UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

ISTITUZIONI DI ALGEBRA SUPERIORE

I parte: 6 crediti

Una introduzione alla Teoria di Galois

M. Chiara Tamburini Bellani

Anno Accademico 2016/2017

Indice

Prefazione

La Teoria di Galois è un importante e affascinante filone, all'origine dell'algebra astratta. Il suo nucleo iniziale consiste in una memoria, scritta da Evaristo Galois (1811-1832), alla vigilia della sua tragica morte. Tale memoria, rifiutata dall'Accademia delle Scienze, fu mandata nel 1843 dall'amico Auguste Chevalier al matematico Joseph Liouville, il quale la pubblicò sul "Journal de Mathematique pure et appliquée" nel 1846. Ma rimase incompresa e ignorata per decenni.

Gli sviluppi della teoria si ebbero soprattutto nel secolo successivo: ad esempio con la classificazione dei gruppi semplici finiti. Essa costituisce ancora oggetto di ricerca. Per citare un problema ancora aperto, non è noto se ogni gruppo finito sia il gruppo di Galois di un polinomio a coefficienti razionali. Va comunque detto che la teoria di Galois nasce per risolvere problemi concreti, aperti da secoli, quali:

1. Il problema della trisezione di un angolo, della duplicazione del cubo, della quadratura del cerchio.... risalenti alla Grecia classica.
2. Il problema della risoluzione delle equazioni algebriche (affrontato nel Rinascimento Italiano).

Il secondo di questi problemi verrà illustrato nei Capitoli 5 e 6. Quanto al primo diamo solo un cenno, rimandando per una trattazione più approfondita a [5].

1. Usando riga e compasso è possibile trisecare un angolo ?

Esso rientra nel problema più generale delle cosiddette "costruzioni con riga e compasso". In un piano, dati due punti distinti $O,\ U$ diciamo che un punto P è *costruibile* se $P \in \{O, U\}$ oppure esiste una sequenza finita di punti del piano

$$P_0 = O,\ P_1 = U,\ P_2, \ldots, P_n = P$$

con la seguente proprietà. Posto

$$S_j := \{P_0,\ P_1,\ \ldots,\ P_j\} \quad 1 \leq j \leq n$$

il punto P_j $(2 \leq j \leq n)$ è uno dei seguenti:

• intersezione di due rette distinte congiungenti, ciascuna, due punti di S_{j-1};

• intersezione di una retta congiungenti due punti di S_{j-1} con una circonferenza avente centro in un punto di S_{j-1} e raggio la distanza fra due punti di S_{j-1};

• intersezione di due circonferenze distinte i cui centri sono punti di S_{j-1} e i cui raggi sono distanze fra due punti di S_{j-1}.

Identificando il piano con l'insieme dei numeri complessi, ossia il punto $P = (x, y)$ con $z = x + iy$, si ha:

(0.1) Teorema *L'insieme* $\mathbb{K}$ *dei punti costruibili è un sottocampo di* $\mathbb{C}$*, chiuso rispetto alle radici quadrate e al coniugio.*

Per il problema della trisezione di un angolo con riga e compasso, serve il seguente:

Criterio *Se* $z = x + iy$ *è costruibile, allora* z *è radice di un polinomio monico, irriducibile, di grado una potenza di* 2*, a coefficienti razionali.*

Deduciamo allora che ci sono angoli non trisecabili: ad esempio l'angolo di 60°.
Infatti, se l'angolo di 20° fosse ottenibile da quello di 60° con riga e compasso, il punto $(cos\ 20°, sin\ 20°)$ sarebbe costruibile. Lo sarebbe quindi anche il piede della perpendocolare da tale punto all'asse x, ossia il punto

$$P = (cos\ 20°, 0)$$

identificabile con il numero complesso $z = cos\ 20° + i\,0$.
Ricordiamo l'identità trigonometrica:

$$cos\ 3\theta = 4cos^3\ \theta - 3cos\ \theta$$

e applichiamola a $\theta = 20°$, ottenendo:

$$cos\ 60° = 4cos^3\ 20° - 3cos\ 20°.$$

Posto si ha:

$$\frac{1}{2} = 4z^3 - 3z.$$

Pertanto z, costruibile, sarebbe radice del polinomio $8x^3 - 6x - 1$. Non è difficile mostrare che tale polinomio non ha radici razionali, quindi è irriducibile in $\mathbb{Q}[x]$. Ne segue che i polinomi di cui z è radice sono i multipli di $8x^3 - 6x - 1$, in contrasto con il Criterio.

Capitolo I

Richiami di Algebra

Questo capitolo è dedicato a un breve ripasso delle nozioni di base, la cui conoscenza è indispensabile per la comprensione dei contenuti del corso. Per le dimostrazioni si rimanda ai testi utilizzati nei corsi di algebra. Ad esempio, [4], [5], [7], [8], [9].

1 Gruppi

(1.1) Definizione *Un* monoide $(S, \cdot, 1_S)$ *è una struttura algebrica in cui* S *è un insieme,* 1_S *un elemento di* S*,* $\cdot$ *è una operazione binaria in* S *per cui valgono le proprietà:*

1) $1_S \cdot s = s \cdot 1_S = s$*, per ogni* $s \in S$*;*

2) $(s_1 \cdot s_2) \cdot s_3 = s_1 \cdot (s_2 \cdot s_3)$ *per ogni* $s_1, s_2, s_3 \in S$ (proprietà associativa).

(1.2) Esempi

• *Il monoide* $(\mathbb{N}, \cdot, 1)$ *dei numeri naturali rispetto al prodotto;*

• *il monoide* $\left(X^X, \cdot, I_X\right)$ *delle funzioni di un insieme* X *in sè, rispetto al prodotto di funzioni.*

Un elemento s del monoide S ha *inverso* se esiste un elemento di S, indicato con s^{-1}, tale che $s \cdot s^{-1} = s^{-1} \cdot s = 1_S$. L'inverso di s, quando esiste, è unico.

Nel monoide $(\mathbb{N}, \cdot, 1)$ l'unico elemento che ha inverso è 1.

(1.3) Definizione *Un* gruppo $(G, \cdot, 1_G)$ *è un monoide in cui ogni elemento ha inverso.*

(1.4) Esempi

• *Il gruppo moltiplicativo* $(\mathbb{C}^*, \cdot, 1)$ *dei numeri complessi diversi da* 0*.*

• *Il gruppo* $(\mathbb{R}^*, \cdot, 1)$ *dei reali diversi da* 0 *e il gruppo* $(\mathbb{Q}^*, \cdot, 1)$ *dei razionali diversi da* 0 *sono sottogruppi di* $(\mathbb{C}^*, \cdot, 1)$*.*

- *Il gruppo additivo* $(\mathbb{C}, +, 0)$ *di tutti i numeri complessi.*
- *I gruppi* $(\mathbb{Q}, +, 0)$ *e* $(\mathbb{R}, +, 0)$ *sono sottogruppi di* $(\mathbb{C}, +, 0)$.

(1.5) Teorema *Per ogni insieme* X*, l'insieme* $\mathrm{Sym}(X)$ *delle funzioni bijettive da* X *a* X *è un gruppo rispetto al prodotto di funzioni. Esso è detto il* gruppo simmetrico *su* X.

Se X è finito, di ordine n, allora $\mathrm{Sym}(X)$ è finito, di ordine $n!$. In tal caso $\mathrm{Sym}(X)$ si indica anche con $\mathrm{Sym}(n)$ e si chiama il gruppo simmetrico di grado n.

(1.6) Esempio *Gli elementi di* $\mathrm{Sym}(3)$ *sono* $\{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

(1.7) Lemma *Un sottoinsieme non vuoto* H *di un gruppo* G *è un sottogruppo se e solo se, per ogni* $h_1, h_2 \in H$*, anche* $h_1 h_2^{-1} \in H$.

Un sottogruppo H di G dà luogo alla relazione definita ponendo, per ogni $a, b \in G$:

$$a \equiv b \pmod{H} \iff ab^{-1} \in H. \tag{1.8}$$

Tale relazione, detta di *congruenza modulo* H, è di equivalenza in G. Si verifica facilmente che, per ogni $g \in G$, l'insieme degli elementi ad esso equivalenti in tale relazione è

$$Hg := \{hg \mid h \in H\} \quad (\textit{laterale destro di } H \textit{ individuato da } g).$$

In particolare

$$a \equiv b \pmod{H} \iff Ha = Hb. \tag{1.9}$$

I laterali destri di H in G, in quanto classi di equivalenza della congruenza modulo H, costituiscono pertanto una partizione di G. Ne segue il

(1.10) Teorema *(di Lagrange). Se* H *è un sottogruppo di un gruppo finito* G*, allora l'ordine di* H *divide l'ordine di* G.

L'intero $m = \frac{|G|}{|H|}$ di chiama l'*indice* di H in G.

(1.11) Definizione *Un sottogruppo* N *di* G *si dice* normale *se si ha* $gng^{-1} \in N$*, per ogni* $g \in G$ *e per ogni* $n \in N$.

(1.12) Esempi

- *In ogni gruppo* G*, i sottogruppi banali* $\{1_G\}$ *e* G *sono normali.*
- *Ogni sottogruppo di un gruppo abeliano è normale.*

• *Nel gruppo simmetrico* $\mathrm{Sym}(n)$ *le permutazioni pari costituiscono un sottogruppo normale, detto il gruppo* alterno *di grado* n *e indicato con* $\mathrm{Alt}(n)$.

Se N è normale in G, la congruenza modulo N è compatibile con il prodotto, ossia:

$$\begin{cases} a \equiv a' \pmod N \\ b \equiv b' \pmod N \end{cases} \implies ab \equiv a'b' \pmod N. \tag{1.13}$$

Infatti

$$(ab)(a'b')^{-1} = abb'^{-1}a'^{-1} = \underbrace{a(a')^{-1}}_{\in N}\ \underbrace{a'\left(b(b')^{-1}\right)(a')^{-1}}_{\in N} \in N.$$

Ne segue che, se un sottogruppo è normale, è possibile definire un prodotto dei suoi laterali, dando luogo a un nuovo gruppo. Si ha infatti:

(1.14) Teorema *Sia* N *un sottogruppo normale di* G. *L'insieme* $\frac{G}{N}$ *dei laterali di* N *in* G *è un gruppo rispetto al prodotto definito ponendo, per ogni* $a, b \in G$:

$$(Na)\,(Nb) := N(ab). \tag{1.15}$$

$\frac{G}{N}$ *si dice il* gruppo quoziente *di* G *rispetto a* N.

(1.16) Definizione *Siano* $(G_1, \cdot, 1_{G_1})$ *e* $(G_2, *, 1_{G_2})$ *due gruppi. Un* omomorfismo *da* G_1 *a* G_2 *è una applicazione* $f : G_1 \to G_2$ *tale che, per ogni* $a, b \in G_1$:

$$f(a \cdot b) = f(a) * f(b). \tag{1.17}$$

(1.18) Definizione *Un omomorfismo* $f : G_1 \to G_2$ *si dice:*

• *un monomorfismo se è iniettivo;*

• *un epimorfismo se è suriettivo;*

• *un isomorfismo se è un monomorfismo e un epimorfismo.*

Un isomorfismo $f : G_1 \to G_1$ si dice un *automorfismo* di G_1. Due gruppi G_1 e G_2 di dicono *isomorfi* e, in tal caso, si scrive $G_1 \simeq G_2$ se esiste un isomorfismo $f : G_1 \to G_2$. Inoltre G_2 si dice *immagine epimorfa* di G_1 se esiste un epimorfismo $f : G_1 \to G_2$.

(1.19) Lemma *Sia* $f : G_1 \to G_2$ *un omomorfismo di gruppi.*

1) $f\left(1_{G_1}\right) = 1_{G_2}$;

2) *per ogni* $g \in G_1$: $f\left(g^{-1}\right) = f(g)^{-1}$;

3) *per ogni sottogruppo* H *di* G_1 *la sua immagine* $f(H)$ *è un sottogruppo di* G_2;

4) *per ogni sottogruppo (normale) N di G_2, la preimmagine $f^{-1}(N) := \{g \in G_1 \mid f(g_1) \in N\}$ è un sottogruppo (normale) di G_1.*

In particolare $\operatorname{Im} f := f(G_1)$ è un sottogruppo di G_2 e

$$\operatorname{Ker} f := \{g \in G_1 \ | \ f(g) = 1_{G_2}\}$$

è un sottogruppo normale di G_1.
Le immagini epimorfe di un gruppo, a meno di isomorfismi, sono tutti e soli i suoi gruppi quozienti, in virtú del seguente:

(1.20) Teorema (fondamentale sugli omomorfismi).

1) *Siano N un sottogruppo normale di G e $\frac{G}{N}$ il corrispondente gruppo quoziente. La proiezione canonica $\pi : G \to \frac{G}{N}$ definita ponendo*

$$\pi(g) := Ng$$

è un omomorfismo suriettivo (epimorfismo). Inoltre $N = \operatorname{Ker} \pi$.

2) *Sia $f : G_1 \to G_2$ un omomorfismo e sia $\pi : G_1 \to \frac{G_1}{\operatorname{Ker} f}$ la proiezione canonica. Allora f induce un unico isomorfismo $\overline{f} : \frac{G_1}{\operatorname{Ker} f} \to \operatorname{Im} f$ tale che $\overline{f}\pi = f$.*
In particolare

$$\frac{G_1}{\operatorname{Ker} f} \simeq \operatorname{Im} f \ . \tag{1.21}$$

Ricordiamo la definizione di *potenza* di un elemento, con esponente intero, in un gruppo moltiplicativo $(G, \cdot, 1_G)$. Per ogni $g \in G$ e per ogni $k \in \mathbb{Z}$, poniamo:

$$g^0 := 1_G, \quad g^k := g^{k-1}g \text{ se } k > 0, \quad g^k := \left(g^{-1}\right)^{-k} \text{ se } k < 0. \tag{1.22}$$

Così : $g^1 = g,\ g^2 = g\,g,\ g^3 = g\,g\,g,\quad g^{-2} = g^{-1}g^{-1},\ g^{-3} = g^{-1}g^{-1}g^{-1}$.

Sia $\mathbb{Z}$ il gruppo additivo dei numeri interi. Fissato $g \in G$, l'applicazione

$$\gamma : (\mathbb{Z}, +, 0) \to (G, \cdot, 1_G) \quad \text{tale che} \quad k \mapsto g^k \tag{1.23}$$

è un omomorfismo di gruppi, per le proprietà delle potenze. In particolare

$$\operatorname{Im} \gamma = \left\{g^k \mid k \in \mathbb{Z}\right\} := \langle g \rangle \tag{1.24}$$

è un sottogruppo di G. Esso è detto il sottogruppo *ciclico* generato da g.

(1.25) Definizione *Il* periodo $o(g)$ *di un elemento* $g \in G$ *è così definito:*

1) $o(g) := 0$ *(*∞*), se* $g^k \neq 1_G$ *per ogni intero* $k \neq 0$*;*

2) $o(g) := n > 0$ *se* $g^n = 1_G$ *e* $g^r \neq 1_G$ *per* $0 < r < n$.

(1.26) Osservazione $\operatorname{Ker}\gamma$ *è il sottogruppo di* $\mathbb{Z}$ *generato da* $o(g)$.

Infatti se $o(g) = 0$ *allora* $\operatorname{Ker}\gamma = \{0\}$. *In particolare* γ *è iniettiva e quindi* $\langle g\rangle$ *è infinito.*

Se $o(g) = n > 0$, *allora* $n\mathbb{Z} \leq \operatorname{Ker}\gamma$. *Infatti* $g^{nz} = (g^n)^z = (1_G)^z = 1_G$. *D'altra parte* $\operatorname{Ker}\gamma \leq n\mathbb{Z}$, *ossia* $g^k = 1_G$ *implica* $n|k$. *Infatti da* $k = nq + r$, $0 \leq r \leq n-1$, *si ha*

$$1_G = g^k = g^{nq+r} = (g^n)^q\, g^r = g^r$$

da cui $r = 0$, *per la minimalità di* n. *Si conclude* $n\mathbb{Z} = \operatorname{Ker}\gamma$, *da cui:*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n \simeq \langle g\rangle\,.$$

Quindi $\langle g\rangle = \left\{g^0,\ g,\ \cdots, g^{n-1}\right\}$ *ha ordine* n.

In particolare, in un gruppo finito G, ogni elemento ha periodo finito. Inoltre, per il Teorema di Lagrange, tale periodo divide l'ordine di G.

(1.27) Esempi *Nel gruppo* $(\mathbb{C}^*, \cdot, 1)$*:*

- $o(3) = \infty$, $\langle 3\rangle = \left\{\ldots \frac{1}{9},\ \frac{1}{3},\ 1,\ 3,\ 9, \ldots\right\}$ *è infinito;*
- $o(-1) = 2$, $\langle -1\rangle = \{1, -1\}$ *ha ordine* 2*;*
- $o(i) = 4$, $\langle i\rangle = \{1, i, -1, -i\}$ *ha ordine* 4.

(1.28) Lemma *Sia* $o(g) = n > 0$. *Per ogni intero* $k > 0$ *si ha:* $o(g^k) = \frac{n}{\operatorname{MCD}(k,n)}$.

In particolare

$$o(g^k) = n \quad \Leftrightarrow \quad \operatorname{MCD}(k, n) = 1.$$

Dimostrazione.
Poniamo $d := \operatorname{MCD}(k, n)$, con $d > 0$, e scriviamo $n = d\overline{n}$, $k = d\overline{k}$. Abbiamo:

$$\left(g^k\right)^{\overline{n}} = g^{\overline{k}d\overline{n}} = g^{n\overline{k}} = (g^n)^{\overline{k}} = 1_G.$$

Indicando con t il periodo di g^k, ne segue che t divide $\overline{n}$. D'altra parte, da $1_G = \left(g^k\right)^t = g^{kt}$ segue che n divide kt, quindi $\overline{n}$ divide $\overline{k}t$. Siccome $\overline{n}$ e $\overline{k}$ sono coprimi, si ottiene che $\overline{n}$ divide t. Si conclude $t = \overline{n}$. ∎

(1.29) Esempio *Se $o(g) = 10$, le potenze di g che hanno periodo 10 sono g, g^3, g^7, g^9. D'altra parte $o\left(g^2\right) = 5$, $o\left(g^4\right) = 5$, $o\left(g^5\right) = 2$, $o\left(g^6\right) = 5$, $o\left(g^8\right) = 5$.*

(1.30) Definizione *Un gruppo G è abeliano se l'operazione è commutativa.*

In tal caso, per l'operazione, si usa a volte il simbolo $+$ (*notazione additiva*).
L'unità si chiama lo *zero* e si indica con 0_G; l'inverso di $g \in G$ si chiama l'*opposto* e si indica con $-g$. Inoltre le potenze di g si chiamano i *multipli*. Pertanto, in un gruppo abeliano $(G, +, 0_G)$, per ogni $k \in \mathbb{Z}$, si ha:

$$0g := 0_G, \quad kg := (k-1)g + g \text{ se } k > 0, \quad kg := -k\,(-g) \text{ se } k < 0. \tag{1.31}$$

.
Così $1\,g = g$, $\quad 2\,g = g{+}g$, $\quad 3\,g = g{+}g{+}g$, $\quad \ldots -2\,g = -g{-}g$, $\quad -3\,g = -g{-}g{-}g, \ldots\ldots$

2 Anelli

(2.1) Definizione *Un anello $(A, +, \cdot, 0_A, 1_A)$ è una struttura algebrica in cui A è un insieme; 0_A, 1_A sono elementi di A; $+$, $\cdot$ sono operazioni binarie in A, tali che:*
1) *$(A, +, 0_A)$ è un gruppo abeliano;*
2) *$(A, \cdot, 1_A)$ è un monoide;*
per ogni $a, b, c \in A$:
3) *$a \cdot (b + c) = a \cdot b + a \cdot c$ (proprietà distributiva sinistra);*
4) *$(a + b) \cdot c = a \cdot c + b \cdot c$ (proprietà distributiva destra).*

Si noti che, in un anello A, la somma è commutativa per definizione, ossia

$$a + b = b + a, \quad \forall\ a, b \in A.$$

Se anche il prodotto è commutativo, si dice che A è un anello commutativo.

(2.2) Esempio *L'anello commutativo $(\mathbb{Z}, +, \cdot, 0, 1)$ dei numeri interi.*

$\mathbb{Z}$ è un anello privo di divisori dello zero, infatti $ab = 0$ implica $a = 0$ oppure $b = 0$.
Inoltre è un dominio euclideo, in virtù del seguente

(2.3) Teorema *Siano $a, b \in \mathbb{Z}$, con $b \neq 0$. Esistono e sono unici $q, r \in \mathbb{Z}$ tali che $a = bq + r$ con $0 \leq r < |b|$.*

q ed r si chiamano rispettivamente il *quoziente* e il *resto* della divisione di a per b.

(2.4) Definizione *Per ogni $a \in A$, si dice* caratteristica *di a e la si indica con* $\mathrm{char}(a)$*, il periodo di a come elemento del gruppo additivo $(A, +, 0_A)$.*

Quindi

1) $\mathrm{char}(a) := 0$ (oppure ∞) se $ka \neq 0_A$ per ogni intero $k \neq 0$;

2) $\mathrm{char}(a) := n > 0$ ($n \in \mathbb{N}$) se $na = 0_A$ e $ka \neq 0_G$ per $0 < k < n$.

(2.5) Esempi

• *Nell'anello $\mathbb{Z}$ dei numeri interi, 0 ha caratteristica 1. Gli altri elementi hanno caratteristica 0.*

• *Nell'anello $\mathbb{Z}_5$ delle classi di resti modulo 5, la classe $[0]_5$ ha caratteristica 1. Le altre classi hanno caratteristica 5.*

• *Nell'anello $\mathbb{Z}_{20}$ delle classi di resti modulo 20, la classe $[5]_{20}$ ha caratteristica 4, la classe $[10]_{20}$ ha caratteristica 2, la classe $[1]_{20}$ ha caratteristica 20.*

(2.6) Teorema *In un anello A, privo di divisori dello zero, tutti gli elementi diversi da zero hanno la stessa caratteristica, detta la* caratteristica di A*. Essa è 0 oppure un numero primo p.*

Dimostrazione. Siano $a, b \in A$, con $a \neq 0_A$, $b \neq 0_A$. Per ogni $k \in \mathbb{Z}$:

$$ka = 0_A \iff (ka)b = 0_A \iff a(kb) = 0_A \iff kb = 0_A.$$

Ne segue che $\mathrm{char}(a) = \mathrm{char}(b)$. Abbiamo così dimostrato che tutti gli elementi di A, diversi da zero, hanno la stessa caratteristica. Se è 0, abbiamo finito. Altrimenti, se è un intero positivo p, resta da dimostrare che è primo.
Per assurdo sia $p = nm$ una fattorizzazione in cui $1 < m < p$, $1 < n < p$.
Posto $b = ma$, si ha $b \neq 0_A$, quindi $\mathrm{char}(b) = p$. D'altra parte:

$$nb = n(ma) = (nm)a = pa = 0_A$$

in contrasto con $1 < n < p$. Si conclude che p è primo. ■

Indichiamo con A^* l'insieme degli elementi *unitari* di un anello A, ossia degli elementi che hanno inverso moltiplicativo in A. Ricordiamo che, se A è commutativo, un elemento $p \in A$ è *irriducibile* se $p \neq 0$, $p \notin A^*$ e gli unici divisori di p sono quelli banali. Ossia, per ogni $a, b \in A$:

$$p = ab \implies (a \in A^* \text{ oppure } b \in A^*)\,.$$

(2.7) Definizione *Un* campo $\mathbb{K}$ *è un anello commutativo in cui ogni elemento* $k \neq 0_{\mathbb{K}}$ *ha inverso moltiplicativo in* $\mathbb{K}$.

Equivalentemente $\mathbb{K}$ è un campo se $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$.
Ogni campo è privo di divisori dello zero. Infatti da $ab = 0_{\mathbb{K}}$ segue $a = 0_{\mathbb{K}}$ oppure $a \neq 0_{\mathbb{K}}$. In tal caso a ha inverso in $\mathbb{K}$ e $a^{-1}ab = 0_{\mathbb{K}}$, da cui $b = 0_{\mathbb{K}}$.
Per il Teorema 2.6, $\mathbb{K}$ ha caratteristica 0, oppure un primo $p > 0$.

(2.8) Esempi *Il campo* $(\mathbb{C}, +, \cdot, 0, 1)$ *dei numeri complessi, con le usuali operazioni di somma e prodotto. Esso ha caratteristica* 0. *Importanti esempi di sottocampi di* $\mathbb{C}$ *sono:*
- *Il campo* $\mathbb{R}$ *dei numeri reali.*
- *Il campo* $\mathbb{Q}$ *dei numeri razionali.*

(2.9) Definizione *Un sottoinsieme* I *di un anello* A *si dice un* ideale *se:*
1) $0_A \in I$;
2) *per ogni* $i_1, i_2 \in I$, *anche* $(i_1 - i_2) \in I$;
3) *per ogni* $a \in A$, *e per ogni* $i \in I$, *anche* $(ai) \in I$ *e* $(ia) \in I$.

Per ogni ideale I di A, vale il seguente fatto:

$$1_A \in I \implies A = I. \tag{2.10}$$

Infatti da $1_A \in I$ segue $A1_A \leq I$. Essendo $A1_A = A$ si conclude che $A = I$.
Una importante conseguenza è questa:

(2.11) Corollario *Gli unici ideali di un campo* $\mathbb{K}$ *sono* $\{0_{\mathbb{K}}\}$ *e* $\mathbb{K}$.

Dato $a \in A$, indichiamo con Aa l'insieme dei multipli di a. In simboli:

$$Aa := \{xa \mid x \in A\}.$$

Se A è commutativo, si dimostra facilmente che Aa è il minimo ideale a cui a appartiene. Esso è detto *l'ideale principale* generato da a, e si indica anche con $< a >$.

(2.12) Esempio *L'insieme dei numeri pari è un ideale dell'anello* $\mathbb{Z}$, *generato da* 2.

(2.13) Teorema *Ogni dominio euclideo è un dominio a ideali principali, i.e., tutti i suoi ideali sono principali.*

(2.14) Teorema *Sia* D *un dominio a ideali principali. Allora* D *è* fattoriale, *ossia:*
1) *ogni elemento* $a \in D$, *con* $a \neq 0_D$ *e* $a \notin D^*$, *è prodotto di un numero finito* ≥ 1 *di elementi irriducibili in* D;

2) *se* $a = p_1 \dots p_n = q_1 \dots q_m$ *dove i* p_i *e i* q_j *sono irriducibili in* D*, allora* $n = m$ *e, per un opportuno ordinamento dei fattori,* $q_j = p_j \lambda_j, \quad \text{con } \lambda_j \in D^*, \quad 1 \leq j \leq n.$

(2.15) Esempio *Ogni ideale* I *dell'anello* $\mathbb{Z}$ *è principale. Infatti se* $I = \{0\}$ *si ha* $I = \mathbb{Z}0$*. In caso contrario, dal Teorema* 2.3 *segue che* $I = \mathbb{Z}n =< n >$*, dove* n *è un elemento di modulo minimo fra gli elementi non nulli di* I*. Pertanto* $\mathbb{Z}$ *è un dominio a ideali principali e quindi anche un dominio fattoriale. Quest'ultima proprietà è nota come il Teorema Fondamentale dell'Aritmetica.*

Un ideale I di un anello A è in particolare, un sottogruppo additivo di A. Per ogni $a \in A$ il corrispondente laterale si indica mediante la notazione additiva, quindi con $I+a$, dove:

$$I + a := \{i + a \mid i \in I\}.$$

La congruenza $\pmod{I}$ è compatibile con la somma, essendo I un sottogruppo normale del gruppo additivo di A, che è abeliano. Per definizione di ideale essa è anche compatibile con il prodotto, come si puó verificare. Ne segue facilmente:

(2.16) Teorema *Nell'insieme* $\frac{A}{I}$ *dei laterali di* I *in* A*, sono ben definite le seguenti operazioni di somma e prodotto. Per ogni* $a, b \in A$*:*

$$(I + a) + (I + b) := I + (a + b)$$

$$(I + a)(I + b) := I + (ab).$$

$\frac{A}{I}$ *è un anello rispetto ad esse, detto l'*anello quoziente *di* A *rispetto a* I*.*

(2.17) Definizione *Siano* A *un anello commutativo e* $I \neq A$ *un suo ideale.*
Si dice che I *è massimale se l'unico ideale che contiene propriamente* I *è* A *stesso.*

In un dominio a ideali principali, che non sia un campo, gli ideali massimali sono quelli generati dagli elementi irriducibili. Notiamo che l'ideale nullo $\{0_A\}$ è massimale se e solo se A è un campo. Più in generale si ha:

(2.18) Teorema *Sia* A *commutativo. L'anello quoziente* $\frac{A}{I}$ *è un campo se e solo se* I *è massimale.*

(2.19) Esempio *L'anello quoziente* $\frac{\mathbb{Z}}{\langle n \rangle}$*, dove* $\langle n \rangle = n\mathbb{Z}$*,* $n \geq 2$*.*
Per ogni laterale $\langle n \rangle + a$*, detto* r *il resto della divisione di* a *per* n*, si ha* $\langle n \rangle + a = \langle n \rangle + r$*,* $0 \leq r \leq n-1$*. Poichè resti distinti danno luogo a laterali distinti, gli elementi dell'anello* $\frac{\mathbb{Z}}{\langle n \rangle}$ *sono gli* n *laterali:*

$$\langle n \rangle + 0, \ \langle n \rangle + 1, \ \dots, \ \langle n \rangle + (n - 1).$$

La somma e il prodotto sono definite da:

$$(\langle n\rangle + a) + (\langle n\rangle + b) := \langle n\rangle + (a+b), \quad (\langle n\rangle + a)(\langle n\rangle + b) := \langle n\rangle + (ab).$$

Poichè ogni laterale $\langle n\rangle + a$ coincide con la classe di resti $[a]_n$, è lo stesso scrivere:

$$[a]_n + [b]_n := [a+b]_n, \quad [a]_n\,[b]_n := [ab]_n.$$

L'anello $\frac{\mathbb{Z}}{\langle n\rangle}$ si dice anche l'anello delle classi di resti modulo *n e si indica con $\mathbb{Z}_n$.*
Per le precedenti considerazioni $\frac{\mathbb{Z}}{\langle n\rangle}$ è un campo se e solo se $n = p$ è un numero primo.
In tal caso il campo $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p$ si indica anche con $\mathbb{F}_p$. Esso ha caratteristica p.

(2.20) Definizione *Siano A, B due anelli. Un omomorfismo da A a B è una applicazione $f : A \to B$ tale che, per ogni $a, b \in A$:*
1) *$f(a+b) = f(a) + f(b)$;*
2) *$f(ab) = f(a)f(b)$;*
3) *$f(1_A) = 1_B$.*

Conviene definire sottoanello di A ogni sottogruppo S di $(A, +, 0_A)$ tale che $1_A \in S$ e, per ogni $a_1, a_2 \in S$, anche $a_1 a_2 \in S$.

(2.21) Teorema *Sia $f : A \to B$ un omomorfismo di anelli.*
1) *Per ogni sottoanello S di A, la sua immagine $f(S)$ è un sottoanello di B;*
2) *per ogni ideale I di B la sua preimmagine $f^{-1}(I)$ è un ideale di A.*
In particolare $f(A)$ è un sottoanello di B e

$$\text{Ker } f := \{a \in A \mid f(a) = 0_B\}$$

è un ideale di A.

Ricordiamo che B si dice *immagine epimorfa* di A, se esiste un epimorfismo $f : A \to B$. Le immagini epimorfe di un anello sono, a meno di isomorfismi, tutti e soli i suoi anelli quoziente. Vale infatti il seguente:

(2.22) Teorema fondamentale sugli omomorfismi
1) *Siano I un ideale di A e $\frac{A}{I}$ il corrispondente anello quoziente. La proiezione canonica $\pi : A \to \frac{A}{I}$ definita ponendo*

$$\pi(a) := I + a$$

è un epimorfismo di anelli. Inoltre Ker $\pi = I$.

2) *Siano* $f : A \to B$ *un omomorfismo di anelli e* $\pi : A \to \frac{A}{\text{Ker } f}$ *la proiezione canonica. Allora* f *induce un unico isomorfismo di anelli*

$$\overline{f} : \frac{A}{\text{Ker } f} \to \text{Im } f \quad \text{tale che} \quad \overline{f}\pi = f.$$

In particolare $\frac{A}{\text{Ker } f}$ *è isomorfo a* Im f.

3 Anelli di polinomi

Sia A un anello commutativo. L'insieme $A[x]$ dei polinomi a coefficienti in A, nella indeterminata x, è un anello commutativo rispetto alla somma e al prodotto di polinomi. Conviene definire $-\infty$ il grado del polinomio nullo e ritenere $-\infty < n$, per ogni $n \in \mathbb{N}$. Se A è privo di divisori dello zero, ad esempio se $A = \mathbb{K}$ è un campo, $A[x]$ è privo di divisori dello zero. Infatti, indicando con deg il grado di un polinomio, si ha:

$$\deg\left(a(x)b(x)\right) = \deg a(x) + \deg b(x), \quad \forall\ a(x), b(x) \in A[x].$$

Notiamo tuttavia che $\mathbb{K}[x]$ **non** è un campo. Infatti gli elementi di $\mathbb{K}[x]$ che hanno inverso moltiplicativo sono solamente i polinomi di grado 0.

(3.1) Teorema *Siano* $a(x), b(x) \in \mathbb{K}[x]$ *con* $b(x) \neq 0_{\mathbb{K}[x]}$. *Allora esistono e sono unici* $q(x)$, $r(x) \in \mathbb{K}[x]$ *tali che:*
$a(x) = b(x)q(x) + r(x)$, $\deg(r(x)) < \deg(b(x))$.

$q(x)$ e $r(x)$ si chiamano il *quoziente* e il *resto* della divisione di $a(x)$ per $b(x)$.

(3.2) Osservazione *Ogni ideale* I *di* $\mathbb{K}[x]$ *è principale. Infatti dal Teorema* 3.1 *segue che* $I =< f(x) >$, *dove* $f(x)$ *è un qualunque polinomio di grado minimo fra gli elementi di* I. *Pertanto* $\mathbb{K}[x]$ *è un dominio a ideali principali e quindi anche a fattorizzazione unica.*

Consideriamo l'anello quoziente $\frac{\mathbb{K}[x]}{<f(x)>}$, $\deg f(x) = n \geq 1$. Per ogni laterale
$< f(x) > + a(x)$, detto $r(x)$ il resto della divisione di $a(x)$ per $f(x)$, si ha:

$$< f(x) > + a(x) =< f(x) > + r(x), \quad \deg r(x) \leq n - 1.$$

Inoltre $r(x)$ è l'unico polinomio di grado $\leq n - 1$ appartenente a $< f(x) > + r(x)$.
È lecito quindi identificare l'anello quoziente $\frac{\mathbb{K}[x]}{<f(x)>}$ con l'anello i cui elementi sono i polinomi di $\mathbb{K}[x]$ di grado $\leq n - 1$, ossia con l'insieme:

$$\left\{k_0 + k_1 x + \cdots + k_{n-1}x^{n-1} \mid k_i \in \mathbb{K}\right\}$$

rispetto alla *usuale somma* di polinomi e al *prodotto* $\mod f(x)$. È lo stesso procedimento con cui si identifica l'anello quoziente $\frac{\mathbb{Z}}{<n>}$ con l'anello $\mathbb{Z}_n$ degli interi mod n.
In particolare, se $\mathbb{K}$ è finito:

$$\left|\frac{\mathbb{K}[x]}{< f(x) >}\right| = |\mathbb{K}|^n . \tag{3.3}$$

(3.4) Osservazione *Per il Teorema* 2.18 *e l'osservazione che lo precede, l'anello quoziente* $\frac{\mathbb{K}[x]}{<f(x)>}$ *è un campo se e solo se* $f(x)$ *è irriducibile in* $\mathbb{K}[x]$.

(3.5) Esempio $\left|\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}\right| = 2^2 = 4$. *Gli elementi dell'anello* $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ *sono:*

$$\{0,\ 1,\ x,\ x+1\}$$

Le tavole di somma e prodotto sono:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
x^2	$x+1$	1	x

Come si vede anche direttamente dalla tavola di moltiplicazione $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ *è un campo. Ciò è in accordo con il fatto che il polinomio* x^2+x+1 *è irriducibile in* $\mathbb{Z}_2[x]$.

Siano A e A' due anelli commutativi e $\psi : A \to A'$ un omomorfismo di anelli.
È facile verificare che ψ induce l'omomorfismo

$$\widehat{\psi} : A[x] \to A'[x]$$

fra i corrispondenti anelli di polinomi, definito ponendo

$$\widehat{\psi}\,(a_0 + a_1x + \cdots + a_nx^n) := \psi(a_0) + \psi(a_1)x + \cdots + \psi(a_n)x^n \tag{3.6}$$

per ogni $a_0 + a_1x + \cdots + a_nx^n$ di $A[x]$. Usando un diagramma:

$$\begin{array}{ccc} A[x] & \xrightarrow{\hat{\psi}} & A'[x] \\ \Big| & & \Big| \\ A & \xrightarrow[\psi]{} & A' \end{array} \tag{3.7}$$

Inoltre se ψ è un isomorfismo, anche $\widehat{\psi}$ è un isomorfismo.

(3.8) Definizione *Sia* $\mathbb{K}$ *un sottocampo di un campo* $\mathbb{F}$*. Un elemento* $\alpha \in \mathbb{F}$ *è* radice *di* $f(x) \in \mathbb{K}[x]$ *se* $f(\alpha) = 0$*.*

(3.9) Teorema (di Ruffini) *Sia* $f(x) \in \mathbb{K}[x]$*, dove* $\mathbb{K}$ *è un campo. Un elemento* $\alpha \in \mathbb{K}$ *è radice di* $f(x)$ *se e solo se* $(x - \alpha)$ *divide* $f(x)$*.*

Dimostrazione.
Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $f(x)$ per $(x-\alpha)$. Poichè $(x-\alpha)$ ha grado 1, deve essere $\deg(r(x)) \leq 0$, ossia $r(x) = kx^0$.
Da $f(x) = (x - \alpha)\, q(x) + kx^0$ segue

$$f(\alpha) \;=\; (\alpha - \alpha)\, q(\alpha) + k\alpha^0 \;=\; 0_{\mathbb{K}}\, q(\alpha) + k\, 1_{\mathbb{K}} \;=\; k.$$

Si conclude

$$f(\alpha) = 0_{\mathbb{K}} \iff k = 0_{\mathbb{K}} \iff r(x) = \underline{0} \iff (x - \alpha) \mid f(x).$$

■

Sia $f(x) \in \mathbb{K}[x]$, di grado n.
• Se $n = 0$, $f(x)$ è unitario;
• se $n = 1$, $f(x)$ è irriducibile in $\mathbb{K}[x]$.
D'altra parte, per il Teorema di Ruffini, valgono i seguenti fatti:
• Se $n = 2, 3$ e $f(x)$ non ha radici in $\mathbb{K}$, allora è irriducibile in $\mathbb{K}[x]$;
• Se $n \geq 2$ e $f(x)$ ha qualche radice in $\mathbb{K}$, allora è riducibile in $\mathbb{K}[x]$;
Ricordando che $\mathbb{K}[x]$ è un dominio fattoriale, si ha il seguente

(3.10) Corollario *Sia* $f(x) \in \mathbb{K}[x]$ *di grado* n*. La somma delle molteplicità delle radici di* $f(x)$ *non supera* n*.*

(3.11) Teorema *(fondamentale dell'algebra) Il campo complesso* $\mathbb{C}$ *è algebricamente chiuso. Ossia gli unici polinomi irriducibili di* $\mathbb{C}[x]$ *sono quelli di grado 1.*

Ben diversa è la situazione in $\mathbb{Q}[x]$, come emerge dalle seguenti considerazioni, basate su un celebre risultato di Gauss.

(3.12) Definizione $f(x) \in \mathbb{Z}[x]$ *è* primitivo *se un MCD dei suoi coefficienti è* 1*.*

(3.13) Lemma *di Gauss. In* $\mathbb{Z}[x]$ *il prodotto di polinomi primitivi è primitivo.*

Dimostrazione.
Supponiamo per assurdo che $f(x), g(x) \in \mathbb{Z}[x]$ siano primitivi, ma che $h(x) = f(x)g(x)$ non lo sia. Allora esisterebbe un primo p che divide $h(x)$, ma non divide nè $f(x)$ nè $g(x)$. Consideriamo l'epimorfismo canonico $\pi : \mathbb{Z} \to \mathbb{Z}_p$ definito ponendo $\pi(a) = [a]_p$ per ogni $a \in \mathbb{Z}$ ed estendiamolo all'omomorfismo $\widehat{\pi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Otteniamo

$$\widehat{\pi}\left(a_n x^n + \ldots a_1 x + a_0\right) := [a_n]_p x^n + \ldots [a_1]_p x + [a_0]_p.$$

Si avrebbe $\widehat{\pi}(h(x)) = 0$, $\widehat{\pi}(f(x)) \neq 0$ e $\widehat{\pi}(g(x)) \neq 0$. D'altra parte $\widehat{\pi}(h(x)) = \widehat{\pi}(f(x))\widehat{\pi}(g(x))$. E questa è una contraddizione perchè l'anello $\mathbb{Z}_p[x]$ è privo di divisori delle zero. ■

Un facile calcolo aritmetico mostra che ogni polinomio $g(x) \in \mathbb{Q}[x]$ si scrive nella forma

$$g(x) = \frac{n}{m}\, \overline{g}(x)$$

con $\overline{g}(x) \in \mathbb{Z}[x]$, primitivo. Per esempio

$$x^3 + \frac{2}{3}x^2 - \frac{1}{5}x + 2 = \frac{1}{15}\left(15x^3 + 10x^2 - 3x + 30\right).$$

(3.14) Corollario *Un polinomio primitivo di $\mathbb{Z}[x]$, di grado > 0, è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$.*

Dimostrazione. Sia $f(x) \in \mathbb{Z}[x]$, primitivo, di grado > 0. Se $f(x)$ è irriducibile in $\mathbb{Q}[x]$ lo è, a maggior ragione, in $\mathbb{Z}[x]$. Viceversa sia $f(x)$ irriducibile in $\mathbb{Z}[x]$.
Supponiamo, per assurdo, che ammetta una fattorizzazione

$$f(x) = f_1(x) f_2(x)$$

con $f_1(x), f_2(x) \in \mathbb{Q}[x]$, entrambi di grado > 0. Scrivendo i due fattori nella forma $f_i(x) = \frac{n_i}{m_i}\overline{f}_i(x)$, con $\overline{f}_i(x) \in \mathbb{Z}[x]$, primitivi, si ha

$$m_1 m_2\ f(x) = n_1 n_2\ \overline{f}_1(x)\overline{f}_2(x).$$

Essendo $f(x)$ primitivo, $m_1 m_2$ è un MCD dei coefficienti del primo membro.
Essendo $\overline{f}_1(x)\overline{f}_2(x)$ primitivo per il Lemma di Gauss, $n_1 n_2$ è un MCD dei coefficienti del secondo membro. Ne segue $m_1 m_2 = \pm n_1 n_2$, da cui:

$$f(x) = \pm\overline{f}_1(x)\overline{f}_2(x).$$

Ma questo contraddice l'irriducibilità di $f(x)$ in $\mathbb{Z}[x]$. ■

(3.15) Corollario (Criterio di Eisenstein) *Dato un polinomio* $f(x) = z_0 + z_1 x + \dots z_n x^n$, *di grado* $n \geq 1$, *a coefficienti interi, si supponga che sia* $\mathrm{MCD}\,(z_0, z_1, \dots, z_n) = 1$ *e che esista un primo* p *tale che:*

$$p \text{ divide } z_j,\ 0 \leq j \leq n-1, \quad p^2 \text{ non divide } z_0.$$

Allora $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo, per assurdo, che $f(x)$ sia riducibile in $\mathbb{Q}[x]$ e quindi in $\mathbb{Z}[x]$, essendo primitivo. Ammetterebbe dunque una fattorizzazione

$$f(x) = a(x)\, b(x), \quad a(x),\ b(x) \in \mathbb{Z}[x].$$

Considerando l'epimorfismo $\pi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ si ha $\pi(f(x)) = [z_n]_p x^n$, con $[z_n]_p \neq [0]_p$. Per l'unicità della fattorizzazione di un polinomio in irriducibili, i divisori di $\pi(f(x))$ sono della forma $[k_m]_p x^m$, $0 \leq m \leq n$. In particolare $\pi(a(x))$ e $\pi(b(x))$ sono di questa forma, e hanno entrambi grado positivo per la primitività di $f(x)$. Detti a_0 e b_0 i loro termini noti, si ha che p divide sia a_0 sia b_0 e si conclude che p^2 divide $a_0 b_0 = z_0$, contraddizione.
■

In particolare, in $\mathbb{Q}[x]$ ci sono polinomi irriducibili di qualsiasi grado $n \geq 1$. Ad esempio, per ogni primo p, il polinomio $x^n - p$ è irriducibile in $\mathbb{Q}[x]$.

4 Sottocampo minimo

(4.1) Definizione *Il* sottocampo minimo $\mathbb{K}_0$ *di un campo* $\mathbb{K}$ *è l'intersezione di tutti i sottocampi di* $\mathbb{K}$.

(4.2) Lemma

- *Se* $\mathbb{K}$ *ha caratteristica* 0, *allora* $\mathbb{K}_0 \simeq \mathbb{Q}$;
- *se* $\mathbb{K}$ *ha caratteristica* $p > 0$, *allora* $\mathbb{K}_0 \simeq \mathbb{Z}_p$.

Dimostrazione.
Se $\mathbb{K}$ ha caratteristica 0, $m1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ per ogni intero $m \neq 0$. Ne segue che $(m1_{\mathbb{K}})^{-1} \in \mathbb{K}$. Possiamo quindi considerare l'applicazione $f : \mathbb{Q} \to \mathbb{F}$ definita ponendo

$$f\left(\frac{n}{m}\right) := (n1_{\mathbb{K}})\ (m1_{\mathbb{K}})^{-1}.$$

Essa è un omomorfismo di anelli. Inoltre è iniettiva perchè $n1_{\mathbb{K}} = 0_{\mathbb{K}}$ solo se $n = 0$.
Ne segue $\mathbb{Q} \simeq \text{Im } f$. Pertanto Im f è un sottocampo di $\mathbb{K}$.
Se $\mathbb{K}$ ha caratteristica $p > 0$, definiamo $f : \mathbb{Z} \to \mathbb{K}$ mediante

$$f(n) := n1_{\mathbb{K}}.$$

Tale applicazione è un omomorfismo di anelli. Inoltre Ker $f = p\mathbb{Z}$ è un ideale massimale di $\mathbb{Z}$, essendo p primo. Ne segue $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p \simeq \text{Im } f$. Di nuovo Im f è un sottocampo di $\mathbb{K}$.
In entrambi i casi $\mathbb{K}_0 \leq \text{Im } f$. D'altra parte, per definizione di sottocampo, $1_{\mathbb{K}} \in \mathbb{K}_0$: quindi anche tutti i suoi multipli $n1_{\mathbb{K}}$, gli inversi $m{1_{\mathbb{K}}}^{-1}$ di quelli non nulli e i prodotti $(n1_{\mathbb{K}})\ (m1_{\mathbb{K}})^{-1}$ appartengono a $\mathbb{K}_0$. Si conclude Im $f = \mathbb{K}_0$. ■

È utile notare che, se $\mathbb{K}$ ha caratteristica 0:

$$\mathbb{K}_0 = \text{Im } f = \left\{ (n1_{\mathbb{K}})\ (m1_{\mathbb{K}})^{-1} \mid n, m \in \mathbb{Z}, m \neq 0 \right\}.$$

Se $\mathbb{K}$ ha caratteristica $p > 0$

$$\mathbb{K}_0 = \text{Im } f = \{0_{\mathbb{K}}, 1_{\mathbb{K}}, \ldots, (p-1)1_{\mathbb{K}}\}.$$

(4.3) Lemma *Siano $\mathbb{K}, \mathbb{F}$ campi e $\sigma : \mathbb{K} \to \mathbb{F}$ un omomorfismo di anelli.*
1) *σ è iniettivo, ossia un monomorfismo;*
2) *se $\mathbb{F} = \mathbb{K}$, la restrizione di σ al sottocampo minimo $\mathbb{K}_0$ è l'identità.*

Dimostrazione.
1) Per definizione di omomorfismo fra anelli, $\sigma(1_{\mathbb{K}}) = 1_{\mathbb{F}}$. Ne segue Ker $\sigma \neq \mathbb{K}$. Siccome Ker σ è un ideale di $\mathbb{K}$ e un campo non ha ideali propri, Ker $\sigma = \{0_{\mathbb{K}}\}$, cioè σ è iniettiva.

2) Si ha $\sigma(n1_{\mathbb{K}}) = n1_{\mathbb{K}}$ per ogni $n \in \mathbb{Z}$. Questo si dimostra per induzione se $n \geq 0$.
Infatti per $n = 0$ è chiaro e, per $n > 0$:

$$\sigma(n1_{\mathbb{K}}) = \sigma\left((n-1)1_{\mathbb{K}} + 1_{\mathbb{K}}\right) = \sigma\left((n-1)1_{\mathbb{K}}\right) + \sigma\left(1_{\mathbb{K}}\right) = (n-1)1_{\mathbb{K}} + 1_{\mathbb{K}} = n1_{\mathbb{K}}.$$

Se $n < 0$ allora $\sigma(-n1_{\mathbb{K}}) = -n1_{\mathbb{K}}$ e, ricordando che $\sigma(-\alpha) = -\sigma(\alpha)$:

$$\sigma\left(n1_{\mathbb{K}}\right) = \sigma\left(-(-n1_{\mathbb{K}})\right) = -\sigma(-n1_{\mathbb{K}}) = -(-n1_{\mathbb{K}}) = n1_{\mathbb{K}}.$$

Siccome σ conserva il prodotto si conclude che, per ogni $n, m \in \mathbb{Z}$ con $m1_{\mathbb{K}} \neq 0_{\mathbb{K}}$,

$$\sigma\left((n1_{\mathbb{K}})\ (m1_{\mathbb{K}})^{-1}\right) = (n1_{\mathbb{K}})\ (m1_{\mathbb{K}})^{-1}$$

da cui l'asserto. ■

5 Campo dei quozienti

Ogni sottoanello D di un campo $\mathbb{K}$ è un dominio di integrità, ossia un anello commutativo privo di divisori dello zero. Viceversa, ogni dominio di integrità può essere immerso in un campo, il cosiddetto *campo dei quozienti* $\mathbb{F}$ di D. Accenniamo brevemente alla costruzione di $\mathbb{F}$, lasciando la verifica delle affermazioni come esercizio.
Nell'insieme delle *frazioni* $\left\{\frac{a}{b} \mid a \in D,\ b \in D \setminus \{0\}\right\}$, definiamo la relazione

$$\frac{a}{b} \equiv \frac{c}{d} \iff ad = bc.$$

Tale relazione è di equivalenza. Chiamiamo $\mathbb{F}$ l'insieme quoziente, ossia l'insieme i cui elementi sono le classi di equivalenza. Rispetto alle usuali operazioni di somma e prodotto del calcolo frazionario la precedente relazione è una congruenza e $\mathbb{F}$ risulta un campo. In particolare D può essere identificato con il sottonallo $\left\{\frac{d}{1} \mid d \in D\right\}$ di $\mathbb{F}$.

6 Il monomorfismo di Frobenius

Tale monomorfismo esiste solo per i campi di caratteristica $p > 0$, ed è basato su una proprietà dei coefficienti binomiali.
Per ogni intero $n \geq 0$ e ogni intero k tale $0 \leq k \leq n$ si pone:

$$\binom{n}{k} := \frac{n!}{(n-k)!\,k!} \quad \text{(coefficiente binomiale)}.$$

Si vede facilmente che $\binom{n}{k}$ è sempre un intero.

(6.1) Lemma *Sia p primo.*
1) *p divide $\binom{p}{k}$ per ogni k tale che $0 < k < p$;*
2) *se $\mathbb{K}$ ha caratteristica p, per ogni $\alpha, \beta \in \mathbb{K}$:*

$$(\alpha + \beta)^p = \alpha^p + \beta^p.$$

Dimostrazione.
1) Il numeratore $p!$ è divisibile per p. Invece $(p-k)!$ e $k!$ non sono divisibili per p, in virtù dell'ipotesi $0 < k < p$. Pertanto p, essendo primo, non divide il denominatore $(p-k)!k!$
2) Per lo sviluppo del binomio,

$$(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^{n-k}\beta^k = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{n-k}\beta^k + \beta^p.$$

Per il punto 1), se $0 < k < p$, i termini $\binom{p}{k}\alpha^{n-k}\beta^k$ sono della forma $p\gamma_k$, con $\gamma_k \in \mathbb{K}$. Siccome $\mathbb{K}$ ha caratteristica p tali termini sono nulli, da cui l'asserto. ■

(6.2) Teorema *Sia $\mathbb{K}$ un campo di caratteristica $p > 0$. L'applicazione $\sigma : \mathbb{K} \to \mathbb{K}$ definita ponendo, per ogni $\alpha \in \mathbb{K}$,*

$$\sigma(\alpha) = \alpha^p \quad \text{(monomorfismo di Frobenius)} \tag{6.3}$$

è un monomorfismo. Se σ è suriettivo, $\mathbb{K}$ si dice perfetto.

Dimostrazione.
$\sigma(1_\mathbb{K}) = 1_\mathbb{K}^p = 1_\mathbb{K}$.
Per il punto 2) del Lemma precedente: $\sigma(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \sigma(\alpha) + \sigma(\beta)$.
Per la commutatività del prodotto: $\sigma(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \sigma(\alpha)\sigma(\beta)$. ■

7 Moduli e spazi vettoriali

Sia A un anello con unità $1_A \neq 0_A$.

(7.1) Definizione *Un gruppo abeliano $(M, +, 0_M)$ è un A-modulo sinistro se è definito un prodotto $(a, m) \mapsto am$ da $A \times M$ a M per cui valgono le seguenti proprietà.*
Per ogni $a,\ a_1,\ a_2 \in A$ e per ogni $m,\ m_1,\ m_2 \in M$:
1) $a(m_1 + m_2) = am_1 + am_2$;
2) $(a_1 + a_2)m = a_1m + a_2m$;
3) $a_1(a_2m) = (a_1a_2)m$;
4) $1_Am = m$.

Se A è un corpo, un A-modulo sinistro si dice anche uno *spazio vettoriale* su A.

(7.2) Esempio *Il gruppo abeliano $(A, +, 0_A)$ è un A-modulo sinistro rispetto al prodotto di anello $(a_1, a_2) \mapsto a_1a_2$. Tale modulo si chiama l'A-modulo* regolare sinistro *e si indica con ${}_AA$ o anche solo con A.*

Il precedente esempio ammette la seguente generalizzazione.

(7.3) Esempio *Il modulo A^n.*

Per ogni $n \geq 1$ il modulo A^n ha come elementi i vettori colonna *a n componenti in A e le operazioni di modulo risultano le seguenti:*

$$\text{(7.4)} \qquad \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \dots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \dots \\ x_n + y_n \end{pmatrix}, \quad r \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} rx_1 \\ \dots \\ rx_n \end{pmatrix}.$$

(7.5) Definizione *Un sottoinsieme N di un A-modulo M si dice un* sottomodulo *(o anche un* sottospazio *quando A è un corpo) se soddisfa i seguenti assiomi:*
1) $0_M \in N$*;*
2) *per ogni $n_1, n_2 \in N$, l'elemento $(n_1 + n_2)$ appartiene a N;*
3) *per ogni $a \in A$, $n \in N$, l'elemento (an) appartiene a N.*

Dato un sottoinsieme S di un A-modulo M, sia $< S >$ l'insieme delle combinazioni lineari finite, a coefficienti in A, degli elementi di S, ossia:

$$\text{(7.6)} \quad < S >:= \left\{ \sum_{i=1}^{n} a_i m_i \mid m_i \in M,\ a_i \in A,\ n \in \mathbb{N} \right\} \quad \text{(sottomodulo generato da } S\text{)}.$$

Si dimostra facilmente che $< S >$ è il minimo sottomodulo di M che contiene S. In particolare $< \emptyset >:= \{0_M\}$.

(7.7) Definizione *Un sottoinsieme S di M* genera *M se il sottomodulo generato da S è M stesso, ossia se $< S >= M$.*

(7.8) Definizione *Siano M e M′ degli A-moduli. Un* A-omomorfismo *da M a M′ è una applicazione $\Phi : M \to M'$ tale che, per ogni $m_1, m_2, m \in M$ e per ogni $r \in A$:*
1*)* $\Phi(m_1 + m_2) = \Phi(m_1) + \Phi(m_2)$,
2*)* $\Phi(rm) = r\,\Phi(m)$.

Quando A è un corpo, un A-omomorfismo si dice anche una *applicazione lineare.*

(7.9) Lemma *Sia $\Phi : M \to M'$ un A-omomorfismo. Per ogni sottomodulo N di M e per ogni sottomodulo N' di M' valgono i seguenti fatti:*
1) *l'immagine $\Phi(N) := \{\Phi(n) \mid n \in N\}$ è un sottomodulo di M';*
2) *la preimmagine $\Phi^{-1}(N') := \{m \in M \mid \Phi(m) \in N'\}$ è un sottomodulo di M.*

(7.10) Definizione *Un sottoinsieme S di un A-modulo M si dice* indipendente *se, per ogni sottoinsieme finito $\{m_1, \dots, m_n\}$ di S e per ogni $a_1 \in A, \dots, a_n \in A$:*

$$\sum_{i=1}^{n} a_i m_i = 0_M \quad \Rightarrow \quad a_1 = \cdots = a_n = 0_A.$$

L'insieme $\emptyset$ è indipendente per definizione.

(7.11) Definizione *Un sottoinsieme $\mathcal{B}$ di un A-modulo M è una* base *di M se genera M ed è indipendente.*

Notiamo che $\{v_1, \cdots, v_n\}$ è una base di M se ogni $m \in M$ si scrive in modo unico nella forma $x_1v_1 + \cdots + x_nv_n$ con $x_i \in A$.
Il modulo nullo ha base $\emptyset$. Il modulo regolare $A = {}_AA$ ha come base il singoletto $\{1_A\}$.
Per $n \geq 2$, è immediato verificare che A^n ha come base l'insieme:

$$\left\{ e_1 := \begin{pmatrix} 1_A \\ \dots \\ 0_A \end{pmatrix}, \ \dots, \ e_n := \begin{pmatrix} 0_A \\ \dots \\ 1_A \end{pmatrix} \right\} \quad \text{(base canonica).} \tag{7.12}$$

(7.13) Teorema *Ogni spazio vettoriale V su un campo $\mathbb{K}$ ha una base. Inoltre tutte le basi di V hanno la stessa cardinalità, detta la* dimensione *di V.*

L'esistenza di una base si ottiene notando che ogni sottoinsieme indipendente massimale di V è un insieme di generatori.

Capitolo II

Primi risultati

1 Estensioni di campi

(1.1) Lemma *Se $\mathbb{K}$ è un sottocampo di un anello commutativo $\mathbb{F}$, l'anello $\mathbb{F}$ risulta, in modo naturale, uno spazio vettoriale su $\mathbb{K}$. Inoltre se $f : \mathbb{F} \to \mathbb{F}$ è un omomorfismo di anello la cui restrizione a $\mathbb{K}$ è l'identità , allora f è una applicazione lineare.*

Dimostrazione. $(\mathbb{F}, +, 0_{\mathbb{F}})$ è un gruppo abeliano. Il prodotto in $\mathbb{F}$ induce un prodotto $\mathbb{K} \times \mathbb{F} \to \mathbb{F}$ rispetto al quale $\mathbb{F}$ risulta uno spazio vettoriale su $\mathbb{K}$. Infatti, per ogni $k_1, k_2 \in \mathbb{K}$, $\alpha \in \mathbb{F}$ si ha: $(k_1 + k_2)\alpha = k_1\alpha + k_2\alpha$, $k_1(k_2\alpha) = (k_1k_2)\alpha$ e $1 \cdot \alpha = \alpha$.
Infine, per definizione di omomorfismo di anelli, per ogni $k \in \mathbb{K}$, $\alpha, \beta \in \mathbb{F}$ si ha $f(\alpha+\beta) = f(\alpha) + f(\beta)$ e, per l' ipotesi $f_{|\mathbb{K}} = \mathrm{id}$, $f(k\alpha) = f(k)f(\alpha) = kf(\alpha)$. Pertanto f è lineare. ■

(1.2) Definizione *La dimensione di $\mathbb{F}$ come spazio vettoriale su $\mathbb{K}$ si chiama il* grado *di $\mathbb{F}$ su $\mathbb{K}$ e si indica mediante $[\mathbb{F} : \mathbb{K}]$.*

Per esempio $[\mathbb{C} : \mathbb{R}] = 2$. Infatti $\{1, i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$.

(1.3) Osservazione *Sia $f(x)$ un polinomio di grado n in $\mathbb{K}[x]$. Ricordiamo che si può identificare il quoziente $\frac{\mathbb{K}[x]}{<f(x)>}$ con l'anello i cui elementi sono i polinomi di $\mathbb{K}[x]$ di grado $\leq n-1$, rispetto alla* usuale somma *di polinomi e al* prodotto $\mod f(x)$. *Da*

$$\frac{\mathbb{K}[x]}{< f(x) >} = \left\{k_0 + k_1x + \cdots + k_{n-1}x^{n-1} \mid k_i \in \mathbb{K}\right\}$$

si ha che $\left\{x^0, x, \ldots, x^{n-1}\right\}$ è una base di tale anello su $\mathbb{K}$. Quindi $[\mathbb{F} : \mathbb{K}] = n$.

(1.4) Definizione *Dati due campi $\mathbb{K}$ e $\mathbb{F}$, diciamo che $\mathbb{F}$ è estensione di $\mathbb{K}$ se esiste un monomorfismo di anelli $\iota : \mathbb{K} \to \mathbb{F}$.*

Chiaramente $\mathbb{K}$ è isomorfo al sottocampo $\iota(\mathbb{K})$ di $\mathbb{F}$. In particolare se $\mathbb{K}$ è un sottocampo di $\mathbb{F}$, allora $\mathbb{F}$ è estensione di $\mathbb{K}$ (prendendo come ι, ad esempio, l'inclusione).

(1.5) Osservazione *Se $\iota : \mathbb{K} \to \mathbb{F}$ è una estensione, poniamo $[\mathbb{F} : \mathbb{K}] := [\mathbb{F} : \iota(\mathbb{K})]$. L' estensione $\mathbb{F}$ si indica anche con $\mathbb{F} : \mathbb{K}$.*

(1.6) Lemma *Siano $\mathbb{F} \geq \mathbb{L} \geq \mathbb{K}$ dei campi. Allora $[\mathbb{F} : \mathbb{K}] < \infty$ se e solo se $[\mathbb{F} : \mathbb{L}] < \infty$ e $[\mathbb{L} : \mathbb{K}] < \infty$. In tal caso si ha:*

$$[\mathbb{F} : \mathbb{K}] \;=\; [\mathbb{F} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Dimostrazione.
Supponiamo $[\mathbb{F} : \mathbb{K}] < \infty$. Sia $\mathcal{B}$ una base di $\mathbb{F}$ su $\mathbb{K}$. Ogni $\alpha \in \mathbb{F}$ è combinazione lineare di elementi di $\mathcal{B}$ con coefficienti in $\mathbb{K} \leq \mathbb{L}$. Quindi $\mathcal{B}$ è, a maggior ragione, un insieme di generatori di $\mathbb{F}$ su $\mathbb{L}$. Ogni sottoinsieme indipendente massimale $\mathcal{C}$ di $\mathcal{B}$ è una base finita per $\mathbb{F}$ su $\mathbb{L}$, da cui $[\mathbb{F} : \mathbb{L}] < \infty$. Chiaramente $\mathbb{L}$, in quanto sottospazio di $\mathbb{F}$, ha dimensione finita su $\mathbb{K}$. Concludiamo $[\mathbb{L} : \mathbb{K}] < \infty$.
Supponiamo ora $[\mathbb{F} : \mathbb{L}] = n < \infty$ e $[\mathbb{L} : \mathbb{K}] = m < \infty$.

$$\begin{array}{c} \mathbb{F} \\ \Big| n \\ \mathbb{L} \\ \Big| m \\ \mathbb{K} \end{array}$$

Siano $\{v_1, \ldots, v_n\}$ una base di $\mathbb{F}$ su $\mathbb{L}$ e $\{w_1, \ldots, w_m\}$ una base di $\mathbb{L}$ su $\mathbb{K}$.
Dimostriamo che l'insieme

$$\mathcal{B} := \{v_i w_j \mid 1 \leq i \leq n, , 1 \leq j \leq m\}$$

è una base di $\mathbb{F}$ su $\mathbb{K}$. A tale scopo, sia $\alpha \in \mathbb{F}$. Esso si scrive nella forma $\alpha = \sum_{i=1}^{n} \ell_i v_i$, per opportuni coefficienti $\ell_i \in \mathbb{L}$. Ciascun ℓ_i, a sua volta, si scrive nella forma $\ell_i = \sum_{j=1}^{m} k_{ij} w_j$, per opportuni coefficienti $k_{ij} \in \mathbb{K}$. Ne segue

$$\alpha = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} k_{ij} w_j \right) v_i \;=\; \sum_{i,j} k_{ij} \left(v_i w_j \right).$$

Pertanto $\mathcal{B}$ genera $\mathbb{F}$ su $\mathbb{K}$. Inoltre $\mathcal{B}$ è indipendente. Supponiamo infatti

$$0_{\mathbb{F}} \;=\; \sum_{i,j} k_{ij} \left(v_i w_j \right) \;=\; \sum_{i=1}^{n} \left(\sum_{j=1}^{m} k_{ij} w_j \right) v_i.$$

Per l'indipendenza dei v_i su $\mathbb{L}$ si conclude:

$$\sum_{j=1}^{m} k_{1j}w_j = 0_{\mathbb{L}}, \quad \sum_{j=1}^{m} k_{2j}w_j = 0_{\mathbb{L}}, \quad \ldots, \quad \sum_{j=1}^{m} k_{nj}w_j = 0_{\mathbb{L}}.$$

Per l'indipendenza dei w_i su $\mathbb{K}$ si ha:

$$k_{1j} = 0_{\mathbb{K}},\ 1 \le j \le m, \quad k_{2j} = 0_{\mathbb{K}},\ 1 \le j \le m, \quad \ldots, \quad k_{nj} = 0_{\mathbb{K}},\ 1 \le j \le m.$$

Pertanto $\mathcal{B}$ è una base di $\mathbb{F}$ su $\mathbb{K}$, da cui $[\mathbb{F} : \mathbb{K}] = |\mathcal{B}| = nm$. ■

2 Estensioni semplici

(2.1) Definizione *Sia $\mathbb{K} \le \mathbb{F}$. Se S è un sottoinsieme di $\mathbb{F}$, si indica con $\mathbb{K}(S)$ l'intersezione di tutti i sottocampi di $\mathbb{F}$ che contengono $\mathbb{K}$ e S.*
L'estensione $\mathbb{K}(S)$ si dice semplice *quando $|S| = 1$.*

Poichè fra i sottocampi di $\mathbb{F}$ che contengono S c'è $\mathbb{F}$ stesso e l'intersezione di sottocampi è un sottocampo, si ha che $\mathbb{K}(S)$ è il minimo sottocampo di $\mathbb{F}$ che contiene $\mathbb{K}$ e S.

Se $S = \{\alpha_1, \ldots, \alpha_n\}$, scriviamo $\mathbb{K}(S) = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$. Esempio: $\mathbb{C} = \mathbb{R}(i)$.

(2.2) Definizione *Siano $\mathbb{K} \le \mathbb{F}$ dei campi e sia $\alpha \in \mathbb{F}$.*
• *α è* algebrico *su $\mathbb{K}$ quando è radice di qualche polinomio non nullo di $\mathbb{K}[x]$;*
• *α è* trascendente *su $\mathbb{K}$ in caso contrario.*

Fissato α, possiamo considerare l'omomorfismo di anelli

$$\varphi_\alpha : \mathbb{K}[x] \to \mathbb{F} \quad \text{tale che} \quad \varphi_\alpha(f(x)) := f(\alpha). \tag{2.3}$$

Per le proprietà degli omomorfismi, Ker φ_α è ideale di $\mathbb{K}[x]$, Im φ_α è sottoanello di $\mathbb{F}$.

α è algebrico su $\mathbb{K}$ precisamente quando l'ideale Ker φ_α è non nullo. Infatti:

$$\text{Ker } \varphi_\alpha = \{f(x) \in \mathbb{K}[x] \mid f(\alpha) = 0_{\mathbb{F}}\}.$$

(2.4) Definizione *Se α è algebrico su $\mathbb{K}$, il generatore monico di* Ker φ_α *si dice il polinomio minimo di α su $\mathbb{K}$. Lo indicheremo con $m_{\alpha,\mathbb{K}}(x)$.*

In base a tale definizione, per ogni $f(x) \in \mathbb{K}[x]$,

$$f(\alpha) = 0_{\mathbb{F}} \iff f(x) \in \text{Ker } \varphi_\alpha \iff m_{\alpha,\mathbb{K}}(x) \text{ divide } f(x). \tag{2.5}$$

(2.6) Esempi

- *Ogni* $k \in \mathbb{K}$ *è algebrico su* $\mathbb{K}$. *Il polinomio minimo* $m_{k,\mathbb{K}}(x)$ *di* k *su* $\mathbb{K}$ *è* $x - k$;
- $\sqrt{3} \in \mathbb{R}$ *è algebrico su* $\mathbb{Q}$. *Il polinomio minimo* $m_{\sqrt{3},\mathbb{Q}}(x)$ *è* $x^2 - 3$.

(2.7) Lemma *Supponiamo* $\mathbb{K} \leq \mathbb{F}$, $\alpha \in \mathbb{F}$, *algebrico su* $\mathbb{K}$.

1) *Il polinomio minimo* $m_{\alpha,\mathbb{K}}(x)$ *è irriducibile in* $\mathbb{K}[x]$;

2) *se* $m(x) \in \mathbb{K}[x]$ *è monico, irriducibile e* $m(\alpha) = 0_{\mathbb{F}}$, *allora* $m(x) = m_{\alpha,\mathbb{K}}(x)$.

Dimostrazione.

1) Supponiamo, per assurdo, che $m_{\alpha,\mathbb{K}}(x)$ sia riducibile e consideriamo una sua fattorizzazione $m_{\alpha,\mathbb{K}}(x) = f(x)g(x)$ con $f(x)$, $g(x)$ polinomi di $\mathbb{K}[x]$ aventi grado inferiore a quello di $m_{\alpha,\mathbb{K}}(x)$. Essendo $\mathbb{F}$ privo di divisori dello zero, in virtù della relazione $0_{\mathbb{F}} = m_{\alpha,\mathbb{K}}(\alpha) = f(\alpha)g(\alpha)$ possiamo supporre $f(\alpha) = 0_{\mathbb{F}}$. Ne segue che $m_{\alpha,\mathbb{K}}(x)$ divide $f(x)$. Contraddizione perchè $f(x)$ è non nullo e ha grado inferiore a quello $m_{\alpha,\mathbb{K}}(x)$.

2) Da $m(\alpha) = 0$ segue che $m_{\alpha,\mathbb{K}}(x)$ divide $m(x)$. Quindi, essendo $m(x)$ irriducibile, $m(x) = k\, m_{\alpha,\mathbb{K}}(x)$ per un opportuno $k \in \mathbb{K}$. Poichè $m(x)$ e $m_{\alpha,\mathbb{K}}(x)$ sono entrambi monici, si conclude $m(x) = m_{\alpha,\mathbb{K}}(x)$. ■

(2.8) Teorema *Siano* $\mathbb{K} \leq \mathbb{F}$, $\alpha \in \mathbb{F}$ *e* $\varphi_\alpha : \mathbb{K}[x] \to \mathbb{F}$ *l'omomorfismo definito in* (2.3).

(1) *Se* α *è algebrico su* $\mathbb{K}$, *con polinomio minimo* $m_{\alpha,\mathbb{K}}(x)$ *di grado* m, *si ha:*

   (*i*) φ_α *induce un isomorfismo* $\overline{\varphi}_\alpha : \frac{\mathbb{K}[x]}{\langle m_{\alpha,\mathbb{K}}(x)\rangle} \to \mathbb{K}(\alpha)$ *tale che:*

$$\overline{\varphi}_\alpha(x) = \alpha, \quad \overline{\varphi}_\alpha(k) = k, \ \forall\ k \in \mathbb{K}.$$

   (*ii*) $\mathcal{B} = \left\{\alpha^0, \alpha, \ldots, \alpha^{m-1}\right\}$ *è una base di* $\mathbb{K}(\alpha)$ *su* $\mathbb{K}$, *da cui* $[\mathbb{K}(\alpha) : \mathbb{K}] = m$.

(2) *Se* α *è trascendente,* φ_α *può essere esteso a un isomorfismo* $\Phi_\alpha : \mathbb{K}(x) \to \mathbb{K}(\alpha)$, *dove* $\mathbb{K}(x)$ *è il campo dei quozienti di* $\mathbb{K}[x]$. *Di nuovo* $\Phi_\alpha(x) = \alpha$ *e* $\Phi_{\alpha|\mathbb{K}} = \mathrm{id}$.

Dimostrazione. Da $\varphi_\alpha\left(f(x)\right) = f(\alpha)$ segue

$$\mathrm{Im}\ \varphi_\alpha = \left\{k_n\alpha^n + \cdots + k_1\alpha + k_0 \mid k_i \in \mathbb{K},\ n \geq 0\right\}.$$

$\mathbb{K}(\alpha)$, essendo un campo, è chiuso rispetto alla somma e al prodotto. Ora, da $\alpha \in \mathbb{K}(\alpha)$, segue $\alpha^i \in \mathbb{K}(\alpha)$ per ogni $i \geq 0$. Quindi, da $\mathbb{K} \leq \mathbb{K}(\alpha)$, segue:

$$\mathrm{Im}\ \varphi_\alpha \leq \mathbb{K}(\alpha). \tag{2.9}$$

(1) Se α è algebrico su $\mathbb{K}$ allora φ_α ha nucleo l'ideale $\langle m_{\alpha,\mathbb{K}}(x)\rangle$.

(i) Per il teorema fondamentale degli omomorfismi fra anelli, φ_α induce l' isomorfismo $\overline{\varphi}_\alpha : \frac{\mathbb{K}[x]}{\langle m_{\alpha,\mathbb{K}}(x)\rangle} \to \text{Im } \varphi_\alpha$ tale che, per ogni $r(x) = k_0 + k_1 x + \cdots + k_{m-1}x^{m-1}$:

$$\overline{\varphi}_\alpha\,(r(x)) \;=\; \varphi_\alpha(r(x)) := k_0 + k_1\alpha + \cdots + k_{m-1}\alpha^{m-1}.$$

L'anello $\frac{\mathbb{K}[x]}{\langle m_{\alpha,\mathbb{K}}(x)\rangle}$ è un campo, per l'irriducibilità di $m_{\alpha,\mathbb{K}}(x)$. Quindi Im $\varphi_\alpha \cong \frac{\mathbb{K}[x]}{\langle m_{\alpha,\mathbb{K}}(x)\rangle}$ è anch' esso un campo. Poichè inoltre Im φ_α contiene $\mathbb{K}$ e $\{\alpha\}$, si ha $\mathbb{K}(\alpha) \leq$ Im φ_α. In virtù di (2.9) si conclude che Im $\overline{\varphi}_\alpha =$ Im $\varphi_\alpha = \mathbb{K}(\alpha)$.

(ii) $\left\{x^0, x, \ldots x^{m-1}\right\}$ è una base di $\frac{\mathbb{K}[x]}{\langle m_{\alpha,\mathbb{K}}(x)\rangle}$ su $\mathbb{K}$, come osservato in (1.3). Ne segue che la sua immagine $\mathcal{B}$, tramite l'isomorfismo $\overline{\varphi}_\alpha$, è una base di $\mathbb{K}(\alpha)$ su $\mathbb{K}$.

(2) Se α è trascendente su $\mathbb{K}$, allora φ_α ha nucleo l'ideale nullo. In tal caso φ_α può essere estesa all' isomorfismo $\Phi_\alpha : \mathbb{K}(x) \to \mathbb{K}(\alpha)$ definito ponendo

$$\Phi_\alpha\left(\frac{f(x)}{g(x)}\right) := \varphi_\alpha(f(x)\,(\varphi_\alpha(g(x))^{-1} = \frac{f(\alpha)}{g(\alpha)}.$$

per ogni $f(x)$, $g(x) \in \mathbb{K}[x]$ con $g(x) \neq 0$. ■

(2.10) Corollario *α è algebrico su $\mathbb{K}$ se e solo se $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$.*

Dimostrazione.
Se α è algebrico su $\mathbb{K}$ si ha $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg m_{\alpha,\mathbb{K}}(x) < \infty$. Viceversa, se α è trascendente su $\mathbb{K}$, il sottoinsieme $\{\alpha^n \mid n \in \mathbb{N}\}$ è infinito e indipendente su $\mathbb{K}$. ■

Il Teorema 2.8 ha il seguente importante:

(2.11) Corollario *Dati $\mathbb{K} \leq \mathbb{F}$, $\mathbb{K}' \leq \mathbb{F}'$ campi, $\psi : \mathbb{K} \to \mathbb{K}'$ un isomorfismo, siano*
- *$\alpha \in \mathbb{F}$ una radice di un polinomio monico irriducibile $m(x) \in \mathbb{K}[x]$,*
- *$\alpha' \in \mathbb{F}'$ una radice di $\widehat{\psi}\,(m(x))$, dove $\widehat{\psi} : \mathbb{K}[x] \to \mathbb{K}'[x]$ è definito come in (3.6).*

Allora esiste un isomorfismo $\Psi : \mathbb{K}(\alpha) \to \mathbb{K}'(\alpha')$ tale che $\Psi(\alpha) = \alpha'$ e $\Psi_{|\mathbb{K}} = \psi$.

(2.12)
$$\begin{array}{ccc} \mathbb{K}(\alpha) & \xrightarrow{\Psi} & \mathbb{K}'(\alpha') \\ | & & | \\ \mathbb{K} & \xrightarrow[\psi]{} & \mathbb{K}' \end{array}$$

In particolare:

(1) *se* α *e* β *sono radici di uno stesso polinomio irriducibile* $m(x)$*, esiste un isomorfismo* $\Psi : \mathbb{K}(\alpha) \to \mathbb{K}(\beta)$ *tale che* $\Psi(\alpha) = \beta$ *e* $\Psi_{|\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$*;*

(2) *se* $\mathbb{K} = \mathbb{K}'$*,* $\alpha = \alpha'$*,* $\widehat{\psi}(m(x)) = m(x)$*, esiste un isomorfismo* $\Psi : \mathbb{K}(\alpha) \to \mathbb{K}(\alpha)$ *tale che* $\Psi(\alpha) = \alpha$ *e* $\Psi_{|\mathbb{K}} = \psi$*.*

Dimostrazione. Il polinomio $m(x)$, essendo monico e irriducibile, è il polinomio minimo di α su $\mathbb{K}$. Per il Teorema 2.8 esiste un isomorfismo $\overline{\varphi}_\alpha : \frac{\mathbb{K}[x]}{\langle m(x)\rangle} \to \mathbb{K}(\alpha)$ tale che:

$$x \mapsto \alpha, \quad kx^0 \mapsto k, \ \forall\ k \in \mathbb{K}.$$

L'isomorfismo $\widehat{\psi}$ porta polinomi monici in polinomi monici e polinomi irriducibili in irriducibili. Ne segue che $\widehat{\psi}\,(m(x))$ è monico, irriducibile e coincide così con il polinomio minimo di α' su $\mathbb{K}'$. Esiste quindi un isomorfismo $\overline{\varphi}_{\alpha'} : \frac{\mathbb{K}'[x]}{\langle \widehat{\psi}(m(x))\rangle} \to \mathbb{K}'(\alpha')$ tale che

$$x \mapsto \alpha', \quad k'x^0 \mapsto k', \quad \forall\ k' \in \mathbb{K}'.$$

$\widehat{\psi}$ induce un ovvio isomorfismo, che indichiamo ancora con $\widehat{\psi}$, fra gli anelli quozienti che stiamo considerando. Si ha quindi la sequenza di isomorfismi:

$$\mathbb{K}(\alpha) \ \overset{(\overline{\varphi}_\alpha)^{-1}}{\longrightarrow}\ \frac{\mathbb{K}[x]}{\langle m(x)\rangle} \ \overset{\widehat{\psi}}{\longrightarrow}\ \frac{\mathbb{K}'[x]}{\left\langle \widehat{\psi}(m(x)\right\rangle} \ \overset{\overline{\varphi}_{\alpha'}}{\longrightarrow}\ \mathbb{K}'(\alpha').$$

Siccome il prodotto di isomorfismi è un isomorfismo, l'applicazione

$$\Psi := \overline{\varphi}_{\alpha'}\, \widehat{\psi}\, (\overline{\varphi}_\alpha)^{-1} \ : \ \mathbb{K}(\alpha) \ \to \ \mathbb{K}'(\alpha')$$

è un isomorfismo. Inoltre:

$$\Psi(\alpha) = \overline{\varphi}_{\alpha'}\, \widehat{\psi}\, (\overline{\varphi}_\alpha)^{-1}(\alpha) = \overline{\varphi}_{\alpha'}\, \widehat{\psi}(x) = \overline{\varphi}_{\alpha'}(x) = \alpha'$$

e, per ogni $k \in \mathbb{K}$:

$$\Psi(k) = \overline{\varphi}_{\alpha'}\, \widehat{\psi}\, (\overline{\varphi}_\alpha)^{-1}(k) = \overline{\varphi}_{\alpha'}\, \widehat{\psi}(k) = \overline{\varphi}_{\alpha'}(k) = k$$

L'ultima osservazione si ottiene per $\mathbb{K}' = \mathbb{K}$, $\psi = \mathrm{id}_{\mathbb{K}}$, $\alpha' = \beta$. ∎

3 Campi di spezzamento

Il risultato chiave di questo paragrafo è che, dato un polinomio a coefficienti in $\mathbb{K}$, esiste una estensione $\mathbb{L}$ di $\mathbb{K}$ in cui il polinomio ha una radice. Più precisamente:

(3.1) Lemma *Sia $m(t) \in \mathbb{K}[t]$ irriducibile. Detto $m(x)$ il polinomio ottenuto da $m(t)$ sostituendo t con x, il campo $\mathbb{L} := \frac{\mathbb{K}[x]}{\langle m(x) \rangle}$ è una estensione di $\mathbb{K}$ tale che:*

(1) *x è radice di $m(t)$ in $\mathbb{L}$;*

(2) *$\mathbb{L} = \mathbb{K}(x)$;*

(3) *$[\mathbb{K}(x) : \mathbb{K}] = \deg m(t) = \deg m(x) := m$.*

Dimostrazione.
(1) $\mathbb{L} = \left\{ \sum_{i=0}^{m-1} k_i x^i \mid k_i \in \mathbb{K} \right\}$ è un campo rispetto all'usuale somma di polinomi e al prodotto modulo $m(x)$. Esso è estensione di $\mathbb{K} = \left\{ k_0 x^0 \mid k_0 \in \mathbb{K} \right\}$ e $[\mathbb{L} : \mathbb{K}] = m$.
Posto $m(x) = x^m + \sum_{i=0}^{m-1} h_i x^i$, la potenza m-esima di x in $\mathbb{L}$ è $-\sum_{i=0}^{m-1} h_i x^i$. Infatti:

$$x^m \equiv -\sum_{i=0}^{m-1} h_i x^i \pmod{m(x)}.$$

Pertanto $x \in \mathbb{L}$ è radice del polinomio $t^m + \sum_{i=0}^{m-1} h_i t^i = m(t)$.

(2) e (3) Ora $m(t)$, essendo irriducibile, è il polinomio minimo di x su $\mathbb{K}$. Quindi $[\mathbb{K}(x) : \mathbb{K}] = m$. Da $\mathbb{K}(x) \leq \mathbb{L}$ segue $\mathbb{K}(x) = \mathbb{L}$, avendo entrambi dimensione m su $\mathbb{K}$. ■

(3.2) Definizione *Siano $\mathbb{K}$ un campo e $f(x) \neq 1_{\mathbb{K}} x^0$ un polinomio monico di $\mathbb{K}[x]$.*
Si dice campo di spezzamento *di $f(x)$ su $\mathbb{K}$ una estensione Σ di $\mathbb{K}$ tale che:*
i) $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ con $\alpha_1, \alpha_2, \dots, \alpha_n \in \Sigma$;
ii) $\Sigma = \mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$.

(3.3) Esempi
1. *$\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$ è il campo di spezzamento di $x^2 + 1$ su $\mathbb{R}$. Chiaramente $\min_{i,\mathbb{R}}(x) = x^2 + 1$, da cui $[\mathbb{C} : \mathbb{R}] = 2$.*
2. *Sia $p > 0$ un numero primo. $\mathbb{Q}(\sqrt{p}, -\sqrt{p}) = \mathbb{Q}(\sqrt{p})$ è il campo di spezzamento di $x^2 - p$ su $\mathbb{Q}$. Si ha $\min_{\sqrt{p},\mathbb{Q}}(x) = x^2 - p$, da cui $[\mathbb{Q}(\sqrt{p}) : Q] = 2$.*
3. *Sia p un numero primo e sia $\omega = e^{\frac{2\pi i}{3}}$ una radice cubica di 1.*

$$\mathbb{Q}(\sqrt[3]{p},\ \omega\sqrt[3]{p},\ \omega^2\sqrt[3]{p}) = \mathbb{Q}(\sqrt[3]{p},\ \omega),$$

è il campo di spezzamento di x^3-p *su* $\mathbb{Q}$. *Da* $\min_{\sqrt[3]{p},\mathbb{Q}}(x) = x^3-p$ *segue* $[\mathbb{Q}(\sqrt[3]{p}) : \mathbb{Q}] = 3$. *Notando che* $\sqrt[3]{p} \in \mathbb{R}$, *mentre* $\omega \notin \mathbb{R}$, *si ha facilmente*

$$[\mathbb{Q}(\sqrt[3]{p},\ \omega) : \mathbb{Q}] \ = \ 3 \cdot 2 \ = \ 6.$$

(3.4) Lemma *Sia* $f(x) = g(x)q(x)$ *con* $g(x), q(x) \in \mathbb{K}[x]$, *monici.*
Se $\mathbb{L}$ *è un campo di spezzamento per* $q(x)$ *su* $\mathbb{K}$ *e* Σ *un campo di spezzamento per* $g(x)$ *su* $\mathbb{L}$, *allora* Σ *è un campo di spezzamento per* $f(x)$ *su* $\mathbb{K}$.

Dimostrazione. Possiamo supporre $\mathbb{K} \leq \mathbb{L} \leq \Sigma$. Inoltre:
i) $q(x) = (x-\alpha_1)\dots(x-\alpha_m)$ con $\alpha_1, \dots, \alpha_m \in \mathbb{L}$;
ii) $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_m)$.
Analogamente:
i) $g(x) = (x-\alpha_{m+1})\dots(x-\alpha_n)$ con $\alpha_{m+1}, \dots, \alpha_n \in \Sigma$;
ii) $\Sigma = \mathbb{L}(\alpha_{m+1}, \dots, \alpha_n)$.
Segue:
i) $f(x) = (x-\alpha_1)\dots(x-\alpha_m)(x-\alpha_{m+1})\dots(x-\alpha_n)$ con $\alpha_1, \dots, \alpha_n \in \Sigma$;
ii) $\Sigma = \mathbb{L}(\alpha_{m+1}, \dots, \alpha_n) = \mathbb{K}(\alpha_1, , \dots, \alpha_m, \alpha_{m+1}, \dots, \alpha_n)$.
Si conclude l'asserto. ■

Il campo di spezzamento di un polinomio $f(x) \in \mathbb{K}[x]$ esiste ed è unico, a meno di isomorfismi, in virtù del seguente:

(3.5) Teorema *Sia* $f(x)$ *un polinomio monico di* $\mathbb{K}[x]$, *avente grado* $n \geq 1$.

(1) *Esiste un campo di spezzamento* Σ *di* $f(x)$ *su* $\mathbb{K}$ *e* $[\Sigma : \mathbb{K}] \leq n!$;

(2) *se* $\psi : \mathbb{K} \to \mathbb{K}'$ *è un isomorfismo e* Σ' *è un campo di spezzamento di* $\widehat{\psi}(f(x))$ *su* $\mathbb{K}'$, *allora esiste un isomorfismo* $\Psi : \Sigma \to \Sigma'$ *tale che* $\Psi_{|\mathbb{K}} = \psi$;

(3) *se* Σ' *è un campo di spezzamento di* $f(x)$ *su* $\mathbb{K}$, *allora esiste un isomorfismo* $\Psi : \Sigma \to \Sigma'$ *tale che* $\Psi_{\mathbb{K}} = id$.

Dimostrazione.
Consideriamo la fattorizzazione $f(x) = p_1(x)\dots p_m(x)$, dove ogni fattore $p_j(x)$ è monico, irriducibile in $\mathbb{K}[x]$. Se tutti i $p_j(x)$ hanno grado 1, in particolare se $f(x)$ ha grado $n = 1$,

$$f(x) = (x-\alpha_1)\dots(x-\alpha_m)$$

con $\alpha_j \in \mathbb{K}$, $1 \leq j \leq m$. In tal caso valgono gli enunciati 1) e 2). Infatti:
i) $\Sigma = \mathbb{K}$ e $[\Sigma : \mathbb{K}] = 1 \leq n!$;
ii) $\widehat{\psi}\,(f(x)) = (x - \psi(\alpha_1)) \cdots (x - \psi(\alpha_m))$, da cui $\Sigma' = \mathbb{K}'$ e $\Psi = \psi$.
Altrimenti possiamo supporre che $p_1(x)$ abbia grado $s \geq 2$. Per il Lemma 3.1 il campo $\frac{\mathbb{K}[x]}{<p_1(x)>}$ è una estensione di $\mathbb{K}$ in cui $p_1(x)$ ha una radice α. Da $\min_{\alpha,\mathbb{K}}(x) = p_1(x)$ segue $[\mathbb{K}\,(\alpha) : \mathbb{K}] = s$. Chiaramente α è anche radice di $f(x)$. Quindi, per il Teorema di Ruffini:

$$f(x) = (x - \alpha)\, q(x), \quad q(x) \in \mathbb{K}\,(\alpha)\,[x].$$

(1) Per induzione su n, possiamo supporre che esista un campo di spezzamento Σ di $q(x)$ su $\mathbb{K}\,(\alpha)$ e, inoltre, che $[\Sigma : \mathbb{K}\,(\alpha)] \leq (n-1)!$. Per il Lemma 3.4 si ha che Σ è un campo di spezzamento di $f(x)$ su $\mathbb{K}$. Infine

$$[\Sigma : \mathbb{K}] = [\Sigma : \mathbb{K}\,(\alpha)][\mathbb{K}\,(\alpha) : \mathbb{K}] \leq (n-1)!\, s \leq n!$$

(2) Chiaramente $\widehat{\psi}\,(p_1(x)) \ldots \widehat{\psi}\,(p_m(x))$ è la fattorizzazione di $\widehat{\psi}(f(x))$ in polinomi monici irriducibili di $\mathbb{K}'[x]$. Fra le radici di $\widehat{\psi}(f(x))$ ne scegliamo una, α', che sia radice di $\widehat{\psi}\,(p_1(x))$. Per il Corollario 2.11 esiste un isomorfismo $\psi_1 : \mathbb{K}\,(\alpha) \to \mathbb{K}'\,(\alpha')$ tale

$$\psi_1(\alpha) = \alpha' \quad \text{e} \quad (\psi_1)_{|\mathbb{K}} = \psi.$$

Posto ora $\widehat{\psi}(f(x)) = (x - \alpha')g(x)$, si ha che Σ' è il campo di spezzamento di $g(x)$ su $\mathbb{K}'(\alpha')$. Avendo $g(x)$ grado $n-1$, per induzione esiste un isomorfismo $\Psi : \Sigma \to \Sigma'$ tale che $\Psi_{|\mathbb{K}(\alpha)} = \psi_1$. Da $\psi_{1|\mathbb{K}} = \psi$, si conclude che $\Psi_{|\mathbb{K}} = \psi$.

$$\begin{array}{ccc} \Sigma & \xrightarrow{\Psi} & \Sigma' \\ {\scriptstyle \leq (n-1)!}\big| & & \big| \\ \mathbb{K}(\alpha) & \xrightarrow[\psi_1]{} & \mathbb{K}'(\alpha') \\ {\scriptstyle s \leq n}\big| & & \big| \\ \mathbb{K} & \xrightarrow[\psi]{} & \mathbb{K}' \end{array}$$

(3) È conseguenza immediata del punto (2) prendendo $\psi = \mathrm{id}_{\mathbb{K}}$. ■

4 La chiusura algebrica di un campo

(4.1) Definizione *Una estensione* $\mathbb{F} : \mathbb{K}$ *si dice* algebrica *se ogni elemento di* $\mathbb{F}$ *è algebrico su* $\mathbb{K}$.

(4.2) Osservazione *Ogni estensione di grado finito è algebrica.*

Sia infatti $[\mathbb{F} : \mathbb{K}] = n < \infty$. Per ogni $\alpha \in \mathbb{F}$ si ha $\mathbb{K} \leq \mathbb{K}(\alpha) \leq \mathbb{F}$ da cui $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$. In virtù del Corollario 2.10 l'elemento α è algebrico su $\mathbb{K}$.

Per le estensioni algebriche vale inoltre la transitività. Ossia:

(4.3) Lemma *Se $\mathbb{L} : \mathbb{F}$ e $\mathbb{F} : \mathbb{K}$ sono estensioni algebriche, allora anche $\mathbb{L} : \mathbb{K}$ è estensione algebrica.*

Dimostrazione. Fissato $\alpha \in \mathbb{L}$, sia $m(x) = \sum_{i=0}^{n-1} f_i x^i + x^n$ il polinomio minimo di α su $\mathbb{F}$. Ciascun f_i è algebrico su $\mathbb{K}$: ne segue che $[\mathbb{K}(f_0, \cdots, f_{n-1}) : \mathbb{K}] < \infty$. Verifichiamo tale fatto per induzione su n, essendo chiaro per $n = 1$. Sia quindi $n > 1$. Per l'ipotesi induttiva $[\mathbb{K}(f_0, \cdots, f_{n-2}) : \mathbb{K}] < \infty$. Inoltre f_{n-1}, essendo algebrico su $\mathbb{K}$, lo è a maggior ragione su $\mathbb{K}(f_0, \cdots, f_{n-2})$. Quindi $[\mathbb{K}(f_0, \cdots, f_{n-2})(f_{n-1}) : \mathbb{K}(f_0, \cdots, f_{n-2})] < \infty$. Si conclude che $[\mathbb{K}(f_0, \cdots, f_{n-1}) : \mathbb{K}] =$

$$[\mathbb{K}(f_0, \cdots, f_{n-2})(f_{n-1}) : \mathbb{K}(f_0, \cdots, f_{n-2})][\mathbb{K}(f_0, \cdots, f_{n-2}) : \mathbb{K}] < \infty.$$

Chiaramente α è algebrico su $\mathbb{K}(f_0, \cdots, f_{n-1})$. Pertanto $[\mathbb{K}(f_0, \cdots, f_{n-1})(\alpha) : \mathbb{K}] =$

$$[\mathbb{K}(f_0, \cdots, f_{n-1})(\alpha) : \mathbb{K}(f_0, \cdots, f_{n-1})][\mathbb{K}(f_0, \cdots, f_{n-1}) : \mathbb{K}] < \infty.$$

Da $\mathbb{K}(\alpha) \leq \mathbb{K}(f_0, \cdots, f_{n-1})(\alpha)$ si ha che $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$, ossia α è algebrico su $\mathbb{K}$. ■

(4.4) Teorema *Siano $\mathbb{K} \leq \mathbb{F}$, campi. L'insieme H degli elementi di $\mathbb{F}$ algebrici su $\mathbb{K}$ è un sottocampo di $\mathbb{F}$ che contiene $\mathbb{K}$. Inoltre, se $\mathbb{F}$ è algebricamente chiuso, anche H è algebricamente chiuso.*

Dimostrazione.
Chiaramente $\mathbb{K} \leq H$. Siano α, β elementi di $\mathbb{F}$, algebrici su $\mathbb{K}$, con $\beta \neq 0_{\mathbb{F}}$. Dobbiamo dimostrare che $\alpha - \beta$ e $\alpha\beta^{-1}$ sono algebrici su $\mathbb{K}$. Ora $\mathbb{K}(\alpha, \beta) = (\mathbb{K}(\alpha))(\beta)$ è estensione algebrica di $\mathbb{K}(\alpha)$ perchè β, essendo algebrico su $\mathbb{K}$, lo è a maggior ragione su $\mathbb{K}(\alpha)$. Inoltre $\mathbb{K}(\alpha)$ è estensione algebrica di $\mathbb{K}$. Dal Lemma precedente si ottiene che $\mathbb{K}(\alpha, \beta)$ è estensione algebrica di $\mathbb{K}$. In particolare $\alpha - \beta$ e $\alpha\beta^{-1}$, in quanto elementi di $\mathbb{K}(\alpha, \beta)$, sono algebrici su $\mathbb{K}$.
Supponiamo ora che $\mathbb{F}$ sia algebricamente chiuso e consideriamo un polinomio irriducibile $m(x) \in H[x]$. Detta α una radice di $m(x)$ in $\mathbb{F}$, si ha che $H(\alpha)$ è estensione algebrica di H, avendo grado finito. Ora H è, per definizione, estensione algebrica di $\mathbb{K}$. Dal Lemma

4.3 si ha che $H(\alpha)$ è estensione algebrica di $\mathbb{K}$. Ne segue che α è algebrico su $\mathbb{K}$, quindi $\alpha \in H$. Si conclude che $m(x)$ ha grado 1, ossia che H è algebricamente chiuso. ■

(4.5) Esempio *Per $\mathbb{K} = \mathbb{Q}$ e $\mathbb{F} = \mathbb{C}$ si ottiene il campo H dei* numeri algebrici*, ossia dei numeri complessi che sono radici dei polinomi a coefficienti razionali. Esso è algebricamente chiuso per il Teorema* 4.4*.*

Per le considerazioni che seguono H è numerabile, quindi un sottoinsieme *piccolo* di $\mathbb{C}$.

Sia $\mathbb{F} \geq \mathbb{K}$ una estensione algebrica. Dalla teoria degli insiemi si ha che:

$$|\mathbb{F}| = |\mathbb{N}|, \text{ se } |\mathbb{K}| < \infty, \quad |\mathbb{F}| = |\mathbb{K}|, \text{ se } |\mathbb{K}| = \infty.$$

Per convincersene è utile notare che ogni polinomio di $\mathbb{K}[x]$ è un elemento di $\mathbb{K}^n$, per qualche $n \geq 0$. Ne segue che $\mathbb{K}[x]$ è numerabile se $\mathbb{K}$ è finito, altrimenti ha la stessa cardinalità di $\mathbb{K}$. Poichè $\mathbb{F}$ è unione di insiemi finiti, ciascuno dei quali è costituito dalle radici in $\mathbb{F}$ di un polinomio $f(x) \in \mathbb{K}[x]$, si ottiene che $\mathbb{F}$ ha la stessa cardinalità di $\mathbb{K}[x]$.

(4.6) Definizione *Una estensione $\mathbb{E}$ di $\mathbb{K}$ di dice una* chiusura algebrica *se:*

- $\mathbb{E}$ *è estensione algebrica di* $\mathbb{K}$*,*
- $\mathbb{E}$ *è algebricamente chiuso.*

(4.7) Teorema *Ogni campo $\mathbb{K}$ ha una chiusura algebrica $\mathbb{E}$.*

Dimostrazione. Immergiamo $\mathbb{K}$ nell' insieme $X := \mathcal{P}(\mathbb{N})$ se $\mathbb{K}$ è finito, $X := \mathcal{P}(\mathbb{K})$ se $\mathbb{K}$ è infinito. Consideriamo quindi l'insieme Y i cui elementi sono le estensioni algebriche $\mathbb{F}$ di $\mathbb{K}$ tali che $\mathbb{F} \subseteq X$. Per ogni $\mathbb{F}_1, \mathbb{F}_2 \in Y$, poniamo $\mathbb{F}_1 \leq \mathbb{F}_2$ se e solo se $\mathbb{F}_1$ è sottocampo di $\mathbb{F}_2$. Chiaramente $(Y, \leq)$ è un insieme parzialmente ordinato. Considerata una catena $\mathcal{C}$ in Y, mostriamo che ha estremo superiore in Y. Sia infatti $\widehat{\mathbb{F}} := \cup_{\mathbb{F} \in \mathcal{C}} \mathbb{F}$. Per ogni $x, y \in \widehat{\mathbb{F}}$ esiste $\mathbb{F}_1 \in \mathcal{C}$ tale che $x, y \in \mathbb{F}_1$. Pertanto $x - y$ e xy^{-1} (per $y \neq 0$) appartengono a $\mathbb{F}_1$, quindi anche a $\widehat{\mathbb{F}}$. (Se $x, y \in \mathbb{F}_2 \in \mathcal{C}$ si ha $\mathbb{F}_1$ sottoanello di $\mathbb{F}_2$ o viceversa: in ogni caso $x - y$ e xy^{-1} sono gli stessi). È evidente che ogni elemento di $\widehat{\mathbb{F}}$ è algebrico su $\mathbb{K}$. Per il Lemma di Zorn, esiste un elemento massimale $\mathbb{E} \in Y$. Verifichiamo che $\mathbb{E}$ è algebricamente chiuso. In caso contrario, esisterebbe un polinomio irriducibile $m(x) \in \mathbb{E}[x]$ di grado $n \geq 2$ e, per il Lemma 3.1, esisterebbe una estensione $\widehat{\mathbb{E}}$ di $\mathbb{E}$ tale che $[\widehat{\mathbb{E}} : \mathbb{E}] = n$. Pertanto $\widehat{\mathbb{E}}$ sarebbe estensione algebrica di $\mathbb{E}$ e quindi anche di $\mathbb{K}$ per

il Lemma 4.3. In particolare $|\widehat{\mathbb{E}}| < |X|$, quindi possiamo supporre $\widehat{\mathbb{E}} \subseteq X$. Si conclude $\widehat{\mathbb{E}} \in Y$, in contrasto con la massimalità di $\mathbb{E}$. ■

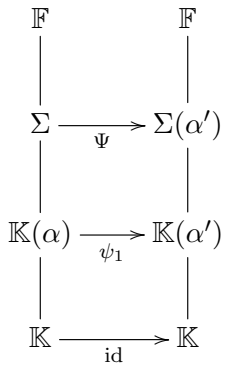
Si può inoltre dimostrare che la chiusura algebrica di un campo è unica, a meno di isomorfismi.

5 Estensioni di Galois

(5.1) Definizione *Una estensione* $\mathbb{F} : \mathbb{K}$ *si dice* normale *se ogni polinomio irriducibile* $m(x) \in \mathbb{K}[x]$*, che ha almeno una radice in* $\mathbb{F}$*, si scompone in fattori di grado* 1 *in* $\mathbb{F}[x]$*.*

(5.2) Teorema *Sia* Σ *il campo di spezzamento di* $f(x) \in \mathbb{K}[x]$*. Allora* $\Sigma : \mathbb{K}$ *è una estensione normale.*

Dimostrazione. Sia $m(x) \in \mathbb{K}[x]$ (monico) irriducibile e sia $\mathbb{F}$ un campo di spezzamento di $m(x)$ su Σ. Dobbiamo dimostrare che se $m(x)$ ha una radice α in Σ, allora ogni altra radice α' di $m(x)$ in $\mathbb{F}$ appartiene a Σ.
Per il Corollario 2.11, con $\mathbb{K} = \mathbb{K}'$, $\psi = \mathrm{id}$, esiste un isomorfismo $\psi_1 : \mathbb{K}(\alpha) \to \mathbb{K}(\alpha')$ tale che $\psi_1(\alpha) = \alpha'$ e $\psi_{1_{|\mathbb{K}}} = \mathrm{id}$.



Possiamo considerare Σ come campo di spezzamento di $f(x)$ su $\mathbb{K}(\alpha)$ e $\Sigma(\alpha')$ come campo di spezzamento di $f(x)$ su $\mathbb{K}(\alpha')$. Per il punto 2) del Teorema 3.5, esiste un isomorfismo $\Psi : \Sigma \to \Sigma(\alpha')$ tale che $\Psi_{|\mathbb{K}(\alpha)} = \varphi_1$. In particolare $\Psi_{|\mathbb{K}} = \mathrm{id}$. Ne segue che $\widehat{\Psi}(f(x)) = f(x)$, ossia Ψ permuta le radici $\alpha_1, \ldots, \alpha_n$ di $f(x)$. Essendo $\Sigma = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ si ha $\Psi(\Sigma) = \Sigma$. Si conclude che $\alpha' = \Psi(\alpha) \in \Sigma$. ■

(5.3) Corollario *Una estensione* $\mathbb{F} : \mathbb{K}$ *è normale di grado finito se e solo se* $\mathbb{F}$ *è campo di spezzamento di un polinomio su* $\mathbb{K}$*.*

Dimostrazione. Se $\mathbb{F}$ è campo di spezzamento di un polinomio $f(x)$ su $\mathbb{K}$, allora $\mathbb{F}$ è estensione normale di $\mathbb{K}$ per il Teorema 5.2. Inoltre $[\mathbb{F} : \mathbb{K}] \leq (\deg f(x))! < \infty$. Viceversa. Essendo $[\mathbb{F} : \mathbb{K}]$ finito, esiste una base finita $\{\alpha_1, \ldots, \alpha_n\}$ di $\mathbb{F}$ su $\mathbb{K}$. Essendo $\mathbb{F}$ normale, il polinomio minimo $m_i(x)$ di α_i su $\mathbb{K}$ ha tutte le sue radici in $\mathbb{F}$, $1 \leq i \leq n$. Si conclude che $\mathbb{F}$ è il campo di spezzamento di $m(x) = \prod_{i=1}^{n} m_i(x)$ su $\mathbb{K}$. ■

(5.4) Osservazione *Sia Σ il campo di spezzamento di $f(x) \in \mathbb{K}[x]$ e sia $\mathbb{K} \leq \mathbb{F} \leq \Sigma$. Dalla Definizione* 3.2 *segue subito che Σ è campo di spezzamento di $f(x)$ su $\mathbb{F}$, quindi l'estensione $\Sigma : \mathbb{F}$ è normale. Tuttavia, in generale, $\mathbb{F} : \mathbb{K}$ non è estensione normale di $\mathbb{K}$. In proposito si veda il Teorema 3.9 del Capitolo successivo.*

(5.5) Definizione *Un polinomio $f(x) \in \mathbb{K}[x]$ si dice* separabile *se non ha radici multiple in un suo campo di spezzamento.*

Uno strumento efficace per stabilire se un polinomio è separabile o meno è costituito dalla derivazione formale.

(5.6) Lemma *Un polinomio $f(x) \in \mathbb{K}[x]$ ha qualche radice multipla in un suo campo di spezzamento Σ se e solo se $d(x) = \mathrm{MCD}\,(f(x), f'(x))$ ha grado > 0.*

Dimostrazione. Supponiamo che $f(x)$ abbia una radice $\alpha \in \Sigma$ di molteplicità ≥ 2. Si ha che $(x-\alpha)^2$ divide $f(x)$, ossia $f(x) = (x-\alpha)^2 q(x)$ in $\Sigma[x]$. Ne segue

$$f'(x) = 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x) = (x-\alpha)\left(2q(x) + (x-\alpha)q'(x)\right).$$

Pertanto $x - \alpha$ divide $f(x)$ e $f'(x)$, quindi anche $d(x)$. Ne segue che $d(x)$ ha grado > 0. Viceversa, supponiamo che $d(x)$ abbia grado > 0 e che $\alpha \in \Sigma$ sia una radice di $d(x)$. Da $f(x) = (x-\alpha)g(x)$ deduciamo $f'(x) = g(x) + (x-\alpha)g'(x)$, ossia

$$g(x) = f'(x) - (x-\alpha)g'(x).$$

Essendo $f'(x)$ divisibile per $(x-\alpha)$ si ha che $g(x) = (x-\alpha)h(x)$. Concludiamo che $f(x) = (x-\alpha)g(x) = (x-\alpha)^2 h(x)$. ■

(5.7) Corollario

1) *Se $\mathbb{K}$ ha caratteristica 0, ogni polinomio irriducibile $f(x) \in \mathbb{K}[x]$ è separabile.*

2) *Se $\mathbb{K}$ ha caratteristica $p > 0$ e $q = p^n$, il polinomio $f(x) = x^q - x$ è separabile.*

Dimostrazione.
Poniamo $d(x) = \mathrm{MCD}\,(f(x), f'(x))$.
1) Sia n il grado di $m(x)$. Se $n = 1$ l'asserto è ovvio. Possiamo quindi supporre $n \geq 2$. Da $m(x) = k_0 + \cdots + k_n x^n$ segue che $m'(x) = k_1 + \cdots + nk_n x^{n-1}$ ha grado $n - 1$. Ne segue che $d(x)$ non può avere grado n. Per l'irriducibilità di $m(x)$ si conclude che $d(x)$ ha grado 0, da cui l'asserto per il Lemma precedente.
2) Si ha che $f'(x) = qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1$ ha grado 0. Di nuovo $d(x)$ ha grado 0. ■

(5.8) Definizione $\mathbb{F}$ *è* estensione separabile *di* $\mathbb{K}$ *se è estensione algebrica e, per ogni* $\alpha \in \mathbb{F}$*, il suo polinomio minimo su* $\mathbb{K}$ *è separabile.*

Conviene infine introdurre la seguente

(5.9) Definizione *Una estensione* $\mathbb{F} : \mathbb{K}$ *si dice* di Galois *se soddisfa le proprietà:*

1) $\mathbb{F}$ *è estensione separabile di* $\mathbb{K}$*;*

2) $\mathbb{F}$ *è estensione normale di* $\mathbb{K}$*;*

3) $[\mathbb{F} : \mathbb{K}]$ *è finito.*

Per il Corollario 5.3 le condizioni 2) e 3) sono equivalenti al fatto che $\mathbb{F}$ sia campo di spezzamento di un polinomio su $\mathbb{K}$.
Inoltre, per il punto 1) del Corollario 5.7, se $\mathbb{K}$ ha caratteristica 0, un'estensione $\mathbb{F} : \mathbb{K}$ è di Galois se e solo se $\mathbb{F}$ è il campo di spezzamento di un polinomio su $\mathbb{K}$.

Capitolo III

La corrispondenza di Galois

1 Gruppi di automorfismi

Siano $\psi_1, \ldots, \psi_n$ dei monomorfismi dal campo $\mathbb{K}$ al campo $\mathbb{F}$. Assegnati n elementi $a_1, \ldots, a_n$ di $\mathbb{F}$, possiamo definire la seguente applicazione da $\mathbb{K}$ a $\mathbb{F}$:

$$\forall\ \alpha \in \mathbb{K}: \quad \alpha \mapsto a_1\psi_1(\alpha) + \cdots + a_n\psi_n(\alpha).$$

Essa, in generale, non è un monomorfismo, ma ha alcune proprietà utili.

(1.1) Lemma *I monomorfismi $\psi_1, \ldots, \psi_n$ da $\mathbb{K}$ a $\mathbb{F}$ siano a due a due distinti. Allora sono linearmente indipendenti su $\mathbb{F}$. Ossia se:*

$$\forall\ \alpha \in \mathbb{K}, \quad a_1\psi_1(\alpha) + \cdots + a_n\psi_n(\alpha) = \sum_{i=1}^{n} a_i\psi_i(\alpha) = 0_{\mathbb{F}} \tag{1.2}$$

allora $a_1 = \cdots = a_n = 0_{\mathbb{F}}$.

Dimostrazione.
Induzione su n. Se $n = 1$, per $\alpha = 1_{\mathbb{K}}$, si ha: $0_{\mathbb{F}} = a_1\psi_1(1_{\mathbb{K}}) = a_1 1_{\mathbb{F}} = a_1$.
Sia quindi $n > 1$. Basta dimostrare $a_n = 0_{\mathbb{F}}$. Infatti, in tal caso, la (1.2) diventa:

$$\forall\ \alpha \in \mathbb{K}, \quad a_1\psi_1(\alpha) + \cdots + a_{n-1}\psi_{n-1}(\alpha) = \sum_{i=1}^{n-1} a_i\psi_i(\alpha) = 0_{\mathbb{F}}.$$

Ne segue, per l'ipotesi induttiva, $a_1 = \cdots = a_{n-1} = 0_{\mathbb{F}}$.
Essendo $\psi_1 \neq \psi_n$, esiste $\beta \in \mathbb{K}$ tale che $\psi_1(\beta) \neq \psi_n(\beta)$. Moltiplicando (1.2) per $\psi_1(\beta)$:

$$\forall\ \alpha \in \mathbb{K}, \quad a_1\psi_1(\alpha)\psi_1(\beta) + \cdots + a_n\psi_n(\alpha)\psi_1(\beta) = \sum_{i=1}^{n} a_i\psi_i(\alpha)\psi_1(\beta) = 0_{\mathbb{F}}. \tag{1.3}$$

D'altra parte, per (1.2) valutata in $\alpha\beta$, si ha $a_1\psi_1(\alpha\beta) + \cdots + a_n\psi_n(\alpha\beta) = 0_{\mathbb{F}}$, da cui:

$$a_1\psi_1(\alpha)\psi_1(\beta) + \cdots + a_n\psi_n(\alpha)\psi_n(\beta) = \sum_{i=1}^{n} a_i\psi_i(\alpha)\psi_i(\beta) = 0_{\mathbb{F}}. \tag{1.4}$$

Sottraendo (1.4) da (1.3) si ha:

$$\forall\ \alpha \in \mathbb{K}, \quad \sum_{i=2}^{n} a_i\, \psi_i(\alpha)\, (\psi_1(\beta) - \psi_i(\beta)) = 0_{\mathbb{F}}.$$

Siccome stiamo supponendo vero l'asserto per $n-1$, otteniamo

$$a_i\, (\psi_1(\beta) - \psi_i(\beta)) = 0_{\mathbb{F}}, \quad 2 \leq i \leq n.$$

Se fosse $a_n \neq 0_{\mathbb{F}}$ si otterrebbe la contraddizione $\psi_1(\beta) = \psi_n(\beta)$. ■

Dato un campo $\mathbb{F}$, indichiamo con $\mathrm{Aut}(\mathbb{F})$ *l'insieme dei suoi automorfismi.* $\mathrm{Aut}(\mathbb{F})$ è un gruppo, in quanto sottogruppo del gruppo $\mathrm{Sym}(\mathbb{F})$ delle applicazioni bijettive di $\mathbb{F}$ in sè. Infatti $\mathrm{id}_{\mathbb{F}} \in \mathrm{Aut}(\mathbb{F})$. Inoltre se σ e τ sono automorfismi di $\mathbb{F}$, per ogni $\alpha, \beta \in \mathbb{F}$ si ha:

$$\sigma\tau(\alpha + \beta) := \sigma\,(\tau(\alpha + \beta)) = \sigma\,(\tau(\alpha) + \tau(\beta)) = \sigma\tau(\alpha) + \sigma\tau(\beta)$$

e

$$\sigma\tau(\alpha\beta) := \sigma\,(\tau(\alpha\beta)) = \sigma\,(\tau(\alpha)\tau(\beta)) = \sigma\tau(\alpha)\sigma\tau(\beta).$$

Quindi $\sigma\tau$ è un automorfismo. Analogamente si vede che anche τ^{-1} lo è .

(1.5) Definizione *Siano $\mathbb{F}$ un campo e G un sottogruppo di* $\mathrm{Aut}(\mathbb{F})$. *Si dice* campo fisso *di G, e si indica con $\mathbb{F}_G$, il sottoinsieme di $\mathbb{F}$ costituito dagli elementi di $\mathbb{F}$ fissati da ogni elemento di G. Ossia:*

$$\mathbb{F}_G := \{\alpha \in \mathbb{F} \mid \psi(\alpha) = \alpha, \forall\ \psi \in G\}\,. \tag{1.6}$$

È immediato verificare che $\mathbb{F}_G$ è un sottocampo di $\mathbb{F}$.
Per esempio, se G il sottogruppo di $\mathrm{Aut}(\mathbb{C})$ costituito dall'identità $\mathrm{id}_{\mathbb{C}}$ e dall'automorfismo coniugio $a + ib \mapsto a - ib$, allora $\mathbb{C}_G = \mathbb{R}$. In particolare $|G| = 2 = [\mathbb{C} : \mathbb{R}]$. Quando G è finito, questo fatto vale in generale, in virtù del seguente:

(1.7) Teorema *Sia G un gruppo finito di automorfismi di un campo $\mathbb{F}$. Allora*

$$|G| = [\mathbb{F} : \mathbb{F}_G].$$

Dimostrazione. Posto $|G| = n$, siano $\psi_1, \ldots, \psi_n$ i suoi elementi. Sia $m := [\mathbb{F} : \mathbb{F}_G] \leq \infty$. Supponiamo dapprima $m < n$. Fissata una base $\{w_1, \ldots, w_m\}$ di $\mathbb{F}$ su $\mathbb{F}_G$, consideriamo il sistema lineare omogeneo di m equazioni nelle n indeterminate $x_1, \ldots, x_n$:

$$\left\{\begin{array}{rcl} \psi_1(w_1)x_1 + \cdots + \psi_n(w_1)x_n & = & 0_{\mathbb{F}} \\ \cdots\cdots\cdots & & \\ \psi_1(w_m)x_1 + \cdots + \psi_n(w_m)x_n & = & 0_{\mathbb{F}} \end{array}\right. \qquad \left\{\begin{array}{rcl} \sum_{i=1}^{n} \psi_i(w_1)x_i & = & 0_{\mathbb{F}} \\ \cdots\cdots\cdots & & \\ \sum_{i=1}^{n} \psi_i(w_m)x_i & = & 0_{\mathbb{F}} \end{array}\right. \tag{1.8}$$

Essendo $m < n$, il sistema (1.8) ha delle soluzioni non nulle. Sia $a_1, \ldots, a_n$ una di queste. Fissato $\alpha \in \mathbb{F}$, esistono opportuni coefficienti $\alpha_i \in \mathbb{F}_G$ tali che

$$\alpha = \alpha_1 w_1 + \ldots \alpha_m w_m = \sum_{j=1}^{m} \alpha_j w_j.$$

Poichè $\psi_i(\alpha_j) = \alpha_j$ per ogni i, j e $\sum_{i=1}^{n} a_i \psi_i(w_j) = 0_{\mathbb{F}}$ per ogni j si deduce

$$\sum_{i=1}^{n} a_i\, \psi_i(\alpha) = \sum_{i=1}^{n} a_i \psi_i \left(\sum_{j=1}^{m} \alpha_j w_j \right) = \sum_{j=1}^{m} \alpha_j \left(\sum_{i=1}^{n} a_i \psi_i(w_j) \right) = \sum_{j=1}^{m} \alpha_j\, 0_{\mathbb{F}} = 0_{\mathbb{F}}.$$

Tale relazione vale per ogni $\alpha \in \mathbb{F}$. Per il Lemma precedente, tutti gli a_i dovrebbero essere nulli, in contrasto con la nostra scelta di una soluzione non nulla.
Supponiamo quindi $n < m$. Esistono $n+1$ elementi $w_1, \ldots, w_{n+1}$ di $\mathbb{F}$ linearmente indipendenti su $\mathbb{F}_G$. Consideriamo il sistema lineare omogeneo di n equazioni nelle $n+1$ indeterminate $x_1, \ldots, x_{n+1}$:

$$(1.9) \qquad \begin{cases} \psi_1(w_1)x_1 + \cdots + \psi_1(w_{n+1})x_{n+1} &= 0_{\mathbb{F}} \\ \qquad\qquad \ldots\ldots\ldots \\ \psi_n(w_1)x_1 + \cdots + \psi_n(w_{n+1})x_{n+1} &= 0_{\mathbb{F}} \end{cases} \qquad \begin{cases} \sum_{i=1}^{m} \psi_1(w_i)x_i &= 0_{\mathbb{F}} \\ \qquad \ldots\ldots\ldots \\ \sum_{i=1}^{m} \psi_n(w_i)x_i &= 0_{\mathbb{F}} \end{cases}$$

Di nuovo il sistema (1.9) ha soluzioni non nulle. Fra queste scegliamone una $b_1, \ldots, b_{n+1}$ che abbia il minimo numero di componenti non nulle. Riordinado eventualmente le indeterminate, possiamo supporre che, per qualche $r \leq n+1$, le prime r componenti siano non nulle, e che le eventuali rimanenti siano nulle. Ossia $b_i \neq 0_{\mathbb{F}}$ per $i \leq r$, $b_i = 0_{\mathbb{F}}$ per $r+1 \leq i \leq n+1$. Abbiamo quindi:

$$(1.10) \qquad \psi_j(w_1)b_1 + \cdots + \psi_j(w_r)b_r = 0_{\mathbb{F}}, \quad 1 \leq j \leq n.$$

Fissiamo $\psi \in G$ e applichiamo ψ a entrambi i membri di (1.10).

$$(1.11) \qquad \psi\psi_j(w_1)\psi(b_1) + \cdots + \psi\psi_j(w_r)\psi(b_r) = 0_{\mathbb{F}}, \quad 1 \leq j \leq n.$$

Osservando che $\{\psi\psi_j \mid 1 \leq j \leq n\} = G = \{\psi_j \mid 1 \leq j \leq n\}$ e riordinando eventualmente gli indici, abbiamo:

$$(1.12) \qquad \psi_j(w_1)\psi(b_1) + \cdots + \psi_j(w_r)\psi(b_r) = 0_{\mathbb{F}}, \quad 1 \leq j \leq n$$

per ogni $\psi \in G$. Moltiplicando le (1.10) per $\psi(b_1)$ e le (1.12) per b_1 e sottraendo

$$(1.13) \quad \psi_j(w_2)\,(b_2\psi(b_1) - b_1\psi(b_2)) + \cdots + \psi_j(w_r)\,(b_r\psi(b_1) - b_1\psi(b_r)) = 0_{\mathbb{F}}, \quad 1 \leq j \leq n.$$

Tali relazioni sono dello stesso tipo di (1.10), eccetto che contengono al più $r-1$ termini.
Per la scelta minimale di r abbiamo

$$b_2\psi(b_1) - b_1\psi(b_2) = 0_{\mathbb{F}}, \ldots, b_r\psi(b_1) - b_1\psi(b_r) = 0_{\mathbb{F}}.$$

Deduciamo che, per ogni $\psi \in G$:

$$b_k\psi(b_1) = b_1\psi(b_k), \quad \text{ossia} \quad \psi\left(b_k b_1^{-1}\right) = b_k b_1^{-1}, \quad 2 \leq k \leq r. \tag{1.14}$$

Pertanto $\lambda_k := b_k b_1^{-1} \in \mathbb{F}_G$, essendo fissato da tutti gli elementi $\psi \in G$.
Dividendo (1.12) per $\psi(b_1)$ si ha:

$$\psi_j(w_1) + \lambda_2\psi_j(w_2) \cdots + \lambda_r\psi_j(w_r) = 0_{\mathbb{F}}, \quad 1 \leq j \leq n.$$

In particolare, posto $\psi_1 = \mathrm{id}_{\mathbb{F}}$ e considerando tale relazione per $j = 1$, si ottiene

$$w_1 + \lambda_2 w_2 + \cdots + \lambda_r w_r = 0_{\mathbb{F}}.$$

Questa è una contraddizione in quanto i w_i sono linearmente indipendenti.
Concludiamo che $n = m$. ■

2 Gruppi di Galois

(2.1) Definizione *Siano $\mathbb{K} \leq \mathbb{F}$ dei campi. Il sottogruppo di* $\mathrm{Aut}(\mathbb{F})$ *costituito dagli automorfismi di $\mathbb{F}$ che fissano ogni elemento di $\mathbb{K}$ si dice il* gruppo di Galois *di $\mathbb{F}$ su $\mathbb{K}$ e si indica con* $\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})$. *In simboli*

$$\mathrm{Gal}_{\mathbb{K}}(\mathbb{F}) := \{\psi \in \mathrm{Aut}(\mathbb{F}) \mid \psi(\alpha) = \alpha, \ \forall\ \alpha \in \mathbb{K}\}\,. \tag{2.2}$$

La verifica che $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$ sia effettivamente un sottogruppo di $\mathrm{Aut}(\Sigma)$ è immediata.
Per le definizioni date si ha che:

$$\mathbb{K} \leq \mathbb{F}_{\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})} \leq \mathbb{F}.$$

Da queste inclusioni e dal Teorema 1.7 segue che, se $\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})$ è finito, allora

$$|\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})| \leq [\mathbb{F} : \mathbb{K}]\,. \tag{2.3}$$

Infatti si ha $|\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})| = \left[\mathbb{F} : \mathbb{F}_{\mathrm{Gal}_{\mathbb{K}}(\mathbb{F})}\right] \leq [\mathbb{F} : \mathbb{K}]$.

In particolare la disuguaglianza (2.3) vale quando $\mathbb{F} = \Sigma$ è il campo di spezzamento di un polinomio $f(x)$ su $\mathbb{K}$. In tal caso gli elementi di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$ possono efficacemente essere rappresentati come permutazioni sulle radici di $f(x)$, nel senso precisato dal seguente:

(2.4) Teorema *Dato $f(x) \in \mathbb{K}[x]$, sia Σ il suo campo di spezzamento su $\mathbb{K}$.*

(1) *Ogni automorfismo $\sigma \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$ permuta le radici di $f(x)$;*

(2) $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$ *è isomorfo a un sottogruppo del gruppo simmetrico* $\mathrm{Sym}\,(\Omega)$*, dove $\Omega = \{\alpha_1, \ldots, \alpha_m\}$ è l'insieme delle radici distinte di $f(x)$.*

Dimostrazione.
(1) Posto $f(x) = k_0 + k_1 x + \cdots + x^n$, si ha:

$$0_\Sigma = k_0 + k_1\alpha_i + \cdots + {\alpha_i}^n, \quad \forall\ \alpha_i \in \Omega. \tag{2.5}$$

Fissiamo una radice α_i. Tenendo presente che ogni coefficiente k_j appartiene a $\mathbb{K}$ e che, di conseguenza, $\sigma(k_j) = k_j$ per definizione di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$, da (2.5) segue

$$0_\Sigma = \sigma(0_\Sigma) = \sigma\left(k_0 + k_1\alpha_i + \cdots + {\alpha_i}^n\right) = k_0 + k_1\sigma(\alpha_i) + \cdots + (\sigma(\alpha_i))^n\,. \tag{2.6}$$

La (2.6) dice che $\sigma(\alpha_i)$ è anch'essa una radice di $f(x)$, ossia che $\sigma(\Omega) \leq \Omega$. D'altra parte, essendo σ iniettiva e Ω finito, $\sigma(\Omega) = \Omega$. Pertanto la restrizione $\sigma_{|\Omega}$ di σ a Ω è un elemento di $\mathrm{Sym}\,(\Omega)$.
(2) L'applicazione

$$\begin{array}{rccc} f: & \mathrm{Gal}_{\mathbb{K}}(\Sigma) & \to & \mathrm{Sym}(\Omega) \\ & \sigma & \mapsto & \sigma_{|\Omega} \end{array}$$

è un omomorfismo. Infatti, per ogni $\sigma, \tau \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$ e per ogni $\alpha_i \in \Omega$, si ha $(\sigma\tau)(\alpha_i) = \sigma(\tau(\alpha_i))$, ossia $(\sigma\tau)_{|\Omega} = \sigma_{|\Omega}\tau_{|\Omega}$.
Verifichiamo che f è iniettiva. A tale scopo supponiamo $\sigma \in \mathrm{Ker}\ f$, ossia $\sigma(\alpha_i) = \alpha_i$ per $1 \leq i \leq m$, e dimostriamo che $\sigma = \mathrm{id}_\Sigma$.
Ragioniamo per induzione su m. Se $m = 1$, ogni elemento di $\Sigma = \mathbb{K}(\alpha_1)$ è della forma $\sum_{i=0}^{t-1} h_i\alpha_1^i$, con $h_i \in \mathbb{K}$. Da $\sigma(h_i) = h_i$ e $\sigma(\alpha_1) = \alpha_1$ segue $\sigma = \mathrm{id}_{\mathbb{K}(\alpha_1)}$. Se $m > 1$, posto $f(x) = (x - \alpha_1)g(x)$ possiamo considerare $\Sigma = \mathbb{K}\,(\alpha_1, \ldots, \alpha_m)$ come il campo di spezzamento di $g(x)$ su $\mathbb{K}(\alpha_1)$ e σ come un elemento di $\mathrm{Gal}_{\mathbb{K}(\alpha_1)}(\Sigma)$. Poichè le radici distinte di $g(x)$ sono $\alpha_2, \ldots, \alpha_m$ abbiamo, per induzione, $\sigma = \mathrm{id}_\Sigma$.
Quindi f è iniettiva. Concludiamo che $\mathrm{Gal}_{\mathbb{K}}(\Sigma) \simeq \mathrm{Im}\ f \leq \mathrm{Sym}(\Omega)$. ∎

(2.7) Teorema *Sia Σ il campo di spezzamento di un polinomio $f(x) \in \mathbb{K}[x]$.*
Se $f(x)$ è separabile, allora $|\mathrm{Gal}_{\mathbb{K}}(\Sigma)| = [\Sigma : \mathbb{K}]$.

Dimostrazione. Se $[\Sigma : \mathbb{K}] = 1$ si ha $\Sigma = \mathbb{K}$, $\mathrm{Gal}_{\mathbb{K}}(\mathbb{K}) = \{\mathrm{id}\}$ e l'asserto è vero. Supponiamo quindi $[\Sigma : \mathbb{K}] > 1$. In tal caso $f(x)$ ha almeno un fattore irriducibile $m(x)$ di grado $m \geq 2$ in $\mathbb{K}[x]$. Detta α una radice di $m(x)$ in Σ si ha $\alpha \notin \mathbb{K}$ e $m(x) = \min_{\alpha,\mathbb{K}}(x)$. Ne segue:

$$[\Sigma : \mathbb{K}] = [\Sigma : \mathbb{K}(\alpha)]\,[\mathbb{K}(\alpha) : \mathbb{K}] = [\Sigma : \mathbb{K}(\alpha)]\,m > [\Sigma : \mathbb{K}(\alpha)].$$

Considerando Σ come campo di spezzamento di $f(x)$ su $\mathbb{K}(\alpha)$, abbiamo

$$\left|\mathrm{Gal}_{\mathbb{K}(\alpha)}(\Sigma)\right| = [\Sigma : \mathbb{K}(\alpha)] := n \tag{2.8}$$

per induzione su $[\Sigma : \mathbb{K}]$. Chiamiamo $\varphi_1, \ldots, \varphi_n$ gli elementi di $\mathrm{Gal}_{\mathbb{K}(\alpha)}(\Sigma)$.
Il polinomio $m(x)$ ha m radici distinte $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$, essendo un fattore di $f(x)$ che è separabile per ipotesi. Esse appartengono tutte a Σ, essendo radici di $f(x)$. Per ogni radice α_i, esiste un isomorfismo $\psi_i : \mathbb{K}(\alpha) \to \mathbb{K}(\alpha_i)$ tale che

$$\begin{cases} \psi_i(\alpha) = \alpha_i \\ \psi_{i|\mathbb{K}} = \mathrm{id}_{\mathbb{K}} \end{cases}$$

(Corollario 2.11 del Capitolo II). Nelle notazioni del Teorema 3.5 del Capitolo II si ha quindi $\widehat{\psi_i}\,(f(x)) = f(x)$. Per il punto 2) dello stesso Teorema, con $\Sigma = \Sigma'$, l'isomorfismo ψ_i può essere esteso ad uno $\Psi_i \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$. In realtà , ciascuno degli n prodotti

$$\left\{\Psi_i\varphi_j \mid \varphi_j \in \mathrm{Gal}_{\mathbb{K}(\alpha)}(\Sigma)\right\}$$

è un elemento di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$ che estende ψ_i. Ne segue $|\mathrm{Gal}_{\mathbb{K}}(\Sigma)| \geq nm$.

$$\begin{array}{ccccc} \Sigma & \xrightarrow{\varphi_j} & \Sigma & \xrightarrow{\Psi_i} & \Sigma \\ {\scriptstyle n}\big| & & {\scriptstyle n}\big| & & {\scriptstyle n}\big| \\ \mathbb{K}(\alpha) & \xrightarrow[\mathrm{id}]{} & \mathbb{K}(\alpha) & \xrightarrow[\psi_i]{} & \mathbb{K}(\alpha_i) \\ {\scriptstyle m}\big| & & {\scriptstyle m}\big| & & {\scriptstyle m}\big| \\ \mathbb{K} & \xrightarrow[\mathrm{id}]{} & \mathbb{K} & \xrightarrow[\mathrm{id}]{} & \mathbb{K} \end{array} \qquad 1 \leq j \leq n,\ 1 \leq i \leq m,$$

Sia ora $\gamma \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$. Da $\gamma_{|\mathbb{K}} = \mathrm{id}_{|\mathbb{K}}$ si ha che $\gamma(\alpha)$ è una radice α_i di $\min_{\mathbb{K},\alpha}(x)$. Ne segue $(\Psi_i)^{-1}\,\gamma(\alpha) = \alpha$, ossia $(\Psi_i)^{-1}\,\gamma \in \mathrm{Gal}_{\mathbb{K}}\,\mathbb{K}(\alpha)$. Posto $(\Psi_i)^{-1}\,\gamma = \varphi_j$ si conclude $\gamma = \Psi_i\varphi_j$. ■

3 Il Teorema fondamentale della Teoria di Galois

Dato un campo Σ, fissiamo un suo sottocampo $\mathbb{K}$. Indichiamo con

• $\mathcal{L}$ l'insieme dei sottogruppi di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$;

• $\mathcal{S}$ l'insieme dei sottocampi di Σ che contengono $\mathbb{K}$.

Possiamo considerare l' applicazione

$$\Phi : \mathcal{L} \to \mathcal{S} \quad \text{con} \quad \Phi(G) = \Sigma_G \tag{3.1}$$

Φ assegna ad ogni sottogruppo G di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$ il sottocampo Σ_G degli elementi fissati. D'altra parte possiamo anche considerare l' applicazione

$$\Psi : \mathcal{S} \to \mathcal{L} \quad \text{con} \quad \Psi(\mathbb{F}) = \mathrm{Gal}_{\mathbb{F}}(\Sigma). \tag{3.2}$$

Ψ assegna ad ogni campo intermedio $\mathbb{F}$, ossia tale che $\mathbb{K} \leq \mathbb{F} \leq \Sigma$, il gruppo di Galois $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$ di Σ su $\mathbb{F}$.

Gli insiemi $\mathcal{L}$ e $\mathcal{S}$ sono parzialmente ordinati rispetto all'inclusione. Notiamo che ciascuna delle precedenti applicazioni inverte l'ordinamento, nel senso precisato dal seguente

(3.3) Lemma *Siano $G_1, G_2 \in \mathcal{L}$ e $\mathbb{F}_1, \mathbb{F}_2 \in \mathcal{S}$. Allora:*

1) $G_1 \leq G_2$ *implica* $\Phi(G_2) \leq \Phi(G_1)$;

2) $\mathbb{K}_1 \leq \mathbb{K}_2$ *implica* $\Psi(K_2) \leq \Psi(\mathbb{K}_1)$.

Dimostrazione.
1) Sia $\alpha \in \Phi(G_2) = \Sigma_{G_2}$. Per definizione α è fissato da tutti gli elementi di G_2. A maggior ragione è fissato da tutti gli elementi di $G_1 \leq G_2$. Ne segue $\alpha \in \Sigma_{G_1} = \Phi(G_1)$.
2) Sia $g \in \Psi(K_2) = \mathrm{Gal}_{\mathbb{K}_2}(\Sigma)$. Per definizione g fissa tutti gli elementi di $\mathbb{K}_2$. A maggior ragione fissa tutti gli elementi di $\mathbb{K}_1 \leq \mathbb{K}_2$. Ne segue $g \in \mathrm{Gal}_{\mathbb{K}_1}(\Sigma) = \Psi(\mathbb{K}_1)$. ■

Sia $G \in \mathcal{L}$. Per definizione di Σ_G, tutti gli elementi di Σ_G sono fissati da G. Quindi G è un gruppo di automorfismi di Σ che fissa tutti gli elementi di Σ_G. Pertanto:

$$G \leq \mathrm{Gal}_{\Sigma_G}(\Sigma). \tag{3.4}$$

Sia $\mathbb{F} \in \mathcal{S}$. Per definizione, $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$ fissa tutti gli elementi di $\mathbb{F}$. Quindi $\mathbb{F}$ è contenuto nel sottocampo degli elementi fissati da $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$. Pertanto:

$$\mathbb{F} \leq \Sigma_{\mathrm{Gal}_{\mathbb{F}}(\Sigma)}. \tag{3.5}$$

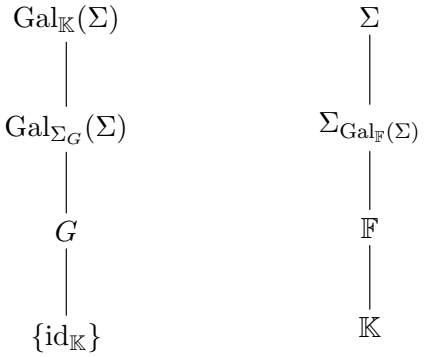
Tuttavia, sotto opportune ipotesi su Σ, in entrambi i casi vale l'uguaglianza anzichè la limitazione $\leq$, come conseguenza del seguente:

(3.6) Teorema *(fondamentale della teoria di Galois, I parte). Sia Σ il campo di spezzamento su $\mathbb{K}$ di un polinomio monico, separabile, $f(x) \in \mathbb{K}[x]$. Allora le applicazioni* (3.2) *ed* (3.1) *sono l'una l'inversa dell'altra. Equivalentemente:*

1) $G = \mathrm{Gal}_{\Sigma_G}(\Sigma)$, *per ogni sottogruppo G di* $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$*;*

2) $\mathbb{F} = \Sigma_{\mathrm{Gal}_{\mathbb{F}}(\Sigma)}$, *per ogni sottocampo $\mathbb{F}$ tale che $\mathbb{K} \leq \mathbb{F} \leq \Sigma$.*

Dimostrazione.
Tenendo presenti le relazioni (3.4) e (3.5) , si hanno le seguenti inclusioni:



1) $[\Sigma : \Sigma_G] = |\mathrm{Gal}_{\Sigma_G}(\Sigma)|$ per il Teorema 2.7. D'altra parte $[\Sigma : \Sigma_G] = |G|$ per il Teorema 1.7. Ne segue $|G| = |\mathrm{Gal}_{\Sigma_G}(\Sigma)|$ e si conclude $G = \mathrm{Gal}_{\Sigma_G}(\Sigma) = \Psi\Phi(G)$.
2) $[\Sigma : \Sigma_{\mathrm{Gal}_{\mathbb{F}}(\Sigma)}] = |\mathrm{Gal}_{\mathbb{F}}(\Sigma)|$ per il Teorema 1.7. D'altra parte $[\Sigma : \mathbb{F}] = |\mathrm{Gal}_{\mathbb{F}}(\Sigma)|$ per il Teorema 2.7. Si conclude $\mathbb{F} = \Sigma_{\mathrm{Gal}_{\mathbb{F}}(\Sigma)} = \Phi\Psi(\mathbb{F})$. ■

Sia H un sottogruppo di un gruppo G. Per ogni $g \in G$ l'insieme

$$g^{-1}Hg := \left\{g^{-1}hg \mid h \in H\right\}$$

è un sottogruppo. Inoltre, l'applicazione $\gamma : H \to g^{-1}Hg$ tale che

$$h \mapsto g^{-1}hg, \ \forall\ h \in H$$

è un isomorfismo. In particolare γ è bijettiva, da cui $|H| = \left|g^{-1}Hg\right|$.
Ricordiamo che H è *normale* in G se

$$gHg^{-1} = H, \ \forall\ g \in G.$$

(3.7) Lemma *Sia Σ il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile $f(x) \in \mathbb{K}[x]$ e sia $\mathbb{F}$ un campo intermedio, ossia: $\mathbb{K} \leq \mathbb{F} \leq \Sigma$. Per ogni $\gamma \in \mathrm{Gal}_{\mathbb{F}}(\Sigma)$, detto $\gamma(\mathbb{F})$ il sottocampo di Σ immagine di $\mathbb{F}$ mediante γ, si ha:*

$$\gamma \,\mathrm{Gal}_{\mathbb{F}}(\Sigma)\gamma^{-1} = \mathrm{Gal}_{\gamma(\mathbb{F})}(\Sigma).$$

Ne segue che

$$\gamma(\mathbb{F}) = \mathbb{F}, \quad \forall\ \gamma \in \mathrm{Gal}_{\mathbb{F}}(\Sigma)$$

se e solo se $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$ è un sottogruppo normale di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$.

Dimostrazione. Siano $\varphi \in \mathrm{Gal}_{\mathbb{F}}(\Sigma)$, $\alpha \in \mathbb{F}$. Da $\gamma\varphi\gamma^{-1}\ (\gamma(\alpha)) = \gamma\varphi(\alpha) = \gamma(\alpha)$
si ottiene l'inclusione

$$\gamma \,\mathrm{Gal}_{\mathbb{F}}(\Sigma)\gamma^{-1} \leq \mathrm{Gal}_{\gamma(\mathbb{F})}(\Sigma). \tag{3.8}$$

Ora i gruppi $\gamma \,\mathrm{Gal}_{\mathbb{F}}(\Sigma)\gamma^{-1}$ e $\mathrm{Gal}_{\gamma(\mathbb{F})}(\Sigma)$ hanno lo stesso ordine. Infatti:

$$\left|\gamma \,\mathrm{Gal}_{\mathbb{F}}(\Sigma)\gamma^{-1}\right| = \left|\mathrm{Gal}_{\mathbb{F}}\,\Sigma\right| = [\Sigma : \mathbb{F}] = [\gamma(\Sigma) : \gamma(\mathbb{F})] = [\Sigma : \gamma(\mathbb{F})] = \left|\mathrm{Gal}_{\gamma(\mathbb{F})}\,\Sigma\right|.$$

Si conclude che coincidono. ■

(3.9) Teorema *(fondamentale della teoria di Galois, II parte). Sia Σ il campo di spezzamento su $\mathbb{K}$ di un polinomio separabile di $\mathbb{K}[x]$ e sia $\mathbb{K} \leq \mathbb{F} \leq \Sigma$. Allora $\mathbb{F}$ è estensione normale di $\mathbb{K}$ se e solo se $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$ è un sottogruppo normale di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$.*
In tal caso

$$\mathrm{Gal}_{\mathbb{K}}(\mathbb{F}) \simeq \frac{\mathrm{Gal}_{\mathbb{K}}(\Sigma)}{\mathrm{Gal}_{\mathbb{F}}(\Sigma)}.$$

Dimostrazione. Supponiamo che $\mathrm{Gal}_{\mathbb{F}}(\Sigma)$ sia un sottogruppo normale di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$. Sia $m(x)$ un polinomio irriducibile di $\mathbb{K}[x]$ che ha una radice $\alpha \in \mathbb{F}$. Per il Teorema 5.2 del Capitolo II, $m(x)$ ha tutte le sue radici in Σ. Verifichiamo che, in realtá, le ha tutte in $\mathbb{F}$. A tale scopo sia β una radice di $m(x)$. Da $\beta \in \Sigma$ segue $\mathbb{K}(\beta) \leq \Sigma$. Inoltre esiste un isomorfismo

$$\varphi : \mathbb{K}(\alpha) \to \mathbb{K}(\beta)$$

tale che $\varphi_{\mathbb{K}} = \mathrm{id}$ e $\varphi(\alpha) = \beta$. Detta $\widehat{\varphi} : \Sigma \to \Sigma$ una estensione di φ a Σ, si ha $\widehat{\varphi} \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$. Per il Lemma precedente:

$$\mathrm{Gal}_{\widehat{\varphi}(\mathbb{F})}(\Sigma) = \widehat{\varphi}\,\mathrm{Gal}_{\mathbb{F}}(\Sigma)\widehat{\varphi}^{-1} = \mathrm{Gal}_{\mathbb{F}}(\Sigma)$$

e, dal Teorema fondamentale della teoria di Galois segue:

$$\widehat{\varphi}(\mathbb{F}) = \Sigma_{\mathrm{Gal}_{\widehat{\varphi}(\mathbb{F})}(\Sigma)} = \Sigma_{\mathrm{Gal}_{\mathbb{F}}(\Sigma)} = \mathbb{F}.$$

Pertanto $\beta = \varphi(\alpha) \in \mathbb{F}$. Concludiamo che $\mathbb{F}$ è estensione normale di $\mathbb{K}$.

Viceversa, $\mathbb{F}$ sia estensione normale di $\mathbb{K}$. Σ ha grado finito su $\mathbb{K}$, essendo campo di spezzamento di un polinomio. A maggior ragione $\mathbb{F}$ ha grado finito su $\mathbb{K}$. Dal Corollario 5.3 del Capitolo 2 segue che $\mathbb{F}$ è campo di spezzamento di un polinomio $g(x) \in \mathbb{K}[x]$. Ogni $\gamma \in \mathrm{Gal}_{\mathbb{K}}(\Sigma)$ fissa i coefficienti di $g(x)$, quindi ne permuta le radici. Ne segue $\gamma(\mathbb{F}) = \mathbb{F}$, ossia la restrizione $\gamma_{|\mathbb{F}}$ di γ al sottocampo $\mathbb{F}$ è un automorfismo di $\mathbb{F}$. Poichè γ fissa tutti gli elementi di $\mathbb{K}$, si ha $\gamma_{|\mathbb{F}} \in \mathrm{Gal}_{\mathbb{K}}(\mathbb{F})$. L'applicazione

$$\rho : \mathrm{Gal}_{\mathbb{K}}(\Sigma) \to \mathrm{Gal}_{\mathbb{K}}(\mathbb{F})$$

tale che $\rho(\gamma) = \gamma_{|\mathbb{F}}$ è un omomorfismo di gruppi. Si ha $\theta \in \mathrm{Ker}\ \rho$ se e solo se $\theta_{\mathbb{F}} = \mathrm{id}_{|\mathbb{F}}$, se e solo se $\theta \in \mathrm{Gal}_{\mathbb{F}}(\Sigma)$. Abbiamo così dimostrato che $\mathrm{Gal}_{\mathbb{F}}(\Sigma) = \mathrm{Ker}\ \theta$ è un sottogruppo normale di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$.
Infine notiamo che ρ è suriettivo. Infatti, per il punto 2) del Teorema 3.5 del Capitolo II, ogni automorfismo di $\mathbb{F}$, che fissi gli elementi di $\mathbb{K}$, può essere esteso a un elemento di $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$. Per il Teorema fondamentale degli omomorfismi fra gruppi si conclude

$$\frac{\mathrm{Gal}_{\mathbb{K}}(\Sigma)}{\mathrm{Ker}\ \rho} \sim \mathrm{Im}\ \rho, \quad \text{ossia} \quad \frac{\mathrm{Gal}_{\mathbb{K}}(\Sigma)}{\mathrm{Gal}_{\mathbb{F}}(\Sigma)} \simeq \mathrm{Gal}_{\mathbb{K}}(\mathbb{F}).$$

■

4 Alcuni esempi

(4.1) Esempio $\mathbb{C} = \mathbb{R}(i) =$ *è il campo di spezzamento di* $x^2 + 1 = (x + i)(x - i)$ *su* $\mathbb{R}$. *Si ha* $[\mathbb{C} : \mathbb{R}] = 2$ *e* $\mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) \simeq \mathrm{Sym}\,(\{i, -i\}) =< (i, -i) >$.

$$\begin{array}{cc} \mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) & \mathbb{C} \\ {\scriptstyle 2}\big| & \big|{\scriptstyle 2} \\ \{\mathrm{id}_{\mathbb{C}}\} & \mathbb{R} \end{array}$$

I due elementi di $\mathrm{Gal}_{\mathbb{R}}(\mathbb{C})$ *agiscono nel modo seguente:*

$$\begin{aligned} \mathrm{id} : &\quad a + bi \mapsto a + bi \\ (i, -i) : &\quad a + bi \mapsto a - bi. \end{aligned}$$

La corrispondenza di Galois è la seguente:

$$\mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) \xrightarrow{\Phi} \mathbb{R} \xrightarrow{\Psi} \mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) \qquad \mathbb{C} \xrightarrow{\Psi} \{\mathrm{id}\} \xrightarrow{\Phi} \mathbb{C}$$

$$\{id_{\mathbb{C}}\} \xrightarrow{\Phi} \mathbb{C} \xrightarrow{\Psi} \{id_{\mathbb{C}}\} \qquad \mathbb{R} \xrightarrow{\Psi} \mathrm{Gal}_{\mathbb{R}}(\mathbb{C}) \xrightarrow{\Phi} \mathbb{R}$$

(4.2) Esempio *Sia $p > 0$ un numero primo. In $\mathbb{Q}[x]$ consideriamo il polinomio*

$$f(x) = x^4 - p^2 = (x^2 - p)(x^2 + p).$$

Le radici di $f(x)$ sono $\pm\sqrt{p}$, $\pm i\sqrt{p}$. Quindi il campo di spezzamento Σ di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\sqrt{p}, i)$. Ne segue $[\Sigma : \mathbb{Q}] = 2 \cdot 2 = 4$. Infatti:

$$\begin{array}{c} \mathbb{Q}(\sqrt{p}, i) \not\leq \mathbb{R} \\ \Big| 2 \\ \mathbb{Q}(\sqrt{p}) \leq \mathbb{R} \\ \Big| 2 \\ \mathbb{Q} \end{array}$$

Pertanto anche $|\mathrm{Gal}_{\mathbb{Q}}(\Sigma)| = 4$. Determiniamo gli elementi $\mathrm{Gal}_{\mathbb{Q}}(\Sigma)$, rappresentandoli come permutazioni sulle radici di $f(x)$. Seguiamo la dimostrazione del Teorema 2.7. Notando che Σ è il campo di spezzamento di $x^2 + p$ su $\mathbb{Q}(\sqrt{p})$, si ha

$$\{\mathrm{id},\ (i\sqrt{p}, -i\sqrt{p})\} = \mathrm{Gal}_{\mathbb{Q}(\sqrt{p})}(\Sigma) \leq \mathrm{Gal}_{\mathbb{Q}}(\Sigma).$$

Inoltre $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}\left(\sqrt{p}\right) = \left\{\mathrm{id},\ \left(\sqrt{p}, -\sqrt{p}\right)\right\}$. Ciascuno di tali automorfismi si estende a un elemento di $\mathrm{Gal}_{\mathbb{Q}}(\Sigma)$ che fissa $i\sqrt{p}$ per il punto (2) del Corollario 2.11 del Capitolo II. Pertanto

$$\{\mathrm{id},\ (\sqrt{p}, -\sqrt{p})\} \leq \mathrm{Gal}_{\mathbb{Q}}(\Sigma).$$

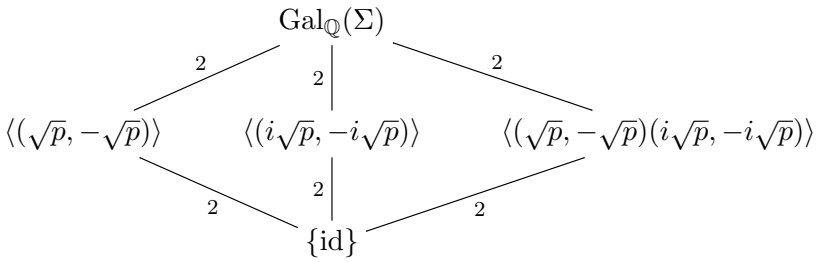
Concludiamo che

$$\mathrm{Gal}_{\mathbb{Q}}(\Sigma) = \{\mathrm{id},\ (\sqrt{p}, -\sqrt{p}),\ (i\sqrt{p}, -i\sqrt{p}),\ (\sqrt{p}, -\sqrt{p})(i\sqrt{p}, -i\sqrt{p})\}.$$

Vogliamo infine vedere gli elementi di $\mathrm{Gal}_{\mathbb{Q}}(\Sigma)$ come automorfismi di Σ come spazio vettoriale su $\mathbb{Q}$. Rispetto alla base $\mathcal{B} = \left\{1,\ \sqrt{p},\ i,\ i\sqrt{p}\right\}$ si ha:

$$\begin{array}{lcl} q_0 + q_1\sqrt{p} + q_2 i + q_3 i\sqrt{p} & \xrightarrow{\mathrm{id}} & q_0 + q_1\sqrt{p} + q_2 i + q_3 i\sqrt{p} \\ q_0 + q_1\sqrt{p} + q_2 i + q_3 i\sqrt{p} & \xrightarrow{(\sqrt{p}, -\sqrt{p})} & q_0 - q_1\sqrt{p} + q_2 i - q_3 i\sqrt{p} \\ q_0 + q_1\sqrt{p} + q_2 i + q_3 i\sqrt{p} & \xrightarrow{(i\sqrt{p}, -i\sqrt{p})} & q_0 + q_1\sqrt{p} - q_2 i - q_3 i\sqrt{p} \\ q_0 + q_1\sqrt{p} + q_2 i + q_3 i\sqrt{p} & \xrightarrow{(\sqrt{p}, -\sqrt{p})(i\sqrt{p}, -i\sqrt{p})} & q_0 - q_1\sqrt{p} - q_2 i + q_3 i\sqrt{p} \end{array} \tag{4.3}$$

Rappresentiamo infine il reticolo dei sottogruppi di $\mathrm{Gal}_{\mathbb{Q}}(\Sigma)$ *e vediamo come opera la corrispondenza di Galois.*



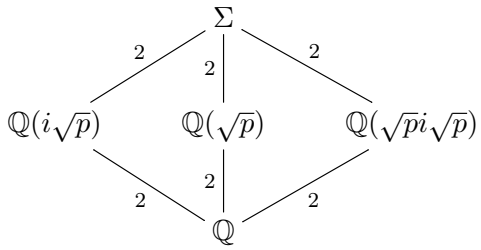
$i\sqrt{p}$ *è fissato dal sottogruppo* $H = \langle(\sqrt{p}, -\sqrt{p})\rangle$. *Quindi*

$$\mathbb{Q}(i\sqrt{p}) \leq \Sigma_H.$$

Essendo $2 = |H| = [\Sigma : \Sigma_H]$ *si ha* $[\Sigma_H : Q] = 2 = \big[\mathbb{Q}(i\sqrt{p}) : \mathbb{Q}\big]$. *Quindi:*

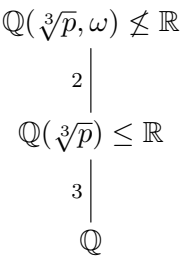
$$\mathbb{Q}(i\sqrt{p}) = \Sigma_H.$$

Ragionando in modo analogo sugli altri sottogruppi si ha il reticolo dei sottocampi di Σ*:*

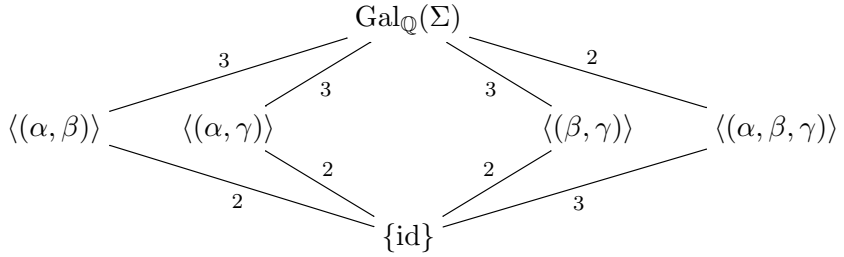


Il gruppo $\mathrm{Gal}_{\mathbb{Q}}(\Sigma)$ *è abeliano, quindi tutti i suoi sottogruppi sono normali. Ne segue che tutti i sottocampi di* Σ *sono estensioni normali di* $\mathbb{Q}$.

(4.4) Esempio *Sia* $p > 0$ *un numero primo. In* $\mathbb{Q}[x]$ *consideriamo* $f(x) = x^3 - p$.
Le radici di $f(x)$ *sono* $\alpha = \sqrt[3]{p}$, $\beta = \omega\sqrt[3]{p}$, $\gamma = \omega^2\sqrt[3]{p}$ *dove* ω *è una radice primitiva cubica di* 1, *ossia una radice di* $x^2 + x + 1$. *Quindi il campo di spezzamento* Σ *di* $f(x)$ *su* $\mathbb{Q}$ *è* $\mathbb{Q}(\sqrt[3]{p}, \omega)$. *Ne segue* $[\Sigma : \mathbb{Q}] = 3 \cdot 2 = 6$. *Infatti:*



Pertanto anche $|\mathrm{Gal}_{\mathbb{Q}}(\Sigma)| = 6$. *Concludiamo che* $\mathrm{Gal}_{\mathbb{Q}}(\Sigma) = \mathrm{Sym}(\{\alpha, \beta, \gamma\})$.
Il reticolo dei suoi sottogruppi è :



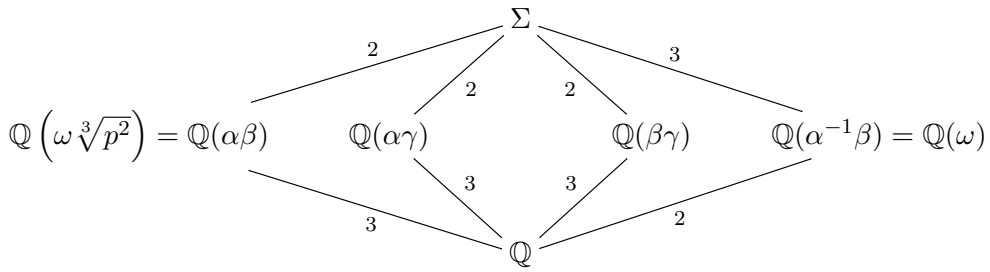
$\alpha\beta = \omega\sqrt[3]{p^2}$ *è fissato dal sottogruppo* $H = \langle(\alpha, \beta)\rangle$. *Quindi*

$$\mathbb{Q}(\omega\sqrt[3]{p^2}) \leq \Sigma_H.$$

Essendo $2 = |H| = [\Sigma : \Sigma_H]$ *si ha* $[\Sigma_H : Q] = 3 = \left[\mathbb{Q}\left(\omega\sqrt[3]{p^2}\right) : \mathbb{Q}\right]$. *Quindi:*

$$\mathbb{Q}\left(\omega\sqrt[3]{p^2}\right) = \Sigma_H.$$

Ragionando in modo analogo sugli altri sottogruppi si ha il reticolo dei sottocampi di Σ*:*



Poichè il sottogruppo $\langle(\alpha, \beta)\rangle$ *non è normale in* $\mathrm{Sym}(\{\alpha, \beta, \gamma\})$, *il suo campo fisso* $\mathbb{Q}\left(\omega\sqrt[3]{p^2}\right)$ *non è estensione normale di* $\mathbb{Q}$.
Poichè il sottogruppo $\langle(\alpha, \beta, \gamma)\rangle$ *è normale in* $\mathrm{Sym}(\{\alpha, \beta, \gamma\})$, *il suo campo fisso* $\mathbb{Q}(\omega)$ *è estensione normale di* $\mathbb{Q}$.

(4.5) Esempio *Se* Σ *è un campo finito di ordine* p^n, *con* p *primo, ogni suo sottocampo* $\mathbb{F}$ *è estensione normale del sottocampo minimo* $\mathbb{F}_p$. *Infatti* $\mathbb{F}$ *è il campo di spezzamento di* $x^{|\mathbb{F}|} - x$ *su* $\mathbb{F}_p$. *Ciò è in accordo con il Teorema fondamentale della teoria di Galois: infatti ogni sottocampo è il campo fisso di un sottogruppo di* $\mathrm{Gal}_{\mathbb{K}}(\Sigma)$. *Questo gruppo è ciclico, quindi abeliano. Ne segue che tutti i suoi sottogruppi sono normali.*

Capitolo IV

Campi finiti e polinomi ciclotomici

1 Esistenza e unicità del campo di ordine $q = p^n$

Sappiamo che, per ogni numero primo p, l'anello $\frac{\mathbb{Z}}{p\mathbb{Z}}$ delle classi di resti modulo p è un campo finito, di ordine p. Lo indicheremo con $\mathbb{F}_p$.

(1.1) Lemma *Sia $\mathbb{F}$ un campo finito, di ordine q. Allora $q = p^n$ per qualche numero primo p e intero $n \geq 1$.*

Dimostrazione. Per il Lemma 4.2 del capitolo I il sottocampo minimo di $\mathbb{F}$ è isomorfo a $\mathbb{F}_p$, dove $p = \text{char } \mathbb{F}$ è un primo. Considerando $\mathbb{F}$ come spazio vettoriale su $\mathbb{F}_p$ e detta n la sua dimensione (necessariamente finita), si ha $q = p^n$. ■

(1.2) Teorema *Un campo finito $\mathbb{F}$ ha ordine $q = p^n$ se e solo se è il campo di spezzamento di $x^q - x$ su $\mathbb{F}_p$. In particolare, per ogni primo p e ogni intero positivo n, esiste un campo di ordine p^n. Inoltre due campi finiti dello stesso ordine sono isomorfi.*

Dimostrazione.
Per il Teorema 3.5 del Capitolo II, esiste un campo di spezzamento Σ del polinomio $x^q - x \in \mathbb{F}_p[x]$. Per il corollario 5.7 del Capitolo II il polinomio $x^q - x$ ha q radici distinte in $\mathbb{F}_q$. Verifichiamo che l'insieme H di tali radici è un sottocampo di Σ. Siano infatti α e β radici di $x^q - x$. Per q dispari, anche $-\alpha$ è radice di $x^q - x$. Infatti, da $\alpha^q = \alpha$ segue $-\alpha^q = -\alpha$, da cui $(-\alpha)^q = -\alpha$. Anche $\alpha + \beta$ è radice di $x^q - x$. Infatti, per le proprietà del monomorfismo di Frobenius, si ha:

$$(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta.$$

Infine, se $\beta \neq 0$, anche $\alpha\beta^{-1}$ è radice di $x^q - x$. Infatti:

$$\left(\alpha\beta^{-1}\right)^q = \alpha^q \left(\beta^{-1}\right)^q = \alpha \left(\beta^q\right)^{-1} = \alpha\beta^{-1}.$$

Abbiamo così dimostrato che le q radici di $x^q - x$ formano un sottocampo H di Σ. Per definizione di campo di spezzamento si ha $H = \Sigma$. Si conclude che Σ ha ordine q.

Viceversa sia $\mathbb{K}$ un campo di ordine q. Ne segue che il gruppo moltiplicativo $\mathbb{K}^*$ degli elementi non nulli di $\mathbb{K}$ ha ordine $q-1$. Per il Teorema di Lagrange ogni elemento α di $\mathbb{K}^*$ ha periodo che divide $q-1$. Ne segue $\alpha^{q-1} = 1$, da cui $\alpha^q = \alpha$. Poichè anche $0^q = 0$, si ha che $\mathbb{K}$ è l'insieme delle radici di $x^q - x$, cioè il suo campo di spezzamento.

Poichè due campi di spezzamento dello stesso polinomio sono isomorfi (Teorema 3.5, Capitolo II), concludiamo che due campi di ordine q sono isomorfi. ■

Per approfondire le proprietà dei campi finiti ci occorre il risultato sui gruppi abeliani finiti espresso dal Corollario 1.5. Esso necessita alcuni richiami.

(1.3) Lemma *Siano x, y due elementi di un gruppo G tali che $xy = yx$. Supponimo che x e y abbiano rispettivi periodi m, n finiti e chiamiamo t il periodo di xy.*

(1) *Se $\langle x\rangle \cap \langle y\rangle = \{1\}$, allora $t = \text{m.c.m.}(m,n)$;*

(2) *se m, n sono coprimi, ossia se $\text{M.C.D.}(m,n) = 1$, allora $t = mn$.*

Dimostrazione.
(1) Poniamo $\text{m.c.m.}(m,n) = mm_1 = nn_1$ con $m_1, n_1 \in \mathbb{N}$. Da $(xy)^{\text{m.c.m.}(m,n)} = (x^m)^{m_1}(y^n)^{n_1} = 1 \cdot 1 = 1$ segue che t divide $\text{m.c.m.}(m,n)$. D'altra parte $(xy)^t = 1$ implica $x^t = y^{-t} \in \langle x\rangle \cap \langle y\rangle = \{1\}$. Da $x^t = 1$ si deduce che m divide t. Analogamente da $y^t = 1$ si deduce che n divide t. Pertanto $\text{m.c.m.}(m,n)$ divide t. Concludiamo $t = \text{m.c.m.}(m,n)$.

(2) Si ha $\langle x\rangle = m$, $\langle y\rangle = n$. Se m, n sono coprimi, dal Teorema di Lagrange segue $\langle x\rangle \cap \langle y\rangle = \{1\}$. Quindi xy ha periodo $\text{m.c.m.}(m,n) = mn$, per il punto (1). ■

(1.4) Definizione *Se G è un gruppo finito, si dice* esponente *di G il minimo comune multiplo dei periodi dei suoi elementi.*

(1.5) Corollario *Sia A un gruppo abeliano finito di esponente e. Esiste in A un elemento a di periodo e.*

Dimostrazione. Possiamo supporre $A \neq \{1\}$, quindi $e = p_1^{s_1} \cdots p_t^{s_t}$, $t \geq 1$, dove i p_i sono numeri primi, a due a due distinti se $t > 1$. Esistono in A elementi $x_1, \ldots, x_t$ di rispettivi periodi $m_1 p_1^{s_1}, \cdots, m_t p_t^{s_t}$, per opportuni $m_i \in \mathbb{N}$. Gli elementi $y_i = x_i^{m_i}$ hanno periodi $p_i^{s_i}$, $1 \leq i \leq t$, a due a due coprimi. Usando ripetutamente il punto (2) del precedente Lemma si ha che $a = \prod_{i=1}^{t} y_i$ ha periodo e. ■

Il precedente risultato si deduce anche dal Teorema di struttura di A. Tale Teorema, visto (in notazione additiva) nel corso di Approfondimenti di Algebra, afferma che esiste (ed è unica) una sequenza di interi positivi $d_1, \ldots, d_t$, ciascuno dei quali divide il successivo, tale che A è prodotto diretto di t gruppi ciclici C_{d_i} di rispettivi ordini d_i. In simboli:

$$A \simeq C_{d_1} \times \cdots \times C_{d_t}, \quad d_i \text{ divide } d_{i+1}, \quad 1 \leq i \leq t-1.$$

Notiamo che un generatore di C_{d_t} è un elemento di A di periodo d_t. Quindi d_t divide l'esponente di A. D'altra parte, siccome ogni d_i divide d_t, si ha:

$$a^{d_t} = 1, \quad \forall\ a \in A. \tag{1.6}$$

Ne segue che il periodo di ogni a divide d_t, ossia che d_t è l'esponente di A è d_t.

(1.7) Teorema *Siano $\mathbb{K}$ un campo e A un sottogruppo finito del gruppo moltiplicativo $\mathbb{K}^*$. Allora A è ciclico. In particolare il gruppo moltiplicativo di un campo finito è ciclico.*

Dimostrazione. Sia e l'esponente del gruppo abeliano finito A. Nelle notazioni del Corollario 1.5 si ha che $< a > \leq A$ ha ordine e. Ne segue $e \leq |A|$. D'altra parte, per definizione di esponente, ogni elemento di A è radice del polinomio $x^e - 1$. Ne segue $e \geq |A|$, da cui $e = |A|$. Si conclude che $A = \langle a \rangle >$ è ciclico. ■

(1.8) Corollario *Per ogni primo p e per ogni n esiste un polinomio irrudicibile di grado n in $\mathbb{F}_p[x]$.*

Dimostrazione.
Poniamo $q = p^n$. Per il Teorema precedente il gruppo moltiplicativo ${\mathbb{F}_q}^*$ è ciclico. Esiste quindi $\alpha \in {\mathbb{F}_q}^*$ tale che

$${\mathbb{F}_q}^* = \left\{\alpha^0, \alpha, \ldots, \alpha^{q-1}\right\}.$$

Ne segue $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Da $[\mathbb{F}_q : \mathbb{F}_p] = n$ segue che α è algebrico su $\mathbb{F}_p$ e che il polinomio minimo $\min_{\alpha,\mathbb{F}_p}(x)$ ha grado n. Siccome $\min_{\alpha,\mathbb{F}_p}(x)$ è irriducibile, si conclude l'asserto. ■

Il precedente Corollario deduce l'esistenza di un polinomio irrudicibile di grado n in $\mathbb{F}_p[x]$ da quella del campo finito di ordine p^n. Viceversa è possibile, come fa L.Dickson in [2], contare i polinomi, dimostrando che per ogni primo p e per ogni n esiste un polinomio irrudicibile $f(x)$ di grado n in $\mathbb{F}_p[x]$. Da qui si deduce facilmente l'esistenza di un campo di ordine $q = p^n$. Si veda il successivo Teorema 1.10.

(1.9) Teorema *Sia $q = p^n$. Il gruppo degli automorfismi di $\mathbb{F}_q$ è ciclico di ordine n. Un suo generatore è l'automorfismo di Frobenius $\sigma : \alpha \mapsto \alpha^p$.*

Dimostrazione.
$\mathbb{F}_q$ è il campo di spezzamento di $x^q - x$ su $\mathbb{F}_p$. Essendo $x^q - x$ separabile, il gruppo di Galois $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$ ha ordine $n = [\mathbb{F}_q : \mathbb{F}_p]$. Notando che ogni automorfismo di $\mathbb{F}_q$ fissa tutti gli elementi del sottocampo minimo $\mathbb{F}_p$, si ha $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$ e si conclude che $\mathrm{Aut}(\mathbb{F}_q)$ ha ordine n.
Le potenze di σ agiscono nel modo seguente

$$\sigma^r(\alpha) = \alpha^{p^r}.$$

Ne segue $\sigma^n = \mathrm{id}$ per il Teorema di lagrange (o anche poichè $\alpha^{p^n} = \alpha$ per ogni $\alpha \in \mathbb{F}_q$). Supponiamo ora che, per qualche esponente intero positivo m, con $1 \leq m < n$, si abbia $\sigma^m = \mathrm{id}$. Avremmo allora

$$\alpha^{p^m} = \alpha$$

per ogni $\alpha \in \mathbb{F}_q$ e quindi

$$\alpha^{p^m - 1} = 1$$

per ogni α non nullo. Ma $\mathbb{F}_q^*$ è ciclico. Detto β un suo generatore, esso ha periodo $q - 1 = p^n - 1 > p^m - 1$, contraddizione. Si conclude che σ ha periodo n e genera quindi il gruppo degli automorfismi di $\mathbb{F}_q$. ■

Come sappiamo, per ottenere un campo finito di ordine $q = p^n$, si può costruire l'anello quoziente $\frac{\mathbb{F}_p[x]}{\langle f(x)\rangle}$ con $f(x) \in \mathbb{F}_p[x]$ irriducibile di grado n. Si veda l'esempio 3.4 del Capitolo I.

(1.10) Teorema *Siano p un primo, $m(x) \in \mathbb{F}_p[x]$ un polinomio monico irriducibile di grado n. Al solito $\langle m(x)\rangle$ indichi l'ideale generato da $m(x)$. L'anello quoziente*

$$\mathbb{L} := \frac{\mathbb{F}_p[x]}{\langle m(x)\rangle}$$

è un campo di ordine $q = p^n$. Il polinomio $m(x)$ divide $x^q - x$ e le radici di $m(x)$ sono

$$\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$$

dove α è una di esse. In particolare $\mathbb{L}$ è campo di spezzamento di $m(x)$ su $\mathbb{F}_p$.

Dimostrazione.
Tramite l'isomorfismo $\iota : \mathbb{F}_p \to \mathbb{L}$ definito da $k \mapsto \langle m(x)\rangle + kx^0$ possiamo identificare $\mathbb{F}_p$ con il sottocampo $\iota(\mathbb{F}_p)$ di $\mathbb{L}$ e, di conseguenza, considerare $m(x)$ come polinomio di $\mathbb{L}[x]$. Per il Lemma 3.1 del Capitolo II, si ha $\mathbb{L} = \mathbb{F}_p(\alpha)$, dove $\alpha := \langle m(x)\rangle + x$ è una radice di $m(x)$. Il polinomio minimo di α su $\mathbb{F}_p$ è $m(x)$, essendo irriducibile. Quindi, avendo $m(x)$ grado n, si ottiene $|\mathbb{L}| = p^n = q$. Dal Teorema 1.2 di questo Capitolo segue che $\mathbb{L}$ è campo di spezzamento di $x^q - x$ su $\mathbb{F}_p$, ossia i suoi elementi sono tutte e sole le radici di $x^q - x$. In particolare $\min_{\mathbb{F}_p,\alpha}(x) = m(x)$ divide $x^q - x$.
Consideriamo l'automorfismo di Frobenius σ di $\mathbb{L}$. Poichè σ e le sue potenze appartengono a $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{L})$ si ha che ciascuno degli elementi

$$\sigma^r(\alpha) = \alpha^{p^r}, \quad 0 \le r \le n-1 \tag{1.11}$$

è radice di $m(x)$. Poichè σ ha periodo n, le sue potenze

$$\sigma^r, \quad 0 \le r \le n-1$$

sono a due a due distinte. Ricordando che $\mathbb{L} = \mathbb{F}_p(\alpha)$ si deduce che le radici in (1.11) sono elementi di $\mathbb{L}$ a due a due distinti, quindi le n radici di $m(x)$. Infine, in $\mathbb{L}[x]$

$$m(x) = \prod_{r=0}^{n-1} \left(x - \alpha^{p^r}\right),$$

ossia $\mathbb{L}$ è campo di spezzamento di $m(x)$ su $\mathbb{F}_p$. ■

Notiamo, in particolare, che polinomi irriducibili distinti di $\mathbb{F}_p[x]$, dello spesso grado, danno luogo a campi isomorfi.

2 Polinomi ciclotomici

Fissato un intero $m \geq 1$, consideriamo il polinomio

$$x^m - 1 \tag{2.1}$$

a coefficienti in un campo $\mathbb{K}$ di caratteristica 0 oppure un primo p che non divide m.

Posto $f(x) = x^m - 1$ si ha $f'(x) = mx^{m-1}$. In virtù dell'ipotesi fatta sulla caratteristica di $\mathbb{K}$, si ottiene $\text{MCD}(f(x), f'(x)) = 1$, cosicchè $f(x)$ ha m radici distinte in un suo campo di spezzamento Σ.
Le radici di (2.1) in Σ costituiscono un sottogruppo moltiplicativo A di Σ^*, come si può facilmente verificare. Per il Teorema 1.7 di questo Capitolo, A è ciclico.

(2.2) Definizione *Si chiama radice primitiva m-esima dell'unità $1_{\mathbb{K}}$ di $\mathbb{K}$ un qualunque generatore ϵ del gruppo A, ossia una qualunque radice ϵ di* (2.1) *il cui periodo moltiplicativo sia m.*

Quindi, per definizione, le m radici di $x^m - 1$ sono le potenze di ϵ, ossia:

$$A = \left\{\epsilon^0, \epsilon, \cdots, \epsilon^{m-1}\right\}. \tag{2.3}$$

(2.4) Esempio *Se $\mathbb{K} = \mathbb{C}$, una radice primitiva m-esima di 1 è $\epsilon = e^{\frac{2\pi}{m}i}$.*
Le m radici di $x^m - 1$ in $\mathbb{C}$ sono

$$A = \left\{e^{\frac{2k\pi}{m}i} \mid \quad 0 \leq k \leq m-1\right\}.$$

Sia ϵ una radice primitiva m-esima dell'unità. Per il Lemma 1.28 del Capitolo I una sua potenza ϵ^k ha periodo m, ossia è a sua volta radice primitiva m-esima dell'unitá, se e solo se $\text{MCD}(k, m) = 1$.

(2.5) Esempi *Sia $\mathbb{K} = \mathbb{C}$.*

- *Per $m = 2$, l'unica radice primitiva seconda (quadrata) di 1 è $\epsilon = -1$.*
- *Per $m = 3$, le radici primitive terze di 1 sono*

$$\epsilon := e^{\frac{2\pi}{3}i},\ \epsilon^2 = e^{\frac{4\pi}{3}i}.$$

- *Per $m = 6$ le radici primitive terze di 1 sono*

$$\epsilon := e^{\frac{\pi}{3}i},\ \epsilon^5 = e^{\frac{5\pi}{3}i} = \epsilon^{-1}.$$

(2.6) Definizione *L'm-esimo polinomio ciclotomico* $\Phi_m(x)$ *di* $\mathbb{K}[x]$ *è così definito:*

$$\Phi_m(x) := \prod_{\substack{1 \le k < m \\ (k,m)=1}} (x - \epsilon^k) \tag{2.7}$$

dove il prodotto è esteso a tutte le radici primitive m-esime dell'unità $1_{\mathbb{K}}$ *di* $\mathbb{K}$*.*

Tenendo presente (2.3) si ha:

$$x^m - 1 = \prod_{0 \le j < m} (x - \epsilon^j). \tag{2.8}$$

Ogni radice ϵ^j, in quanto elemento del gruppo A di ordine m, ha periodo un divisore d di m. D'altra parte, per ogni divisore positivo d di m, esiste qualche radice di periodo d: ad esempio $\epsilon^{\frac{m}{d}}$. Pertanto, suddividendo le radici in base ai loro periodi, e associando tutti i fattori relativi a radici aventi lo stesso periodo d, la (2.8) diventa

$$x^m - 1 := \prod_{d|m} \Phi_d(x). \tag{2.9}$$

Per definizione i polinomi ciclotomici sono monici. In realtà si ha:

(2.10) Lemma *Per ogni* $m \ge 1$ *i coefficienti del polinomio ciclotomico* $\Phi_m(x)$ *appartengono al sottoanello* R *di* $\mathbb{K}$ *costituito dai multipli interi di* $1_{\mathbb{K}}$*. Chiaramente* $R \simeq \mathbb{Z}$ *se* $\mathbb{K}$ *ha caratteristica* 0*,* $R \simeq \mathbb{Z}_p$ *se* $\mathbb{K}$ *ha caratteristica* $p > 0$*.*

Dimostrazione. Induzione su m.
Per $m = 1$ si ha $\Phi_1(x) = x - 1$ e l'asserto è vero. Sia quindi $m > 1$.
Isolando il fattore $\Phi_m(x)$ e associando i rimanenti fattori, la (2.9) diventa:

$$x^m - 1 \;=\; \Phi_m(x)\, g(x), \quad g(x) := \prod_{\substack{d|m \\ d \ne m}} \Phi_d(x).$$

Per l'ipotesi induttiva, per ogni $d < m$ si ha $\Phi_d(x) \in R[x]$. Poichè $R[x]$ è chiuso rispetto al prodotto, anche $g(x) \in R[x]$. Ora $\Phi_m(x)$ è il quoziente della divisione di $x^m - 1$ per $g(x)$, che è monico. Considerando l'algoritmo della divisione, si vede subito che $\Phi_m(x)$ ha i coefficienti in R. ∎

Notiamo che il grado di $\Phi_m(x)$ è uguale al numero degli elementi dell'insieme

$$\{k \in \mathbb{N} \mid 1 \le k \le m,\ \mathrm{MCD}(k,m) = 1\}\,.$$

Tale numero si indica generalmente con $\varphi(m)$, dove $\varphi : \mathbb{N} \to \mathbb{N}$ è la funzione di Eulero. Per il calcolo di $\varphi(m)$ notiamo che:

• Se p è primo si ha ovviamente $\varphi(p) = p - 1$;

• se p^n è una potenza del primo p, allora $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$;

• se $m = ab$, con $\text{MCD}(a, b) = 1$, per il Teorema Cinese del resto $\varphi(m) = \varphi(a)\varphi(b)$.

Queste osservazioni permettono di concludere che se

$$m = \prod_{j=1}^{r} p_j^{m_j}$$

è la fattorizzazione di m in potenze di numeri primi $p_1, \cdots, p_r$ a due a due distinti, allora

$$\varphi(m) = \prod_{j=1}^{r} p_j^{m_j - 1} (p_j - 1).$$

D'altra parte, per un risultato classico, si ha anche

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

dove il prodotto è esteso a tutti i divisori primi di m.

A titolo di esempio calcoliamo i primi 18 valori della funzione di Eulero.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6

Se $\mathbb{K}$ è un campo arbitrario, $\Phi_m(x)$ non è necessariamente irriducibile in $\mathbb{K}[x]$. Tuttavia lo è sul campo razionale $\mathbb{Q}$, per il seguente importante risultato dovuto a Gauss. Conviene premettere la seguente

(2.11) Osservazione *Dato il polinomio*

$$g(x) = k_0 + k_1 x + k_2 x^2 + \cdots + k_r x^r,$$

è naturale definire, per ogni intero positivo t:

$$g(x^t) = k_0 + k_1 x^t + k_2 x^{2t} + \cdots + k_r x^{rt}.$$

Chiaramente α^t è radice di $g(x)$ se e solo se α è radice di $g(x^t)$.
Infatti, posto $\overline{g}(x) = g(x^t)$ si ha $g(\alpha^t) = \overline{g}(\alpha)$.

Per esempio 2^3 è radice di

$$g(x) = 8 - 25x - 5x^2 + x^3.$$

Equivalentemente 2 è radice di

$$g(x^3) = 8 - 25x^3 - 5x^6 + x^9.$$

Infatti $0 = 8 - 25\,2^3 - 5\,(2^3)^2 + (2^3)^3 = 8 - 25\,2^3 - 5\,2^6 + 2^9$.

(2.12) Teorema *Per ogni $m \geq 1$ il polinomio ciclotomico $\Phi_m(x)$ è irriducibile in $\mathbb{Q}[x]$.*

Dimostrazione.
$\Phi_m(x)$ appartiene a $\mathbb{Z}[x]$ ed è monico, quindi primitivo. Sia $f(x)$ un suo fattore monico, irriducibile in $\mathbb{Z}[x]$, di grado > 0. Consideriamo la relativa fattorizzazione

$$\Phi_m(x) = f(x)g(x) \tag{2.13}$$

con $g(x)$ monico, a coefficienti interi. Per il Lemma di Gauss $f(x)$ è irriducibile in $\mathbb{Q}[x]$. Quindi dobbiamo dimostrare $g(x) = 1$.
A tale scopo, sia ϵ una radice di $f(x)$ in un suo campo di spezzamento. Da

$$\Phi_m(\epsilon) = f(\epsilon)g(\epsilon) = 0\,g(\epsilon) = 0$$

segue che ϵ è radice di $\Phi_m(x)$, ossia è radice primitiva m-esima di 1. Per ogni primo p che non divide m, anche ϵ^p è radice di $\Phi_m(x)$, da cui $f(\epsilon^p)\,g(\epsilon^p) = 0$. Supponiamo $f(\epsilon^p) \neq 0$. Ne segue $g(\epsilon^p) = 0$, ossia ϵ^p è radice di $g(x)$. Per l'osservazione fatta sopra ϵ è radice di $g(x^p)$, quindi $f(x)$ divide $g(x^p)$. Infatti $f(x)$, essendo irriducibile in $\mathbb{Q}[x]$, è il polinomio minimo di ϵ su $\mathbb{Q}$. Esiste quindi $h(x) \in \mathbb{Z}[x]$, monico, tale che:

$$g(x^p) = f(x)\,h(x). \tag{2.14}$$

Consideriamo l'epimorfismo $\pi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ indotto dall'epimorfismo $\mathbb{Z} \to \mathbb{F}_p$.
Posto $g(x) = k_0 + k_1x + \cdots + k_sx^s$, si ha:

$$\pi\,(g(x)) = [k_0]_p + [k_1]_px + \cdots + [k_s]_px^s.$$

Ricordiamo che l'applicazione $\mathbb{F}_p[x] \to \mathbb{F}_p[x]$ che consiste nell'elevamento a p è un monomorfismo (detto di Frobenius) che fissa ogni elemento di $\mathbb{F}_p$. Ne segue

$$\pi\,(g(x^p)) = (\pi(g(x)))^p\,. \tag{2.15}$$

Infatti:

$$\pi\,(g(x^p)) = [k_0]_p + [k_1]_px^p + \cdots + [k_s]_px^{ps} = ([k_0]_p + [k_1]_px + \cdots + [k_s]_px^s)^p\,.$$

Applicando l'omomorfismo π ai due membri di (2.14) e usando la (2.15) si ha allora:

$$(\pi(g(x))^p \;=\; \pi\left(f(x)\right)\,\pi\left(h(x)\right). \tag{2.16}$$

Essendo $f(x)$ monico, $\pi\left(f(x)\right) \in \mathbb{F}_p[x]$ ha lo stesso grado di $f(x)$, che è positivo. Pertanto $\pi\left(f(x)\right)$ ammette almeno un fattore monico irriducibile $\overline{m}(x) \in \mathbb{F}_p[x]$. In virtù di (2.16) $\overline{m}(x)$ divide $(\pi(g(x))^p$, e quindi anche $\pi\left(g(x)\right)$. Deduciamo così che $\overline{m}(x)^2$ divide

$$\pi\left(\Phi_m(x)\right) = \pi\left(f(x)\right)\pi\left(g(x)\right). \tag{2.17}$$

Ma, in tal caso, ogni radice di $\overline{m}(x)$, è radice di $\pi\left(\Phi_m(x)\right)$ di molteplicità ≥ 2. Tuttavia è facile verificare che $\pi\left(\Phi_m(x)\right)$ è l'm-esimo polinomio ciclotomico su $\mathbb{F}_p$, ed è quindi separabile in virtù dell'ipotesi $(m,p) = 1$: contraddizione.
Pertanto $f(\epsilon^p) = 0$. Riassumendo, abbiamo fin qui dimostrato che se ϵ è una radice di $f(x)$ e p è un primo che non divide m, anche ϵ^p è radice di $f(x)$.
Se $g(x)$ avesse grado > 0, avrebbe una radice θ in un campo di spezzamento. Sia ϵ sia θ sarebbero radici di $\Phi_m(x)$, quindi radici primitive m-esime di 1. In particolare

$$\theta = \epsilon^s$$

per qualche intero s con $(s,m) = 1$. Consideriamo la fattorizzazione di s in primi (non necessariamente distinti)

$$s = p_1 \cdots p_t.$$

Nessuno di tali primi divide m. Quindi ϵ^{p_1} è radice di $f(x)$. Ne segue, per induzione su t, che $(\epsilon^{p_1 \cdots p_{t-1}})^{p_t} = \theta$ è radice anche di $f(x)$, ossia è radice di $\Phi_m(x)$ di molteplicità ≥ 2, contraddizione.
Si conclude che $g(x)$ ha grado 0. Essendo monico, $g(x) = 1$. ■

(2.18) Esempio *Per ogni numero primo p si consideri il polinomio $x^p - 1 \in \mathbb{Q}[x]$. Da*

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

in virtù di (2.9) *si ha che*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

E, per il Teorema precedente, tale polinomio è irriducibile in $\mathbb{Q}[x]$. In particolare

$$\min_{\mathbb{Q}}\left(e^{\frac{2\pi i}{p}}\right) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Inoltre da

$$\left(e^{\frac{2\pi i}{p}}\right)^{p-1} + \left(e^{\frac{2\pi i}{p}}\right)^{p-2} + \cdots + e^{\frac{2\pi i}{p}} + 1 = 0$$

segue che la somma delle radici p-esime complesse di 1 *è 0.*

(2.19) Esercizio *Si mostri che* $\min_{\mathbb{R}}\left(e^{\frac{2\pi i}{p}}\right) = x^2 - 2\cos\left(\frac{2\pi}{p}\right)x + 1$.

Il gruppo $\mathbb{Z}_m^*$ degli elementi unitari di $\mathbb{Z}_m$ è costituito dalle classi di resti $[k]_m$, $1 \leq k < m$, tali che $(k, m) = 1$. In particolare $\mathbb{Z}_m^*$ ha ordine $\varphi(m)$, dove φ è la funzione di Eulero.

(2.20) Teorema $\mathrm{Gal}_{\mathbb{Q}}(\Phi_m(x)) \simeq \mathbb{Z}_m^*$.

Dimostrazione. Come abbiamo visto, il numero complesso $\epsilon := e^{\frac{2\pi i}{p}}$ e le sue potenze ϵ^k, con $(k, m) = 1$, sono le $\varphi(m)$ radici primitive m-esime di 1. Quindi il campo di spezzamento di $\Phi_m(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\epsilon)$. Inoltre, per l'irriducibilità di $\Phi_m(x)$ in $\mathbb{Q}[x]$, si ha

$$\Phi(x) = \min_{\mathbb{Q}}(\epsilon) = \min_{\mathbb{Q}}(\epsilon^k)$$

per ogni k tale che $(k, m) = 1$. Ne segue che esiste un automorfismo σ_k di $\mathbb{Q}(\epsilon)$ tale che

$$\epsilon \xrightarrow{\sigma_k} \epsilon^k.$$

Ponendo $f([k]_m) := \sigma_k$ si definisce una applicazione

$$f : \mathbb{Z}_m^* \to \mathrm{Aut}(\mathbb{Q}(\epsilon)).$$

Infatti $[k]_m = [h]_m$ se e solo se $k - h = mt$, $t \in \mathbb{Z}$, se e solo se $\epsilon^k = \epsilon^h$.
Verifichiamo che f è un omomorfismo di gruppi. Per ogni $[k_1]_m, [k_2]_m \in \mathbb{Z}_m^*$

$$f([k_1]_m[k_2]_m) = f([k_1k_2]_m) = \sigma_{k_1k_2}.$$

$$f([k_1]_m)\, f([k_2]_m) = \sigma_{k_1}\sigma_{k_2}.$$

Notando che

$$\sigma_{k_1k_2}(\epsilon) = \epsilon^{k_1k_2} = \left(\epsilon^{k_2}\right)^{k_1} = \sigma_{k_1}\sigma_{k_2}(\epsilon).$$

si conclude $\sigma_{k_1k_2} = \sigma_{k_1}\sigma_{k_2}$, ossia che $f([k_1]_m[k_2]_m) = f([k_1]_m)\, f([k_2]_m)$. Sia ora $[k]_m \in \mathrm{Ker}\ f$, cioè $\sigma_k = f([k]_m) = \mathrm{id}$. In particolare $\epsilon^k = \epsilon$, da cui $k \equiv 1 \pmod{m}$, $[k]_m = [1]_m$. Quindi f è iniettiva. Ricordando che

$$\mathrm{Gal}_{\mathbb{Q}}(\Phi_m(x)) = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\epsilon)) = \mathrm{Aut}(\mathbb{Q}(\epsilon))$$

si ha

$$|\mathbb{Z}_m^*| = \varphi(m) = \deg\Phi(x) = [\mathbb{Q}(\epsilon) : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\epsilon))| = |\mathrm{Gal}_{\mathbb{Q}}(\Phi_m(x))|.$$

Si conclude che il monomorfismo f è suriettivo, quindi un isomorfismo. ■

Capitolo V

Un problema classico

In questo Capitolo $\mathbb{K}$ indica un campo di caratteristica 0.

1 Equazioni algebriche

Una equazione algebrica è una equazione delle forma $f(x) = 0$, dove $f(x)$ è un polinomio a coefficienti in $\mathbb{K}$. Per ogni elemento non nullo k di $\mathbb{K}$, le equazioni $f(x) = 0$ e $k^{-1}f(x) = 0$ sono equivalenti, ossia hanno le stesse radici. Infatti da $f(\alpha) = 0$ segue $k^{-1}f(\alpha) = k^{-1}0 = 0$ e da $k^{-1}f(\alpha) = 0$ segue $kk^{-1}f(\alpha) = k\,0 = 0$, per ogni $\alpha \in \Sigma$, campo di spezzamento di $f(x)$ su $\mathbb{K}$. Di conseguenza, se $f(x) \neq 0$, moltiplicando eventualmente $f(x)$ per l'inverso del suo coefficiente direttivo, possiamo sempre supporre $f(x)$ monico.

(1.1) Esempio $f(x) = 3x + 4 \in \mathbb{Q}[x]$. *L'equazione* $3x + 4 = 0$ *è equivalente a*

$$x + \frac{4}{3} = 0.$$

(1.2) Esempio $f(x) = 5x^2 + 4x + 6 \in \mathbb{Q}[x]$. *L'equazione* $f(x) = 0$ *è equivalente a*

$$x^2 + \frac{4}{5}x + \frac{6}{5} = 0.$$

Fissate n indeterminate $a_0, \ldots, a_{n-1}$, consideriamo l'anello $\mathbb{Q}[a_0, \ldots, a_{n-1}]$ dei polinomi a coefficienti razionali, nelle indeterminate $a_0, \ldots, a_{n-1}$. Tale anello è privo di divisori dello zero, e ammette quindi un campo dei quozienti $\mathbb{K} := \mathbb{Q}(a_0, \ldots, a_{n-1})$. Ricordiamo che gli elementi di $\mathbb{K}$ si rappresentano come *frazioni* $\frac{f}{g}$ con $f, g \in \mathbb{Q}[a_0, \ldots, a_{n-1}]$, $g \neq 0$. Due frazioni $\frac{f}{g}$, $\frac{h}{k}$ rappresentano lo stesso elemento di $\mathbb{K}$ se e solo se $fk = gh$. Le operazioni di somma e prodotto sono governate dalle usuali regole del calcolo sulle frazioni.

(1.3) Definizione *Si chiama* equazione algebrica generale *di grado* n*, l'equazione*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

i cui coefficienti sono delle indeterminate.

Chiaramente, una eventuale formula che esprima le radici dell'equazione generale come funzioni dei suoi coefficienti, consente di risolvere ogni equazione particolare di grado n a coefficienti razionali. Basta infatti sostituire nella formula, alle indeterminate $a_0, \ldots, a_{n-1}$, i coefficienti particolari dell'equazione assegnata.
Per le equazioni algebriche di grado ≤ 4 tali formule esistono.

Grado 1. L'equazione generale $x + a_0 = 0$ ha radice $\alpha = -a_0$.

Grado 2. L'equazione generale $x^2 + a_1 x + a_0 = 0$ ha radici

$$\alpha = \frac{1}{2}\left(-a_1 + \sqrt{\Delta}\right), \quad \beta = \frac{1}{2}\left(-a_1 - \sqrt{\Delta}\right)$$

dove $\Delta := a_1^2 - 4a_0$ è detto il *discriminante* dell'equazione.
Considerando la fattorizzazione $x^2 + a_1 x + a_0 = (x - \alpha)(x - \beta)$ si ottengono i seguenti valori per la somma e il prodotto delle radici:

$$\alpha + \beta = -a_1, \quad \alpha\beta = a_0. \tag{1.4}$$

Grado 3. Consideriamo l'equazione cubica $x^3 + a_2 x^2 + a_1 x + a_0 = 0$.
Con il cambio di variabile $x = y - \frac{1}{3}a_2$ la possiamo riscrivere nella forma:

$$y^3 + 3ay + b = 0 \tag{1.5}$$

in cui manca il termine quadratico.

Caso $a = 0$. L'equazione (1.5) è equivalente a $y^3 = -b$. Indicando con $\sqrt[3]{-b}$ una sua radice, le altre sono $\sqrt[3]{-b}\,\omega$ e $\sqrt[3]{-b}\,\omega^2$, dove ω è una radice primitiva cubica di 1.

Caso $a \neq 0$. Detta α una radice di (1.5), consideriamo l'equazione

$$t^2 - \alpha t - a = 0.$$

Dette $r, \overline{r}$ le sue radici, si ha $r\overline{r} = -a$, $r + \overline{r} = \alpha$. Quindi scriviamo α nella forma:

$$\alpha = r - \frac{a}{r} \tag{1.6}$$

Da $\alpha^3 + 3a\alpha + b = 0$ otteniamo:

$$r^3 - \frac{a^3}{r^3} = -b.$$

Ne segue che r^3 è una radice dell'equazione $t^2 + bt - a^3 = 0$. Ossia $r^3 \in \{u, v\}$, dove

$$u = \frac{1}{2}\left(-b + \sqrt{b^2 + 4a^3}\right), \quad v = \frac{1}{2}\left(-b - \sqrt{b^2 + 4a^3}\right).$$

Fissata una radice cubica r di u, le altre radici cubiche di u sono $r\omega$ e $r\omega^2$, con ω radice primitiva cubica di 1. Da (1.6) si ottengono quindi i seguenti valori per le radici di (1.5):

$$r - \frac{a}{r}, \quad r\omega - \frac{a}{r}\omega^2, \quad r\omega^2 - \frac{a}{r}\omega. \tag{1.7}$$

Notiamo che da $uv = -a^3$ segue che $s = -\frac{a}{r}$ è una radice cubica di v. Pertanto

$$s - \frac{a}{s} = r - \frac{a}{r}.$$

Quindi scegliendo una radice cubica s di v si perviene agli stessi valori di (1.7).

Grado 4. Per l'equazione quartica $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ sussistono analoghe formule risolutive.

(1.8) Osservazione *Notiamo che la formula risolutiva dell'equazione di grado* 2*, coinvolgendo l'inverso di* 2*, vale solo su campi di caratteristica* $\neq 2$*. Le formule risolutive delle equazioni di grado* 3 *e* 4 *richiedono analoghe restrizioni sulla caratteristica del campo, quando questa è finita. Questo giustifica l'ipotesi char* $\mathbb{K} \neq 0$*, fatta all'inizio del Capitolo.*

L'applicazione delle formule risolutive non è quasi mai efficiente. Per risolvere le equazioni algebriche sono preferibili altri metodi, soprattutto quelli dell'analisi numerica, che portano a soluzioni approssimate. A volte anche la trigonometria può essere utile.

(1.9) Esempio

Supponiamo di voler trovare $\sin 10°$*. Utilizzando l'identità trigonometrica*

$$\sin(3\theta) = 3\sin\theta - 4\sin^3\theta$$

e ricordando che $\sin 30° = \sin 150° = \frac{1}{2}$*, si ha che* $\sin 10°$ *e* $\sin 50°$ *sono radici di*

$$x^3 - \frac{3}{4}x + \frac{1}{8} = 0. \tag{1.10}$$

Dette α, β, γ *le radici di* (1.10)*, si ha:*

$$x^3 - \frac{3}{4}x + \frac{1}{8} = (x - \alpha)(x - \beta)(x - \gamma)$$

da cui, in particolare, $\alpha\beta\gamma = -\frac{1}{8}$*. Ne segue che* (1.10) *ha* 3 *radici reali:*

$$\alpha = \sin 10°, \ \beta = \sin 50°, \ \gamma = \frac{-1}{8\sin 10°\sin 50°}.$$

Per contro, la formula risolutiva dell'equazione (1.10)*, coinvolge numeri complessi. Infatti essa è del tipo* (1.5) *con* $a = -\frac{1}{4}$*,* $b = \frac{1}{8}$*. Ne segue che una radice, pur essendo reale, è espressa dalla formula*

$$\frac{1}{2}\sqrt[3]{\frac{-1-\sqrt{3}\,i}{2}} + \frac{1}{2}\sqrt[3]{\frac{-1+\sqrt{3}\,i}{2}}.$$

Un approccio alternativo alla risoluzione di (1.10)*, utilizza le funzioni trigonometriche. Detta* $\theta := \cos 40^\circ + i \sin 40^\circ$*, una radice primitiva nona di* 1*, le radici di* (1.10) *sono:*

$$\frac{1}{2}(\theta + \overline{\theta}), \quad \frac{1}{2}(\theta^2 + \overline{\theta}^2), \quad \frac{-1}{8(\theta + \overline{\theta})(\theta^2 + \overline{\theta}^2)}.$$

Infatti: $\frac{1}{2}(\theta + \overline{\theta}) = \cos 40^\circ = \sin 50^\circ$*,* $\frac{1}{2}(\theta^2 + \overline{\theta}^2) = \cos 80^\circ = \sin 10^\circ$*.*

2 Cenni storici

La risoluzione delle equazioni algebriche è un problema classico, in matematica.
La formula risolutiva dell'equazione generale di grado 2 era nota, in sostanza, fin dai tempi degli antichi Babilonesi. Durante il Rinascimento italiano, molti sforzi furono rivolti alla ricerca di analoghe formule per le equazioni generali di grado 3 e 4. Esse ebbero alla fine un esito positivo. Quella per l'equazione di terzo grado fu scoperta da Scipione del Ferro, professore di matematica all'Università di Bologna dal 1496 al 1526 e, indipendentemente da Nicolò Tartaglia (1500-1557), bresciano. La soluzione di Tartaglia fu pubblicata da Geronimo Cardano in *Ars Magna* nel 1545 e, per tale ragione, è generalmente conosciuta come *formula di Cardano*. Un metodo per risolvere l'equazione generale di grado 4 fu pure pubblicato da Cardano in Ars Magma, anche se è attribuito a un suo assistente, Ludovico Ferrari.
Tali formule sono all'origine della seguente:

(2.1) Definizione *Una equazione algebrica* $f(x) = 0$ *si dice* risolubile per radicali *se ammetta una formula risolutiva che coinvolge operazioni razionali* $(+, -, \times, :)$ *e estrazioni di radici di qualunque ordine sui coefficienti di* $f(x)$*.*

Dopo il Rinascimento, per più di due secoli, le formule risolutive delle equazioni di grado superiore a 4 resistettero ad ogni tentativo di ottenerle. In particolare si cimentarono matematici del calibro di Leonhard Euler (1707-1783) e Louis Lagrange (1736-1813), ma senza successo. Finchè si cominciò a sospettare che non esistessero. La conferma venne da Paolo Ruffini (1765-1822), medico, e indipendentemente da Niels Abel (1802-1829),

matematico norvegese di grande profonditá. Precisamente essi dimostrarono, anche se in modo piuttosto oscuro e probabilmente lacunoso, il seguente risultato, noto come:

(2.2) Teorema di Ruffini-Abel *L' equazione algebrica generale di grado n è risolubile per radicali se e solo se $n \leq 4$.*

La soluzione completa del problema è tuttavia dovuta al matematico francese Evaristo Galois, morto nel 1832 all'età di soli 21 anni, in un tragico duello d'onore [6]. Egli non solo diede una dimostrazione rigorosa del risultato negativo di Ruffini-Abel concernente le equazioni generali, ma formulò la condizione necessaria e sufficiente perchè una qualunque equazione algebrica $f(x) = 0$ sia risolubile per radicali. Tale condizione si enuncia in termini radicalmente nuovi per la matematica del tempo: infatti corrisponde alla cosiddetta *risolubilità* del gruppo di Galois del campo di spezzamento Σ di $f(x)$ sul campo $\mathbb{K}$ dei suoi coefficienti, brevemente del gruppo di Galois di $f(x)$. Precisamente

(2.3) Teorema *(***Criterio di Galois)** *Un' equazione algebrica di grado $n \geq 1$ è risolubile per radicali se e solo se il suo gruppo di Galois è risolubile.*

Dire che un gruppo G è *risolubile* significa che è G è abeliano oppure si ottiene mediante successive estensioni di gruppi abeliani. La classe dei gruppi risolubili estende quella dei gruppi abeliani. Ad esempio i gruppi simmetrici Sym(3) e Sym(4) sono risolubili, pur non essendo abeliani. D'altra parte, per $n \geq 5$, il gruppo simmetrico Sym(n) non è risolubile. Questo spiega perchè l'equazione generale di grado n, il cui gruppo di Galois è Sym(n), sia risolubile per radicali se e solo se $n \leq 4$.
Alla base della soluzione del problema fornita da Galois sta il risultato principale delle sue ricerche, cioè la corrispondenza bijettiva fra i sottocampi di Σ che contengono $\mathbb{K}$, e i sottogruppi del gruppo di Galois di Σ su $\mathbb{K}$.
La teoria di Galois, che fu pubblicata solo nel 1846, circa 15 anni dopo la sua morte, iniziò una nuova branca della matematica, la teoria dei gruppi. Hermann Weyl, nel suo libro *Symmetry*, ne dà la seguente valutazione:
Galois's ideas, which for several years remained a book with seven seals but later exerted a more and more profound influence upon the whole development of mathematics, are contained in a far-well letter written to a friend on the eve of his death, which he met in a silly duel at the age of 21. *This letter, if judged by the novelty and profoundity of ideas it contains, is perhaps the most substancial piece of writing in the whole literature of mankind.*

Bibliografia

[1] E. Artin, Galois Theory, Dover Publications, Inc. (1998).

[2] L.Dickson, Linear Groups, Dover Publications, Inc. (1958).

[3] J.M. Howie, Fields and Galois Theory, Springer (2006).

[4] M.Isaacs, Algebra: a graduate course, Brooks/Cole Publishing Company, 1994.

[5] N.Jacobson, Basic Algebra I, W.H.Freeman and company, San Francisco,1974.

[6] P.Pagli, L.Toti Rigatelli, Evariste Galois, morte di un matematico, Archinto (1998).

[7] M.C. Tamburini, Algebra I unità , Dispensa in rete.

[8] M.C. Tamburini, Algebra II unità , Dispensa in rete.

[9] M.C. Tamburini, Approfondimenti di Algebra, Dispensa in rete.