =$$

$$= \prod_{i>1} (x_i - x_1) \begin{vmatrix} 1 & x_2+x_1 & x_2^2+(x_1+x_2)x_1 & \cdots \\ 1 & x_3+x_1 & x_3^2+(x_1+x_3)x_1 & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & x_n+x_1 & \cdot & \cdots \end{vmatrix} =$$

$$= \prod_{i>1} (x_i - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 & \dots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} \end{vmatrix}$$

Nell'ultimo passaggio si è sottratta ad ogni colonna la precedente moltiplicata per x_1. Per l'induzione ammessa si ottiene quindi il risultato finale.

II Dimostrazione Pensiamo $V(x_1,\dots,x_n)$ come polinomio (di grado n-1) nella x_1 ed a coefficienti nel campo delle funzioni razionali in $x_2,\dots,x_n$. Se sostituiamo ad x_1 uno degli x_i per $i > 1$, otteniamo un determinante con due righe uguali e quindi nullo. Segue che $x_2,\dots,x_n$ sono le radici di tale polinomio e quindi:

$$V(x_1,\dots,x_n) = a \prod_{j\neq 1} (x_1 - x_j) = a(-1)^{n-1} \prod_{j>1} (x_j - x_1)$$

ove a è il coefficiente di x_1^{n-1} e può essere determinato espandendo direttamente il determinante di Vandermonde secondo gli elementi della prima riga:

$$a = (-1)^{n-1} V(x_2,\dots,x_n) = (-1)^{n-1} \prod_{i>j>1} (x_i - x_j) \quad \text{(per l'induzione ammessa).}$$

In definitiva si ha:

$$V(x_1,\dots,x_n) = a(-1)^{n-1} \prod_{j>1} (x_j - x_1) = \prod_{i>j} (x_i - x_j). \quad \square$$

Osserviamo che il determinante di Vandermonde $V(x_1,\dots,x_n)$ *non* è una funzione simmetrica; infatti si ha $V(x_{\tau(1)}x_{\tau(2)}\dots x_{\tau(n)}) = \varepsilon^\tau V(x_1,\dots,x_n)$. La stessa uguaglianza mostra però che $V^2(x_1,\dots,x_n)$ è una funzione simmetrica. Per esprimere V^2 tramite le funzioni simmetriche elementari $\sigma_1,\dots,\sigma_n$ conviene trovarne l'espressione mediante i polinomi di Newton ψ_k. E infatti si ha:

$$V^2 = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & & & \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & & & & \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} \psi_0 & \psi_1 & \psi_2 & \dots & \psi_{n-1} \\ \psi_1 & \psi_2 & \psi_3 & \dots & \psi_n \\ \psi_2 & \cdot & \cdot & \dots & \cdot \\ \vdots & & & & \\ \psi_{n-1} & \cdot & \cdot & \dots & \psi_{2n-2} \end{vmatrix}$$

L'ultima matrice scritta prende il nome di *matrice di Bézout*.

Sia $p(x_1,\dots,x_n)$ un polinomio e τ una permutazione su $(1,2,\dots,n)$. Denotiamo con p_τ il polinomio:

$$p_\tau(x_1,\dots,x_n) = p(x_{\tau(1)},x_{\tau(2)},\dots,x_{\tau(n)}).$$

TEOREMA 17.4 *Siano $p(x_1,\dots,x_n)$, $q(x_1,\dots,x_n)$ due polinomi e supponiamo che gli n! polinomi p_{τ_i} $\tau_i \in \mathcal{S}_n$ siano tutti distinti. Esiste allora un polinomio, effettivamente costruibile, $\tau(\sigma_1,\sigma_2,\dots,\sigma_n,y)$ tale che:*

$$qV^2(p_{\tau_1},p_{\tau_2},\dots,p_{\tau_{n!}}) = r(\sigma_1,\sigma_2,\dots,\sigma_n,p).$$

Dimostrazione Proviamo che si possono determinare delle funzioni simmetriche α_i per le quali si abbia:

$$q = \sum_{i=0}^{n!-1} \alpha_i p^i$$

1° Metodo Se $h(x_1,\dots,x_n)$ è un qualunque polinomio, denotiamo con $t(h)$ il polinomio simmetrico:

$$t(h) = \sum_{\tau\in\mathcal{S}_n} h(x_{\tau(1)},\dots,x_{\tau(n)}) = \sum_{\tau\in\mathcal{S}_n} h_\tau$$

Si ha allora:

$$t(qp^j) = \sum_{i=0}^{n!-1} \alpha_i t(p^{i+j}) \qquad j = 0,\dots,n!-1 \ .$$

Il sistema ora scritto è risolubile nelle variabili α_i in quanto il determinante dei coefficienti è il determinante di Bézout degli elementi $p_{\tau_1},p_{\tau_2},\dots,p_{\tau_{n!}}$ che sono per ipotesi distinti; quindi tale determinante è non nullo.

Applicando la regola di Cramer si ha:

$$\alpha_i = \frac{|A_i|}{V^2}$$

dove A_i è una matrice con elementi polinomi simmetrici.

Sostituendo si ha $qV^2 = \sum_{i=0}^{n!-1} |A_i| p^i$, cioè il risultato richiesto.

2° Metodo Applichiamo alla relazione $q = \sum_{i=0}^{n!-1} \alpha_i p^i$ tutte le permutazioni $\tau\in\mathcal{S}_n$:

$$q_\tau = \sum_{i=0}^{n!-1} \alpha_i p_\tau^i .$$

Possiamo pensare di aver dato i valori di q, pensato come polinomio nella variabile p, i cui coefficienti α_i sono da determinare, negli $n!$ punti p_τ. Applicando la formula di interpolazione di Lagrange otteniamo:

$$q = \sum \alpha_i p^i = \sum_{\rho\in\mathcal{S}_n} q_\rho \frac{\prod_{\rho\neq\tau\in\mathcal{S}_n}(p-p_\tau)}{\prod_{\tau\neq\rho}(p_\rho-p_\tau)}$$

Da questa formula si ricava subito la tesi. □

§ 18 RADICI MULTIPLE, IRRIDUCIBILITA'

Vogliamo innanzi tutto mostrare come, dato un polinomio $f(x)$, sia possibile determinare un polinomio $g(x)$ che abbia le stesse radici di $f(x)$, ma per il quale le suddette radici siano tutte semplici.

Abbiamo già visto che le radici multiple di $f(x)$ sono quelle radici che $f(x)$ ha in comune con la sua derivata $f'(x)$ (cfr. lemma 8.14). Se α è una radice di molteplicità n per $f(x)$ allora α ha molteplicità esattamente n-1 come radice di $f'(x)$.

Indichiamo con $h(x)$ il massimo comun divisore di $f(x)$ ed $f'(x)$. Risulta allora $f(x) = g(x)h(x)$ ed il polinomio $g(x)$ ha le proprietà richieste.

Passiamo ora ad illustrare il *criterio di Kronecker* per la determinazione dei fattori irriducibili di un polinomio $f(x)\in\mathbb{Q}[x]$. Tale criterio si estende ai campi F di dimensione finita su $\mathbb{Q}$; ma la dimostrazione richiederebbe ulteriori precisazioni e quindi la tralasciamo.

L'idea è di trovare un test aritmetico, simile a quello per la determinazione di eventuali radici razionali per un'equazione algebrica.

Facendo uso del teorema di Gauss (cfr. 5.5) ci si può limitare a cercare la fattorizzazione di un polinomio a coefficienti interi, tramite polinomi essi stessi a coefficienti interi.

Una prima osservazione fatta da Kronecker è la seguente: come si può determinare un fattore lineare $ax+b$ di $f(x)$? Si scelgono due interi distinti α e β (per esempio $\alpha = 0$ e $\beta = 1$) e si calcolano $f(\alpha)$, $f(\beta)\in\mathbb{Z}$.

Se $ax+b \mid f(x)$ allora si avrà $\gamma_1 = a\alpha+b \mid f(\alpha)$ e $\gamma_2 = a\beta+b \mid f(\beta)$. Pertanto γ_1 e γ_2 devono variare nell'insieme finito delle coppie (γ_1,γ_2) per cui $\gamma_1 \mid f(\alpha)$ e $\gamma_2 \mid f(\beta)$. Per ogni tale coppia (γ_1,γ_2) è univocamente determinato il polinomio $ax+b$ per cui risulta $a\alpha+b = \gamma_1$, $a\beta+b = \beta_1$. Si ha quindi una lista finita di polinomi di primo grado (da cui possiamo scartare quelli a coefficienti non interi) fra cui ricercare gli eventuali fattori di $f(x)$.

Si tratta quindi di effettuare la divisione di $f(x)$ per tutti i possibili candidati e vedere in quali casi il resto è nullo.

In realtà per la determinazione dei fattori lineari $ax+b$ di $f(x) = a_0 + a_1x + \dots + a_nx^n$ si può più semplicemente usare il criterio di Ruffini: $b \mid a_0$, $a \mid a_n$. Noi abbiamo esposto un metodo più lungo che però ha il vantaggio di generalizzarsi alla ricerca dei fattori irriducibili di qualunque grado.

Supponiamo di voler determinare gli eventuali fattori di grado k di $f(x)$. Fissiamo $k+1$ numeri interi distinti $\alpha_1,\alpha_2,\dots,\alpha_{k+1}$ e calcoliamo i valori $f(\alpha_1),f(\alpha_2),\dots,f(\alpha_{k+1})$.

Se $g(x) = \sum_{i=0}^{k} b_ix^i$ divide $f(x)$, si avrà $g(\alpha_i) \mid f(\alpha_i)$. Pertanto si dovranno scrivere tutte

le $(k+1)$-ple $\gamma_1,\gamma_2,\ldots,\gamma_{k+1}$ di divisori di $f(\alpha_1),f(\alpha_2),\ldots,f(\alpha_{k+1})$ rispettivamente. Per ogni $(k+1)$-pla si dovrà determinare $g(x)$ facendo uso delle relazioni

$$g(\alpha_j)=\sum_{i=0}^{k} b_i(\alpha_j)^i=\gamma_j$$

ed infine determinare quali di tali $g(x)$ dividono $f(x)$. Il tutto si basa sul fatto che un polinomio di grado k è determinato dai valori $\gamma_1,\ldots,\gamma_{k+1}$ che assume in $k+1$ numeri distinti. Infatti le $k+1$ equazioni:

$$\sum_{i=0}^{k} b_i(\alpha_j)^i=\gamma_j$$

considerate nelle incognite b_i, hanno per determinante dei coefficienti delle incognite il determinante di Vandermonde

$$V(\alpha_1,\alpha_2,\ldots,\alpha_{k+1})=\prod_{i>j}(\alpha_i-\alpha_j)\neq 0\ .$$

Il polinomio si può direttamnte scrivere facendo uso della formula di interpolazione di Lagrange

$$g(x)=\sum_{j=1}^{k+1}\gamma_j\frac{\prod_{i\neq j}(x-\alpha_i)}{\prod_{i\neq j}(\alpha_j-\alpha_i)}$$

§ 19 METODI EFFETTIVI PER IL CALCOLO DEL GRUPPO DI GALOIS DI UNA EQUAZIONE ALGEBRICA

Sia $f(x)\in\mathbb{Q}[x]$ un polinomio di grado n con radici tutte distinte $\alpha_1,\ldots,\alpha_n$, (confrontare la discussione iniziale del §18).
Per prima cosa vogliamo far vedere che:

PROPOSIZIONE 19.1 *Si possono determinare effettivamente numeri interi $m_1,m_2,\ldots,m_n$ in modo tale che gli $n!$ elementi della forma:*

$$a_\sigma=\sum_i m_i\alpha_{\sigma(i)}\ ,\qquad \sigma\in\mathcal{S}_n$$

siano tutti distinti.

Dimostrazione Questo è equivalente a provare che il prodotto $\prod_{\sigma\neq\tau}(a_\sigma-a_\tau)$ sia non nullo. Ragioniamo formalmente nel modo seguente. Il polinomio $\prod_{\sigma\neq\tau}(\sum_{i=1}^{n} x_i(\alpha_{\sigma(i)}-\alpha_{\tau(i)}))=$
$=p(x_1,\ldots,x_n)$ è non nullo poichè i fattori $\sum_{i=1}^{n} x_i(\alpha_{\sigma(i)}-\alpha_{\tau(i)})$ sono non nulli (vista la

ipotesi che gli α_i sono distinti). I coefficienti di $p(x_1,\ldots,x_n)$ sono funzioni simmetriche negli $\alpha_1,\ldots,\alpha_n$ e quindi si possono calcolare come espressioni polinomiali nei coefficienti di $f(x)$ (cfr. Fatto II del §18).
Si tratta quindi di determinare gli interi $m_1,\ldots,m_n$ tali che $p(m_1,\ldots,m_n)\neq 0$. Questo è chiaramente possibile (lo si verifichi per esempio per induzione). ▽
Supponiamo di aver scelto gli interi m_i come nella proposizione precedente, di conseguenza gli elementi a_σ sono tutti distinti. Per essi sussiste la seguente:

PROPOSIZIONE 19.2 *Per ogni $\sigma\in\mathcal{S}_n$ si ha $\mathbb{Q}(a_\sigma)=\mathbb{Q}(\alpha_1,\ldots,\alpha_n)=E$.*

Dimostrazione E' chiaro che $\mathbb{Q}(a_\sigma)\subseteq\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$. D'altra parte sappiamo che il grado di $\mathbb{Q}(a_\sigma)$ su $\mathbb{Q}$ è uguale al numero dei trasformati distinti di a_σ tramite il gruppo di Galois $G=G(E/\mathbb{Q})$. Ora G è un sottogruppo del gruppo $\mathcal{S}_n$ di tutte le permutazioni e se $\tau\in G$ allora $\tau(a_\sigma)=a_{\tau\sigma}$. Poichè questi elementi sono tutti distinti, la proposizione è provata. ▽

Esercizio 19.3 Si provi a dimostrare la 19.2 direttamente, partendo dal teorema 17.4 sulle funzioni simmetriche.

Passiamo ora a determinare esplicitamente il grado dell'estensione $\mathbb{Q}\subseteq\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$.
Consideriamo il polinomio, di grado $n!$, $\prod_{\sigma\in\mathcal{S}_n}(x-a_\sigma)=g(x)$, che prende il nome di *primo risolvente*. I coefficienti di $g(x)$ sono funzioni simmetriche negli α_i e pertanto si possono calcolare esplicitamente come espressioni polinomiali nei coefficienti di $f(x)$. Segue pertanto che $g(x)\in\mathbb{Q}(x)$.
$g(x)$ ha come radici gli $n!$ elementi distinti a_σ. Detto $m=[E:\mathbb{Q}]$, per la proposizione 18.2 sappiamo che $E=\mathbb{Q}(a_\sigma)$, pertanto a_σ ha grado m, per ogni $\sigma\in\mathcal{S}_n$. Ne segue, in particolare, che $g(x)$ si fattorizza in $\mathbb{Q}[x]$ nella forma:

$$g(x)=h_1(x)h_2(x)\ldots h_s(x),\quad n!=ms$$

dove gli $h_i(x)$ sono i fattori irriducibili di $g(x)$, ciascuno dei quali è il polinomio minimo di m fra gli a_σ. Ciascuno degli $h_i(x)$ prende il nome di *secondo risolvente*.
I fattori $h_i(x)$, di grado m da determinare, si possono trovare grazie al metodo di Kronecker (esposto nel §18).
Il procedimento descritto permette pertanto di determinare effettivamente il grado della estensione $\mathbb{Q}(\alpha_1,\alpha_2,\ldots,\alpha_n)$.
Vogliamo infine illustrare un metodo effettivo per determinare il gruppo di Galois di un polinomio $f(x)\in\mathbb{Q}[x]$ che abbia n radici tutte distinte.
Si consideri il primo risolvente $g(x)=\prod_{\sigma\in\mathcal{S}_n}(x-a_\sigma)$ e sia $h(x)$ uno dei suoi fattori irriducibili. Possiamo assumere che le radici di $f(x)$ (che non conosciamo) siano indicate con indici tali che l'elemento $a=\sum m_i\alpha_i$ è radice di $h(x)$. Dalle osservazioni fatte nella di-

mostrazione 19.2 è chiaro che il gruppo di Galois di E è quel particolare sottogruppo $G \subseteq \mathcal{S}_n$ formato dalle permutazioni τ per le quali l'elemento $a_\tau = \sum m_i \alpha_{\tau(i)}$ è ancora una radice di $h(x)$. L'insieme di tali permutazioni può essere determinato facendo uso del teorema 17.4 nel modo seguente. Si considerano i polinomi $p(x_1,\dots,x_n) = \sum m_i x_i$, $q(x_1,\dots,x_n) = \sum m_i x_{\tau(i)}$, (ove $\tau \in \mathcal{S}_n$ è una permutazione fissata), e si costruisce il polinomio $r(z_1,\dots,z_n,y)$ per il quale risulta

$$qV^2(p_{\tau_1},\dots,p_{\tau_{n!}}) = r(\sigma_1,\dots,\sigma_n,p)$$

Calcolando le funzioni simmetriche che appaiono nell'espressione ora scritta riusciamo infine a determinare effettivamente un polinomio $g_\tau(x)$ a coefficienti razionali tale che $a_\tau = g_\tau(a)$.
Ora, affinchè $\tau \in G$ si deve avere $h(a_\tau) = 0$ ovvero $h(g_\tau(a)) = 0$. Pertanto il polinomio $h(g_\tau(x))$ deve essere un multiplo del polinomio minimo di a, cioè di $h(x)$. Certamente questo è verificabile effettivamente e quindi si può determinare se τ appartiene a G oppure no.
In pratica questo metodo è assolutamente impraticabile visto il numero di calcoli che esso coinvolge e nonostante vi siano varie semplificazioni possibili. Esso è astronomico persino per un'equazione di 5° grado!.
Il significato di questo metodo è, congiuntamente a quanto visto nelle ipotesi che G sia risolubile, di mostrare la validità del seguente teorema:

TEOREMA 19.4 *Dato un polinomio $f(x) \in Q[x]$ esiste un metodo effettivo per determinare se l'equazione $f(x) = 0$ è risolubile per radicali e, in caso affermativo, per determinare effettivamente la formula (per radicali) per le soluzioni.*

Non sarebbe difficile a questo punto ricostruire i teoremi fondamentali della teoria di Galois, usando i teoremi sviluppati per le funzioni simmetriche e i metodi effettivi esposti, evitando quindi il punto di vista moderno degli isomorfismi. Storicamente la strada seguita è stata appunto tramite la teoria delle funzioni simmetriche, si confronti per esempio l'esposizione di L. Bianchi.

PARTE II LA TEORIA ASTRATTA

In questa parte vogliamo sviluppare la teoria dei campi in generale, senza restringerci alla considerazione dei campi numerici.
Incominciamo con alcune premesse che ci porteranno a vedere come, dato un campo F, sia possibile costruire un campo $\overline{F}$ che giuoca lo stesso ruolo del campo $\mathbb{C}$ nel caso dei campi numerici.
Poichè molte dimostrazioni sono simili a quelle già sviluppate nella Parte I saremo più brevi nei dettagli.

§ 1 CAMPO DI DECOMPOSIZIONE. CHIUSURA ALGEBRICA

PROPOSIZIONE 1.1 *Sia F un campo ed $f(x) \in F[x]$ un polinomio. Esiste un campo $E \supseteq F$ in cui $f(x)$ si spezza in fattori di primo grado.*

Dimostrazione Procediamo per induzione, (si osservi però che il procedimento è costruttivo). Sia $g(x)$ un fattore irriducibile di $f(x)$ su F, ($f(x) = g(x)q(x)$) e consideriamo lo anello $E_1 = F[x]/(g(x))$.
Poichè $g(x)$ è irriducibile, E_1 è un campo; detta $\overline{x}$ la classe di x in E_1, si ha per costruzione $g(\overline{x}) = 0$ da cui $g(x) = (x - \overline{x})g_1(x)$, ovvero $f(x) = (x - \overline{x})g_1(x)q(x)$. Il polinomio $f_1(x) = g_1(x)q(x)$ ha grado inferiore a quello di $f(x)$, basta quindi fattorizzarlo e procedere per induzione. ▽Δ

DEFINIZIONE 1.2 Se $E \supseteq F$ è un campo in cui il polinomio $f(x) \in F[x]$ si fattorizza in $f(x) = \prod_{i=1}^{m} (x - \alpha_i)$, $\alpha_i \in E$, e inoltre $E = F(\alpha_1,\dots,\alpha_m)$ diremo che E è *campo minimo di decomposizione* di $f(x)$.

Mostriamo che il campo di decomposizione è essenzialmente unico.

PROPOSIZIONE 1.3 *Se $E \supseteq F$ è campo minimo di decomposizione di $f(x) \in F[x]$ ed $H \supseteq F$ è un*

campo in cui $f(x)$ si spezza in fattori lineari, allora esiste un F-isomorfismo $j : E \to H$ (non necessariamente suriettivo).

Dimostrazione Procediamo per induzione sul grado m di $f(x)$. Se $m = 1$, allora $f(x) = x - \alpha$, $E = F$ e non vi è nulla da dimostrare. Altrimenti sia $\alpha \in E$ una radice di $f(x)$, risulta $f(x) = (x - \alpha)h(x)$, $h(x) \in E[x]$. Sia $F' = F(\alpha) \subseteq E$; α è radice di uno dei fattori irriducibili $g(x)$ di $f(x)$ (su F) pertanto $F(\alpha) \simeq F[x]/(g(x))$.
Ora $f(x)$ si spezza in fattori lineari in H, quindi $g(x)$ ammette una radice $\beta \in H$ da cui segue che $F(\beta) = F[x]/(g(x)) \simeq F(\alpha)$. Possiamo pensare di aver identificato tramite tali isomorfismi $F(\beta)$ ed $F(\alpha)$. Allora $E \supseteq F' = F(\alpha)$ è campo di decomposizione di $h(x)$ il quale si spezza in fattori lineari in $H \supseteq F' = F(\beta)$. Possiamo procedere per induzione e concludere la dimostrazione. ▽△

Si noti che questa proposizione è, nella sostanza della dimostrazione, una variante del teorema di estensione degli isomorfismi (cfr. Parte I, 8.11).
La nozione fondamentale su cui si baserà la trattazione successiva è la seguente:

DEFINIZIONE 1.4 Un campo E si dice *algebricamente chiuso* se ogni polinomio a coefficienti in E si spezza ivi in fattori di primo grado.
Si noti che tale definizione è equivalente alle seguenti:
1) Ogni polinomio $f(x) \in E[x]$ possiede una radice in E.
2) Ogni polinomio $f(x) \in E[x]$ irriducibile è di primo grado.
3) Se $H \supset E$ è un'estensione algebrica, allora $H = E$.

DEFINIZIONE 1.5 Dato un campo F, si dice che un campo $\overline{F} \supseteq F$ è una *chiusura algebrica* se:
1) $\overline{F}$ è algebrico su F
2) $\overline{F}$ è algebricamente chiuso.

Proviamo il seguente criterio.

CRITERIO 1.6 Se $H \supseteq F$ è algebrico ed ogni polinomio $f(x) \in F[x]$ si spezza completamente in H, allora H è chiusura algebrica di F.

Dimostrazione Dobbiamo provare solo che H è algebricamente chiuso. Sia $f(x) \in H[x]$ un polinomio irriducibile e consideriamo il campo $K = H[x]/(f(x))$. Sia $\overline{x}$ la classe di x; $\overline{x}$ è algebrico su H il quale per ipotesi è algebrico su F, pertanto $\overline{x}$ è algebrico su F. Sia $g(x)$ il suo polinomio minimo. Per ipotesi $g(x)$ si spezza in fattori lineari su H, ovvero $g(x) = \prod (x - \alpha_i)$, $\alpha_i \in H$. Poichè $g(\overline{x}) = 0$ si ha $\prod (\overline{x} - \alpha_i) = 0$ in K. Essendo K un campo si ha $\overline{x} = \alpha_j$ per un opportuno j, ovvero $K = H$ e quindi $f(x)$ ha una radice in H. ▽△

Possiamo ora enunciare e dimostrare il teorema principale sulla chiusura algebrica.

Ci servirà per questo un assioma della teoria degli insiemi che va sotto il nome di *assioma della scelta* o, in altra forma, *Lemma di Zorn*.
L'assioma detto permette da asserire che, dato un insieme S , su S esiste un *buon ordinamento*, ovvero un ordinamento per cui valga la seguente proprietà: ogni sottoinsieme non vuoto $T \subseteq S$ possiede un minimo.
Questa proprietà è vera per i numeri naturali e da ciò consegue il principio di induzione. Più in generale vale il principio di induzione per insieme ben ordinati qualunque, (per una discussione dettagliata si confronti per esempio Bourbaki - *Theorie des ensambles*).
Noi faremo uso dell'assioma della scelta per operare una *costruzione transfinita*.

TEOREMA 1.7 1) *Dato un campo F, esiste una sua chiusura algebrica $\overline{F}$.*
2) *Se $H \supseteq F$ è algebrico, esiste un F-isomorfismo (in) di H in $\overline{F}$.*
3) *Due chiusure algebriche di F sono F-isomorfe.*

Dimostrazione 1) Sia S l'insieme dei polinomi irriducibili a coefficienti in F. Per l'assioma della scelta è possibile dotare S di un *buon ordinamento*. Supponiamo di averlo fatto, in qualche modo e pensiamo gli elementi di S come indici di se stessi; quindi ogni polinomio $s \in S$ lo scriveremo anche $f_s(x)$.
Per ogni $f_s(x)$ ci proponiamo di costruire un campo F_s contenente F e tale che per esso valgano le seguenti proprietà:
i) $f_s(x)$ si decompone in F_s in fattori lineari.
ii) Se $s < t$ allora $F_s \subset F_t$.
iii) F_s è algebrico su F.
Se riusciamo a fare tale costruzione, basterà porre $\overline{F} = \bigcup_s F_s$ ed applicare il criterio 1.6, per ottenere una chiusura algebrica di F. Per la costruzione degli F_s si procede per induzione. Supponiamo di conoscere gli F_t, per ogni $t < s$ e costruiamo F_s. Basta considerare $H = \bigcup_{t<s} F_t$ ed usare la proposizione 1.1 (considerando $f_s(x)$ a coefficienti in H).
Le proprietà i), ii), iii) sono ora evidenti.
2) Sia $T \subseteq H$ un insieme (eventualmente infinito) di generatori di H su F, cioè $H = F(T)$. Ordiniamo l'insieme T e poniamo:

$$H_t = F(T_t) \quad \text{ove} \quad T_t = \{s \in T \mid s < t\}.$$

Vogliamo costruire una famiglia di isomorfismi $\varphi_t : H_t \to \overline{F}$ tale che se $t < t'$ risulti $\varphi_{t'}|_{H_t} = \varphi_t$.
Supponiamo, per induzione, di aver costruito φ_s per $s < t$,e cerchiamo di costruire φ_t. Si possono presentare due casi. Se T_t non ha un massimo allora $H_t = \bigcup_{s<t} H_s$ e basta porre $\varphi_t = \varphi_s$ su ogni H_s.
Se T_t ha un massimo u (in tal caso esso è unico per l'ipotesi di buon ordinamento), allora

$T_t = T_u \cup \{u\}$ e $H_t = H_u(u)$ (estensione semplice). Ne segue che possiamo estendere ad H_t l'isomorfismo $\varphi_u : H_u \to \overline{F}$ usando il teorema di estensione degli isomorfismi ed il fatto che $\overline{F}$ è algebricamente chiuso.

3) Siano $\overline{F}_1$ ed $\overline{F}_2$ due chiusure algebriche di F. Da 2) segue che esiste un F-isomorfismo $j : \overline{F}_1 \to \overline{F}_2$. Ora $j(\overline{F}_1)$, essendo isomorfo a $\overline{F}_1$, è algebricamente chiuso. D'altra parte $\overline{F}_2$ è algebrico su $j(\overline{F}_1)$ quindi $\overline{F}_2 = j(F_1)$. ▽△

Commento Il risultato principale di questo paragrafo è stato quello di costruire la chiusura algebrica di un campo e cominciare a mostrare che è un ambito appropriato per sviluppare in astratto la teoria svolta nella Parte I. Rispetto a quest'ultima abbiamo aggiunto sostanzialmente solo alcune idee costruttive della teoria degli insiemi.

§ 2 LA TEORIA DI GALOIS. ESTENSIONI SEPARABILI

Sia F un campo ed $\overline{F}$ una sua chiusura algebrica; se cerchiamo di ripetere con riferimento ad $\overline{F}$ anzicchè a $\mathbb{C}$, la teoria svolta nei §8, §9 , §10, della Parte I ci accorgiamo che le dimostrazioni in essa date valgono senza alcun cambiamento tranne quelle che dipendono dal lemma 8.12 nel quale si afferma che un polinomio irriducibile ammette radici distinte. E' facile vedere che non solo la dimostrazione di 8.12 non è valida in car$F = p > 0$, ma che l'enunciato stesso è falso. La ragione di tale fatto risiede innanzi tutto nell'esistenza dell'*isomorfismo di Frobenius*.

TEOREMA 2.1 *Se A è un anello commutativo di caratteristica p, allora l'applicazione $\psi : A \to A$ data da $\psi(a) = a^p$ $(a \in A)$ è un morfismo (omomorfismo di Frobenius).*

Dimostrazione $(ab)^p = a^p b^p$ per la legge commutativa.

$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$; ma se $k \neq 0, p$, $p \mid \binom{p}{k}$, cioè $\binom{p}{k} = 0$ (cfr. Lemma 7.7 della Parte I).

Pertanto $(a+b)^p = a^p + b^p$. ▽△

Un controesempio al lemma 8.12 in caratteristica $p \neq 0$ è il seguente. Sia $G = \mathbb{Z}/_{(p)}(x)$ il campo delle funzioni razionali in x a coefficienti in $\mathbb{Z}/_{(p)}$ e sia $F = \mathbb{Z}/_{(p)}(x^p)$. L'elemento $x \in G$ soddisfa su F il polinomio $f(y) = y^p - x^p$ ed è facile verificare che $f(y)$ è il polinomio minimo. D'altra parte su G il polinomio $f(y)$ si spezza, per 2.1, in $y^p - x^p = (y-x)^p$ ovvero ammette la sola radice x contata con molteplicità p.

Ci proponiamo pertanto di analizzare questo fenomeno. Per semplicità *tutti i campi che considereremo saranno contenuti in un campo algebricamente chiuso Ω fissato.*

DEFINIZIONE 2.2 1) Dato un campo F diremo che un polinomio $f(x) \in F[x]$ è *separabile* se le sue radici sono tutte distinte.

2) Dato F ed $a \in \Omega$ diremo che a è *separabile su F* se il suo polinomio minimo è separabile.

3) Dato $F \subseteq G$ diremo che G è *separabile su F* se ogni elemento $a \in G$ è separabile su F.

PROPOSIZIONE 2.3 *Se a è separabile su F e $G \supset F$, allora a è separabile su G.*

Dimostrazione Immediata poichè il polinomio minimo di a su G divide quello su F. ▽△

Ci proponiamo di studiare le estensioni separabili. Iniziamo dallo studio delle estensioni semplici.

Sia K un campo, $E = K(a)$ ed $f(x)$ il polinomio minimo di a su K. Quante sono le radici di $f(x)$? Se la derivata $f'(x)$ non è nulla, il lemma 8.12 permette di affermare che sono tutte distinte.

Se $f'(x) = 0$ vuol dire che tutti i monomi x^k che appaiono effettivamente in $f(x)$ sono tali che $kx^{k-1} = 0$, ovvero $k = 0$ cioè $p \mid k$ (p la caratteristica). In definitiva $f(x) = g(x^p)$. Certamente esiste una potenza massima p^h di p tale che $f(x) = q(x^{p^h})$ e $q(y)$ non è polinomio in y^p ovvero $q'(y) \neq 0$.

E' evidente che $q(y)$ è irriducibile poichè se $q(y) = s(y)t(y)$ si ha anche $f(x) = s(x^{p^h})t(x^{p^h})$. Pertanto $q(y)$ ha tutte le radici distinte. Se ne deduce che, se il grado di $f(x)$ è n, quello di $q(y)$ è m e $\beta_1, \beta_2, \ldots, \beta_m$ sono le m radici distinte di $q(y)$, allora $n = mp^h$ e inoltre:

PROPOSIZIONE 2.4 i) *Dato $\alpha \in \Omega$ esiste un unico $\gamma \in \Omega$ con $\gamma^{p^h} = \alpha$*

ii) *Detti $\alpha_1, \alpha_2, \ldots, \alpha_m$ gli elementi di Ω per cui si ha $\alpha_i^{p^h} = \beta_i$, allora $\alpha_1, \alpha_2, \ldots, \alpha_m$ sono le radici distinte di $f(x)$ e ciascuna ha molteplicità p^h.*

Dimostrazione i) Si ha $x^{p^h} - \alpha = x^{p^h} - \gamma^{p^h} = (x - \gamma)^{p^h}$, ovvero γ è l'unica radice, con molteplicità p^h.

ii) Si ha: $f(x) = q(x^{p^h}) = \prod (x^{p^h} - \beta_i) = \prod (x - \alpha_i)^{p^h}$. ▽△

DEFINIZIONE 2.5 I numeri m e p^h sopra introdotti prendono rispettivamente il nome di *grado di separabilità* e *grado di inseparabilità* di a (ovvero di $f(x)$) su K.

Ora possiamo passare al teorema che lega le nozioni date con quelle di isomorfismi e permette di determinare la teoria per estensioni non necessariamente semplici.

TEOREMA 2.6 *Sia $K \subseteq E$ un'estensione finita. Esiste un numero, detto grado di separabilità dell'estensione e indicato con $[E : K]_s$ tale che:*

1) *Ogni isomorfismo $\varphi : K \to \Omega$ si estende in esattamente $[E : K]_s$ modi distinti*

2) $[E : K] = [E : K]_s \, p^h$

3) *E è separabile su K se e solo se* $[E:K] = [E:K]_s$

4) *Se $K \subset E \subset G$ allora* $[G:K]_s \quad [G:E]_s [E:K]_s$

5) $[K(a):K]_s$ *è il grado di separabilità di a su K.*

Dimostrazione La dimostrazione segue fedelmente quella già data sulla estensione degli isomorfismi (cfr. teorema 8.11), riducendosi al caso di una estensione semplice.
Sia $E = K(a)$ e $\varphi: K \to \Omega$ un isomorfismo. In quanti modi si può estendere φ? Chiaramente in tanti modi quante sono le radici del polinomio $\varphi(f(x))$, ove $f(x)$ è il polinomio minimo di a.

Se $f(x) = q(x^{p^h})$, $q'(y) \neq 0$ si ha $\varphi(f(x)) = \varphi(q(x^{p^h}))$ e $(\varphi(q(y)))' = \varphi(q'(y)) \neq 0$.
E' pertanto evidente che il numero di estensioni di φ è indipendente da φ ed è esattamente il grado di separabilità di a.
Ora i punti 1), 2), 4), 5) seguono esattamente, come nel teorema 8.11, per induzione.
Per quanto riguarda 3) si osservi che se $E = K(a_1, a_2, \ldots, a_r)$ e a_i è separabile su $K(a_1, a_2, \ldots, a_{i-1})$ allora:

$$[E:K]_s = \prod [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1})]_s = \prod [K(a_1, \ldots, a_i) : K(a_1, \ldots, a_{i-1}] = [E:K].$$

Viceversa, se $[E:K] = [E:K]_s$ ed $a \in E$, si ha: $[E:K] = [E:K]_s = [E:K(a)]_s [K(a):K]_s$; ne segue che deve essere $[E:K(a)]_s = [E:K(a)]$ e $[K(a):K]_s = [K(a):K]$. ▽△

E' ora chiaro che per le estensioni separabili vale, senza quasi alcuna modifica, la teoria svolta nella prima parte.
In particolare si ha:

PROPOSIZIONE 2.7 *Una estensione finita separabile è semplice.*

Dimostrazione Questa è l'unica osservazione per cui è necessario un commento. Se $K \subseteq E$ è finita e separabile possiamo provare (come nel corollario 9.3) che vi è solo un numero finito di campi intermedi. Ora non possiamo copiare esattamente la dimostrazione data in caratteristica 0. In effetti se K è infinito, dati $a, b \in E$ possiamo considerare gli infiniti elementi $a + \lambda b$, $\lambda \in K$, e concludere come nella proposizione 9.4. Se però K è finito anche E è finito e la proposizione segue dal teorema, assai più preciso, che afferma che il gruppo moltiplicativo di E è generato da un unico elemento a, e a maggior ragione $E = K(a)$.
Di tale teorema daremo la dimostrazione nel §4, relativo ai campi finiti. ▽△

DEFINIZIONE 2.8 1) Si dice che una estensione $K \subseteq E$ è *puramente inseparabile* se $[E:K]_s = 1$.
2) Si definisce *grado di inseparabilità*, e si indica con $[E:K]_i$, il numero per cui risulta $[E:K] = [E:K]_s [E:K]_i$.

PROPOSIZIONE 2.9 *$K \subseteq E$ è puramente inseparabile se e seolo se, per ogni $a \in E$, esiste un h per cui $a^{p^h} \in K$.*

Dimostrazione Se $a^{p^h} \in K$, a soddisfa il polinomio $x^{p^h} - a^{p^h}$ che ha una sola radice. Pertanto il polinomio minimo di a ha una sola radice e $[K(a):K]_s = 1$. Procedendo per induzione si vede che $[E:K]_s = 1$ anche nel caso $E = K(a_1, \ldots, a_n)$.
Viceversa se $[E:K]_s = 1$, da 4) e 5) del teorema 2.6 si ha che, se $a \in E$, il suo grado di separabilità è 1 ovvero il suo polinomio minimo $f(x)$ è della forma $q(x^{p^h})$ con q polinomio di primo grado, ovvero $f(x) = x^{p^h} - \alpha$ da cui $a^{p^h} = \alpha \in K$. ▽△

Vogliamo ora mostrare come ogni estensione si possa costruire in due passi, una separabile ed una puramente inseparabile. Sussiste infatti il seguente:

TEOREMA 2.10 *Sia $K \subset E$ un'estensione e sia $E_s = \{a \in E \mid a$ è separabile su $K\}$. Allora:*

1) *E_s è un campo.*

2) *$K \subseteq E_s$ è separabile*

3) *$E_s \subseteq E$ è puramente inseparabile.*

Dimostrazione Sia E_s' l'estensione generata dagli elementi separabili, allora E_s' si può ottenere per successive estensioni semplici separabili. Segue immediatamente dal teorema 2.6 che E_s' su K è separabile e che ogni suo elemento è separabile. Pertanto $E_s' = E_s$ e 1), 2) sono provati.
3) Sia $a \in E$ e sia $f(x)$ il suo polinomio minimo su E_s: $f(x) = q(x^{p^h})$, con $q(y)$ separabile. Ne segue che a^{p^h} è separabile su E_s, da cui $E_s(a^{p^h})$ è separabile su K e quindi $a^{p^h} \in E_s$. Ovvero a è puramente inseparabile su E_s. ▽△

Il teorema precedente assume una forma ancor più precisa se l'estensione è *normale*.

DEFINIZIONE 2.11 Un'estensione $K \subseteq E$ è *normale* se ogni isomorfismo $\varphi: E \to \Omega$ è un automorfismo (ovvero $\varphi(E) \subseteq E$).

Per arrivare alla struttura delle estensioni normali premettiamo il seguente teorema:

TEOREMA 2.12 *Sia E un campo, G un gruppo finito di automorfismi di E, $E^G = \{a \in E \mid a = g(a), \ \forall g \in G\}$. Si ha: $[E:E^G] = o(G)$; in particolare $E \supseteq E^G$ è separbile e normale.*

Dimostrazione Prima di tutto proviamo che ogni elemento $a \in E$ è algebrico e separabile su E^G di grado al più $o(G)$ (ordine di G). Infatti, sia $H = \{h \in G \mid h(a) = a\}$; è evidente che H è un sottogruppo di G. Se $g_1, \ldots, g_s$ sono rappresentanti delle classi laterali gH, $g \in G$, gli elementi $g_1(a), \ldots, g_s(a)$ sono distinti e dipendono solo dalle classi. In particolare se $g \in G$, $gg_1(a), \ldots, gg_s(a)$ è una permutazione di $g_1(a), \ldots, g_s(a)$. Ne segue che il polinomio $f(x) = \prod (x - g_i(a))$ ha coefficienti in E^G e radici distinte, per cui a è separabile su E^G di grado al più $o(G)$.
Ora, dati comunque $a_1, \ldots, a_n \in E$, l'estensione $E^G(a_1, \ldots, a_n)$ è separabile e pertanto sem-

plice; se a la genera sappiamo che il suo grado è al più $o(G)$, da cui $\left[E^G(a_1,\dots,a_n) : E^G\right] \leq o(G)$. Poichè $a_1,\dots,a_n$ sono arbitrari ne segue immediatamente che $\left[E : E^G\right] \leq o(G)$.
Poichè $o(G) \leq o(\mathcal{J}(E/E^G)) = \left[E : E^G\right]_s \leq \left[E : E^G\right]$ segue che $G = \mathcal{J}(E/E^G)$ e $\left[E : E^G\right] = o(G)$, ovvero E è separabile e normale su E^G (una estensione di Galois). ▽△

Sia ora $K \subseteq E$ un'estensione normale e G il suo gruppo di automorfismi. Per ipotesi $G = \mathcal{J}(E/K)$, da cui $o(G) = \left[E : K\right]_s$. Ne segue che $\left[E : K\right]_s = \left[E : E^G\right]$.

TEOREMA 2.13 *Sia $K \subseteq E$ un'estensione normale. Allora:*
1) *$E^G \supseteq K$ è puramente inseparabile.*
2) *$E_s \supseteq K$ è normale con gruppo di Galois G.*
3) *$E = E_s E^G$ (composto) e $\left[E : K\right] = \left[E_s : K\right] \cdot \left[E^G : K\right]$.*

Dimostrazione 1) Poichè $\left[E : E^G\right] = \left[E : K\right]_s$ ne segue che $\left[E^G : K\right]_s = 1$.
2) E' chiaro che la nozione di separabilità è invariante per automorfismi: se $g \in G$, $g(E_s) \subseteq E_s$ (da cui $g(E_s) = E_s$). Poichè $K \subseteq E$ è normale ed $E_s \subseteq E$ è puramente inseparabile, *ogni* K-isomorfismo di E_s si estende in *modo unico* ad un automorfismo (necessariamente in G) di E. Ne segue che E_s è normale su K ed il suo gruppo di Galois è isomorfo a G.
3) Sia $F = E_s E^G$. Dal teorema 2.6 si ha:

$$\left[E : K\right]_s = \left[E_s : K\right]_s \mid \left[F : K\right]_s$$
$$\left[E : K\right]_i = \left[E^G : K\right]_i \mid \left[F : K\right]_i$$

da cui $\left[E : K\right] = \left[E : K\right]_s \cdot \left[E : K\right]_i \mid \left[F : K\right]$.
Poichè $F \subseteq E$ si ha anche $\left[F : K\right] \mid \left[E : K\right]$ da cui $F = E$. ▽△

Osservazione 2.14 Nella dimostrazione del teorema precedente ci siamo trovati in presenza di un fenomeno che vale la pena di commentare.
Se E,F sono due estensioni di K ed EF è il loro composto, in generale *non* avremo:

$$\left[EF : K\right] = \left[E : K\right]\left[F : K\right].$$

Se tale uguaglianza è verificata diremo che E ed F sono *linearmente disgiunti*.
Per il lettore che conosca la definizione di prodotto tensoriale di algebre forniamo la seguente discussione (cfr. Bourbaki, *Algébre* capitoli II - III).
Si formi l'algebra $E \otimes_K F$, la quale ha dimensione $\left[E : K\right] \cdot \left[F : K\right]$ su K. Vi è chiaramente un omomorfismo $j : E \otimes_K F \to EF$ dato da $a \otimes b \rightsquigarrow ab$. Dire che E ed F sono linearmente disgiunti vuol dire pertanto che j è un isomorfismo. Questo avverrà se e solo se $E \otimes_K F$ è essa stessa un campo.
In generale $E \otimes_K F$ non è un campo, infatti potrà persino avere elementi nilpotenti (cioè $r \in E \otimes F$, $r \neq 0$ ma $r^n = 0$ per qualche n).

Dati due K-isomorfismi $\varphi : E \to \Omega$, $\psi : F \to \Omega$ si determinerà un omomorfismo:

$$E \otimes_K F \to \Omega \quad \text{dato da} \quad a \otimes b \rightsquigarrow \varphi(a)\psi(b)$$

il cui nucleo è un ideale massimale e la cui immagine è il composto di $\varphi(E)$ e $\psi(F)$. Viceversa se M è un ideale massimale di $E \otimes_K F$, $G = E \otimes_K F/_M$ è un campo che contiene una copia isomorfa di E e di F ed è da essi generato. In definitiva possiamo dire che date E ed F due estensioni di K, se esse sono già contenute in qualche modo in un campo più grande allora il composto è semplicemente il campo generato; se invece ci poniamo astrattamente e cerchiamo di formare un composto di E ed F arriviamo ai campi descritti $G = E \otimes_K F/_M$ i quali si possono pensare come composti di E ed F (in senso astratto).
I composti astratti non sono necessariamente isomorfi, per esempio sia $K = \mathbb{Q}$, $E = F = \mathbb{Q}(a)$ con $a^3 = 2$, allora $E \otimes_K F$ è isomorfo a $\mathbb{Q}(a)[x] / (x^3 - 2)$, il polinomio $x^3 - 2$ si fattorizza su $\mathbb{Q}(a)$ come $(x - a)(x^2 + ax + a^2)$.
Pertanto $E \otimes_K F$ è isomorfo a $\mathbb{Q}(a) \oplus \mathbb{Q}(a,b)$ con $b^2 + ab + a^2 = 0$. $\mathbb{Q}(a)$ è un campo di dimensione 3 su $\mathbb{Q}$ isomorfo a $\mathbb{Q}(\sqrt[3]{2})$ mentre $\mathbb{Q}(a,b)$ è di dimensione 6 su $\mathbb{Q}$ ed è il campo di decomposizione del polinomio $x^3 - 2$, pertanto è isomorfo a $\mathbb{Q}(\sqrt[3]{2}, \varepsilon\sqrt[3]{2})$, ε radice cubica primitiva di 1.
Il lettore che voglia capire i meccanismi della teoria di Galois rispetto alla nozione di prodotto tensoriale potrà cercare di dimostrare il seguente:

TEOREMA 1) *$K \subseteq E$ è separabile se e solo se $E \otimes_K E$ è privo di elementi nilpotenti.*
2) *Sia $K_i = \{a \in \Omega \mid \left[K(a) : K\right]_s = 1\}$; allora K_i è un campo. Inoltre $K \subseteq E$ è separabile se e solo se $E \otimes_K K_i$ è un campo.*
3) *$K \subseteq E$ è separabile e normale se e solo se $E \otimes_K E \simeq E \oplus E \oplus \dots \oplus E$.*
4) *Se $K \subseteq E$ è separabile allora $E \otimes_K F$ è privo di elementi nilpotenti, per ogni campo $F \supseteq K$.*
5) *Detti $\overline{K}$ la chiusura algebrica di K, K_i e K_s rispettivamente i campi degli elementi puramente inseparabili e separabili, si ha $\overline{K} = K_s \otimes_K K_i$.*

§ 3 CAMPI PERFETTI

Sia G un campo algebricamente chiuso di caratteristica $p > 0$ e sia $\psi : G \to G$ l'omomorfismo di Frobenius dato dalla formula $\psi(a) = a^p$.
Il campo $\psi(G)$ è algebricamente chiuso, in quanto isomorfo a G, d'altra parte G è algebrico su $\psi(G)$ poichè, se $a \in G$ esso soddisfa su $\psi(G)$ il polinomio $x^p - a^p$. Ne segue che $G = \psi(G)$, in particolare ψ è un isomorfismo. Dato $a \in G$ scriveremo $a^{1/p}$ al posto di $\psi^{-1}(a)$.

Dato un campo $K \subset G$ scriveremo K^p, rispettivamente $K^{1/p}$ al posto di $\psi(K)$, $\psi^{-1}(K)$.

PROPOSIZIONE 3.1 *Dato un campo K le tre affermazioni seguenti sono equivalenti:*

1) $K = K^p$

2) $K = K^{1/p}$

3) *Ogni estensione algebrica di K è separabile.*

Dimostrazione $\psi^{-1}\psi(K) = K$ pertanto se $\varphi(K) = K$ si ha $K^{1/p} = K$ e 1)⇒2). 2)⇒1) nello stesso modo. 3)⇒2) Sia $a \in K^{1/p}$, $E = K(a)$ è separabile su K pertanto $a \in K$.
1)⇒3) Sia a un elemento algebrico su K e $f(x) = x^n + b_1 x^{n-1} + \ldots + b_n$ il suo polinomio minimo su K, dobbiamo provare che $f(x)$ è separabile. Se $f(x)$ fosse inseparabile si avrebbe $f(x) = h(x)^p$ e i coefficienti di $h(x)$ sono in $K^{1/p}$, ma per ipotesi $K = K^{1/p}$ da cui segue che $h(x) \in K[x]$ e $f(x)$ non è irriducibile, una contraddizione. ▽△

DEFINIZIONE 3.2 Un campo K, soddisfacente alle tre condizioni equivalenti della 3.1, viene detto *perfetto*.

Vari modi per generare campi perfetti vengono dati dal seguente teorema:

TEOREMA 3.3 1)*Ogni campo algebricamente chiuso, ogni campo finito, è perfetto.*
2) *Se K è perfetto ed E è algebrico su K, E è perfetto.* 3) *K^{1/p^∞} è perfetto.*

Dimostrazione 1) Abbiamo visto all'inizio di questo paragrafo che un campo algebricamente chiuso è perfetto. Se K è finito, poichè l'omomorfismo di Frobenius ψ è iniettivo, esso deve essere necessariamente biunivoco; pertanto K è perfetto.
2) Sia $a \in E$, dobbiamo trovare un $b \in E$ con $b^p = a$. Consideriamo $H = K(a)$; poichè ψ è un isomorfismo è evidente che $[H^p : K^p] = [H : K]$. Per ipotesi $K^p = K$ e, chiaramente, $H^p \subset H$ da cui $H^p = H$. In particolare si ha $a = b^p$ per un opportuno $b \in H$.
3) Se $a \in K^{1/p^\infty}$ si ha $a \in K^{1/p^h}$ per qualche h e quindi $a^{1/p} \in K^{1/p^{h+1}} \subset K^{1/p^\infty}$.

ESERCIZIO 3.4 Provare che:

1) $K^{p^\infty} = \bigcap_h K^{p^h}$ è perfetto.

2) Se $E = K(a)$ è una estensione semplice, E è perfetto se e solo se K è perfetto e a è algebrico su K.

Per ulteriori complementi, in particolare il legame fra inseparabilità e derivazioni, rimandiamo a: N.Jacobson - *Lectures in Abstract Algebra*, volume III.

§ 4 CAMPI FINITI

Vogliamo determinare le proprietà principali dei campi possedenti solo un numero finito di elementi. Tali campi sono detti anche campi di Galois, ma noi non useremo tale terminologia. E' chiaro che un campo finito ha necessariamente una caratteristica positiva p. Fissiamo la caratteristica p; ogni campo di tale caratteristica contiene il campo fondamentale $F_p = \mathbb{Z}/(p)$.
Se $G \supset F_p$ è finito, $[G : F_p] = n < \infty$ e viceversa. Sia $u_1, u_2, \ldots, u_n$ una base di G su F_p. Poichè ogni elemento di G si scrive in modo unico nella forma $\sum \alpha_i u_i$ con $\alpha_i \in F_p$ ne risulta immediatamente, contando gli elementi, il teorema:

TEOREMA 4.1 *Se $[G : F_p] = n$, G ha p^n elementi.*

Consideriamo il gruppo moltiplicativo G' di un tale campo G. $G' = G - \{0\}$ ha $p^n - 1$ elementi, pertanto per proprietà elementari dei gruppi finiti, dato comunque $a \in G'$ si ha $a^{p^n-1} = 1$ da cui $a^{p^n} = a$. Questa equazione vale certamente anche per $a = 0$ e possiamo enunciare, poichè $x^{p^n} - x$ ha grado p^n:

TEOREMA 4.2 *Se $[G : F_p] = n$ gli elementi di G sono tutte le soluzioni della equazione $x^{p^n} - x$.*

Dalla proposizione 1.3, che asserisce l'unicità del campo di decomposizione di un polinomio, segue:

TEOREMA 4.3 *Se G_1, G_2 hanno p^n elementi sono isomorfi.*

Dimostrazione Entrambi sono il campo di decomposizione su F_p del polinomio $x^{p^n} - x$. ▽△

Ci poniamo ora all'interno di una chiusura algebrica $\overline{F}$ di F_p. Denoteremo, come sempre, con ψ l'automorfismo di Frobenius $\psi(a) = a^p$.

TEOREMA 4.4 1) *Dato comunque un numero naturale n esiste un unico campo $F_{p^n} \subset \overline{F}$ con p^n elementi.*
2) $F_{p^n} = \{a \in \overline{F} \mid \psi^n(a) = a\}$.
3) $F_{p^n} \subseteq F_{p^m}$ *se e solo se* $n \mid m$.
4) F_{p^n} *è una estensione Galoissiana di* F_p *con gruppo di Galois ciclico, generato da* ψ.
5) *Più in generale se* $n \mid m$, F_{p^n} *è una estensione Galoissiana di* F_{p^n} *con gruppo di Galois ciclico generato da* ψ^n.

Dimostrazione 1) e 2) Dai teoremi 4.2 e 4.3 è chiaro che F_{p^n}, se esiste, è unico ed è l'insieme degli elementi descritti da 2) ovvero $F_{p^n} = \{a \in \overline{F} \mid a^{p^n} = \psi^n(a) = a\}$.

E' chiaro che l'insieme di tali elementi è un campo, poichè ψ^n è un automorfismo. Basterà mostrare quindi che tali elementi sono esattamente p^n. Gli elementi in considerazione sono le radici del polinomio $x^{p^n} - x$. La derivata di $x^{p^n} - x$ è -1 pertanto esso non ha radici multiple e le nostre asserzioni sono provate.

3) Se $m = q\,n$ si ha $\psi^m = (\psi^n)^q$; ne discende che se $\psi^n(a) = a$ anche $\psi^m(a) = a$, ovvero $F_{p^n} \subset F_{p^m}$. Viceversa se $F_{p^n} \subset F_{p^m}$ e $q = [F_{p^m} : F_{p^n}]$ contando gli elementi di F_{p^m}, come abbiamo fatto nel teorema 4.1, otteniamo $p^m = (p^n)^q \quad m = n\,q$.

4) e 5) E' chiaro che ψ^n è un F_{p^n}-isomorfismo. Per dimostrare 4) e 5) basterà (dalla teoria finora svolta, cfr. 8.11 parte I) mostrare che ψ^n ha ordine q nel gruppo degli automorfismi di $F_{p^{nq}}$. Chiaramente su $F_{p^{nq}}$ si ha $(\psi^n)^q = 1$. Se ψ^n avesse ordine $q' < q$ si avrebbe $\psi^{nq'} = 1$ su $F_{p^{nq}}$ da cui $F_{p^{nq}} \subset F_{p^{nq'}}$ una contradizione. ▽△

Terminiamo la teoria dei campi finiti con il seguente:

TEOREMA 4.5 *Il gruppo moltiplicativo di un campo finito è ciclico.*

Dimostrazione In effetti dimostreremo di più: se G è un sottogruppo finito del gruppo moltiplicativo di un campo F allora G è ciclico.

Sia n l'ordine di G, dobbiamo mostrare che in G esiste un elemento di ordine esattamente n. Detto m il minimo comune multiplo degli ordini degli elementi di G, si ha $a^m = 1$ per ogni elemento $a \in G$. Poichè G ha n elementi ogni elemento di G soddisfa anche la relazione $a^n = 1$ e pertanto $m \mid n$. Ma l'equazione $x^m = 1$ possiede almeno n soluzioni (gli elementi di G) pertanto $n = m$.

Per terminare basterà utilizzare un fatto generale che dimostriamo nel lemma seguente:

LEMMA 4.6 *Sia A un gruppo commutativo. Se $a_1,\ldots,a_h \in A$ hanno ordini $n_1,\ldots,n_h$ e m è il minimo comune multiplo di tali ordini, esiste $b \in A$ di ordine esattamente m.*

Dimostrazione Sia $m = \prod_{j=1}^{s} p_j^{k_j}$ la decomposizione in fattori primi. Per ogni j esiste un indice i_j tale che $p_j^{k_j} \mid n_{i_j}$. Posto $n_{i_j} = p_j^{h_j} q_j$ è chiaro che l'elemento $b_j = a_{i_j}^{q_j}$ ha ordine esattamente $p_j^{k_j}$. Affermiamo che $b = b_1 b_2 \ldots b_s$ ha ordine esattamente m.

Chiaramente $b^m = \prod b_i^m = 1$ pertanto l'ordine di b divide m. Per ogni j i due numeri $p_j^{k_j}$ e

$t_j = m/p_j^{k_j}$ sono primi fra loro. Esistono dunque due interi r,s per cui $r\,p_j^{k_j} + s\,t_j = 1$. Si ha $b^{st_j} = \prod b_i^{st_j} = b_j^{t_j s} = b_j^{(1-rp_j^{k_j})} = b_j$. Poichè b_j è una potenza di b il suo ordine $p_j^{k_j}$ divide l'ordine di b; ne segue pertanto che tale ordine è necessariamente m. ▽△

§ 5 ESEMPI

Vogliamo corredare la teoria astratta con alcuni esempi significativi.

i) *Funzioni simmetriche* Sia $E = K(x_1,\ldots,x_n)$ il campo delle funzioni razionali su K in n variabili. Il gruppo $\mathcal{S}_n$ opera su E permutando le variabili.

TEOREMA 5.1 $E^{\mathcal{S}_n} = K(\sigma_1,\sigma_2,\ldots,\sigma_n)$.

Dimostrazione Sia $F = K(\sigma_1,\sigma_2,\ldots,\sigma_n) \subseteq E^{\mathcal{S}_n}$, basta mostrare che $[E : F] \leqslant n!$. Le variabili $x_1,\ldots,x_n$ sono radici del polinomio

$$\prod (y - x_i) = y^n - \sigma_1 y^{n-1} + \ldots \pm \sigma_n \in F[y]$$

ne segue che E è il campo di decomposizione di tale polinomio su F, in particolare $[E : F] \leqslant n!$ ▽△

Esercizio Si noti la differenza fra la dimostrazione di questo teorema, appoggiata sulla teoria generale, e quella del teorema 1.2 sulle funzioni simmetriche. Si cerchi di capire il legame logico fra i due approcci alla teoria di Galois, quello astratto e quello effettivo tramite le funzioni simmetriche.

ii) *Funzioni trigonometriche* Sia M il campo di tutte le funzioni meromorfe sul piano complesso (cioè le funzioni olomorfe in $\mathbb{C}$ tranne in alcuni poli).
Consideriamo le funzioni esponenziali $e^{\alpha z}$, $\alpha \in \mathbb{C}$.

LEMMA 5.2 *Se $\alpha_1,\alpha_2,\ldots,\alpha_m$ sono numeri distinti le funzioni $e^{\alpha_1 z}, e^{\alpha_2 z}, \ldots, e^{\alpha_n z}$ sono linearmente indipendenti su $\mathbb{C}$.*

Dimostrazione Supponiamo che si abbia $\sum_{i=1}^{m} \lambda_i e^{\alpha_i z} = 0$. Facendo successivamente la derivata si ha, per ogni intero k, $\sum \lambda_i \alpha_i^k e^{\alpha_i z} = 0$.
In particolare ponendo $k = 0,1,\ldots,m-1$ otteniamo un sistema di m equazioni lineari nelle $\lambda_i e^{\alpha_i z}$ il cui determinante è il Vandermonde dei numeri $\alpha_1,\ldots,\alpha_m$. Poichè tali numeri sono distinti il determinante è non nullo e quindi $\lambda_i e^{\alpha_i z} = 0$ per ogni i, da cui $\lambda_i = 0$. ▽△

COROLLARIO 5.3 *Se* $\alpha_1,\alpha_2,\ldots,\alpha_m \in \mathbb{C}$ *sono linearmente indipendenti sui numeri razionali, le funzioni* $e^{\alpha_1 z},\ldots,e^{\alpha_m z}$ *sono algebricamente indipendenti su* $\mathbb{C}$.

Dimostrazione Supponiamo che si abbia una relazione polinomiale del tipo $0 = \sum \lambda_{n_1\ldots n_m} (e^{\alpha_1 z})^{n_1}\ldots(e^{\alpha_m z})^{n_m}$; si deduce $0 = \sum \lambda_{n_1\ldots n_m} e^{(\Sigma \alpha_i n_i)z}$, ma gli elementi $\sum \alpha_i n_i$ sono distinti per le ipotesi fatte e pertanto $\lambda_{n_1\ldots n_m} = 0$. ∇Δ

Nota Non si confondano queste due semplici asserzioni con i famosi teoremi di Lindemann sulla trascendenza dei *valori* presi dalle funzioni esponenziali. ∇Δ

Consideriamo ora il gruppo dei movimenti analitici del piano: $z \to \alpha z + \beta$, $\alpha \neq 0$. Tale gruppo opera sul campo M delle funzioni meromorfe e trasforma le funzioni esponenziali in se stesse. Vogliamo studiare un esempio speciale. Sia T il sottocampo di M generato dalle funzioni $e(az) = e^{2\pi i a z}$, $a \in \mathbb{Q}$. Sia, per $b \in \mathbb{Q}$, $\tau_b : z \to z+b$. τ_b trasforma il campo T in se stesso. Sia T_b il sottocampo fissato da τ_b, certamente $e(\frac{1}{b} z) \in T_b$. Sia $Z_b = \mathbb{C}(e(\frac{1}{b} z))$. Chiaramente se $b = nc$, $n \in \mathbb{Z}$ si ha $e(\frac{1}{c} z) = e(\frac{n}{b} z) = e(\frac{1}{b} z)^n \in Z_b$ da cui $Z_c \subseteq Z_b$. Dati comunque h numeri razionali $q_1,\ldots,q_h$ è facile provare che il sottogruppo di $\mathbb{Q}$, da essi additivamente generato, è ciclico; sia p un generatore. Segue che $\mathbb{C}(e(q_1 z), e(q_2 z),\ldots, e(q_h z)) = \mathbb{C}(e(pz))$.

TEOREMA 5.4 i) $T_b = Z_b$
ii) *Se* $b = nc$, $n \in \mathbb{Z}$, Z_b *è di Galois su* Z_c *con gruppo di Galois* $\mathbb{Z}/_{(n)}$
iii) *Il polinomio minimo di* $e(\frac{1}{b} z)$ *su* Z_c *è* $x^n - e(\frac{1}{c} z)$.

Dimostrazione Consideriamo la trasformazione $\tau_c : Z_b \to Z_b$. $\tau_c(e(\frac{1}{b} z)) = e(\frac{1}{b}(z+c)) = e(\frac{1}{b} z)\, e^{2\pi i/n}$ pertanto τ_c ha ordine n in Z_b.
Poichè $e(\frac{1}{b} z)$ soddisfa il polinomio $x^n - e(\frac{1}{c} z)$ segue che $Z_b^{\tau_c} = Z_c$ e il gruppo di Galois è ciclico generato da τ_c.
Sia ora $f \in T_b$, certamente $f \in Z_d$ per qualche d con $d = nb$. Poichè $Z_b = Z_d^{\tau_b}$ si ha $f \in Z_b$.

Esercizi 1) Si sviluppi la teoria di Galois facendo intervenire anche l'automorfismo $z \to -z$.
2) Si sviluppi la teoria per il campo generato sui numeri reali dalle funzioni sen $2\pi ax$, cos $2\pi ax$, $a \in Q$. (*suggerimento*: si ricordi che $e^{2\pi i x} = \cos 2\pi x + i \operatorname{sen} 2\pi x$).

iii) *Serie di Puiseux* Si considerino le serie di Laurent $f(z) = \sum_{i=n}^{\infty} a_i z^i$, $n \in \mathbb{Z}$ convergenti in un intorno (dipendente da f) bucato di 0.
Tali serie (ovvero i germi di funzioni da esse rappresentate) formano un campo M_0. Determiniamone la chiusura algebrica. Dobbiamo a tale scopo richiamare alcuni fatti elementari sulla polidromia. Una serie di Puiseux in z è una serie di Laurent $f(w)$ in una variabile w legata a z dalla relazione $w^n = z$ (supporremo la serie convergente in un intorno bucato di 0). Si può pensare $w = z^{1/n}$ una funzione polidroma di z.

Notazione Indichiamo con M_n il campo delle serie di Puiseux in $z^{1/n}$.

TEOREMA 5.6 1) M_{nk} *è una estensione di Galois su* M_n *con gruppo di Galois* $\mathbb{Z}/_{(k)}$.
2) $M_\infty = \bigcup_n M_n$ *è la chiusura algebrica di* M_0.

Dimostrazione 1) Se introduciamo un parametro τ legato a z dalla eguaglianza $z = e^{2\pi i \tau}$ si ha $z^{1/n} = e^{2\pi i \tau/n}$. La trasformazione $\gamma : \tau \to \tau + 1$ manda $z^{1/n}$ in $\varepsilon z^{1/n}$, $\varepsilon = e^{2\pi i/n}$; la parte 1) si dimostra allora come nell'esempio ii).
2) Per questo fatto rimandiamo ai libri di variabile complessa. L'idea è che, data una equazione $y^n + f_1 y^{n-1} + \ldots + f_n$ in cui le f_i sono serie di Laurent, le n radici danno luogo ad una funzione polidroma la quale diviene meromorfa in un intorno di 0 in una nuova variabile $w = z^{1/m}$. ∇Δ

L'esempio di gran lunga più interessante per la geometria è la teoria di Galois del campo $F = \mathbb{C}(x)$ delle funzioni razionali in x. F deve essere pensato come campo delle funzioni meromorfe sulla sfera di Riemann Σ. Una sua estensione algebrica finita $G \supset F$ può essere considerata come il campo delle funzioni meromorfe su una superficie Σ' che riveste Σ con ramificazioni e viceversa. Pertanto la teoria delle estensioni di F equivale alla teoria dei rivestimenti ramificati e connessi di Σ.
E' possibile dare una classificazione completa di tali rivestimenti. Se $P_1,\ldots,P_m$ sono punti di Σ, dare un rivestimento finito di Σ ramificato al più in $P_1,\ldots,P_m$ equivale a dare un rivestimento non ramificato finito di $\Sigma - P_1 - P_2 - \ldots - P_m$. La teoria generale dei rivestimenti non ramificati asserisce che un tale rivestimento è dato una volta assegnati un insieme S ed una azione del gruppo di omotopia di $\Sigma - P_1 - P_2 - \ldots - P_m$ su S. Nel nostro caso il rivestimento si suppone finito e connesso, pertanto S deve essere finito e l'azione del gruppo di omotopia transitiva.
La teoria si conclude provando che il gruppo di omotopia di una sfera bucata in m punti è un gruppo libero in $m-1$ generatori. Assegnare un rivestimento connesso di grado n equivale, pertanto, a dare $m-1$ permutazioni su n elementi tali che il gruppo generato operi transitivamente.

INDICE ANALITICO

INDICE DEI SIMBOLI MAGGIORMENTE USATI