Elementi di Teoria dei Campi

Stefania Gabelli

Dipartimento di Matematica, Università degli Studi Roma Tre
Largo San L. Murialdo, 1 - 00146 Roma, Italy

e-mail: gabelli@mat.uniroma3.it

a.a. 2004-2005

Indice

Queste note raccolgono alcune nozioni di base di Teoria dei Campi che sono propedeutiche alla maggior parte dei corsi di Algebra e di Geometria dei Corsi di Laurea in Matematica. L'esposizione è elementare ed include molti esempi, illustrati dettagliatamente. Gli esercizi alla fine di ogni paragarafo costituiscono un necessario strumento di verifica.

Un utile complemento è dato dalle dispense a cura di S. Gabelli e F. Girolami: *Anelli di Polinomi*,

http://www.mat.uniroma3.it/users/gabelli/dispense/Polinomi.pdf.

1 Campi e Sottocampi

Un anello K si dice un *campo* se l'insieme dei suoi elementi non nulli $K^* := K\backslash\{0\}$ è un gruppo commutativo rispetto alla moltiplicazione. In particolare un campo è un anello commutativo unitario ed integro.

Esempi

1.1. Gli insiemi numerici $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono campi, mentre $\mathbb{Z}$ non è un campo.

1.2. L'anello $\mathbb{Q}(\sqrt{2}) := \left\{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\right\}$ è un campo. Infatti

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

1.3. Se $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ delle classi resto modulo n è un campo se e soltanto se n è un numero primo. Infatti $\mathbb{Z}/n\mathbb{Z}$ è un anello commutativo unitario ed integro ed inoltre i suoi elementi invertibili sono le classi dei numeri interi coprimi con n. Se p è un numero primo, il campo $\mathbb{Z}/p\mathbb{Z}$ si indica con $\mathbb{F}_p$.

1.4. Se F è un campo contenuto in $\mathbb{R}$, l'insieme

$$\mathcal{M}_{a,b}(F) := \left\{ M_{a,b} := \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,;\, a, b \in F \right\}$$

è un campo. Infatti,

$$M_{a,b} - M_{c,d} = M_{a-c,b-d} \quad \text{e} \quad M_{a,b}M_{c,d} = M_{c,d}M_{a,b} = M_{ac-bd,ad+bc}.$$

Dunque $\mathcal{M}_{a,b}(F)$ è un sottoanello commutativo unitario dell'anello di tutte le matrici 2×2 su F, con unità la matrice $M_{1,0}$. Inoltre, se $M_{a,b} \neq 0$, si ha che $M_{a,b}M_{a,-b} = (a^2 + b^2)M_{1,0}$ con $a^2 + b^2 \neq 0$, perciò

$$M_{a,b}^{-1} = \frac{1}{a^2 + b^2} M_{a,-b} \in M_{a,b}(F).$$

Una proprietà importante del gruppo moltiplicativo K^* è il fatto che ogni suo sottogruppo finito è un gruppo ciclico. Per dimostrare questo, abbiamo bisogno di un risultato sui gruppi abeliani finiti.

Ricordiamo che, se G è un gruppo abeliano finito, il minimo comune multiplo degli ordini degli elementi di G si dice l'*esponente* di G e si indica con $e(G)$.

Lemma 1.1 *Ogni gruppo abeliano finito G ha un elemento di ordine $e(G)$.*

Dimostrazione: Sia $e(G) = p_1^{k_1} \cdots p_s^{k_s}$ la fattorizzazione di $e(G)$ in numeri primi distinti. Per come è definito $e(G)$, $p_i^{k_i}$ divide l'ordine di qualche elemento di G per ogni $i = 1, \ldots, s$.

Sia $g_i \in G$ di ordine $p_i^{k_i} d_i$. Allora $h_i := g_i^{d_i}$ ha ordine $p_i^{k_i}$ e il prodotto $g := h_1 \cdots h_s$ ha ordine $e(G)$. Infatti è chiaro che $g^{e(G)} = 1$. D'altra parte, se $g^n = 1$, allora $h_1^n = h_2^{-n} \cdots h_s^{-n}$. Posto $m_1 := \frac{e(G)}{p_1^{k_1}} = p_2^{k_2} \cdots p_s^{k_s}$, si ha $h_2^{m_1} = \cdots = h_s^{m_1} = 1$; da cui $h_1^{nm_1} = 1$. Poiché h_1 ha ordine $p_1^{k_1}$, allora $p_1^{k_1}$ divide nm_1 e quindi divide n.

Ripetendo questo ragionamento, si ottiene che $p_i^{k_i}$ divide n per ogni $i = 1, \ldots, s$ e dunque $e(G)$ divide n.

Proposizione 1.2 *Se K è un campo, ogni sottogruppo finito del gruppo moltiplicativo K^* è ciclico.*

Dimostrazione: Sia G un sottogruppo di K^* di ordine $m \geq 1$. Poiché l'ordine di ogni elemento di G divide m, allora $e(G)$ divide m e in particolare $e(G) \leq m$. D'altra parte, ogni elemento di G è una radice in K del polinomio $X^{e(G)} - 1$. Poiché questo polinomio ha al più $e(G)$ radici in K, allora $m \leq e(G)$. Ne segue che G ha esattamente $e(G)$ elementi ed inoltre, per il lemma precedente, ha anche un elemento di ordine $e(G)$. Quindi G è ciclico.

Ricordiamo che, se G è un gruppo moltiplicativo ciclico di ordine n e g è un generatore di G, ovvero $G = \langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = e\}$, tutti gli altri generatori di G sono gli elementi g^k con $\mathrm{MCD}(n, k) = 1$. Il numero di questi generatori è dato dal valore dell'applicazione $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ che ad ogni intero positivo n associa il numero $\varphi(n)$ degli interi positivi minori di n e primi con n. Questa applicazione si chiama la *funzione di Eulero* ed è una funzione aritmetica moltiplicativa, nel senso che, se $\mathrm{MCD}(r, s) = 1$, allora $\varphi(rs) = \varphi(r)\varphi(s)$. Un semplice calcolo mostra che, se p è un numero primo, si ha

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p}).$$

Dunque, se $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ è la fattorizzazione di n in numeri primi distinti, risulta

$$\varphi(n) = \varphi(p^{k_1}) \cdots \varphi(p^{k_s}) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_s^{k_s} - p_s^{k_s - 1}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_s}).$$

Esempi

1.5. I numeri complessi z tali che $z^n = 1$ si dicono le *radici complesse n-sime dell'unità*. Essi sono tutti e soli gli n numeri complessi

$$z_k := \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

per $0 \leq k \leq n-1$ e formano un sottogruppo moltiplicativo di $\mathbb{C}^*$. Dunque le radici complesse n-sime dell'unità formano un sottogruppo ciclico di $\mathbb{C}^*$; infatti è facile vedere che, per ogni k, si ha $z_k = z_1^k$. I generatori di questo gruppo si chiamano le *radici primitive* n-sime dell'unità: esse sono esattamente i numeri complessi z_k con $\mathrm{MCD}(n,k) = 1$.

Il termine radice primitiva fu introdotto da L. Euler mentre l'esistenza di radici primitive, ovvero il fatto che il gruppo delle radici n-sime è ciclico, fu dimostrata da F. Gauss (1801).

1.6. Il gruppo moltiplicativo $\mathbb{F}_p^*$, dove p è un numero primo, è un gruppo ciclico con $p-1$ elementi.

Ad esempio, il gruppo $\mathbb{F}_5^*$ è ciclico di ordine 4 ed ha $\varphi(4) = 2$ generatori, precisamente la classe di 2 o la classe di 3. Il gruppo $\mathbb{F}_{11}^*$ ha $\varphi(10) = \varphi(2)\varphi(5) = 4$ generatori, precisamente le classi di 2, 6, 7, 8.

Un sottoinsieme di un campo K che risulta essere un campo rispetto alle stesse operazioni di K si dice un *sottocampo* di K. Un sottocampo di $\mathbb{C}$ si dice un *campo numerico*; un sottocampo di $\mathbb{R}$ si dice un *campo numerico reale*.

Proposizione 1.3 *Un sottoinsieme F di un campo K è un sottocampo di K se e soltanto se, per ogni x , $y \in F$, risulta $x - y \in F$ e $xy^{-1} \in F$, per $y \neq 0$.*

Dimostrazione: Se $x, y \in F$, il fatto che $x - y \in F$ ci assicura che F è un sottogruppo additivo di K ed il fatto che $xy \in F$, per $y \neq 0$, implica che F^* è un sottogruppo moltiplicativo di K^*. Poiché la proprietà distributiva vale in K, ne segue che F è un sottocampo di K. Il viceversa è ovvio.

Esempi

1.7. Un insieme di numeri è un campo se e soltanto se esso è chiuso rispetto alle operazioni di somma, prodotto, differenza e quoziente. Questa è la definizione originaria di campo di numeri data da R. Dedekind nel 1871.

Ricordiamo che, se A è un anello commutativo unitario integro, si può costruire un campo, unico a meno di isomorfismi, con la proprietà di contenere una copia isomorfa di A ed essere contenuto isomorficamente in ogni campo contenente una copia isomorfa di A. Questo campo si chiama il *campo dei quozienti di A* e si indica con $\mathrm{Qz}(A)$. I suoi elementi sono le classi

di equivalenza dell'insieme $A \times A^*$ rispetto alla relazione di equivalenza ρ definita da:

$$(a,b)\,\rho\,(a',b') \Leftrightarrow ab' = a'b.$$

Si usa indicare la classe di (a,b) rispetto a ρ con $\frac{a}{b}$, in modo tale che

$$\mathrm{Qz}(A) := \left\{ \frac{a}{b}\,;\, a,b \in A, b \neq 0 \right\}.$$

Le operazioni in $\mathrm{Qz}(A)$ sono definite da:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \quad \text{e} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bc}.$$

Se A è un anello contenuto in un campo K, allora ogni elemento non nullo di A ha un inverso in K. In questo caso si verifica facilmente che l'applicazione $\mathrm{Qz}(A) \longrightarrow \left\{ab^{-1}\,;\, a,b \in A\,,\, b \neq 0\right\}$ definita da $\frac{a}{b} \mapsto ab^{-1}$ è un isomorfismo di campi. Quindi si può supporre che $\mathrm{Qz}(A)$ sia contenuto in K.

Esempi

1.8. Il campo dei quozienti di $\mathbb{Z}$ è $\mathbb{Q}$. Poiché ogni campo numerico contiene $\mathbb{Z}$ (perché contiene 1 ed è chiuso rispetto all'addizione e alla sottrazione), allora esso contiene $\mathbb{Q}$. Ne segue che $\mathbb{Q}$ è il più piccolo campo numerico.

1.9. Se $\mathbb{Z}[i] := \{a+bi\,;\, a,b \in \mathbb{Z}\}$ è l'*anello degli interi di Gauss*, allora il campo dei quozienti di $\mathbb{Z}[i]$ è

$$\mathbb{Q}(i) := \left\{ \frac{a+bi}{c+di}\,;\, a,b,c,d \in \mathbb{Z}\,, c,d \neq 0 \right\} = \{x+yi\,;\, x,y \in \mathbb{Q}\}\,.$$

Infatti, se $c+di \neq 0$, con $c,d \in \mathbb{Z}$, risulta $\frac{1}{c+di} = \frac{c-di}{c^2+d^2}$.

1.10. Se $\mathbf{X} := \{X_i\}_{i\in I}$ è un insieme di indeterminate algebricamente indipendenti su un campo F, il campo dei quozienti dell'anello dei polinomi $F[\mathbf{X}] := F[X_i\,;\, i \in I]$ è il *campo delle funzioni razionali nelle indeterminate* $\mathbf{X}$.

$$F(\mathbf{X}) := \left\{ \frac{f(\mathbf{X})}{g(\mathbf{X})}\,;\, f(\mathbf{X}), g(\mathbf{X}) \in F[\mathbf{X}]\,,\, g(\mathbf{X}) \neq 0 \right\}.$$

Proposizione 1.4 *Un anello commutativo unitario è un campo se e soltanto se i suoi unici ideali sono* (0) *e* (1).

Dimostrazione: Siano K un campo, I un ideale di K e $x \in I$. Se $x \neq 0$, poiché $x^{-1} \in K$, allora $1 = xx^{-1} \in I$. Ne segue che $y = 1y \in I$, per ogni $y \in K$. Perciò $I = K$.

Viceversa, sia A un anello commutativo unitario i cui ideali siano soltanto (0) e (1). Se $a \in A$ e $a \neq 0$, allora $(a) = (1)$. Ne segue che $ax = 1$ per qualche $x \in A$. Dunque a è invertibile in A.

ESERCIZI

1.1. Mostrare che $\mathbb{Q}$ e $\mathbb{F}_p$ non hanno sottocampi propri.

1.2. Mostrare che, per ogni primo p, $\mathbb{Q}(\sqrt{p}) := \left\{a + b\sqrt{p}\,;\, a, b \in \mathbb{Q}\right\}$ è un campo numerico.

1.3. Mostrare che un'intersezione di sottocampi di K è un sottocampo di K.

1.4. Mostrare che se

$$F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots \subseteq F_n \subseteq \ldots$$

è una catena di campi, allora $K := \bigcup_{i \geq 1} F_i$ è un campo.

1.5. Mostrare che un anello commutativo unitario integro con un numero finito di elementi è un campo.

1.6. Sia $K := \{0, 1, \alpha, \beta\}$ un insieme su cui siano definite una addizione e una moltiplicazione (con elementi neutri 0 e 1 rispettivamente) e in cui valgano le relazioni $2x = 0$, per ogni $x \in K$, $1 + \alpha = \beta$ e $\alpha^2 + \beta = 0$. Mostrare che K è un campo e determinare la tabella additiva e la tabella moltiplicativa di K.

1.7. Determinare i generatori dei gruppi ciclici $\mathbb{F}_7^*$ e $\mathbb{F}_{13}^*$.

1.8. Mostrare che $\mathbb{Q}^*$ non è un gruppo ciclico.

2 Sottocampi Fondamentali e Caratteristica

L'intersezione di tutti i sottocampi di un campo K è un campo che si dice il *sottocampo fondamentale* di K. Esso è chiaramente il più piccolo sottocampo di K e perciò viene anche detto il *sottocampo minimo* di K.

Se $\alpha \in K$ e $n \geq 1$, poniamo

$$0\alpha := 0\,, n\alpha := \alpha + \alpha + \cdots + \alpha \text{ (n volte) e } (-n)\alpha := -(n\alpha).$$

Sia poi 1_K l'unità moltiplicativa di K e consideriamo l'applicazione

$$f : \mathbb{Z} \longrightarrow K \quad \text{definita da} \quad a \mapsto a1_K.$$

Si verifica subito che f è un omomorfismo di anelli; perciò l'immagine di f, ovvero l'insieme degli elementi $f(\mathbb{Z}) := \{a1_K\,;\, a \in \mathbb{Z}\}$, è un sottoanello di K. Inoltre, ogni sottocampo di K contiene $f(\mathbb{Z})$, perché contiene l'elemento $f(1) = 1_K$ ed è un gruppo additivo. Ne segue che il sottocampo fondamentale di K è il più piccolo sottocampo contenente $f(\mathbb{Z})$, dunque è il campo dei quozienti di $f(\mathbb{Z})$.

Proposizione 2.1 (E. Steinitz, 1910) *Se K è un campo, il suo sottocampo fondamentale è isomorfo a $\mathbb{Q}$ oppure a $\mathbb{F}_p$, per qualche primo p.*

Dimostrazione: Consideriamo l'omomorfismo di anelli $f : \mathbb{Z} \longrightarrow K$ definito da $a \mapsto a1_K$. Abbiamo già osservato che il sottocampo fondamentale di K è il campo dei quozienti di $f(\mathbb{Z})$. Il nucleo di f è un ideale di $\mathbb{Z}$; perciò esso è un ideale principale, generato da un intero $m \geq 0$.

Se $\mathrm{Ker}(f) = (0)$, allora $f(\mathbb{Z})$ è isomorfo a $\mathbb{Z}$; quindi il suo campo dei quozienti è isomorfo al campo dei quozienti di $\mathbb{Z}$, cioè a $\mathbb{Q}$.

Altrimenti, poiché f non è nullo, $\mathrm{Ker}(f) = m\mathbb{Z}$ con $m \geq 2$. In questo caso, per il Teorema Fondamentale di Omomorfismo, si ha che $f(\mathbb{Z})$ è isomorfo a $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Ma allora, poiché $f(\mathbb{Z})$ è integro (essendo contenuto in K), $m\mathbb{Z}$ deve essere un ideale primo. In conclusione $m = p$ è un numero primo e $f(\mathbb{Z}) \cong \mathbb{F}_p$ è un campo.

Con la terminologia introdotta da Steinitz, si dice che K ha *caratteristica zero* se il suo sottocampo fondamentale è isomorfo a $\mathbb{Q}$; si dice che K ha *caratteristica finita* (oppure *prima*, oppure *positiva*), uguale a p, se il suo sottocampo fondamentale è isomorfo a $\mathbb{F}_p$. Segue dalla definizione che ogni sottocampo di K ha la stessa caratteristica di K.

Notiamo che K ha caratteristica prima p se e soltanto se la sua unità moltiplicativa ha ordine additivo finito uguale a p ed ha caratteristica zero se e soltanto se la sua unità moltiplicativa ha ordine additivo non finito.

Esempi

2.1. Ogni campo numerico ha caratteristica zero.

2.2. Ogni campo finito ha caratteristica finita. Il campo $\mathbb{F}_p(X)$ delle funzioni razionali nell'indeterminata X su $\mathbb{F}_p$ è un campo infinito di caratteristica finita uguale a p.

ESERCIZI

2.1. Sia K un campo, $\alpha \in K$ e $n \geq 0$. Mostrare che:

(a) se K è un campo di caratteristica zero, allora $n\alpha = 0$ se e soltanto se $\alpha = 0$;

(b) se K è un campo di caratteristica prima p, allora $n\alpha = 0$ se e soltanto se p divide n oppure $\alpha = 0$.

2.2. Mostrare che, se K ha caratteristica prima uguale a p e $\alpha_1, \ldots, \alpha_n \in K$, $n \geq 2$, allora

$$(\alpha_1 + \cdots + \alpha_n)^{p^s} = \alpha_1^{p^s} + \cdots + \alpha_n^{p^s}$$

per ogni $s \geq 1$. (*Suggerimento*: Osservare che, se p è un numero primo, allora p divide tutti i coefficienti binomiali $\binom{p}{k}$ per $0 < k < p$. Procedere poi per doppia induzione, su n ed s).

2.3. Mostrare che, se $f(X) \in \mathbb{F}_p[X]$, allora $f(X)^p = f(X^p)$ (*Suggerimento*: Ricordare che, per ogni intero a ed ogni numero primo p, $a^p \equiv a \mod p$ (Piccolo Teorema di Fermat, 1640) ed usare l'esercizio precedente).

3 Omomorfismi di Campi

Se F e K sono campi, un'applicazione $\varphi : F \longrightarrow K$ si dice un *omomorfismo di campi* se, comunque scelti $x, y \in F$, risulta

$$\varphi(x+y) = \varphi(x) + \varphi(y)\,, \quad \varphi(xy) = \varphi(x)\varphi(y).$$

Un omomorfismo di campi non è dunque altro che un omomorfismo di anelli tra due campi.

Proposizione 3.1 *Ogni omomorfismo di campi non nullo $\varphi : F \longrightarrow K$ è iniettivo.*

Dimostrazione: Ricordando che un omomorfismo di anelli è iniettivo se e soltanto se il suo nucleo è l'ideale nullo, basta osservare che, essendo F un campo, se $\mathrm{Ker}(\varphi) \neq F$, necessariamente $\mathrm{Ker}(\varphi) = (0)$ (Proposizione 1.5).

Per la proposizione precedente, se $\varphi : F \longrightarrow K$ è un omomorfismo di campi non nullo, l'immagine $\varphi(F)$ di φ è un sottocampo di K isomorfo a F, cioè K contiene isomorficamente F. Per questo motivo un omomorfismo di campi non nullo $\varphi : F \longrightarrow K$ si dice anche un *isomorfismo* oppure una *immersione di F in K*.

Ogni omomorfismo di campi suriettivo è un isomorfismo.

Esempi

3.1. L'applicazione $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$ definita da $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ è un isomorfismo di $\mathbb{Q}(\sqrt{2})$ in $\mathbb{C}$ (Esempio 1.2).

3.2. Se $\mathcal{M}_{a,b}(\mathbb{R})$ è il campo di matrici reali definito nell'Esempio 1.4, l'applicazione $\mathbb{C} \longrightarrow \mathcal{M}_{a,b}(\mathbb{R})$ definita da $a + bi \mapsto M_{a,b}$ è un isomorfismo di campi.

Proposizione 3.2 *Siano F e K due campi e sia $\varphi : F \longrightarrow K$ un isomorfismo di F in K. Se $\mathbb{F}$ è il sottocampo fondamentale di F, allora $\varphi(\mathbb{F})$ è il sottocampo fondamentale di K. In particolare F e K hanno stessa caratteristica.*

Dimostrazione: Se $\mathbb{K}$ è il sottocampo fondamentale di K, allora $\mathbb{K} \subseteq \varphi(\mathbb{F})$. Ma allora $\varphi^{-1}(\mathbb{K}) \subseteq \mathbb{F}$. Per la minimalità di $\mathbb{F}$, si ha l'uguaglianza e dunque $\mathbb{K} = \varphi(\mathbb{F})$.

Proposizione 3.3 *Siano F, e K due campi e sia $\varphi : F \longrightarrow K$ un isomorfismo di F in K. Allora la restrizione di φ al sottocampo fondamentale $\mathbb{F}$ di F è l'identità, cioè risulta $\varphi(x) = x$, per ogni $x \in \mathbb{F}$.*

Dimostrazione: Siano 1_F e 1_K le unità moltiplicative di F e K rispettivamente. È sufficiente notare che, essendo φ un omomorfismo non nullo, deve risultare $\varphi(1_F) = 1_K$ e dunque $\varphi(a1_F) = a\varphi(1_F) = a1_K$, per ogni $a \in \mathbb{Z}$.

Se F e K sono due campi, tutte le applicazioni di dominio F e codominio K costituiscono uno spazio vettoriale su K con le operazioni definite da:

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)\,; \quad (k\varphi)(x) = k(\varphi(x))$$

per ogni $x \in F$, $k \in K$. Osserviamo però che se $\varphi_1, \ldots, \varphi_n$ sono isomorfismi distinti di F in K e $c_1, \ldots, c_n \in K$, l'applicazione $c_1\varphi_1 + \cdots + c_n\varphi_n$ non è in generale un isomorfismo di F in K.

La seguente proposizione, dovuta a R. Dedekind (1894), asserisce che, per $n \geq 1$, n isomorfismi distinti di F in K sono sempre linearmente indipendenti su K. La dimostrazione che riportiamo è dovuta ad E. Artin (1934).

Proposizione 3.4 (Lemma di Dedekind) *Siano F, K campi e siano $\varphi_1, \ldots, \varphi_n$ isomorfismi distinti di F in K, $n \geq 1$. Allora, comunque scelti $c_1, \ldots, c_n \in K$ non tutti nulli, l'applicazione $c_1\varphi_1 + \cdots + c_n\varphi_n$ è non nulla, cioè esiste $a \in F$ tale che $c_1\varphi_1(a) + \cdots + c_n\varphi_n(a) \neq 0$.*

Dimostrazione: Supponiamo per assurdo che esistano $c_1, \ldots, c_n \in K$ non tutti nulli per i quali risulti $c_1\varphi_1(x) + \cdots + c_n\varphi_n(x) = 0$ per ogni $x \in F$ e sia $s \geq 1$ il minimo numero possibile di coefficienti non nulli che è possibile scegliere tra $c_1, \ldots, c_n$. Dunque, a meno dell'ordine, possiamo supporre che $c_1, \ldots, c_s$ siano tutti diversi da zero e che $c_1\varphi_1(x) + \cdots + c_s\varphi_s(x) = 0$ per ogni $x \in F$. Inoltre possiamo supporre che, se $1 \leq r < s$ e $c'_1, \ldots, c'_r$ sono tutti diversi da zero, allora esiste $y \in F$ tale che $c'_1\varphi_1(y) + \cdots + c'_r\varphi_r(y) \neq 0$. Mostriamo che questo porta a una contraddizione.

Se $s = 1$, essendo φ_1 non nullo, non c'è niente da dimostrare; sia perciò $s \geq 2$. Poiché $\varphi_1 \neq \varphi_s$, esiste $z \in F$ tale che $\varphi_1(z) \neq \varphi_s(z)$ (necessariamente $\varphi_1(z) \neq 0$). Considerando l'elemento $zy \in F$, si ottiene:

$$\begin{aligned} &c_1\varphi_1(zy) + c_2\varphi_2(zy) + \cdots + c_s\varphi_s(zy) = \\ &c_1\varphi_1(z)\varphi_1(y) + c_2\varphi_2(z)\varphi_2(y) + \cdots + c_s\varphi_s(z)\varphi_s(y) = 0. \end{aligned}$$

Da cui:

$$\begin{aligned} &\varphi_1(z)0 - 0 = \\ &\varphi_1(z)[c_1\varphi_1(y) + c_2\varphi_2(y) + \cdots + c_s\varphi_s(y)] - \\ &[c_1\varphi_1(z)\varphi_1(y) + c_2\varphi_2(z)\varphi_2(y) + \cdots + c_s\varphi_s(z)\varphi_s(y)] = \\ &c_2(\varphi_1(z) - \varphi_2(z))\varphi_2(y) + \cdots + c_s(\varphi_1(z) - \varphi_s(z))\varphi_s(y) = 0. \end{aligned}$$

Poiché $\varphi_1(z) - \varphi_s(z) \neq 0$, quest'ultima espressione è del tipo $c'_1\varphi_1(y) + \cdots + c'_r\varphi_r(y)$ con $r \leq s-1$ e $c'_1, \ldots, c'_r$ tutti non nulli; dunque non è possibile che

essa sia uguale a zero. Ne segue che deve esistere un elemento $a \in F$ tale che $c_1\varphi_1(a) + \cdots + c_n\varphi_n(a) \neq 0$.

Un isomorfismo $\varphi : K \longrightarrow K$ si dice un *automorfismo* di K. È facile verificare che l'insieme degli automorfismi di K è un gruppo (generalmente non commutativo) rispetto alla composizione di funzioni. Tale gruppo si indica con $\mathrm{Aut}(K)$.

Esempi

3.3. Se F è un campo numerico e φ è un isomorfismo di F in $\mathbb{C}$ allora $\varphi(x) = x$, per ogni $x \in \mathbb{Q}$.

3.4. Se $F = \mathbb{Q}$, oppure $F = \mathbb{F}_p$, l'unico automorfismo di F è l'identità.

3.5. L'unico automorfismo del campo reale $\mathbb{R}$ è l'identità. Per vedere questo, mostriamo intanto che ogni automorfismo φ di $\mathbb{R}$ mantiene necessariamente l'ordinamento naturale.

Siano $r, s \in \mathbb{R}$ tali che $r \geq s$, ovvero $r - s \geq 0$. Allora

$$\varphi(r) - \varphi(s) = \varphi(r - s) = \varphi((\sqrt{r - s})^2) = \varphi(\sqrt{r - s})^2 \geq 0,$$

da cui $\varphi(r) \geq \varphi(s)$.

Per l'Esempio 3.3, l'automorfismo φ è l'identità su $\mathbb{Q}$. Sia ora r un numero reale irrazionale e siano $(a_n)_{n\geq 1}$ e $(b_n)_{n\geq 1}$ due successioni di numeri razionali che approssimano r per difetto e per eccesso rispettivamente. Poiché $a_n < r < b_n$, si ottiene $\varphi(a_n) = a_n < \varphi(r) < b_n = \varphi(b_n)$, per ogni $n \geq 1$, e allora, per n tendente all'infinito, risulta $\varphi(r) = r$.

3.6. L'applicazione di coniugio $\mathbb{C} \longrightarrow \mathbb{C}$ definita da $a + bi \mapsto a - bi$, per ogni $a, b \in \mathbb{R}$, è un automorfismo di $\mathbb{C}$. Dunque $\mathrm{Aut}(\mathbb{C}) \neq \{id\}$. Vedremo nel Paragrafo 17 che $\mathbb{C}$ ha infiniti automorfismi.

ESERCIZI

3.1. Mostrare che, se $\varphi : F \longrightarrow K$ è un omomorfismo di campi non nullo, allora $\varphi(1_F) = 1_K$ e $\varphi(x^{-1}) = \varphi(x)^{-1}$, per ogni $x \in F \setminus \{0\}$.

3.2. Mostrare che, se K è un campo, $\mathrm{Aut}(K)$ è un gruppo rispetto alla composizione di funzioni.

3.3. Mostrare che, se K è un campo di caratteristica prima p, l'applicazione $K \longrightarrow K$ definita da $x \mapsto x^{p^s}$ è un omomorfismo di campi, per ogni $s \geq 1$ (*Suggerimento*: Usare l'Esercizio 2.2).

Mostrare inoltre con un esempio che, se K non è finito, tale omomorfismo non è necessariamente un automorfismo di K (*Suggerimento*: Considerare il campo $K := \mathbb{F}_p(X)$).

3.4. Stabilire se l'applicazione $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$, definita da $a + b\sqrt{2} \mapsto a + b\sqrt{3}$, è un omomorfismo di campi.

3.5. Siano A e A' due domini con campo dei quozienti K e K' rispettivamente. Mostrare che, se $f : A \longrightarrow A'$ è un isomorfismo di anelli, allora l'applicazione $\varphi : K \longrightarrow K'$ definita da $\varphi(\frac{a}{b}) = \frac{f(a)}{f(b)}$ è un isomorfismo di campi.

3.6. Mostrare direttamente, senza usare la nozione di ideale, che se $\varphi : F \longrightarrow K$ è un omomorfismo di campi ed esiste un elemento non nullo $x \in F$ tale che $\varphi(x) = 0$, allora φ è l'omomorfismo nullo.

4 Ampliamenti di Campi

Un campo K si dice un *ampliamento* del campo F se esiste un isomorfismo di F in K, cioè se K contiene un sottocampo isomorfo a F. In particolare, se F è un sottocampo di K, allora K è un ampliamento di F. Per semplicità di notazione, se K è un ampliamento di F, identificando F con la sua immagine isomorfa in K, scriveremo semplicemente $F \subseteq K$.

Esempi

4.1. Ogni campo K è un ampliamento del suo sottocampo fondamentale. Precisamente K ha caratteristica zero se e soltanto se è un ampliamento di $\mathbb{Q}$ e K ha caratteristica finita uguale a p se e soltanto se è un ampliamento di $\mathbb{F}_p$.

4.2. Ogni campo numerico è un ampliamento di $\mathbb{Q}$.

4.3. Il campo $F(\mathbf{X})$ delle funzioni razionali nell'insieme di indeterminate indipendenti $\mathbf{X} = \{X_i\}_{i \in I}$ su F è un ampliamento di F.

Se K è un campo e S è un sottoinsieme di K, l'intersezione di tutti i sottocampi di K contenenti S è il più piccolo sottocampo di K contenente S. Esso si chiama il *sottocampo di K generato da S* e si indica con $\langle S \rangle$. Poiché ogni sottocampo di K contiene il sottocampo fondamentale $\mathbb{F}$ di K, si vede subito che il sottocampo $\langle S \rangle$ di K coincide con il sottocampo $\langle \mathbb{F} \cup S \rangle$. più in generale, se F è un qualsiasi sottocampo di K, si può considerare il sottocampo di K generato da $F \cup S$, ovvero il più piccolo sottocampo di K contenente sia F che S. Esso si dice l'*ampliamento di F in K generato da S* e si indica con $F(S)$. Segue subito dalla definizione che, se F è un sottocampo di K e S, T sono sottoinsiemi di K, allora $F(S) = F(T)$ se e soltanto se $S \subseteq F(T)$ e $T \subseteq F(S)$.

Ci interessa in modo particolare il caso in cui $S = \{\alpha_1, \ldots, \alpha_n\}$ sia un sottoinsieme finito di K; in questo caso si pone $F(S) := F(\alpha_1, \ldots, \alpha_n)$. Se $F \subseteq K$ è un ampliamento di campi e $\mathbf{X} = \{X_1, \ldots, X_n\}$, $n \geq 1$, è un insieme di indeterminate indipendenti su K, allora $F[\mathbf{X}] \subseteq K[\mathbf{X}]$. Posto $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in K^n$, indichiamo con $f(\boldsymbol{\alpha})$ il valore del polinomio $f(\mathbf{X}) \in F[\mathbf{X}]$ calcolato in $\boldsymbol{\alpha}$, ovvero l'elemento di K che si ot-

tiene sostituendo ordinatamente gli elementi $\alpha_1, \ldots, \alpha_n$ alle indeterminate $X_1, \ldots, X_n$.

Per ogni $\boldsymbol{\alpha} \in K^n$, si può allora definire l'applicazione $v_{\boldsymbol{\alpha}}$ che ad ogni polinomio $f(\mathbf{X})$ di $F[\mathbf{X}]$ associa il suo valore in $\boldsymbol{\alpha}$, cioè

$$v_{\boldsymbol{\alpha}} : F[\mathbf{X}] \longrightarrow K, \quad f(\mathbf{X}) \mapsto f(\boldsymbol{\alpha}).$$

È facile verificare che

$$(f+g)(\boldsymbol{\alpha}) = f(\boldsymbol{\alpha}) + g(\boldsymbol{\alpha}) \quad \text{e} \quad (fg)(\boldsymbol{\alpha}) = f(\boldsymbol{\alpha})g(\boldsymbol{\alpha});$$

dunque l'applicazione $v_{\boldsymbol{\alpha}}$ è un omomorfismo di anelli. Denotiamo con $F[\boldsymbol{\alpha}]$ l'immagine di $v_{\boldsymbol{\alpha}}$, cioè

$$F[\boldsymbol{\alpha}] := \{f(\boldsymbol{\alpha});\, f(\mathbf{X}) \in F[\mathbf{X}]\} = \left\{ \sum c_{k_1 \ldots k_n} \alpha_1^{k_1} \cdots \alpha_n^{k_n} \,;\, c_{k_1 \ldots k_n} \in F;\, k_i \geq 0 \right\}.$$

$F[\boldsymbol{\alpha}]$ è un sottoanello di K e il suo campo dei quozienti è

$$F(\boldsymbol{\alpha}) := \left\{ \frac{f(\boldsymbol{\alpha})}{g(\boldsymbol{\alpha})} \,;\, f(\mathbf{X}), g(\mathbf{X}) \in F[\mathbf{X}]\,,\, g(\boldsymbol{\alpha}) \neq 0 \right\}.$$

Se $f(\mathbf{X}) := c \in F$ è un polinomio costante, esso assume valore c in $\boldsymbol{\alpha}$, perciò $F \subseteq F[\boldsymbol{\alpha}]$. Inoltre, poiché α_i è il valore che assume il polinomio X_i calcolato in $\boldsymbol{\alpha}$, allora $\{\alpha_1, \ldots, \alpha_n\} \subseteq F[\boldsymbol{\alpha}]$. D'altra parte, per chiusura additiva e moltiplicativa, ogni sottoanello di K contenente sia F che $\{\alpha_1, \ldots, \alpha_n\}$ contiene $F[\boldsymbol{\alpha}]$. Ne segue che il minimo sottocampo di K contenente sia F che l'insieme $\{\alpha_1, \ldots, \alpha_n\}$ è il campo dei quozienti $F(\boldsymbol{\alpha}) := F(\alpha_1, \ldots, \alpha_n)$ di $F[\boldsymbol{\alpha}]$. In altre parole, $F(\alpha_1, \ldots, \alpha_n)$ è costituito dai valori in $\alpha_1, \ldots, \alpha_n$ delle funzioni razionali su F. È evidente che $F(\boldsymbol{\alpha}) = F$ se e soltanto se $\alpha_i \in F$ per $i = 1, \ldots, n$.

Si dice che K è un ampliamento *finitamente generato* di F se esistono $\alpha_1, \ldots, \alpha_n \in K$, $n \geq 1$, tali che $K = F(\alpha_1, \ldots, \alpha_n)$; si dice che K è un *ampliamento semplice* di F se esiste $\alpha \in K$ tale che $K = F(\alpha)$.

Ogni ampliamento finitamente generato si può costruire come una successione finita di ampliamenti semplici. Infatti, se $\alpha_1, \ldots, \alpha_n \in K$, posto

$$F_0 := F \quad \text{e} \quad F_i := F_{i-1}(\alpha_i) \text{ per } i = 1, \ldots, n,$$

risulta

$$F \subseteq F_1 = F(\alpha_1) \subseteq \ldots \subseteq F_i = F(\alpha_1, \ldots, \alpha_i) \subseteq \ldots \subseteq F_n = F(\alpha_1, \ldots, \alpha_n).$$

Osserviamo che tale costruzione non dipende dalla scelta dell'ordine degli α_i, per la commutatività della moltiplicazione.

Daremo in seguito condizioni su $\alpha_1, \ldots, \alpha_n$ sufficienti ad assicurare che l'ampliamento $F(\alpha_1, \ldots, \alpha_n)$ sia semplice, ovvero che esista un elemento

$\alpha \in K$ (detto *elemento primitivo*) tale che $F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$ (Teorema 13.8).

Se F è un campo e $f(X) := c_0 + c_1X + \cdots + c_nX^n \in F[X]$, si può considerare il campo $\mathbb{F}(c_0, c_1, \ldots, c_n)$, dove $\mathbb{F}$ è il sottocampo fondamentale di F. Questo è il più piccolo sottocampo di F contenente i coefficienti di $f(X)$ e si dice il *campo di definizione* (o *di razionalità*) di $f(X)$.

Il Teorema Fondamentale dell'Algebra asserisce che ogni polinomio $f(X)$ a coefficienti in un campo numerico F ha tutte le sue radici in $\mathbb{C}$. Questo teorema fu dimostrato per la prima volta in modo completo da C. F. Gauss nella sua Tesi di Laurea del 1797 e pubblicato nel 1799 (vedi il successivo Esempio 12.9). Se le radici complesse distinte di $f(X)$ sono $\alpha_1, \ldots, \alpha_s$, $s \leq n := \deg(f(X)$, il campo $F(\alpha_1, \ldots, \alpha_s)$ è il più piccolo campo numerico contenente F su cui $f(X)$ si spezza in fattori lineari. Infatti su $F(\alpha_1, \ldots, \alpha_s)$ risulta $f(X) = c_n(X - \alpha_1)^{m_1} \ldots (X - \alpha_s)^{m_s}$, dove m_i è la *molteplicità* della radice α_i e $m_1 + \cdots + m_s = n$. Il campo $F(\alpha_1, \ldots, \alpha_s)$ si dice il *campo di spezzamento* di $f(X)$ su F.

Vedremo nel Paragrafo 8 che, se F è un campo qualsiasi e $f(X) \in F[X]$, si può sempre costruire un campo minimale contenente F in cui $f(X)$ abbia tutte le sue radici.

Esempi

4.4. Il sottocampo fondamentale di un campo K è il sottocampo generato da $S = \{1_K\}$.

4.5. L'ampliamento di $\mathbb{Q}$ in $\mathbb{C}$ generato da $\{i\}$ è $\mathbb{Q}(i) = \{a + bi\,;\, a, b \in \mathbb{Q}\}$.

4.6. Se F è un qualsiasi campo numerico e d è un numero intero privo di fattori quadratici, allora

$$F(\sqrt{d}) = \left\{a + b\sqrt{d}\,;\, a, b \in F\right\}.$$

L'inverso di $a + b\sqrt{d}$ è $\frac{a-b\sqrt{d}}{a^2-db^2}$.

4.7. $\mathbb{C}$ è un ampliamento semplice di $\mathbb{R}$. Infatti risulta

$$\mathbb{C} := \{a + bi\,;\, a, b \in \mathbb{R}\} = \mathbb{R}(i).$$

4.8. Per costruire $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, si può costruire prima

$$F := \mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\right\}.$$

Poiché $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (altrimenti si avrebbe $\sqrt{3} = a + b\sqrt{2}$ e, quadrando, $\sqrt{2}$ sarebbe razionale), allora $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e risulta

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = F(\sqrt{3}) &= \left\{a' + b'\sqrt{3}\,;\, a', b' \in F\right\} \\ &= \left\{c_0 + c_1\sqrt{2} + c_2\sqrt{3} + c_3\sqrt{2}\sqrt{3}\,;\, c_i \in \mathbb{Q}\right\}.\end{aligned}$$

Allo stesso risultato si giunge costruendo prima

$$F' := \mathbb{Q}(\sqrt{3}) = \left\{ a + b\sqrt{3}\,;\, a, b \in \mathbb{Q} \right\}$$

e successivamente

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = F'(\sqrt{2}) &= \left\{ a' + b'\sqrt{2}\,;\, a', b' \in F' \right\} \\ &= \left\{ c_0 + c_1\sqrt{3} + c_2\sqrt{2} + c_3\sqrt{3}\sqrt{2}\,;\, c_i \in \mathbb{Q} \right\}. \end{aligned}$$

4.9. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è un ampliamento semplice di $\mathbb{Q}$. Infatti risulta

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha); \quad \alpha := \sqrt{2} + \sqrt{3}.$$

Per vedere ciò, osserviamo che chiaramente $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Viceversa, si ha:

$$2 = (\alpha - \sqrt{3})^2 = \alpha^2 - 2\sqrt{3}\alpha + 3,$$

da cui

$$\sqrt{3} = (\alpha^2 + 1)(2\alpha)^{-1} \in \mathbb{Q}(\alpha) \quad \text{e} \quad \sqrt{2} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha).$$

Segue che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$.

4.10. Se $\mathbf{X} = \{X_1, \ldots, X_n\}$, $n \geq 2$, è un insieme di indeterminate algebricamente indipendenti su F, il campo delle funzioni razionali $F(\mathbf{X}) := F(X_1, \ldots, X_n)$ è un ampliamento finitamente generato di F che non è semplice; altrimenti esisterebbe una relazione algebrica tra le indeterminate X_i.

4.11. Il campo di definizione del polinomio $X^5 - \sqrt{3}X^2 + (\sqrt{2} + 1)$ è $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

4.12. Il campo di spezzamento del polinomio $X^2 - 2\sqrt{2}X + 3$ sul suo campo di definizione $\mathbb{Q}(\sqrt{2})$ è $\mathbb{Q}(\sqrt{2}, i)$, mentre il suo campo di spezzamento su $\mathbb{R}$ è $\mathbb{R}(i) = \mathbb{C}$.

Se $F \subseteq K$ è un ampliamento di campi e L è un ampliamento di F contenuto in K, si dice che L è un *campo intermedio* dell'ampliamento.

Se L_1 e L_2 sono due campi intermedi, l'ampliamento di F in K generato da $L_1 \cup L_2$ si dice il *composto di* L_1 *e* L_2 *in* K. Esso è per definizione il più piccolo sottocampo di K contenente L_1 e L_2.

Se $L_1 = F(S)$ e $L_2 = F(T)$, allora, come si verifica facilmente, il composto di di L_1 e L_2 è $F(S \cup T)$. In particolare, se $L_1 = F(\alpha)$ e $L_2 = F(\beta)$ sono due ampliamenti semplici di F in K, allora il composto di di L_1 e L_2 è $F(\alpha, \beta)$.

ESERCIZI

4.1. Mostrare che $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{6}) = \mathbb{Q}(\sqrt{3},\sqrt{6})$.

4.2. Stabilire se $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i\sqrt{2})$.

4.3. Mostrare che, se F è un qualsiasi campo numerico e d è un numero intero privo di fattori quadratici, allora $F(\sqrt{d}) = F(a+b\sqrt{d}) = F(c\sqrt{d})$, per ogni a, b, $c \in F$.

4.4. Mostrare che, se F è un qualsiasi campo numerico e a, b, sono due interi privi di fattori quadratici, allora $F(\sqrt{a},\sqrt{b}) = F(\sqrt{a}+\sqrt{b})$.

4.5. Costruire esplicitamente i campi:

$$\mathbb{Q}(\sqrt{3},\sqrt{5})\,,\ \mathbb{Q}(i,\sqrt{2})\,,\ \mathbb{Q}(\sqrt{3},1+\sqrt{3}),\ \mathbb{Q}(i\sqrt{2})\,,\ \mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7})\,.$$

4.6. Determinare l'inverso di $4+2\sqrt[3]{2}+\sqrt[3]{4}$ in $\mathbb{Q}(\sqrt[3]{2})$ (*Suggerimento*: Razionalizzare usando l'identità $(a^3-b^3) = (a-b)(a^2+ab+b^2)$).

4.7. Mostrare che il campo di matrici $\mathcal{M}_{a,b}(F)$ definito nell'Esempio 1.4 è un ampliamento di F.

4.8. Sia $F \subseteq K$ un ampliamento di campi e sia S un sottoinsieme di K. Mostrare che:

$$F(S) = \left\{ \frac{\sum a_{k_1\dots k_n}\alpha_1^{k_1}\dots\alpha_n^{k_n}}{\sum b_{h_1\dots h_m}\beta_1^{h_1}\dots\beta_m^{h_m}} \right\};$$

dove n, $m \geq 1$, α_i, $\beta_j \in S$, $a_{k_1\dots k_n}$, $b_{h_1\dots h_m} \in F$ e k_i, $h_j \geq 0$ per $1 \leq i \leq n$, $1 \leq j \leq m$.

4.9. Sia $f(X)$ un polinomio di secondo grado a coefficienti in un campo numerico F e $\alpha \in \mathbb{C}$ una sua radice. Mostrare che $F(\alpha)$ è il campo di spezzamento di $f(X)$ su F.

4.10. Mostrare che il campo di spezzamento del polinomio X^4+2X^2+9 su $\mathbb{Q}$ è $\mathbb{Q}(i\sqrt{2})$.

4.11. Mostrare che i polinomi X^4-9 e X^4-2X^2-3 hanno lo stesso campo di spezzamento su $\mathbb{Q}$.

4.12. Determinare il campo di spezzamento dei seguenti polinomi sul loro campo di definizione:

$$X^3-1\,;\ X^3+1\,;\ X^4-2; X^4-2X^2+49\,;\ X^5-1\,;\ X^5-3X^3+3X^2-9\,;$$

$$X^3-(6\sqrt{5}+1)X^2+(6\sqrt{5}+47)X-47\,;\ 2X^3-(2\sqrt{3}+1)X^2+(\sqrt{3}+1)X-\sqrt{3}.$$

4.13. Sia F un campo numerico e sia $a \in F$. Determinare il campo di spezzamento su F del polinomio X^n-a, dove $n \geq 2$.

4.14. Sia $f(X)$ un polinomio monico a coefficienti numerici e siano α_1, $\dots$, α_s le sue radici complesse. Mostrare che il campo $\mathbb{Q}(\alpha_1,\dots,\alpha_s)$ contiene i coefficienti di $f(X)$ e dunque è il campo di spezzamento di $f(X)$ sul suo campo di definizione.

4.15. Sia $f(X) \in \mathbb{Q}[X]$ e sia L il suo campo di spezzamento su $\mathbb{Q}$. Mostrare che, se K è un altro campo numerico, il campo di spezzamento di $f(X)$ su K è il composto di L e K.

4.16. Sia F un campo numerico e siano $f(X), g(X) \in F[X]$. Indichiamo con L_1 e L_2 i campi di spezzamento su F di $f(X)$ e $g(X)$ rispettivamente. Mostrare che il composto di L_1 e L_2 è il campo di spezzamento su F del polinomio $f(X)g(X)$.

5 Elementi Algebrici e Trascendenti

Sia $F \subseteq K$ un ampliamento di campi. Un elemento $\alpha \in K$ di dice *algebrico* su F se esso è radice di qualche polinomio non nullo $f(X)$ a coefficienti in F. Altrimenti α si dice *trascendente* su F. Se α è algebrico su F allora lo è anche su ogni campo intermedio dell'ampliamento $F \subseteq K$.

Un numero complesso (rispettivamente reale) algebrico su $\mathbb{Q}$ si dice semplicemente un *numero complesso* (rispettivamente *reale*) *algebrico*. Un numero trascendente su $\mathbb{Q}$ si dice semplicemente un *numero trascendente*.

L'esistenza dei numeri trascendenti fu dimostrata da J. Liouville nel 1844. Egli provò in particolare la trascendenza del numero reale

$$\sum_{k\geq 1} \frac{1}{10^{k!}} = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^{3!}} + \cdots + \frac{1}{10^{n!}} + \cdots = 0,1100010000\ldots$$

Una dimostrazione molto elegante dell'esistenza dei numeri trascendenti fu poi data da G. F. Cantor nel 1874. Essa si basa sul fatto che la cardinalità dell'insieme dei numeri reali è strettamente maggiore di quella dell'insieme dei numeri reali algebrici.

Esempi

5.1. Ogni elemento $\alpha \in F$ è algebrico su F, essendo radice del polinomio $X - \alpha \in F[X]$.

5.2. Se d è un intero positivo, allora $\sqrt[n]{d}$ è un numero reale algebrico, perché annulla il polinomio $X^n - d \in \mathbb{Q}[X]$.

5.3. L'unità immaginaria i è un numero complesso algebrico, essendo radice del polinomio $X^2 + 1 \in \mathbb{Q}[X]$.

5.4. La trascendenza del numero di Nepero

$$e := \sum_{k\geq 1} \frac{1}{k!} = 1 + \frac{1}{2} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \ldots,$$

base del logaritmo naturale, fu congetturata da L. Euler nel 1784 e dimostrata da C. Hermite nel 1873.

F. Lindemann dimostrò nel 1882 che e^a è trascendente per ogni numero algebrico $a \neq 0$. Da questo risultato segue che, se x è un numero reale algebrico diverso da 0 e 1, allora $\ln(x)$ è trascendente.

5.5. La trascendenza di π fu congetturata da A. M. Legendre nel 1806 e dimostrata da F. Lindemann nel 1882. Essa implica che il problema di quadrare il cerchio non è risolubile con riga e compasso.

5.6. Se a è un numero algebrico diverso da 0 e 1 e b è un numero irrazionale algebrico, allora a^b è trascendente; questo fatto fu congetturato da D. Hilbert e dimostrato da A. O. Gelfond e T. Schneider nel 1934. Ad esempio $2^{\sqrt{2}}$ è trascendente (C. Siegel, 1930).

Un'applicazione di questo teorema mostra che e e^π è trascendente. Infatti, ricordando che ogni numero reale x soddisfa la formula

$$e^{ix} = \cos(x) + i\sin(x)$$

(L. Euler, 1746), risulta $e^\pi = i^{-2i}$, dove sia i che $-2i$ sono algebrici. Non è ancora noto se più generalmente a^b è trascendente quando lo sono a e b. Ad esempio non è noto se π^e è trascendente.

A. Baker ha dimostrato nel 1966 che il prodotto di un numero finito di numeri trascendenti del tipo a^b, dove a è un numero algebrico diverso da 0 e 1 e b è un numero irrazionale algebrico, è un numero trascendente. Tuttavia non è noto se $e\pi$ è trascendente.

5.7. Ogni indeterminata X su un campo F è trascendente su F (Principio di Uguaglianza tra Polinomi).

Se $F \subseteq K$ è un ampliamento di campi e $\alpha \in K$ è algebrico su F, per il Principio del Buon Ordinamento dei numeri naturali, esiste un polinomio di grado minimo annullato da α.

Proposizione 5.1 *Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Se $m(X) \in F[X]$ è un polinomio di grado minimo annullato da α, allora $m(X)$ divide ogni altro polinomio annullato da α. In particolare due polinomi di grado minimo annullati da α sono associati.*

Dimostrazione: Sia $f(X) \in F[X]$ un polinomio annullato da α. Dividendo $f(X)$ per $m(X)$ si ottiene:

$$f(X) = m(X)q(X) + r(X) \quad \text{con} \quad \deg r(X) < \deg m(X) \ \text{ oppure } \ r(X) = 0$$

Se $r(X) \neq 0$, calcolando in α, risulta $r(\alpha) = 0$, il che è impossibile per la minimalità del grado di $m(X)$. Dunque $r(X) = 0$ e $m(X)$ divide $f(X)$.

Proposizione 5.2 *Sia α algebrico su F e sia $m(X) \in F[X]$ un polinomio annullato da α. Allora $m(X)$ è un polinomio di grado minimo annullato da α se e soltanto se $m(X)$ è irriducibile su F.*

Dimostrazione: Sia $m(X)$ un polinomio di grado minimo annullato da α e sia $m(X) = g(X)h(X)$. Allora $m(\alpha) = g(\alpha)h(\alpha) = 0$, da cui $g(\alpha) = 0$ oppure $h(\alpha) = 0$. Per la minimalità del grado di $m(X)$, nel primo caso $m(X)$ e $g(X)$ sono associati (Proposizione 5.1), nel secondo caso lo sono $m(X)$ e $h(X)$. Dunque $m(X)$ è irriducibile.

Viceversa, se $m(X)$ è annullato da α, allora $m(X)$ è diviso da un polinomio di grado minimo annullato da α (Proposizione 5.1). Perciò, se $m(X)$ è irriducibile, esso ha grado minimo.

Se α è algebrico su F, per quanto appena visto, esiste un unico polinomio $m(X) \in F[X]$ annullato da α che sia monico e di grado minimo (Proposizione 5.1). Esso si dice il *polinomio minimo di α su F* ed è irriducibile su F (Proposizione 5.2). Il grado di $m(X)$ si dice anche il *grado di α su F*. Dunque diremo che α è *algebrico di grado n* su F se il grado del suo polinomio minimo su F è n.

Notiamo che, se $f(X)$ è un qualsiasi polinomio di $F[X]$ annullato da α, allora il polinomio minimo di α su F è il fattore monico irriducibile di $f(X)$ annullato da α. In particolare, ogni polinomio monico irriducibile a coefficienti numerici è il polinomio minimo di ogni sua radice complessa.

Inoltre, se $F \subseteq L \subseteq K$ sono ampliamenti di campi e $\alpha \subseteq K$ è algebrico su F, allora il suo grado su F è maggiore uguale al suo grado su L. Infatti il polinomio minimo di α su F può essere riducibile in $L[X]$ e in questo caso è diviso propriamente in $L[X]$ dal polinomio minimo di α su L.

Esempi

5.8. Se $F \subseteq K$ e $\alpha \in K$, α è algebrico di grado 1 su F se e soltanto se $\alpha \in F$.

5.9. Se $F \subseteq K$ e $\alpha \in K \setminus F$ annulla un polinomio di secondo grado su F, allora esso ha grado 2 su F.

5.10. Se p è un numero primo e $n \geq 2$, $\sqrt[n]{p}$ ha grado n su $\mathbb{Q}$, infatti esso è radice del polinomio $X^n - p$, che è irriducibile su $\mathbb{Q}$ per il Criterio di Eisenstein.

5.11. Il numero $\alpha := \sqrt{2} + \sqrt{3}$ ha grado 2 su $\mathbb{Q}(\sqrt{2})$ e grado 4 su $\mathbb{Q}$. Infatti $\alpha \notin \mathbb{Q}(\sqrt{2})$ perché $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (Esempio 4.8). Inoltre risulta

$$3 = (\alpha - \sqrt{2})^2 = \alpha^2 - 2\sqrt{2}\alpha + 2,$$

per cui α è radice del polinomio $X^2 - 2\sqrt{2}X - 1$ a coefficienti in $\mathbb{Q}(\sqrt{2})$. Infine si ha

$$2\sqrt{2}\alpha = \alpha^2 - 1 \quad \text{da cui} \quad 8\alpha^2 = \alpha^4 - 2\alpha^2 + 1.$$

Ne segue che α è anche radice del polinomio a coefficienti razionali $X^4 - 10X^2 + 1$, che è irriducibile su $\mathbb{Q}$ (perché non ha radici razionali e non ha

fattori di secondo grado a coefficienti razionali). Notiamo che in $\mathbb{Q}(\sqrt{2})[X]$ risulta

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1).$$

5.12. Se $\alpha := a + bi \in \mathbb{C} \setminus \mathbb{R}$, allora α è algebrico di grado 2 su $\mathbb{R}$. Infatti esso è radice del polinomio a coefficienti reali $f(X) := X^2 - 2aX + (a^2 + b^2)$.

ESERCIZI

5.1. Sia F un campo e $\alpha = \frac{X^3}{X+1} \in F(X)$. Mostrare che α è trascendente su F e X è algebrico su $F(\alpha)$. Determinare inoltre il polinomio minimo di X su $F(\alpha)$.

5.2. Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$. Mostrare che, se α è trascendente su F, allora $f(\alpha)$ è trascendente su F, per ogni polinomio $f(X) \in F[X]$.

5.3. Mostrare che ogni funzione razionale non costante $\varphi(X) \in F(X)$ è trascendente sul campo F.

5.4. Mostrare che π è algebrico su $\mathbb{Q}(\pi^2)$.

5.5. Mostrare che $e^{i\pi}$ è algebrico su $\mathbb{Q}$.

5.6. Mostrare che $\log_{10}(2)$ è un numero irrazionale. Usando il Teorema di Gelfond-Schneider (Esempio 5.6) mostrare poi che esso è trascendente.

5.7. Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Mostrare che l'insieme dei polinomi $f(X) \in F[X]$ annullati da α è un ideale di $F[X]$.

5.8. Sia α una radice del polinomio $X^4 + 1$. Mostrare che α ha grado 4 su $\mathbb{Q}$ ma ha grado 2 su $\mathbb{R}$.

5.9. Mostrare che i seguenti numeri sono algebrici e determinare il loro polinomio minimo su $\mathbb{Q}$ e su $\mathbb{Q}(\sqrt{2})$:

$$\frac{3-\sqrt{2}}{2},\ 1 + 3\sqrt{2},\ i\sqrt[4]{3},\ \frac{\sqrt{2}}{2}(1+i),\ \sqrt{2} + \sqrt{5},\ \sqrt{3} + 3\sqrt{2}.$$

5.10. Mostrare che l'elemento $M_{0,1} \in \mathcal{M}_{a,b}(F)$ definito nell'Esempio 1.4 è algebrico di grado 2 su F.

6 Ampliamenti Semplici

Sia $K := F(\alpha)$ un ampliamento semplice del campo F e sia $v_\alpha : F[X] \longrightarrow K$ l'omomorfismo di anelli definito da $f(X) \mapsto f(\alpha)$. Il nucleo di v_α è l'ideale di $F[X]$ costituito dai polinomi che si annullano in α; dunque esso è non nullo se e soltanto se α è algebrico su F. In questo caso inoltre $f(X) \in \mathrm{Ker}(v_\alpha)$ se e soltanto se $f(X)$ è un multiplo del polinomio minimo $m(X)$ di α su F (Proposizione 5.1). Ne segue che $\mathrm{Ker}(v_\alpha) = \langle m(X) \rangle$ è l'ideale principale di $F[X]$ generato dal polinomio $m(X)$. Questa osservazione ci permette di determinare la struttura di tutti gli ampliamenti semplici di F.

Teorema 6.1 (L. Kronecker, 1882) *Sia $K = F(\alpha)$ un ampliamento semplice del campo F.*

(*a*) *Se α è trascendente su F, allora K è isomorfo al campo $F(X)$ delle funzioni razionali in una indeterminata su F.*

(*b*) *Se α è algebrico su F e $m(X)$ è il suo polinomio minimo su F. Allora K è isomorfo all'anello quoziente $\frac{F[X]}{\langle m(X)\rangle}$.*

Dimostrazione: Sia $v_\alpha : F[X] \longrightarrow F(\alpha)$ l'omomorfismo di anelli definito da $f(X) \mapsto f(\alpha)$.

(*a*) Se α è trascendente su F, allora $\mathrm{Ker}(v_\alpha) = (0)$. Ne segue che v_α è iniettivo e l'immagine $F[\alpha]$ di v_α è un dominio isomorfo a $F[X]$. Perciò i rispettivi campi dei quozienti $F(\alpha)$ e $F(X)$ sono isomorfi (Esercizio 3.5).

(*b*) Se α è algebrico su F, allora $\mathrm{Ker}(v_\alpha) = \langle m(X)\rangle$ (Proposizione 5.1) e dunque, per il Teorema di Omomorfismo, $\mathrm{Im}(v_\alpha) = F[\alpha]$ è canonicamente isomorfo all'anello quoziente $\frac{F[X]}{\langle m(X)\rangle}$. Poiché $m(X)$ è irriducibile su F (Proposizione 5.2), tale quoziente è un campo. Dunque anche $F[\alpha]$ è un campo e, poiché esso contiene α ed è contenuto in $F(\alpha)$, coincide con $F(\alpha)$.

L'ampliamento semplice $F(\alpha)$ di F si dice *algebrico* (rispettivamente *trascendente*) se α è algebrico (rispettivamente trascendente) su F.

Corollario 6.2 *Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Allora α è algebrico su F se e soltanto se $F[\alpha] = F(\alpha)$. In questo caso, se α ha grado n, allora*

$$F(\alpha) = \left\{ c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \,;\, c_i \in F \right\}.$$

Dimostrazione: Per quanto visto nella dimostrazione del teorema precedente, se α è algebrico su F, allora $\mathrm{Im}(v_\alpha) = F[\alpha]$ è canonicamente isomorfo al campo $\frac{F[X]}{\langle m(X)\rangle}$. Dunque $F[\alpha] = F(\alpha)$. Altrimenti, se α è trascendente su F, $\mathrm{Im}(v_\alpha) = F[\alpha]$ è canonicamente isomorfo all'anello dei polinomi $F[X]$ e non è un campo.

Se il polinomio minimo $m(X)$ di α su F ha grado n, allora gli elementi non nulli dell'anello quoziente $\frac{F[X]}{\langle m(X)\rangle}$ possono essere rappresentati dai polinomi di grado minore di n. Infatti, se $f(X) = m(X)q(X) + r(X)$, allora $f(X)$ e $r(X)$ appartengono alla stessa classe modulo $m(X)$. Per concludere, basta allora osservare che, per la dimostrazione del Teorema 6.1, l'applicazione $\frac{F[X]}{\langle m(X)\rangle} \longrightarrow F[\alpha]$ definita da $r(X) + \langle m(X)\rangle \mapsto r(\alpha)$ è un isomorfismo di campi.

Quando α è algebrico di grado n su F, con polinomio minimo $m(X)$, il Corollario 6.2. ci fornisce un metodo per determinare l'inverso di un elemento non nullo $\beta \in F(\alpha)$.

Sia infatti $\beta := c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \in F(\alpha)$ e si consideri il corrispondente polinomio $r(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in F[X]$. Poiché $m(X)$ è irriducibile di grado n, allora $r(X)$ e $m(X)$ sono coprimi e l'algoritmo della divisione euclidea ci permette di determinare due polinomi $g(X)$ e $h(X)$ tali che $g(X)r(X) + h(X)m(X) = 1$. Calcolando in α, si ottiene che $g(\alpha)r(\alpha) = g(\alpha)\beta = 1$. Dunque $g(\alpha)$ è l'inverso di β in $F(\alpha)$.

Esempi

6.1. Il polinomio minimo di $\alpha := \sqrt[3]{2}$ su $\mathbb{Q}$ è $X^3 - 2$; perciò risulta $\mathbb{Q}(\alpha) = \{c_0 + c_1\alpha + c_2\alpha^2 \,;\, c_i \in \mathbb{Q}\}$. L'inverso di $\beta := 1 + \alpha + \alpha^2$ in $\mathbb{Q}(\alpha)$ è $\alpha - 1$. Infatti il polinomio corrispondente a β in $\mathbb{Q}[X]$ è $X^2 + X + 1$. Inoltre risulta $X^3 - 2 = (X^2 + X + 1)(X - 1) - 1$ da cui, calcolando in α, si ottiene $\beta(\alpha - 1) = 1$.

6.2. Il polinomio minimo di $\alpha := \sqrt{2} + \sqrt{3}$ su $\mathbb{Q}$ è $X^4 - 10X^2 + 1$ (Esempio 5.11). Se $\beta := \alpha + 1$, allora il polinomio corrispondente a β è $X + 1$ e risulta $X^4 - 10X^2 + 1 = (X + 1)(X^3 - X^2 - 9X - 9) - 8$. Calcolando in α, si ottiene che l'inverso di β in $\mathbb{Q}(\alpha)$ è $\frac{1}{8}(\alpha^3 - \alpha^2 - 9\alpha - 9)$.

Corollario 6.3 *Sia $F \subseteq K$ un ampliamento di campi e siano α, $\beta \in K$ due elementi algebrici su F di grado n che abbiano lo stesso polinomio minimo. Allora l'applicazione $F(\alpha) \longrightarrow F(\beta)$ definita da*

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mapsto c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$$

è un isomorfismo di campi.

Dimostrazione: Per il Teorema 6.1, se $m(X)$ è il polinomio minimo di α e β e $r(X) := c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, allora si hanno due isomorfismi:

$$F(\alpha) \longrightarrow \frac{F[X]}{\langle m(X)\rangle} \longrightarrow F(\beta)$$

definiti da:

$$r(\alpha) \mapsto r(X) + \langle m(X)\rangle \mapsto r(\beta).$$

La loro composizione è l'isomorfismo cercato.

Esempi

6.3. Se ξ è una radice primitiva terza dell'unità, ad esempio $\xi := \frac{-1+i\sqrt{3}}{2}$, allora l'applicazione $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ definita da $r(\sqrt[3]{2}) \mapsto r(\sqrt[3]{2}\xi)$, per ogni polinomio $r(X) \in \mathbb{Q}[X]$ di grado al più uguale a due, è un isomorfismo di campi la cui immagine è $\mathbb{Q}(\sqrt[3]{2}\xi)$; infatti $\sqrt[3]{2}$ e $\sqrt[3]{2}\xi$ hanno lo stesso polinomio minimo $X^3 - 2$ su $\mathbb{Q}$. In particolare i campi $\mathbb{Q}(\sqrt[3]{2})$ e $\mathbb{Q}(\sqrt[3]{2}\xi)$ sono isomorfi. Osserviamo inoltre che $\mathbb{Q}(\sqrt[3]{2})$ è un campo numerico reale, ma $\mathbb{Q}(\sqrt[3]{2}\xi)$ non è reale.

ESERCIZI

6.1. Determinare, per ogni $n \geq 2$, due numeri complessi algebrici α e β di grado n su $\mathbb{Q}$ tali che i campi $\mathbb{Q}(\alpha)$ e $\mathbb{Q}(\beta)$ siano isomorfi ma non uguali.

6.2. Mostrare che $\mathbb{Q}(\pi^2)$ e $\mathbb{Q}(\pi)$ sono due ampliamenti isomorfi di $\mathbb{Q}$ ma $\mathbb{Q}(\pi^2) \subsetneq \mathbb{Q}(\pi)$.

6.3. Costruire esplicitamente i campi:

$$\mathbb{Q}(\pi, 1+\sqrt{2}) \quad \mathbb{Q}(\pi^2, \pi) \quad \mathbb{Q}(\pi, \sqrt{2}, \sqrt{5}) \quad \mathbb{Q}(\sqrt[3]{5}, \sqrt{2}).$$

6.4. Sia $m(X) \in \mathbb{Q}[X]$ un polinomio irriducibile su $\mathbb{Q}$ e sia α una radice complessa di $m(X)$. Determinare l'inverso di β in $\mathbb{Q}(\alpha)$ in ognuno dei seguenti casi:

$$\begin{aligned} &m(X) := X^2 - 5\,, && \beta := \alpha + 1\,; \\ &m(X) := 4X^4 + 5X + 10\,, && \beta := \alpha^3 + \alpha + 1\,; \\ &m(X) := X^3 + 3X^2 + 9X + 6\,, && \beta := \alpha^2. \end{aligned}$$

7 Il Grado di un Ampliamento

Se F è un campo, A è un anello commutativo unitario e $f : F \longrightarrow A$ è un omomorfismo non nullo di anelli, allora A è uno spazio vettoriale su F con la moltiplicazione scalare definita da $xa = f(x)a$, per ogni $x \in F$ e $a \in A$. Dunque, se $F \subseteq K$ è un ampliamento di campi, K è uno spazio vettoriale su F. In questo caso, la dimensione di K su F si indica con $[K : F]$.

Si dice che K è un *ampliamento finito* di F (o che K *è finito su* F) se la sua dimensione su F è finita. In questo caso $[K : F]$ si chiama anche il *grado* di K su F. Se $[K : F]$ è infinito, si dice anche che K ha *grado infinito* su F.

Esempi

7.1. $\mathbb{C}$ è un ampliamento finito di grado due di $\mathbb{R}$. Infatti una base di $\mathbb{C}$ su $\mathbb{R}$ è $\{1, i\}$.

7.2. Ogni campo finito di caratteristica p è un ampliamento finito di $\mathbb{F}_p$ (Paragrafo 10).

7.3. Il campo $\mathcal{M}_{a,b}(F)$ delle matrici $M_{a,b}$ a coefficienti in un campo reale F, definito nell'Esempio 1.4, ha grado due su F. Infatti una base di $\mathcal{M}_{a,b}(F)$ su F è $\{M_{1,0}, M_{0,1}\}$.

7.4. Il campo $F(X)$ delle funzioni razionali nell'indeterminata X sul campo F non è un ampliamento finito di F. Infatti gli elementi 1, X, X^2, $\ldots$, X^n sono linearmente indipendenti su F, per ogni $n \geq 1$ (Principio di Uguaglianza tra Polinomi).

Proposizione 7.1 *Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$.*

(*a*) *Se α è algebrico di grado n su F, allora $[F(\alpha) : F] = n$ e una base di $F(\alpha)$ su F è $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

(*b*) *Se α è trascendente su F, allora $F(\alpha)$ ha grado infinito su F.*

Dimostrazione: (*a*) Se α è algebrico di grado n su F, gli elementi $1, \alpha, \alpha^2$, $\ldots, \alpha^{n-1}$ di K sono linearmente indipendenti su F, altrimenti α annullerebbe un polinomio di $F[X]$ di grado minore di n. Poiché essi generano $F(\alpha)$ su F (Corollario 6.2), allora costituiscono una base di $F(\alpha)$ su F. In particolare $[F(\alpha) : F] = n$.

(*b*) Se α è trascendente su F, per ogni $n \geq 1$ gli elementi $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ di $F(\alpha)$ sono linearmente indipendenti su F, perché α non è radice di nessun polinomio non nullo a coefficienti in F. Dunque $F(\alpha)$ non ha una base finita su F.

Corollario 7.2 *Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$. Allora α è algebrico su F se e soltanto se $F[\alpha]$ è uno spazio vettoriale di dimensione finita su F. In questo caso $F[\alpha] = F(\alpha)$ è un campo e $[F(\alpha) : F]$ è uguale al grado di α su F.*

Dimostrazione: Se α è algebrico su F, allora $F[\alpha] = F(\alpha)$ (Corollario 6.2) e $[F(\alpha) : F]$ è uguale al grado di α su F (Proposizione 7.1). Se viceversa $F[\alpha]$ è uno spazio vettoriale di dimensione finita n su F, gli $n + 1$ elementi $1, \alpha, \alpha^2, \ldots, \alpha^n$ di $F[\alpha]$ sono linearmente dipendenti su F. Dunque α annulla un polinomio di grado n su F e quindi è algebrico (di grado n) su F.

Proposizione 7.3 *Se $F \subseteq L \subseteq K$ sono ampliamenti di campi, allora K è finito su F se e soltanto se K è finito su L e L è finito su F. In questo caso risulta*

$$[K : F] = [K : L][L : F].$$

Inoltre, se $\{\alpha_1, \ldots, \alpha_s\}$ è una base di K su L e $\{\beta_1, \ldots, \beta_t\}$ è una base di L su F, allora $\{\alpha_1\beta_1, \ldots, \alpha_s\beta_t\}$ è una base di K su F.

Dimostrazione: Basta verificare che, se $\{\alpha_\lambda\,;\ \lambda \in \Lambda\}$ è una base di K su L e $\{\beta_\sigma\,;\ \sigma \in \Sigma\}$ è una base di L su F, allora una base di K su F è $\{\alpha_\lambda\beta_\sigma\,;\ \lambda \in \Lambda, \sigma \in \Sigma\}$.

Per vedere questo, osserviamo intanto che $\{\alpha_\lambda\beta_\sigma\,;\ \lambda \in \Lambda, \sigma \in \Sigma\}$ è un insieme di generatori per K su F. Infatti, se $a \in K$, allora $a = \sum_{j=1}^{n} b_j\alpha_j$, per opportuni $b_j \in L$, e $b_j = \sum_{i=1}^{m} c_{ij}\beta_i$, per opportuni $c_{ij} \in F$. Dunque $a = \sum_{i,j} c_{ij}\beta_i\alpha_j$. Inoltre, se $\sum_{h,k} c_{hk}\beta_h\alpha_k = \sum_k(\sum_h c_{hk}\beta_h)\alpha_k = 0$, con $c_{hk} \in F$, $h = 1, \ldots, u$, $k = 1, \ldots, v$, l'indipendenza degli α_k su L implica che $\sum_h c_{hk}\beta_h = 0$ per ogni k, e allora l'indipendenza dei β_h su F implica che $c_{hk} = 0$ per ogni h, k. Dunque gli elementi $\alpha_\lambda\beta_\sigma$, $\lambda \in \Lambda, \sigma \in \Sigma$ sono tutti linearmente indipendenti su F.

Corollario 7.4 *Siano $F \subseteq L \subseteq K$ ampliamenti finiti di campi.*

(*a*) *Se $[K : F] = [L : F]$, allora $L = K$.*

(*b*) *Se $[K : F] = [K : L]$, allora $L = F$.*

Dimostrazione: Per la Proposizione 7.3, se $[K : F] = [L : F]$, allora $[K : L] = 1$; da cui $K = L$. Analogamente, se $[K : F] = [K : L]$, allora $[L : F] = 1$; da cui $L = F$.

Il Corollario 7.4. non è vero senza l'ipotesi che $[K : F]$ sia finito. Per vedere questo, basta considerare la catena di campi $\mathbb{Q} \subseteq \mathbb{Q}(\pi^2) \subsetneq \mathbb{Q}(\pi)$ e notare che, essendo π e π^2 entrambi trascendenti, per la Proposizione 7.1, si ha che $[\mathbb{Q}(\pi) : \mathbb{Q}] = [\mathbb{Q}(\pi^2) : \mathbb{Q}]$ è infinito (Esercizio 6.2).

Corollario 7.5 *Se K è un ampliamento finito di F e $\alpha \in K$, allora α è algebrico su ogni campo intermedio L e il suo grado su L divide $[K : F]$. Se inoltre $L \subseteq F(\alpha)$, il grado di α su L divide il grado di α su F.*

Dimostrazione: Si ha $F \subseteq L \subseteq L(\alpha) \subseteq K$ e $[L(\alpha) : L]$ divide $[K : F]$ per la Proposizione 7.3. Inoltre $[L(\alpha) : L]$ è il grado di α su L per il Corollario 7.2 (notare che $[L(\alpha) : L] = 1$ se e soltanto se $\alpha \in L$). Se poi $F \subseteq L \subseteq F(\alpha)$, allora risulta $L(\alpha) = F(\alpha)$ e $[L(\alpha) : L] = [F(\alpha) : L]$ divide $[F(\alpha) : F]$, ancora per la Proposizione 7.3.

Il Corollario precedente ci dice in particolare che, se $F \subseteq L \subseteq F(\alpha)$ e $[F(\alpha) : F] = n$, allora il polinomio minimo di α su L (che divide il polinomio minimo di α su F) ha per grado un divisore di n.

Corollario 7.6 *Se $F \subseteq K$ è un ampliamento di campi e $[K : F] = p$ è un numero primo, allora $K = F(\alpha)$ per ogni $\alpha \in K \setminus F$. Inoltre una base di $F(\alpha)$ su F è $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\right\}$.*

Dimostrazione: $[F(\alpha) : F]$ è finito e divide $[K : F]$ per il Corollario 7.5. Se inoltre $\alpha \in K \setminus F$, allora $[F(\alpha) : F] \neq 1$ e quindi $[F(\alpha) : F] = p$. La conclusione segue allora dalla Proposizione 7.1.

Esempi

7.5. Ampliamenti quadratici. Se $F \subseteq K$ è un ampliamento di campi e $[K : F] = 2$, K si dice un *ampliamento quadratico* di F. In questo caso, per ogni $\alpha \in K \setminus F$, risulta $[F(\alpha) : F] = 2$ e dunque $K = F(\alpha)$. Inoltre α è radice di un polinomio $m(X) = X^2 + bX + c$ a coefficienti in F e una base di K su F è $\{1, \alpha\}$.

Sia ora F un campo numerico reale. Posto $\Delta := b^2 - 4c$ allora risulta $\alpha = \frac{-b \pm \sqrt{\Delta}}{2}$. Notiamo che $\Delta \in F$ e $K = F(\sqrt{\Delta})$, perché $\sqrt{\Delta} = 2a - b \in$

$F(\alpha) = K$ e viceversa $\alpha \in F(\sqrt{\Delta})$. In particolare Δ non è un quadrato in F, altrimenti si avrebbe $K = F$. Viceversa è chiaro che se $\delta \in F$ e δ non è un quadrato in F, allora $[F(\sqrt{\delta}) : F] = 2$, essendo $\sqrt{\delta}$ radice del polinomio irriducibile $X^2 - \delta$.

In conclusione, tutti e soli gli ampliamenti quadratici di un campo numerico reale F sono quelli del tipo $F(\sqrt{\delta})$, dove $\delta \in F$ e δ non è un quadrato in F.

Nello stesso modo si può vedere che, se F è un campo la cui caratteristica è diversa da 2, ogni suo ampliamento quadratico è del tipo $F(\gamma)$ con $\gamma^2 \in F$. In caratteristica 2 invece questo non è vero (Esercizio 7.4).

7.6. Ampliamenti biquadratici. Se F è un campo e $F(\alpha)$, $F(\beta)$ sono ampliamenti quadratici distinti di F, l'ampliamento $F(\alpha, \beta)$ si dice un *ampliamento biquadratico* di F.

Notiamo che $F(\alpha)$ e $F(\beta)$ sono distinti se e soltanto se $\beta \notin F(\alpha)$ (equivalentemente $\alpha \notin F(\beta)$). Ne segue che α ha grado 2 su $F(\beta)$ (e β ha grado 2 su $F(\alpha)$); perciò $[F(\alpha, \beta) : F] = 4$ e una base di $F(\alpha, \beta)$ su F è $\{1, \alpha, \beta, \alpha\beta\}$ (Proposizione 7.3).

Supponiamo ora che F abbia caratteristica diversa da 2. Allora, senza perdere di generalità, per quanto visto nell'esempio precedente, possiamo supporre che $a := \alpha^2$ e $b := \beta^2$ appartengano ad F. Poniamo $\gamma := \alpha + \beta$. Poiché $\gamma \in F(\alpha, \beta) \setminus F$, se $F(\gamma) \neq F(\alpha, \beta)$, allora γ deve avere grado 2 su F. Supponiamo che $m(X) = X^2 + cX + d$ sia il polinomio minimo di γ su F. Sviluppando i calcoli allora deve risultare

$$(d + a + b) + c\alpha + c\beta + 2\alpha\beta = 0,$$

ma questo è impossibile perché $1, \alpha, \beta, \alpha\beta$ sono linearmente indipendenti su F. Perciò risulta $F(\alpha, \beta) = F(\gamma)$. Inoltre una base per $F(\alpha, \beta)$ su F è anche $\{1, \gamma, \gamma^2, \gamma^3\}$.

Notiamo che il polinomio minimo $m(X)$ di γ su F è un polinomio monico *biquadratico*, cioè del tipo $X^4 + a_2X^2 + a_0$; infatti risulta

$$m(X) = X^4 - 2(a + b)X^2 + (a - b)^2.$$

Viceversa, se il polinomio minimo $m(X)$ di γ su F è un polinomio biquadratico, non è detto che $F(\gamma)$ sia un ampliamento biquadratico di F. Ad esempio, se $\gamma := \sqrt[4]{2}$, allora $m(X) = X^4 - 2$ è un polinomio biquadratico (per $a_2 = 0$, $a_0 = -2$), ma $\mathbb{Q}(\sqrt[4]{2})$ non è un ampliamento biquadratico.

7.7. Se $\alpha := \sqrt{3}$ e $\beta := \sqrt[3]{2}$, allora $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$. Per vedere questo, poiché $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$, basta mostrare che $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha + \beta) : \mathbb{Q}]$. Poiché

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}],$$

allora $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ è diviso da $2 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ e da $3 = [\mathbb{Q}(\beta) : \mathbb{Q}]$ e perciò è diviso anche da 6. D'altra parte ad esempio $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ è al più uguale

a 3, perché β ha grado 3 su $\mathbb{Q}$. Perciò $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=6$. Inoltre una base di $\mathbb{Q}(\alpha,\beta)$ su $\mathbb{Q}$ è

$$\left\{1,\alpha,\beta,\beta^2,\alpha\beta,\alpha\beta^2\right\}.$$

Poiché $\alpha+\beta\in\mathbb{Q}(\alpha,\beta)$, il suo grado su $\mathbb{Q}$ può essere 2, 3 oppure 6. Se

$$a(\alpha+\beta)^2+b(\alpha+\beta)+c=0\,,\quad \text{con}\ \ a,\,b,\,c\in\mathbb{Q}\,,$$

allora

$$(3a+c)+b\alpha+b\beta+a\beta^2+2a\alpha\beta=0,$$

da cui, poiché 1, α, β, β^2, $\alpha\beta$ sono linearmente indipendenti su $\mathbb{Q}$,

$$a=b=c=0.$$

Dunque $\alpha+\beta$ non ha grado 2 su $\mathbb{Q}$. Nello stesso modo si vede che esso non può avere grado 3 su $\mathbb{Q}$. Ne segue che $\alpha+\beta$ ha grado 6 su $\mathbb{Q}$ e perciò $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\alpha+\beta)$.

Notiamo che $\alpha+\beta$ deve avere grado 3 su $\mathbb{Q}(\alpha)$ e grado 2 su $\mathbb{Q}(\beta)$. Per calcolare il polinomio minimo di $\alpha+\beta$ su $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ e su $\mathbb{Q}$, si può procedere nel seguente modo.

Sia $\gamma:=\alpha+\beta$. Allora $\gamma-\alpha=\beta$, da cui, elevando al cubo,

$$\gamma^3-3\alpha-3\gamma^2\alpha+9\gamma=2.$$

Ne segue che il polinomio minimo di γ su $\mathbb{Q}(\alpha)$ è

$$g(X):=X^3-3\alpha X^2+9X-(3\alpha+2).$$

Analogamente, si ha $\gamma-\beta=\alpha$, da cui, elevando al quadrato,

$$\gamma^2-2\beta\gamma+\beta^2=3.$$

Dunque il polinomio minimo di γ su $\mathbb{Q}(\beta)$ è

$$h(X):=X^2-2\beta X+(\beta^2-3).$$

Infine, elevando al quadrato la relazione

$$\gamma^3+9\gamma-2=3(1+\gamma^2)\alpha,$$

si ottiene

$$\gamma^6-9\gamma^4-4\gamma^3+27\gamma^2-36\gamma-23=0.$$

Perciò il polinomio minimo di γ su $\mathbb{Q}$ è

$$f(X)=X^6-9X^4-4X^3+27X^2-36X-23.$$

Osserviamo infine che una base di $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\gamma)$ su $\mathbb{Q}$ è anche

$$\left\{1,\,\gamma,\,\gamma^2,\,\gamma^3,\,\gamma^4,\,\gamma^5\right\}.$$

7.8. Campi di spezzamento di polinomi a coefficienti numerici. Sia F un campo numerico e sia $f(X) \in F[X]$ un polinomio di grado n. Indichiamo con $\alpha_1, \ldots, \alpha_n$ le radici complesse (non necessariamente tutte distinte) di $f(X)$ e consideriamo il campo $K := F(\alpha_1, \ldots, \alpha_n)$. Ricordiamo che K si dice il campo di spezzamento di $f(X)$ su F ed è il più piccolo campo numerico contenente F su cui $f(X)$ si fattorizza in polinomi lineari (Paragrafo 4).

Per determinare il grado di K su F, si consideri la catena di campi (non necessariamente tutti distinti)

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_n := F_{n-1}(\alpha_n) = K.$$

Il grado di α_1 su F è al più uguale a n, perché il polinomio minimo $m(X)$ di α_1 su F divide $f(X)$. Poiché su $F_1 := F(\alpha_1)$ si ha $f(X) = (X - \alpha_1)f_1(X)$ con $\deg(f_1(X)) = n - 1$ e il polinomio minimo $m_1(X)$ di α_2 su F_1 divide $f_1(X)$, il grado di α_2 su F_1 è al più uguale a $n - 1$. Così proseguendo, si ottiene che il grado di a_i su F_{i-1} è al più uguale a $n - i + 1$ e dunque, per la Proposizione 7.3,

$$\begin{aligned} 1 \leq [K : F] &= [K : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_2 : F_1][F_1 : F] \\ &\leq 2 \cdot 3 \cdots (n-1) \cdot n = n! \end{aligned}$$

Notiamo che il calcolo di $[K : F]$ nel modo precedentemente illustrato non dipende dall'ordine scelto per l'aggiunzione delle radici; infatti il campo $K = F(\alpha_1, \ldots, \alpha_n)$ è univocamente determinato.

Se $f(X)$ è irriducibile sul campo F, allora per ogni radice α di $f(X)$, il grado $[F(\alpha) : F]$ è uguale a n. Dunque, in questo caso, n divide $[K : F]$ e in particolare $n \leq [K : F]$. Inoltre si ha l'uguaglianza se e soltanto se $K = F(\alpha)$, ovvero tutte le radici di $f(X)$ appartengono a $F(\alpha)$.

- Se $f(X) := X^2 + bX + c$ è un polinomio di secondo grado irriducibile su F, allora il suo campo di spezzamento su F ha grado 2. Infatti, se α è una radice di $f(X)$, l'altra sua radice è $\beta = -b - \alpha$. Dunque $\beta \in F(\alpha)$.

- Se f(X) è un polinomio irriducibile su F di grado 3, il suo campo di spezzamento può avere grado 3 oppure 6.

  (a) Sia $f(X) := X^3 - 3X + 1 \in \mathbb{Q}[X]$. Questo è un polinomio irriducibile su $\mathbb{Q}$, non avendo radici razionali. Se α è una radice (reale) di $f(X)$, una verifica diretta mostra che le altre due radici di $f(X)$ sono $\beta := \alpha^2 - 2$ e $\gamma := -\alpha^2 - \alpha + 2$. Poiché β, $\gamma \in \mathbb{Q}(\alpha)$, il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha)$ ed esso ha grado $3 = \deg(f(X))$ su $\mathbb{Q}$.

  (b) Se $f(X) := X^3 - 2 \in \mathbb{Q}[X]$, allora il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ ha grado $3! = 6$. Infatti, se ξ è una radice primitiva terza

dell'unità, ad esempio $\xi := \frac{-1+i\sqrt{3}}{2}$, le radici di $f(X)$ sono $\alpha := \sqrt[3]{2}$, $\alpha\xi$, $\alpha\xi^2$. Ne segue che il campo di spezzamento di $f(X)$ su $\mathbb{Q}$ è

$$K := \mathbb{Q}(\alpha, \alpha\xi, \alpha\xi^2) = \mathbb{Q}(\alpha, \xi) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}).$$

Poiché $i\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$ (essendo questo un campo numerico reale) il suo polinomio minimo su $\mathbb{Q}(\sqrt[3]{2})$ è $X^2 + 3$. Dunque

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

Allo stesso risultato si giunge verificando che $\sqrt[3]{2} \notin \mathbb{Q}(i\sqrt{3})$; dunque $[K : \mathbb{Q}(i\sqrt{3})] = 3$ e

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(i\sqrt{3})][\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 3.2 = 6.$$

Ricordiamo che, se L_1 e L_2 sono due sottocampi di K, il composto di L_1 e L_2 è il sottocampo di K generato da $L_1 \cup L_2$ (Paragrafo 4).

Indichiamo con L_1L_2 l'insieme degli elementi di K del tipo $x_1y_1 + \cdots + x_ny_n$, con $x_i \in L_1$ e $y_i \in L_2$ per $i = 1, \ldots, n$.

Proposizione 7.7 *Sia K un ampliamento di F e siano L_1, L_2 due campi intermedi. Se L_1 è finito su F, allora L_1L_2 è un campo ed è il composto di L_1 e L_2 in K. Inoltre $[L_1L_2 : L_2] \leq [L_1 : F]$.*

Dimostrazione: Si verifica facilmente che L_1L_2 è un sottoanello di K. È chiaro inoltre che L_1L_2 contiene sia L_1 che L_2.

Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di L_1 su F e sia $\gamma = x_1y_1 + \cdots + x_ny_n \in L_1L_2$ un elemento non nullo, con $x_i \in L_1$ e $y_i \in L_2$. Poiché ogni elemento x_i è combinazione lineare di $\alpha_1, \ldots, \alpha_n$ su F, allora γ è combinazione lineare di $\alpha_1, \ldots, \alpha_n$ su L_2. Dunque $\{\alpha_1, \ldots, \alpha_n\}$ è un insieme di generatori di L_1L_2 come spazio vettoriale su L_2 e la dimensione di L_1L_2 su L_2 è al più uguale a n. Ne segue che $L_2[\gamma]$ ha dimensione finita su L_2. Perciò γ è algebrico su L_2 e $L_2[\gamma] = L_2(\gamma)$ è un campo (Corollario 7.2). Allora $\gamma^{-1} \in L_2[\gamma] \subseteq L_1L_2$ e quindi L_1L_2 è un campo.

Poiché il composto di L_1 e L_2 contiene, per chiusura additiva e moltiplicativa, gli elementi di L_1L_2, per minimalità risulta che questi due campi coincidono. Per la prima parte della dimostrazione, $[L_1L_2 : L_2] \leq [L_1 : F]$.

Proposizione 7.8 *Sia K un ampliamento di F e siano L_1, L_2 due ampliamenti finiti di F contenuti in K. Allora*

$$[L_1L_2 : F] \leq [L_1 : F][L_2 : F].$$

Se inoltre $[L_1 : F]$ e $[L_2 : F]$ sono due interi coprimi, allora vale l'uguaglianza.

Dimostrazione: Sia $\{\alpha_1, \ldots, \alpha_n\}$ una base di L_1 su F e sia $\{\beta_1, \ldots, \beta_n\}$ una base di L_2 su F. Allora $\{\alpha_i\beta_j\,;\ i = 1, \ldots, n,\ j = 1, \ldots, m\}$ è un insieme di generatori di L_1L_2 su F. Infatti, ogni elemento di L_1L_2 è del tipo $x_1y_1 + \cdots + x_ny_n$ con $x_i \in L_1$ e $y_i \in L_2$ ed inoltre x_i e y_i sono combinazioni lineari su F di $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_m$ rispettivamente. Ne segue che $x_1y_1 + \cdots + x_ny_n$ è combinazione lineare su F degli elementi a_ib_j di K.

Se inoltre $[L_1 : F] = n$ e $[L_2 : F] = m$ sono due interi coprimi, allora nm divide $[L_1L_2 : F]$, perché lo dividono sia m che n (Proposizione 7.3). Dunque vale l'uguaglianza.

Esempi

7.9. Sia K un ampliamento di F e siano $\alpha, \beta \in K$ algebrici su F di gradi m e n rispettivamente. Se $L_1 = F(\alpha)$ e $L_2 = F(\beta)$, si ha $L_1L_2 = F(\alpha, \beta)$ e, se $\mathrm{MCD}(m, n) = 1$, allora risulta

$$F(\alpha) \cap F(\beta) = F \quad \text{e} \quad [F(\alpha, \beta) : F] = [F(\alpha) : F][F(\beta) : F] = mn.$$

ESERCIZI

7.1. Mostrare che $\mathbb{C} = \mathbb{R}(a + bi)$ per ogni numero complesso $a + bi$ con $b \neq 0$. Questo è un modo di dimostrare che tutti i polinomi di $\mathbb{R}[X]$ irriducibili su $\mathbb{R}$ hanno grado al più uguale a 2.

7.2. Sia K un ampliamento quadratico di $\mathbb{Q}$. Mostrare che $K = \mathbb{Q}(\sqrt{d})$, dove $d \in \mathbb{Z}$ e $|d| = p_1 \ldots p_n$, dove $p_1, \ldots, p_n$ sono numeri primi distinti.

7.3. Siano a e b due interi privi di fattori quadratici. Mostrare che $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ se e soltanto se $\sqrt{\frac{a}{b}} \in \mathbb{Q}$.

7.4. Sia F un campo di caratteristica diversa da 2. Mostrare che ogni ampliamento quadratico di F è del tipo $F(\gamma)$ con $\gamma^2 \in F$. Mostrare inoltre che il campo descritto nell'Esercizio 1.6 è un ampliamento quadratico di $\mathbb{F}_2$ che non è di questo tipo.

7.5. Sia F un campo di caratteristica diversa da 2. Supponiamo che $m(X) := X^2 + bX + c$ sia irriducibile su F e sia $\Delta := b^2 - 4c$. Mostrare che gli anelli quoziente $\frac{F[X]}{\langle m(X)\rangle}$ e $\frac{F[X]}{(X^2-\Delta)}$ sono isomorfi, definendo esplicitamente un isomorfismo tra di essi.

7.6. Siano $F \subseteq L \subseteq K$ ampliamenti di campi. Mostrare con un esempio che se $\alpha \in K$ è algebrico su L, non è detto che esso sia algebrico anche su F (*Suggerimento*: Usare l'Esercizio 5.4).

7.7. Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Mostrare che α è algebrico su F se e soltanto se α^n è algebrico su F, per ogni $n \geq 2$.

7.8. Sia $K := \mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$ un ampliamento biquadratico di $\mathbb{Q}$. Posto $\alpha := \sqrt{a} + \sqrt{b}$, determinare le formule del cambiamento di base tra le basi

$$\mathcal{B} := \left\{1,\ \sqrt{a},\ \sqrt{b},\ \sqrt{a}b\right\} \quad \text{e} \quad \mathcal{B}' := \left\{1,\ \alpha,\ \alpha^2,\ \alpha^3\right\}$$

di K su $\mathbb{Q}$.

7.9. Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$ algebrico di grado dispari su F. Mostrare che $F(\alpha) = F(\alpha^2)$.

7.10. Sia $F \subseteq K$ un ampliamento di campi e sia $[K : F] = p^k$, dove p è un numero primo e $k \geq 1$. Mostrare che ogni polinomio irriducibile $f(X) \in F[X]$ di grado minore di p non ha radici in K.

7.11. Determinare il grado su $\mathbb{Q}$ dei seguenti campi numerici:

$$\mathbb{Q}(\sqrt[3]{2}, 3\sqrt{5})\,;\ \mathbb{Q}(\pi,\ \sqrt[19]{2})\,;\ \mathbb{Q}(\sqrt[3]{2} + i).$$

7.12. Sia K il campo di spezzamento del polinomio $f(X)$ su $\mathbb{Q}$. Determinare $[K : \mathbb{Q}]$ quando $f(X)$ è uno dei seguenti polinomi:

$$X^4 - 5X^2 + 6\,;\ X^4 - 6X^2 + 1\,;\ X^4 - X^3 - 3X + 3\,;\ X^4 - 2X^3 + X^2 - X - 2.$$

7.13. Sia $F \subseteq K$ un ampliamento di campi e siano α, $\beta \in K$ algebrici su F di gradi rispettivamente m e n tali che $\mathrm{MCD}(m, n) = 1$. Mostrare che $F(\alpha, \beta) = F(\alpha + \beta)$.

7.14. Sia $F \subseteq K$ un ampliamento di campi e siano α, $\beta \in K$ algebrici su F con polinomi minimi $p(X)$ e $q(X)$ rispettivamente. Mostrare che, se i gradi di $p(X)$ e $q(X)$ sono coprimi, allora $q(X)$ è irriducibile su $F(\alpha)$ e $p(X)$ è irriducibile su $F(\beta)$.

7.15. Siano F un campo e $a \in F$. Mostrare che, se $\mathrm{MCD}(m, n) = 1$, allora il polinomio $X^{mn} - a$ è irriducibile su F se e soltanto se i polinomi $X^m - a$ e $X^n - a$ sono irriducibili su F.

8 Campi di Spezzamento

Nel Paragrafo 4 abbiamo ricordato che un polinomio $f(X)$ a coefficienti in un campo numerico F ha tutte le sue radici in $\mathbb{C}$ (Teorema Fondamentale dell'Algebra) e abbiamo chiamato l'ampliamento di F in $\mathbb{C}$ generato dalle radici di $f(X)$ il campo di spezzamento di $f(X)$ su F; questo campo è il più piccolo sottocampo di $\mathbb{C}$ su cui $f(X)$ si spezza in fattori lineari. In questo paragrafo ci proponiamo di mostrare che, qualunque sia il campo F, è possibile costruire un ampliamento di F in cui il polinomio $f(X)$ abbia almeno una radice. Questo ci permetterà di costruire un campo minimale in cui $f(X)$ abbia tutte le sue radici e quindi si spezzi in fattori lineari.

Il modo in cui procedere ci viene indicato dal fatto che, se F è un campo numerico, $p(X) \in F[X]$ è un polinomio irriducibile su F e α è una radice complessa di $p(X)$, allora l'ampliamento semplice $F(\alpha)$ è isomorfo al campo $K := \frac{F[X]}{\langle p(X) \rangle}$ (Teorema 6.1).

Teorema 8.1 *Sia F un campo e $p(X) \in F[X]$ un polinomio irriducibile su F di grado n. Allora il campo $K := \frac{F[X]}{\langle p(X)\rangle}$ è un ampliamento semplice di F di grado n e $p(X)$ ha una radice in K. Precisamente, se α è la classe di X in K, risulta $p(\alpha) = 0$ e*

$$K = F(\alpha) = \left\{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}; c_i \in F\right\}.$$

Dimostrazione: K è un campo perché $p(X)$ è irriducibile su F. Se $f(X) \in F[X]$, indichiamo con $\overline{f(X)}$ la classe di $f(X)$ in K, ovvero poniamo

$$\overline{f(X)} := f(X) + \langle p(X)\rangle.$$

Se $r(X)$ è il resto della divisione di $f(X)$ per $p(X)$, si ha che $f(X) - r(X) \in \langle p(X)\rangle$ e perciò $\overline{f(X)} = \overline{r(X)}$. Dunque

$$K = \left\{\overline{r(X)}\,;\ r(X) \in F[X],\ r(X) = 0 \text{ oppure } \deg(r(X)) < n\right\}.$$

La restrizione ad F della proiezione canonica di $F[X]$ su K è un omomorfismo di campi non nullo $F \longrightarrow K$. Perciò la sua immagine

$$F' := \{\overline{c} := c + \langle p(X)\rangle\,;\ c \in F\}$$

è un sottocampo di K isomorfo ad F e K è un ampliamento di F.

Se poi $f(X) := c_0 + c_1X + \cdots + c_tX^t$, allora si ha

$$\overline{f(X)} := \overline{c}_0 + \overline{c}_1\overline{X} + \cdots + \overline{c}_t\overline{X}^t.$$

Ponendo $\alpha := \overline{X}$ e identificando F con F', allora possiamo scrivere

$$\overline{f(X)} = c_0 + c_1\alpha + \cdots + c_t\alpha^t = f(\alpha).$$

In particolare otteniamo $0 = \overline{p(X)} = p(\alpha)$ e dunque $\alpha := \overline{X} \in K$ è una radice di $p(X)$.

Inoltre $p(X)$, essendo irriducibile, è il polinomio minimo di α su F. Perciò α ha grado n su F e l'insieme $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ è una base di K su F (Proposizione 7.1). Infine si ha

$$\begin{aligned} K &= \left\{\overline{r(X)}\,;\ r(X) \in F[X], \deg(r(X)) < n\right\} \cup \left\{\overline{0}\right\} \\ &= \left\{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}\,;\ c_i \in F\right\} = F(\alpha). \end{aligned}$$

Per il Teorema precedente, se $p(X) \in F[X]$ è un polinomio irriducibile su F, allora il campo $K := \frac{F[X]}{\langle p(X)\rangle}$ può essere visto come l'ampliamento semplice di F generato da un simbolo α che verifica la relazione $p(\alpha) = 0$. Per questo motivo il campo $K = F(\alpha)$ si dice anche un *ampliamento (algebrico) semplice simbolico* di F.

Notiamo che, se $p(X)$ è di primo grado, allora $K := \frac{F[X]}{\langle p(X)\rangle}$ ha grado 1 su F, dunque $K = F$.

L'inverso di un elemento di K si può calcolare, come nel caso numerico, tramite l'Algoritmo Euclideo della divisione (Paragrafo 6).

Esempi

8.1. Il polinomio $p(X) := 1+X+X^2 \in \mathbb{F}_2[X]$ è irriducibile su $\mathbb{F}_2$, perché non ha radici in $\mathbb{F}_2$. Il campo $K := \frac{\mathbb{F}_2[X]}{\langle p(X)\rangle}$ ha quattro elementi. Infatti i soli polinomi di $\mathbb{F}_2[X]$ di grado minore di 2 sono: 0, 1, X, $1+X$. Possiamo allora scrivere

$$K = \left\{0,\, 1,\, \alpha,\, 1+\alpha\,;\; 1+\alpha+\alpha^2 = 0\right\}.$$

Osserviamo che nessun elemento di $K \setminus \mathbb{F}_2$ ha il quadrato in $\mathbb{F}_2$ (Esempio 7.5 ed Esercizio 7.4).

8.2. Sia $p(X) := 2 + 4X + 2X^2 + X^3 \in \mathbb{F}_5[X]$. Poiché $p(X)$ non ha radici in $\mathbb{F}_5$, esso è irriducibile su $\mathbb{F}_5$. Allora

$$K := \frac{\mathbb{F}_5[X]}{\langle p(X)\rangle} = \left\{c_0 + c_1\alpha + c_2\alpha^2\,;\; c_i \in \mathbb{F}_5\,,\, p(\alpha) = 0\right\}.$$

Notiamo che K ha $5^3 = 125$ elementi.

Calcoliamo l'inverso dell'elemento $\beta := 1 + 3\alpha + \alpha^2$. A β corrisponde il polinomio $1 + 3X + X^2 \in \mathbb{F}_5[X]$. Poiché in $\mathbb{F}_5[X]$ risulta

$$1 = -Xp(X) + (1 + 3X + X^2)(1 + 4X + X^2),$$

calcolando in α si ottiene che l'inverso di β in K è $1 + 4\alpha + \alpha^2$.

Sia F un campo e $f(X) \in F[X]$ un polinomio di grado n. Un ampliamento K di F si dice un *campo di spezzamento* di $f(X)$ su F se esistono $\alpha_1, \ldots, \alpha_n \in K$ (non necessariamente tutti distinti) tali che $K = F(\alpha_1, \ldots, \alpha_n)$ e $f(X) = c(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)$ in $K[X]$. Nel caso numerico, questa definizione coincide con quella data nel Paragrafo 4.

Teorema 8.2 *Sia F un campo e $f(X) \in F[X]$ un polinomio di grado n. Allora esiste un campo di spezzamento K di $f(X)$. Inoltre K è finito su F e $[K : F] \leq n!$.*

Dimostrazione: Supponiamo che $f(X)$ non abbia già tutte le sue radici in F e sia $p(X)$ un fattore di $f(X)$ irriducibile su F di grado almeno uguale a 2. Per il Teorema 8.1, $p(X)$ ha una radice α_1 nel campo

$$F_1 := \frac{F[X]}{\langle p(X)\rangle} = F(\alpha_1).$$

Dunque in $F_1[X]$ si ha $f(X) = (X - \alpha_1)g(X)$, dove $\deg(g(X)) = n - 1$. Se $g(X)$ ha tutte le sue radici in F_1, allora F_1 è il campo di spezzamento di $f(X)$.

Altrimenti, sia $p_1(X)$ un fattore di $g(X)$ irriducibile in $F_1[X]$ di grado almeno uguale a 2. Allora $p_1(X)$ ha una radice α_2 nel campo

$$F_2 := \frac{F_1[X]}{\langle p_1(X)\rangle} = F_1(\alpha_2) = F(\alpha_1, \alpha_2).$$

Dunque in $F_2[X]$ si ha $f(X) = (X - \alpha_1)(X - \alpha_2)g_1(X)$, dove $\deg(g_1(X)) = n-2$. Poiché, per motivi di grado, $f(X)$ ha al più n radici in un qualsiasi ampliamento di F, al più dopo n passi, si otterrà un campo $K := F(\alpha_1, \ldots, \alpha_n)$ su cui $f(X) = c(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)$.

Per determinare il grado di K su F, si consideri la catena di campi (non necessariamente tutti distinti)

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_n := F_{n-1}(\alpha_n) = K.$$

Il grado di α_1 su F è al più uguale a n, perché il polinomio minimo $p(X)$ di α_1 su F divide $f(X)$. Poiché su $F_1 := F(\alpha_1)$ si ha $f(X) = (X - \alpha_1)g(X)$ con $\deg(g(X)) = n-1$ e il polinomio minimo $p_1(X)$ di α_2 su F_1 divide $g(X)$, il grado di α_2 su F_1 è al più uguale a $n-1$. Così proseguendo, si ottiene che il grado di α_i su F_{i-1} è al più $n - i + 1$ e dunque

$$\begin{aligned} 1 \leq [K : F] &= [K : F_{n-1}][F_{n-1} : F_{n-2}]\ldots[F_2 : F_1][F_1 : F] \\ &\leq 2 \cdot 3 \cdots (n-1) \cdot n = n! \end{aligned}$$

Notiamo che, se $f(X)$ è irriducibile di grado n sul campo F, allora ogni sua radice ha grado n su F. Dunque, in questo caso, n divide $[K : F]$, in particolare $n \leq [K : F]$. Inoltre si ha l'uguaglianza se tutte le radici di $f(X)$ appartengono a $F(\alpha)$.

Nel caso numerico il campo di spezzamento di un polinomio è unicamente determinato in $\mathbb{C}$. In generale, come mostreremo nel prossimo paragrafo, due campi di spezzamento di uno stesso polinomio sono isomorfi.

Esempi

8.3. Il polinomio $p(X) := X^3 + X + 1 \in \mathbb{F}_2[X]$ è irriducibile su $\mathbb{F}_2$ (perché non ha radici in $\mathbb{F}_2$) e ha una radice α nel campo $K := \frac{\mathbb{F}_2[X]}{\langle p(X)\rangle}$. Inoltre su K risulta $p(X) = (X - \alpha)g(X)$ dove

$$g(X) := X^2 + \alpha X + (\alpha^2 + 1) = (X + \alpha^2)(X + (\alpha + \alpha^2)).$$

Dunque

$$K = \mathbb{F}_2(\alpha) = \left\{0,\ 1,\ \alpha,\ 1 + \alpha,\ \alpha^2,\ 1 + \alpha^2,\ \alpha + \alpha^2,\ 1 + \alpha + \alpha^2\,;\ \alpha^3 = \alpha + 1\right\}$$

è un campo di spezzamento di $f(X)$ su $\mathbb{F}_2$.

8.4. Determiniamo un campo di spezzamento del polinomio

$$f(X) := X^5 + X^4 + 1 \in \mathbb{F}_2[X].$$

La fattorizzazione di $f(X)$ in polinomi irriducibili su $\mathbb{F}_2$ è

$$f(X) = (X^2 + X + 1)(X^3 + X + 1).$$

Se $p(X) := X^2 + X + 1$ e $F_1 := \frac{\mathbb{F}_2[X]}{\langle p(X)\rangle}$, allora $p(X)$ ha una radice α in F_1 e in $F_1[X]$ risulta $p(X) = (X + \alpha)(X + (1 + \alpha))$. Inoltre

$$F_1 = \mathbb{F}_2(\alpha) = \left\{0,\, 1,\, \alpha,\, \alpha + 1\,;\ \alpha^2 = \alpha + 1\right\}.$$

Poiché F_1 ha grado 2 su $\mathbb{F}_2$ e $q(X) := X^3 + X + 1$ è di terzo grado, esso è irriducibile su F_1. Altrimenti F_1 conterrebbe una radice di $q(X)$, che ha grado 3 su $\mathbb{F}_2$. Costruiamo allora il campo $F_2 := \frac{F_1[X]}{\langle q(X)\rangle}$. Il polinomio $q(X)$ ha una radice β in F_2 e in $F_2[X]$ risulta

$$q(X) = (X + \beta)(X^2 + \beta X + (1 + \beta^2)) = (X + \beta)(X + \beta^2)(X + (\beta + \beta^2))$$

(vedi l'esempio precedente). Quindi F_2 è un campo di spezzamento di $f(X)$ su $\mathbb{F}_2$. Notiamo che il grado di F_2 su $\mathbb{F}_2$ è 6. Inoltre

$$F_2 = \mathbb{F}_2(\alpha, \beta) = \left\{a + b\beta + c\beta^2\,;\ a,\, b,\, c \in \mathbb{F}_2(\alpha) \text{ e } \beta^3 = \beta + 1\right\}$$

ha $4^3 = 64 = 2^6$ elementi.

Alternativamente, si può porre

$$K_1 := \frac{\mathbb{F}_2[X]}{\langle q(X)\rangle} = \mathbb{F}_2(\gamma) = \left\{a + b\gamma + c\gamma^2\,;\ a,\, b,\, c \in \mathbb{F}_2 \text{ e } \gamma^3 = \gamma + 1\right\}$$

$$K_2 := \frac{K_1[X]}{\langle p(X)\rangle} = \mathbb{F}_2(\gamma, \delta) = \left\{r + s\delta\,;\ r,\, s \in \mathbb{F}_2(\gamma) \text{ e } \delta^2 + \delta = 1\right\}.$$

Si verifica facilmente che l'applicazione

$$F_2 \longrightarrow K_2 \quad \text{definita da} \quad \sum c_{ij}\alpha^i\beta^j \mapsto \sum c_{ij}\delta^i\gamma^j$$

è un isomorfismo di campi.

8.5. Determiniamo un campo di spezzamento di

$$f(X) := X^4 + 2X^3 + 2X + 2 \in \mathbb{F}_3[X].$$

La fattorizzazione di $f(X)$ in polinomi irriducibili su $\mathbb{F}_3$ è

$$f(X) = (X^2 + 2X + 2)(X^2 + 1).$$

Se $p(X) := X^2 + 1$ e $F_1 := \frac{\mathbb{F}_3[X]}{\langle p(X)\rangle}$, allora $p(X)$ ha una radice α in F_1 e in $F_1[X]$ risulta $p(X) = (X + \alpha)(X + 2\alpha)$. Inoltre

$$F_1 = \mathbb{F}_3(\alpha) = \left\{0,\, 1,\, 2,\, \alpha,\, \alpha + 1,\, \alpha + 2,\, 2\alpha,\, 2\alpha + 1,\, 2\alpha + 2\,;\, \alpha^2 = 2\right\}.$$

Per vedere se $q(X) := X^2 + 2X + 2$ ha radici in F_1, poiché siamo in caratteristica $3 \neq 2$, possiamo applicare la usuale formula di risoluzione delle equazioni di secondo grado. Otteniamo che le radici di $q(X)$ in un suo campo di spezzamento sono $2 + \gamma$ e $2 + 2\gamma$, dove $\gamma^2 = 2$. Poiché un elemento il cui quadrato è 2 sta in F_1 ed è α, allora le radici di $q(X)$ stanno in F_1 e sono precisamente $2 + \alpha$ e $2 + 2\alpha$. In conclusione, in $F_1[X]$ si ha

$$f(X) = (X + \alpha)(X + 2\alpha)(X + (2\alpha + 1))(X + (\alpha + 1)).$$

Ne segue che F_1 è un campo di spezzamento di $f(X)$.

Si può anche procedere considerando prima il polinomio $q(X)$. Poniamo $K_1 := \frac{\mathbb{F}_3[X]}{\langle q(X)\rangle}$, allora $q(X)$ ha una radice β in K_1 e in $K_1[X]$ risulta $q(X) = (X + 2\beta)(X + (\beta + 2))$. Inoltre

$$K_1 = \mathbb{F}_3(\beta) = \left\{0,\, 1,\, 2,\, \beta,\, \beta + 1,\, \beta + 2,\, 2\beta,\, 2\beta + 1,\, 2\beta + 2\,;\; \beta^2 = \beta + 1\right\}.$$

Le radici di $p(X)$ in un suo campo di spezzamento sono α e 2α con $\alpha^2 = 2$. Poiché un elemento α con questa proprietà sta in K_1 ed è precisamente $\beta^2 = \beta + 1$, anche K_1 è un campo di spezzamento di $f(X)$ su $\mathbb{F}_3$. Infatti in K_1 risulta

$$f(X) = (X + 2\beta)(X + (\beta + 2))(X + (\beta + 1))(X + (2\beta + 2)).$$

Non è difficile verificare che l'applicazione

$$F_1 \longrightarrow K_1 \quad \text{definita da} \quad r(\alpha) \mapsto r(\beta^2)$$

per ogni $r(X) \in \mathbb{F}_3[X]$ (di grado al più uguale a uno) è un isomorfismo di campi.

ESERCIZI

8.1. Sia $m(X) := X^3 + 3X + 3 \in \mathbb{F}_5[X]$ e sia α una radice di $m(X)$ in un suo campo di spezzamento. Determinare l'inverso di α^2 e $1 + \alpha$ in $\mathbb{F}_5(\alpha)$.

8.2. Determinare un campo di spezzamento di $f(X)$ su $\mathbb{F}_p$ e il suo grado su $\mathbb{F}_p$ nei seguenti casi:

$$f(X) := X^3 + 2X + 1\,,\ p := 3, 5\,; \quad f(X) := X^4 + 5\,,\ p := 2, 3, 7.$$

8.3. Siano F un campo e $f(X) \in F[X]$. Sia inoltre

$$f(X) = p_1(X)^{k_1} \dots p_s(X)^{k_s},$$

$k_i \geq 1$, la fattorizzazione di $f(X)$ in polinomi distinti irriducibili su F. Mostrare che i polinomi $f(X)$ e $g(X) := p_1(X)^{h_1} \dots p_s(X)^{h_s}$ hanno lo stesso campo di spezzamento su F, comunque scelti $h_1, \dots, h_s \geq 1$.

8.4. Mostrare che ogni ampliamento algebrico semplice del campo complesso $\mathbb{C}$ è isomorfo a $\mathbb{C}$ (*Suggerimento*: Usare il Teorema Fondamentale dell'Algebra e il Teorema 8.1)

9 F-isomorfismi. Unicità del Campo di Spezzamento

Siano $F \subseteq K$ e $F' \subseteq K'$ ampliamenti di campi. Se $\varphi : F \longrightarrow F'$ è un omomorfismo, si dice che un omomorfismo $\psi : K \longrightarrow K'$ *estende* φ (o che φ *si può estendere a* ψ) se $\psi(x) = \varphi(x)$ per ogni $x \in F$, ovvero se la restrizione di ψ a F coincide con φ.

Esempi

9.1. Ogni omomorfismo non nullo di campi $F \longrightarrow F'$ estende l'identità sul sottocampo fondamentale di F (Proposizione 3.3).

Nel seguito, se $\varphi : F \longrightarrow F'$ è un omomorfismo di campi, indicheremo con φ^* l'applicazione di dominio $F[X]$ e codominio $F'[X]$ che associa al polinomio $f(X) := c_0 + c_1X + \dots + c_nX^n \in F[X]$ il polinomio $f^*(X) := \varphi(c_0) + \varphi(c_1)X + \dots + \varphi(c_n)X^n \in F'[X]$.

Lemma 9.1 *Sia $\varphi : F \longrightarrow F'$ un omomorfismo non nullo di campi. Allora:*

(*a*) *L'applicazione $\varphi^* : F[X] \longrightarrow F'[X]$ è un omomorfismo di anelli;*

(*b*) *Se $f(X) \in F[X]$ è non nullo, allora $f(X)$ e $\varphi^*(f(X))$ hanno lo stesso grado.*

Se inoltre φ è un isomorfismo, allora:

(*c*) *φ^* è un isomorfismo di anelli;*

(*d*) *$f(X)$ è irriducibile su F se e soltanto se $\varphi^*(f(X))$ è irriducibile su F'.*

Dimostrazione: $(a), (c)$ Si verifica facilmente che φ^* è un omomorfismo. Se inoltre φ è un isomorfismo, allora φ^* è biiettivo perché l'omomorfismo $(\varphi^{-1})^*$ è l'inverso di φ^*.

(b) Sia $f(X) \neq 0$. Se c_n è il coefficiente direttore di $f(X)$, allora, essendo φ iniettivo, si ha $\varphi(c_n) \neq 0$ e perciò $\varphi(c_n)$ è il coefficiente direttore di $\varphi^*(f(X))$.

(d) Sia $f(X)$ un polinomio non costante. Per i punti (b) e (c), $f(X)$ è prodotto di due fattori di grado positivo se e soltanto se anche $\varphi^*(f(X))$ lo è.

Proposizione 9.2 *Siano $F \subseteq K$ e $F' \subseteq K'$ ampliamenti di campi e sia $\alpha \in K$ algebrico di grado n su F, con polinomio minimo $m(X)$. Allora un omomorfismo non nullo $\varphi : F \longrightarrow F'$ si può estendere a un omomorfismo di campi $\psi : F(\alpha) \longrightarrow K'$ se e soltanto se il polinomio $\varphi^*(m(X)) =: m^*(X) \in F'[X]$ ha una radice in K'.*

In questo caso le estensioni di φ sono tante quante sono le radici distinte $\beta_1, \ldots, \beta_s$ di $m^*(X)$ in K' e sono tutti e soli gli omomorfismi

$$\psi_i : F(\alpha) \longrightarrow K'$$

definiti ponendo, per ogni $i = 1, \ldots, s$,

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mapsto \varphi(c_0) + \varphi(c_1)\beta_i + \cdots + \varphi(c_{n-1})\beta_i^{n-1},$$

dove $c_j \in F$ per $j = 0, \ldots, n-1$.

Inoltre $s \leq n$ e $s = n$ se il campo di spezzamento di $m^*(X)$ è contenuto in K' e $m^*(X)$ ha tutte radici distinte.

Dimostrazione: Sia $m(X) := c_0 + c_1X + \cdots + c_nX^n$. Se $\psi : F(\alpha) \longrightarrow K'$ è un omomorfismo che estende φ, allora deve risultare

$$\psi(0) = \psi(m(\alpha)) = \varphi(c_0) + \varphi(c_1)\psi(\alpha) + \cdots + \varphi(c_n)\psi(\alpha)^n = m^*(\psi(\alpha)) = 0.$$

Dunque $\psi(\alpha)$ è una radice di $m^*(X)$.

Viceversa, sia β una radice di $m^*(X)$. Consideriamo l'omomorfismo composto

$$\vartheta : F[X] \longrightarrow F'[X] \longrightarrow K' \quad \text{definito da} \quad r(X) \mapsto r^*(X) \mapsto r^*(\beta).$$

Allora $\langle m(X)\rangle \subseteq \mathrm{Ker}(\vartheta)$ e, poiché $F(\alpha)$ è canonicamente isomorfo a $\frac{F[X]}{\langle m(X)\rangle}$ (Teorema 6.1), allora φ induce un omomorfismo di campi $\psi : F(\alpha) \longrightarrow K'$ definito da $r(\alpha) \mapsto r^*(\beta)$, per ogni polinomio $r(X) \in F[X]$ (di grado al più $n-1$). È evidente che $\psi(\alpha) = \beta$. Inoltre, essendo ψ univocamente determinato da β, si hanno tante estensioni di φ quante sono le radici distinte di $m^*(X)$ in K'.

Per finire, basta ricordare che $\deg(m^*(X)) = \deg(m(X))$ per il Lemma 9.1 (b).

Se $F \subseteq K$ e $F \subseteq K'$ sono ampliamenti di campi, un isomorfismo di K in K' che estende l'identità su F si dice un *F-isomorfismo*. Se inoltre $K = K'$ esso si dice un *F-automorfismo* di K. Non è difficile verificare che l'insieme $\mathrm{Aut}_F(K)$ degli F-automorfismi di K è un sottogruppo del gruppo $\mathrm{Aut}(K)$ di tutti gli automorfismi. Inoltre $\mathrm{Aut}_F(K) = \mathrm{Aut}(K)$ se F è il sottocampo fondamentale di K.

Il seguente corollario è immediato.

Corollario 9.3 *Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$ algebrico di grado n su F con polinomio minimo $m(X)$. Allora la corrispondenza definita da $\psi \mapsto \psi(\alpha)$ è una corrispondenza biunivoca tra gli F-isomorfismi ψ di $F(\alpha)$ in K e le radici distinte di $m(X)$ in K.*

Precisamente, se $\alpha = \alpha_1, \ldots, \alpha_s$, $n \geq s \geq 1$, sono le radici distinte di $m(X)$ in K, allora gli F-isomorfismi distinti di $F(\alpha)$ in K sono tutti e soli gli F-isomorfismi $\psi_i : F(\alpha) \longrightarrow K$, $1 \leq i \leq s$, definiti rispettivamente da $r(\alpha) \mapsto r(\alpha_i)$, per ogni $r(X) \in F[X]$ (di grado al più uguale a $n-1$). Inoltre ψ_i è un F-automorfismo di $F(\alpha)$ se e soltanto se $\alpha_i \in F(\alpha)$.

Saremo particolarmente interessati al caso in cui F abbia caratteristica zero. Mostriamo ora che, sotto questa ipotesi, ogni polinomio irriducibile di grado n a coefficienti in F ha esattamente n radici distinte in un qualsiasi suo campo di spezzamento K; dunque, se α è algebrico di grado n su F, esistono esattamente n F-isomorfismi di $F(\alpha)$ in K.

Per il nostro scopo, è utile ricordare i seguenti fatti.

Proposizione 9.4 *Sia $F \subseteq K$ un ampliamento di campi e siano $f(X)$ e $g(X)$ due polinomi a coefficienti in F. Allora:*

(*a*) *La divisione euclidea di $f(X)$ per $g(X)$ effettuata in $F[X]$ oppure in $K[X]$ dà lo stesso risultato;*

(*b*) *$g(X)$ divide $f(X)$ in $F[X]$ se e soltanto se lo divide in $K[X]$;*

(*c*) *$f(X)$ e $g(X)$ hanno lo stesso massimo comune divisore monico in $F[X]$ e $K[X]$;*

(*d*) *$f(X)$ e $g(X)$ hanno un fattore comune di grado positivo in $F[X]$ se e soltanto se essi hanno una radice comune in un opportuno ampliamento di F;*

(*e*) **(N. H. Abel, 1829)** *Se $g(X)$ è irriducibile in $F[X]$ e se $f(X)$ e $g(X)$ hanno una radice comune in K, allora $g(X)$ divide $f(X)$ in $F[X]$.*

Dimostrazione: (*a*) I coefficienti del quoziente e del resto della divisione euclidea di $f(X)$ per $g(X)$ sono univocamente determinati come funzioni razionali dei coefficienti di $f(X)$ e $g(X)$. In particolare, se $f(X) := \sum a_i X^i$, $g(X) = \sum b_j X^j$ e $\mathbb{F}$ è il sottocampo fondamentale di F, tali coefficienti appartengono al campo $\mathbb{F}(a_i, b_j)$, che è il minimo campo su cui sono definiti sia $f(X)$ che $g(X)$ (Paragrafo 4).

(*b*) e (*c*) seguono direttamente da (*a*), ricordando che il massimo comune divisore di due polinomi si può determinare con l'algoritmo euclideo delle divisioni successive.

(*d*) $f(X)$ e $g(X)$ hanno un fattore comune non costante in $F[X]$ se e soltanto se il loro massimo comune divisore ha grado positivo, ovvero ha una radice in un suo campo di spezzamento su F.

(*e*) Se $f(X)$ e $g(X)$ hanno una radice comune $\alpha \in K$, il loro massimo comune divisore in $K[X]$ è diviso da $(X-\alpha)$. Perciò esso ha grado positivo. Per il punto (*c*), $f(X)$ e $g(X)$ hanno un fattore comune di grado positivo in $F[X]$. Allora poiché $g(X)$ è irriducibile su F, $g(X)$ deve dividere $f(X)$ in $F[X]$.

Se F è un campo e $f(X) := c_0 + c_1X + \cdots + c_nX_n \in F[X]$, indichiamo con $f'(X)$ la *derivata formale* di $f(X)$, ovvero il polinomio

$$f'(X) := c_1 + 2c_2X \cdots + nc_nX^{n-1}.$$

È evidente che $f'(X) \in F[X]$; esiste perciò un ampliamento finito K di F in cui sia $f(X)$ che $f'(X)$ hanno tutte le loro radici, precisamente un campo di spezzamento su F del polinomio $f(X)f'(X)$.

Ricordiamo che, se $m \geq 1$, una radice α di $f(X)$ ha *molteplicità* m, se $(X-\alpha)^m$ divide $f(X)$ in $K[X]$ ma $(X-\alpha)^{m+1}$ non lo divide.

Una radice di molteciplità almeno uguale a 2 si dice anche una *radice multipla*, mentre una radice di molteciplità uguale a 1 si dice anche una *radice semplice*.

Proposizione 9.5 *Sia F un campo e $f(X) \in F[X]$. Allora una radice α di $f(X)$ è una radice multipla se e soltanto se $f'(\alpha) = 0$.*

Dimostrazione: Sia K un campo di spezzamento del polinomio $f(X)f'(X)$. Per definizione, un elemento $\alpha \in K$ è una radice multipla di $f(X)$ se e soltanto se $(X-\alpha)^2$ divide $f(X)$ in $K[X]$. Se $f(X) = (X-\alpha)^2g(X)$, passando alle derivate formali si ottiene

$$f'(X) = 2(X-\alpha)g(X) + (X-\alpha)^2g'(X).$$

Quindi $f'(\alpha) = 0$.

Viceversa, se $f(\alpha) = f'(\alpha) = 0$, allora $(X-\alpha)$ divide sia $f(X)$ che $f'(X)$ in $K[X]$. Se $f(X) = (X-\alpha)h(X)$, si ottiene $f'(X) = h(X) + (X-\alpha)h'(X)$. Poiché $(X-\alpha)$ divide $f'(X)$, ne segue che $(X-\alpha)$ divide $h(X)$ e allora $(X-\alpha)^2$ divide $f(X)$.

Corollario 9.6 *Sia F un campo e sia $p(X) \in F[X]$ un polinomio irriducibile. Allora $p(X)$ ha una radice multipla se e soltanto se $p'(X) = 0$.*

Dimostrazione: Per le Proposizioni 1.9.4(e) e 1.9.5, $p(X)$ ha una radice multipla se e soltanto se $p(X)$ divide $p'(X)$. Questo non è possibile se $p'(X) \neq 0$, perché in questo caso $p'(X)$ ha grado minore di $p(X)$.

Proposizione 9.7 *Sia F un campo di caratteristica zero e sia $p(X) \in F[X]$ un polinomio irriducibile. Allora le radici di $p(X)$, in un qualsiasi suo campo di spezzamento, sono tutte semplici.*

Dimostrazione: Poiché $p(X)$ è non costante, se F ha caratteristica zero, si ha che $p'(X) \neq 0$. Per il Corollario 9.6, allora $p(X)$ non può avere radici multiple.

Corollario 9.8 *Sia F un campo numerico e sia $p(X) \in F[X]$ un polinomio irriducibile di grado n. Allora $p(X)$ ha esattamente n radici complesse distinte.*

Esempi

9.2. Sia F un campo numerico e sia $\alpha \in \mathbb{C}$ algebrico su F di grado n, con polinomio minimo $p(X)$. Poiché le n radici complesse di $p(X)$ sono tutte distinte, ci sono esattamente n F-isomorfismi distinti di $F(\alpha)$ in $\mathbb{C}$. Precisamente, se $\alpha = \alpha_1, \ldots, \alpha_n$ sono le radici complesse di $p(X)$, gli F-isomorfismi $F(\alpha) \longrightarrow \mathbb{C}$ sono tutti e soli quelli definiti ponendo $f(\alpha) \mapsto f(\alpha_i)$, per ogni $f(X) \in F[X]$ e $1 \leq i \leq n$.

Viceversa, se $\gamma \in \mathbb{C}$ è algebrico su F e si conoscono tutti gli F-isomorfismi distinti $\varphi_1, \ldots, \varphi_m$ di $F(\gamma)$ in $\mathbb{C}$, si può concludere che γ ha grado m su F ed il suo polinomio minimo su F è $m(X) = (X - \varphi_1(\gamma)) \ldots (X - \varphi_m(\gamma))$.

9.3. Tutti gli F-isomorfismi di un ampliamento finito di F in $\mathbb{C}$ si possono costruire per iterazione. Infatti, siano α e β algebrici su F. Se $q(X)$ è il polinomio minimo di β su $F(\alpha)$, allora $\mathbb{C}$ contiene tutte le radici del polinomio $\varphi^*(q(X)) =: q^*(X)$ per ognuno degli F-isomorfismi φ di $F(\alpha)$ in $\mathbb{C}$. Poiché $q^*(X)$ è irriducibile, tali radici sono tutte distinte ed il loro numero è uguale a $\deg(q^*(X)) = \deg(q(X)) = [F(\alpha, \beta) : F(\alpha)]$. Perciò ogni φ si può estendere a $[F(\alpha, \beta) : F(\alpha)]$ F-isomorfismi di $F(\alpha, \beta)$ in $\mathbb{C}$ (Proposizione 9.2).

Illustriamo questo procedimento con alcuni esempi.

(*a*) Il polinomio $p(X) := X^3 - 3X + 1 \in \mathbb{Q}[X]$ è irriducibile su $\mathbb{Q}$, non avendo radici razionali. Se α è una radice di $p(X)$, le altre due radici di $p(X)$ sono $\beta := (\alpha^2 - 2)$ e $\gamma := (-\alpha(\alpha + 1) + 2)$ (Esempio 7.8(a)). Dunque gli isomorfismi di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ sono tre e sono definiti da:

$$\psi_1 := id : f(\alpha) \mapsto f(\alpha) \; ; \; \psi_2 : f(\alpha) \mapsto f(\beta) \; ; \; \psi_3 : f(\alpha) \mapsto f(\gamma),$$

per ogni polinomio $f(X) \in \mathbb{Q}[X]$ (di grado al più uguale a 2). Poiché $\beta, \gamma \in \mathbb{Q}(\alpha)$, questi sono tutti e soli gli automorfismi di $\mathbb{Q}(\alpha)$. Quindi $\mathrm{Aut}(\mathbb{Q}(\alpha))$ ha tre elementi e perciò è un gruppo ciclico di ordine 3.

(*b*) Il polinomio minimo di $\alpha := \sqrt[3]{2}$ su $\mathbb{Q}$ è $p(X) := X^3 - 2$ e le sue radici complesse sono $\alpha, \alpha\xi$ e $\alpha\xi^2$, dove $\xi := \frac{-1+i\sqrt{3}}{2}$ è una radice primitiva terza dell'unità (Esempio 7.8(b)). Dunque gli isomorfismi di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ sono ancora tre e sono definiti da:

$$\psi_1 := id : f(\alpha) \mapsto f(\alpha) \; ; \; \psi_2 : f(\alpha) \mapsto f(\alpha\xi) \; ; \; \psi_3 : f(\alpha) \mapsto f(\alpha\xi^2),$$

per ogni polinomio $f(X) \in \mathbb{Q}[X]$ (di grado al più uguale a 2). Poiché $\alpha\xi$ e $\alpha\xi^2$ non stanno in $\mathbb{Q}(\alpha)$, soltanto l'identità è un automorfismo di $\mathbb{Q}(\alpha)$.

(*c*) Siano $\alpha := \sqrt[3]{2}$ e $\beta := \sqrt{3}$. Determiniamo gli isomorfismi di $K := \mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$.

Il polinomio minimo di β su $\mathbb{Q}(\alpha)$ è $q(X) := X^2 - 3$, che ha radici β e $-\beta$. Allora ognuno degli isomorfismi $\psi_1 := id, \psi_2, \psi_3$ di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ precedentemente costruiti si estende a due isomorfismi di $\mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$. In tutto si ottengono 6 isomorfismi, precisamente:

$$\begin{aligned}
\psi_{11} := id : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha,\beta) \qquad & (\alpha \mapsto \alpha, \quad \beta \mapsto \beta) \\
\psi_{21} : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha\xi,\beta) \qquad & (\alpha \mapsto \alpha\xi, \quad \beta \mapsto \beta) \\
\psi_{31} : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha\xi^2,\beta) \qquad & (\alpha \mapsto \alpha\xi^2, \quad \beta \mapsto \beta) \\
\psi_{12} : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha,-\beta) \qquad & (\alpha \mapsto \alpha, \quad \beta \mapsto -\beta) \\
\psi_{22} : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha\xi,-\beta) \qquad & (\alpha \mapsto \alpha\xi, \quad \beta \mapsto -\beta) \\
\psi_{32} : K \longrightarrow \mathbb{C},\ h(\alpha,\beta) \mapsto h(\alpha\xi^2,-\beta) \qquad & (\alpha \mapsto \alpha\xi^2, \quad \beta \mapsto -\beta)
\end{aligned}$$

per ogni elemento

$$h(\alpha,\beta) = c_0 + c_1\alpha + c_2\alpha^2 + c_3\beta + c_4\alpha\beta + c_5\alpha^2\beta \in \mathbb{Q}(\alpha,\beta).$$

Notiamo che i soli automorfismi di $K := \mathbb{Q}(\alpha, \beta)$ sono $\psi_{11} = id$ e ψ_{12}. Questi sono anche i $\mathbb{Q}(\alpha)$-isomorfismi di K in $\mathbb{C}$.

(*d*) Sia $F \subseteq \mathbb{R}$ e $K := F(\sqrt{a}, \sqrt{b})$ un ampliamento biquadratico di F. Gli F-isomorfismi di K in $\mathbb{C}$ possono essere costruiti considerando la catena di ampliamenti

$$F \subseteq F(\sqrt{a}) \subseteq F(\sqrt{a}, \sqrt{b}).$$

Gli F-isomorfismi di $F(\sqrt{a})$ in $\mathbb{C}$ sono 2, precisamente:

$$\begin{aligned}
\varphi_1 := id : F(\sqrt{a}) \longrightarrow \mathbb{C},\ x + y\sqrt{a} \mapsto x + y\sqrt{a} \quad & (\sqrt{a} \mapsto \sqrt{a}) \\
\varphi_2 : F(\sqrt{a}) \longrightarrow \mathbb{C},\ x + y\sqrt{a} \mapsto x - y\sqrt{a} \quad & (\sqrt{a} \mapsto -\sqrt{a}).
\end{aligned}$$

Questi sono anche F-automorfismi di $F(\sqrt{a})$. Gli F-isomorfismi di K in $\mathbb{C}$ che estendono l'identità su $F(\sqrt{a})$ (ovvero gli $F(\sqrt{a})$-isomorfismi) sono:

$$\begin{aligned}
\varphi_{11} := id : K \longrightarrow \mathbb{C},\ h(\sqrt{a},\sqrt{b}) \mapsto h(\sqrt{a},\sqrt{b}) \qquad & (\sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}) \\
\varphi_{12} : K \longrightarrow \mathbb{C},\ h(\sqrt{a},\sqrt{b}) \mapsto h(\sqrt{a},-\sqrt{b}) \qquad & (\sqrt{a} \mapsto \sqrt{a}, \quad \sqrt{b} \mapsto -\sqrt{b})
\end{aligned}$$

gli F-isomorfismi di K che estendono φ_2 sono:

$$\begin{aligned}
\varphi_{21} : K \longrightarrow \mathbb{C},\ h(\sqrt{a},\sqrt{b}) \mapsto h(-\sqrt{a},\sqrt{b}) \qquad & (\sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto \sqrt{b}) \\
\varphi_{22} : K \longrightarrow \mathbb{C},\ h(\sqrt{a},\sqrt{b}) \mapsto h(-\sqrt{a},-\sqrt{b}) \qquad & (\sqrt{a} \mapsto -\sqrt{a}, \quad \sqrt{b} \mapsto -\sqrt{b})
\end{aligned}$$

per ogni elemento

$$h(\sqrt{a},\sqrt{b}) = c_0 + c_1\sqrt{a} + c_2\sqrt{b} + c_3\sqrt{a} + c_4\sqrt{ab} \in F(\sqrt{a},\sqrt{b}).$$

Questi sono tutti automorfismi di K. Quindi $\mathrm{Aut}_F(K)$ ha 4 elementi e non è difficile verificare che esso è un gruppo di Klein.

9.4. Se $\alpha \in \mathbb{C}$ ha grado alto su F, per determinare gli F-isomorfismi di $F(\alpha)$ in $\mathbb{C}$, conviene talvolta considerare un campo intermedio L dell'ampliamento $F \subseteq F(\alpha)$, costruire prima gli F-isomorfismi di L in $\mathbb{C}$ ed estendere poi a $F(\alpha) = L(\alpha)$ ognuno di questi F-isomorfismi.

Sia ad esempio $\alpha := \sqrt[3]{\sqrt{2}+\sqrt{3}}$. Allora $\sqrt{2}+\sqrt{3} = \alpha^3 \in \mathbb{Q}(\alpha)$ e possiamo considerare il sottocampo $L := \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ di $\mathbb{Q}(\alpha)$.

Gli isomorfismi di L in $\mathbb{C}$ sono quattro e si possono costruire come nell'esempio precedente per $a = 2, b = 3$. Poiché α ha grado 3 su L, con polinomio minimo $m(X) = X^3 - (\sqrt{2}+\sqrt{3})$, allora ognuno di questi quattro isomorfismi si estende a 3 isomorfismi di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$.

Ad esempio, consideriamo l'isomorfismo

$$\varphi_{12} : L \longrightarrow \mathbb{C} \text{ definito da } \sqrt{2} \mapsto \sqrt{2} \text{ e } \sqrt{3} \mapsto -\sqrt{3}.$$

Le radici del polinomio $\varphi_{12}^*(m(X)) = X^3 - (\sqrt{2}-\sqrt{3})$ sono

$$\beta := \sqrt[3]{\sqrt{2}-\sqrt{3}}, \quad \beta\xi, \quad \beta\xi^2,$$

dove $\xi := \frac{-1+i\sqrt{3}}{2}$ è una radice primitiva terza dell'unità. Dunque gli isomorfismi di $L(\alpha) = \mathbb{Q}(\alpha)$ in $\mathbb{C}$ che estendono φ_{12} sono:

$$\begin{aligned}
&\psi_1 : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}, \ \text{ definito da } \alpha \mapsto \beta;\\
&\psi_2 : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}, \ \text{ definito da } \alpha \mapsto \beta\xi;\\
&\psi_3 : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}, \ \text{ definito da } \alpha \mapsto \beta\xi^2.
\end{aligned}$$

In modo analogo si possono costruire tutti gli isomorfismi di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$, che sono 12. Ne segue che α ha grado 12 su $\mathbb{Q}$ e le radici del suo polinomio minimo sono le immagini di α tramite questi isomorfismi.

Teorema 9.9 *Sia F un campo, $f(X) \in F[X]$ e K un suo campo di spezzamento. Se φ è un isomorfismo di F in F' e il campo K' è un ampliamento di F' contenente un campo di spezzamento del polinomio $f^*(X) := \varphi^*(f(X))$ su F', allora esiste un isomorfismo ψ di K in K' che estende φ. Inoltre il numero di tali estensioni è al più $[K:F]$ ed è esattamente $[K:F]$ se $f^*(X)$ non ha radici multiple in K'.*

Dimostrazione: Procediamo per induzione sul grado $[K:F]$.

Se $[K : F] = 1$, allora $F = K$ è un campo di spezzamento di $f(X)$. Inoltre, se $f(X) = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$ su F, allora su F' si ha $f^*(X) = \varphi(c)(X - \varphi(\alpha_1))(X - \varphi(\alpha_2)) \dots (X - \varphi(\alpha_n))$ e perciò F' contiene un campo di spezzamento di $f^*(X)$. Ne segue che $\varphi : F \longrightarrow F'$ è esso stesso un isomorfismo di $K = F$ in K'.

Supponiamo che $[K : F] > 1$. Allora $f(X)$ ha una radice $\alpha \in K \setminus F$ e il polinomio minimo $m(X)$ di α su F è un fattore irriducibile di $f(X)$ di grado $m > 1$. Dunque $m^*(X)$ è un fattore (irriducibile) di $f^*(X)$ e per ipotesi ha una radice in K'. Per la Proposizione 9.2, ci sono allora $s \leq m = [F(\alpha) : F]$ omomorfismi $\psi_i : F(\alpha) \longrightarrow K'$, $i = 1, \dots, s$, che estendono φ ed inoltre $s = m$ se $m^*(X)$ non ha radici multiple in K'.

Osserviamo ora che K è anche un campo di spezzamento di $f(X)$ su $F(\alpha)$ e analogamente K' contiene anche un campo di spezzamento di $f^*(X)$ su $\mathrm{Im}(\psi_i) = \psi_i(F(\alpha)) = F'(\psi_i(\alpha))$. Poiché si ha

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)]m,$$

allora in particolare $[K : F(\alpha)] < [K : F]$.

Per l'ipotesi induttiva, per ogni $i = 1, \dots, s$, ci sono $r_i \leq [K : F(\alpha)]$ isomorfismi di K in K' che estendono l'isomorfismo $\psi_i : F(\alpha) \longrightarrow F'(\psi_i(\alpha))$ e inoltre $r_i = [K : F(\alpha)]$ se $\psi_i^*(f(X)) = \varphi^*(f(X)) = f^*(X)$ non ha radici multiple in K'. Poiché la restrizione a $F(\alpha)$ di un isomorfismo di K in K' che estende φ deve coincidere con uno degli omomorfismi ψ_i, le estensioni $K \longrightarrow K'$ di φ sono al più $[K : F(\alpha)][F(\alpha) : F] = [K : F]$ e sono esattamente $[K : F]$ se $f^*(X)$ non ha radici multiple in K'.

Corollario 9.10 *Due campi di spezzamento K e K' di $f(X)$ su F sono isomorfi. Inoltre il numero degli F-isomorfismi di K in K' è al più $[K : F]$ ed è esattamente uguale a $[K : F]$ se $f(X)$ non ha radici multiple in K (e K').*

In particolare K ha al più $[K : F]$ F-automorfismi. Se inoltre $f(X)$ non ha radici multiple in K, allora gli F-automorfismi di K sono esattamente $[K : F]$.

Dimostrazione: Basta applicare il teorema precedente al caso in cui φ sia l'identità su F.

Una dimostrazione diretta del Corollario 9.10, che illustra meglio il procedimento induttivo, è la seguente.

Dimostrazione diretta del Corollario 9.10. Sia α_1 una radice di $f(X)$ in K e sia $m_1(X)$ il suo polinomio minimo su F. Poiché $m_1(X)$ divide $f(X)$ in $F[X]$ e $f(X)$ si spezza linearmente su K', $m_1(X)$ ha tutte le sue radici in K'. Allora, se $\beta_1, \dots, \beta_s$ sono le radici distinte di $m_1(X)$ in K', gli F-isomorfismi di $F(\alpha_1)$ in K' sono esattamente quelli definiti da

$$\varphi_i : F(\alpha_1) \longrightarrow F(\beta_i) \subseteq K', \quad \varphi_i(\alpha_1) = \beta_i, \quad \text{per } i = 1, \dots, s$$

(Proposizione 9.2). Notiamo che $s \leq \deg(m_1(X)) = [F(\alpha_1) : F]$ e vale l'uguaglianza se tutte le radici di $m_1(X)$ in K' sono distinte.

Osserviamo ora che possiamo scrivere $f(X) = (X - \alpha_1)^k g_1(X)$, con $g_1(X) \in F(\alpha_1)[X] \subseteq K[X]$ e $g_1(\alpha_1) \neq 0$. Dunque

$$f(X) = \varphi_i^*(f(X)) = (X - \varphi_i(\alpha_1))^k \varphi_i^*(g_1(X)) = (X - \beta_i)^k \varphi_i^*(g_1(X))$$

su $F(\beta_i)$.

Se $\deg(g_1(X)) = 0$, ovvero $g_1(X) \in F(\alpha_1)$, allora $K = F(\alpha_1)$. Inoltre, in questo caso, $\varphi_i^*(g_1(X)) \in F(\beta_i)$ e dunque $f(X)$ si spezza linearmente su $F(\beta_i)$. Perciò risulta $K' = F(\beta_i)$ e $\varphi_i : K \longrightarrow K'$ è un isomorfismo di campi.

Se invece $\deg(g_1(X)) > 0$, allora $g_1(X)$ ha una radice α_2, distinta da α_1, in K. In questo caso, sia $m_2(X)$ il polinomio minimo di α_2 su $F(\alpha_1)$ e sia $g_1(X) = m_2(X)h_1(X)$, con $h_1(X) \in F(\alpha_1)$. Allora $\varphi_i^*(g_1(X)) = \varphi_i^*(m_2(X))\varphi_i^*(h_1(X))$ e $\varphi_i^*(m_2(X))$ divide $f(X)$ su K'. Ne segue che il polinomio $\varphi_i^*(m_2(X))$ si spezza linearmente su K' e, per ogni radice β_j di $\varphi_i^*(m_2(X))$ (necessariamente distinta da β_i), l'isomorfismo $\varphi_i : F(\alpha_1) \longrightarrow F(\beta_i)$ si può estendere ad un F-isomorfismo $\varphi_{ij} : F(\alpha_1, \alpha_2) \longrightarrow F(\beta_i, \beta_j) \subseteq K'$ ponendo $\varphi_{ij}(\alpha_1) = \beta_i$ e $\varphi_{ij}(\alpha_2) = \beta_j$. Il numero delle possibili estensioni di φ_i è uguale al numero delle radici distinte di $\varphi_i^*(m_2(X))$ in K', dunque al più uguale a $\deg(\varphi_i^*(m_2(X))) = \deg(m_2(X)) = [F(\alpha_1, \alpha_2) : F(\alpha_1)]$. Ne segue che il numero degli F-isomorfismi di $F(\alpha_1, \alpha_2)$ in K' è al più uguale a

$$\deg(m_2(X)) \deg(m_1(X)) = [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] = [F(\alpha_1, \alpha_2) : F]$$

e l'uguaglianza è raggiunta se $f(X)$ non ha radici multiple in K'.

A questo punto, su $F(\alpha_1, \alpha_2)$, risulta $f(X) = (X - \alpha_1)^k (X - \alpha_2)^h g_2(X)$ con $g_2(\alpha_1) \neq 0$ e $g_2(\alpha_2) \neq 0$. Inoltre $\varphi_{ij}^* f(X) = (X - \beta_1)^k (X - \beta_2)^h \varphi_{ij}^*(g_2(X))$. Se $g_2(X) \in F(\alpha_1, \alpha_2)$, allora $\varphi_{ij}^*(g_2(X)) \in F(\beta_1, \beta_2)$. Dunque $K = F(\alpha_1, \alpha_2)$, $K' = F(\beta_1, \beta_2)$ e $\varphi_{ij} : K \longrightarrow K'$ è un isomorfismo. Altrimenti si ripete il procedimento.

Dopo un numero finito di passi si ottiene che $K = F(\alpha_1, \ldots, \alpha_n)$ e $K' = (\beta_1, \ldots, \beta_n)$, dove $\alpha_1, \ldots, \alpha_n$ sono le radici distinte di $f(X)$ nel campo K e $\beta_1, \ldots, \beta_n$ sono le radici distinte di $f(X)$ nel campo K'. Inoltre K e K' sono isomorfi, il numero degli F-isomorfismi tra K e K' è al più uguale a $[K : F] = [K' : F]$ e l'uguaglianza è raggiunta se le radici di $f(X)$ in K' (e K) sono tutte distinte.

Seguendo il procedimento indicato in questa ultima dimostrazione, se K è un campo di spezzamento di $f(X)$ su F, possiamo determinare gli F-automorfismi di K nel seguente modo.

Siano $\alpha_1, \ldots, \alpha_n$ le radici distinte di $f(X)$ nel campo K. Consideriamo la catena di ampliamenti semplici

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_n := F_{n-1}(\alpha_n) = K.$$

Se $m_1(X)$ è il polinomio minimo di α_1 su F, gli F-isomorfismi di F_1 in K sono tanti quante sono le radici distinte di $m_1(X)$ in K e, per ogni tale radice β, si ha l'isomorfismo $\psi_\beta : F_1 \longrightarrow K$ definito da

$$c_0 + c_1\alpha_1 + \cdots + c_s\alpha_1^s \mapsto c_0 + c_1\beta + \cdots + c_s\beta^s,$$

dove $s = \deg(m_1(X)) - 1$ e $c_i \in F$ per $i = 1, \ldots, s$.

Gli F-isomorfismi di F_2 in K, ristretti a F_1 devono coincidere con uno degli omomorfismi ψ_β appena costruiti e quindi sono estensioni di qualche ψ_β. Se $m_2(X)$ è il polinomio minimo di α_2 su F_1, gli isomorfismi di F_2 in K che estendono ψ_β sono tanti quante sono le radici distinte di $\psi_\beta^*(m_2(X))$ in K e, per ogni tale radice γ, si ha l'isomorfismo $\psi_{\beta\gamma} : F_2 \longrightarrow K$ definito da:

$$d_0 + d_1\alpha_2 + \cdots + d_r\alpha_2^r \mapsto \psi_\beta(d_0) + \psi_\beta(d_1)\gamma + \cdots + \psi_\beta(d_r)\gamma^r,$$

dove $r = \deg(m_2(X)) - 1$ e $d_i \in F_1$ per $i = 1, \ldots, r$.

Così proseguendo, dopo n passi, si ottengono tutti gli F-automorfismi di K. Notiamo che, se ψ è uno di questi automorfismi e α è una radice di $f(X)$, allora anche $\psi(\alpha)$ è una radice di $f(X)$.

Come abbiamo appena visto, i campi di spezzamento di un polinomio $f(X)$ su un campo F sono tutti isomorfi. Nel seguito, se F è un campo numerico, parleremo del campo di spezzamento di $f(X)$ riferendoci al suo campo di spezzamento in $\mathbb{C}$.

Esempi

9.5. Se $f(X)$ è un polinomio a coefficienti in un campo numerico F e $K \subseteq \mathbb{C}$ è il suo campo di spezzamento, gli F-automorfismi di K sono esattamente gli F-isomorfismi di K in $\mathbb{C}$ e si possono costruire come visto nell'Esempio 9.3. Infatti, se $\alpha_1, \ldots, \alpha_n$ sono le radici complesse distinte di $f(X)$, il polinomio minimo di α_i su $F_{i-1} := F(\alpha_1, \ldots, \alpha_{i-1})$ divide $f(X)$ in $\mathbb{C}[X]$ e perciò ha tutte le sue radici nel campo K.

9.6. Sia $f(X) := (X^2 + X + 1)(X^3 + X + 1) \in \mathbb{F}_2[X]$ e sia K un suo campo di spezzamento. Abbiamo visto nell'Esempio 8.4 che i polinomi $p(X) := X^2 + X + 1$ e $q(X) := X^3 + X + 1$ hanno tutte radici distinte in K e che K ha grado 6 su $\mathbb{F}_2$. Dunque ci sono 6 automorfismi di K, perché ogni automorfismo di K è l'identità sul suo sottocampo fondamentale $\mathbb{F}_2$. Per costruirli, procediamo nel seguente modo.

Se α è una radice di $p(X)$ e β è una radice di $q(X)$, consideriamo la catena:

$$\mathbb{F}_2 \subseteq \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_2(\alpha, \beta) = K.$$

Il polinomio minimo di α su $\mathbb{F}_2$ è $p(X)$ e il polinomio minimo di β su $\mathbb{F}_2(\alpha)$ è $q(X)$. Le radici di $p(X)$ in K sono α e $\alpha + 1 = \alpha^2$ e le radici di $q(X)$ in K sono β, β^2 e $\beta + \beta^2 = \beta^4$. Allora risulta:

$$K = \left\{ \sum c_{ij}\alpha^i\beta^j ; c_{ij} \in \mathbb{F}_2,\ i = 1, 2,\ j = 1, 2, 3;\ \alpha^2 = \alpha + 1,\ \beta^3 = \beta + 1 \right\}.$$

Gli isomorfismi di $\mathbb{F}_2(\alpha)$ in K che estendono l'identità su $\mathbb{F}_2$ sono:

$$\begin{aligned} \varphi_1 := id : \mathbb{F}_2(\alpha) &\longrightarrow K, \quad \text{l'identità su } \mathbb{F}_2(\alpha); \\ \varphi_2 : \mathbb{F}_2(\alpha) &\longrightarrow K, \quad \text{definito da } \alpha \mapsto \alpha^2. \end{aligned}$$

Ci sono poi tre automorfismi di K che estendono l'identità su $\mathbb{F}_2(\alpha)$ e tre automorfismi di K che estendono φ_2. I tre automorfismi di K che estendono l'identità su $\mathbb{F}_2(\alpha)$ sono:

$$\begin{aligned} \varphi_{11} := id : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha,\beta) \quad (\alpha \mapsto \alpha,\ \ \beta \mapsto \beta) \\ \varphi_{12} : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha,\beta^2) \quad (\alpha \mapsto \alpha,\ \ \beta \mapsto \beta^2) \\ \varphi_{13} : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha,\beta^4) \quad (\alpha \mapsto \alpha,\ \ \beta \mapsto \beta^4) \end{aligned}$$

e i tre automorfismi di K che estendono φ_2 sono:

$$\begin{aligned} \varphi_{21} : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha^2,\beta) \quad (\alpha \mapsto \alpha^2,\ \ \beta \mapsto \beta) \\ \varphi_{22} : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha^2,\beta^2) \quad (\alpha \mapsto \alpha^2,\ \ \beta \mapsto \beta^2) \\ \varphi_{23} : K \longrightarrow K,\ h(\alpha,\beta) \mapsto h(\alpha^2,\beta^4) \quad (\alpha \mapsto \alpha^2,\ \ \beta \mapsto \beta^4) \end{aligned}$$

per ogni elemento $h(\alpha,\beta) = \sum c_{ij}\alpha^i\beta^j \in K$.

Vedremo successivamente che $\mathrm{Aut}(K)$ è un gruppo ciclico (Esempio 10.12).

ESERCIZI

9.1. Mostrare che la composizione di due F-isomorfismi è un F-isomorfismo.

9.2. Sia $F \subseteq K$ un ampliamento di campi. Verificare che gli F-automorfismi di K formano un sottogruppo di $\mathrm{Aut}(K)$.

9.3. Mostrare che, se $F \subseteq K$ e $F \subseteq K'$ sono ampliamenti di campi, un F-isomorfismo di K in K' è una applicazione F-lineare. Dare inoltre un esempio di una applicazione F-lineare tra due ampliamenti di F che non è un omomorfismo di campi.

9.4. Determinare tutti gli $\mathbb{R}$-automorfismi di $\mathbb{C}$.

9.5. Determinare tutti gli isomorfismi in $\mathbb{C}$ dei seguenti campi e stabilire quali tra essi sono automorfismi:

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

9.6. Determinare tutti gli isomorfismi in $\mathbb{C}$ del campo $\mathbb{Q}(\sqrt[4]{\sqrt[3]{2} + \sqrt{3}})$.

9.7. Siano K e K' campi di spezzamento rispettivamente dei polinomi

$$X^2 + X + 1, \quad X^2 + 4X + 1 \in \mathbb{F}_5[X].$$

Mostrare che K e K' sono isomorfi e determinare tutti i possibili isomorfismi tra di essi (*Suggerimento*: Procedere come nella dimostrazione del Corollario 9.10).

9.8. Determinare tutti gli automorfismi del campo di spezzamento su $\mathbb{Q}$ dei polinomi:

$$X^2 + X + 1, \quad X^3 - 5, \quad X^4 + X^2 + 2X + 2.$$

9.9. Sia $\varphi : F \longrightarrow F'$ un isomorfismo di campi. Siano $X_1, \ldots, X_n$ indeterminate algebricamente indipendenti su F e $Y_1, \ldots, Y_n$ indeterminate indipendenti su F'. Mostrare che φ si può estendere a un isomorfismo $\psi : F(X_1, \ldots, X_n) \longrightarrow F'(Y_1, \ldots, Y_n)$ ponendo $\psi(c) = \varphi(c)$ per ogni $c \in F$ e $\psi(X_i) = Y_i$ per ogni $= 1, \ldots, n$.

10 Campi Finiti

Un *campo finito* è un campo con un numero finito di elementi. Dunque esso ha necessariamente caratteristica finita e grado finito sul suo sottocampo fondamentale.

Proposizione 10.1 *Se K è un campo finito allora il suo ordine è p^n, dove p è la caratteristica di K e $n := [K : \mathbb{F}_p]$. Inoltre il gruppo moltiplicativo $K^* := K \setminus \{0\}$ è un gruppo ciclico.*

Dimostrazione: Se $[K : \mathbb{F}_p] = n$, allora K è isomorfo a $\mathbb{F}_p^n$ come spazio vettoriale su $\mathbb{F}_p$ e dunque ha p^n elementi. Inoltre K^* è un gruppo ciclico per la Proposizione 1.2.

L'esistenza di campi finiti di ogni ordine ammissibile è stata dimostrata da E. Galois nel 1830. Successivamente E. H. Moore dimostrò, nel 1893, che due campi finiti dello stesso ordine sono isomorfi.

Lemma 10.2 *Se K è un campo di caratteristica prima p, allora $(x+y)^{p^h} = x^{p^h} + y^{p^h}$ per ogni $x, y \in K$, $h \geq 1$.*

Dimostrazione: Sia $h = 1$. Se $p > k > 0$, allora p divide tutti i coefficienti binomiali $\binom{p}{k} := \frac{p!}{k!(p-k)!}$, perché non divide $k!(p-k)!$. Dunque tali coefficienti sono nulli in caratteristica p e l'uguaglianza è verificata. Si procede poi per induzione su h.

Teorema 10.3 (E. Galois - E. H. Moore) *Per ogni primo p e ogni $n \geq 1$ esiste un campo finito K con p^n elementi ed esso è unico a meno di isomorfismi. Precisamente K è un campo di spezzamento del polinomio $f_{p^n}(X) := X^{p^n} - X$ su $\mathbb{F}_p$ ed è costituito esattamente dalle radici di $f_{p^n}(X)$.*

Dimostrazione: Sia K un campo di ordine $q = p^n$. Allora il gruppo moltiplicativo K^* ha $q - 1$ elementi e dunque, per ogni $\alpha \in K^*$, risulta $\alpha^{q-1} = 1$. Ne segue che ogni elemento di K è radice del polinomio $f_q(X)$ e

in particolare K è un campo di spezzamento di $f_q(X)$. Perciò, se K esiste, K è unico a meno di isomorfismi (Teorema 9.9).

Resta da mostrare che un campo di spezzamento del polinomio $f_q(X)$ ha esattamente q elementi. Osserviamo intanto che le radici di $f_q(X)$ in un suo campo di spezzamento sono tutte distinte; infatti $f_q(X)$ e la sua derivata formale $f'_q(X) = qX^{q-1} - 1 = -1$ non hanno radici comuni.

Verifichiamo per finire che le q radici di $f_q(X)$ formano un campo; ovvero che, se α, β sono radici di $f_q(X)$, $\beta \neq 0$, allora anche e $\alpha - \beta$ e $\alpha\beta^{-1}$ sono radici di $f_q(X)$. Per il Lemma 10.2 risulta $(\alpha - \beta)^p = \alpha^p - \beta^p$ e dunque, per induzione su n, $(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta$. Infine è evidente che $(\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1}$.

Nel seguito indicheremo come d'uso con $\mathbb{F}_{p^n}$ un campo con p^n elementi. Tale notazione non è ambigua essendo tale campo univocamente determinato a meno di isomorfismi. Il campo $\mathbb{F}_{p^n}$ si dice anche il *campo di Galois di ordine* p^n.

Proposizione 10.4 *Il campo $\mathbb{F}_{p^n}$ è un ampliamento semplice di $\mathbb{F}_p$ (di grado n). Precisamente, se α è un generatore di $\mathbb{F}^*_{p^n}$ come gruppo ciclico, allora $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.*

Dimostrazione: Se α è un generatore di $\mathbb{F}^*_{p^n}$, si ha che $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$. Poiché chiaramente vale anche l'inclusione opposta, si ha l'uguaglianza.

La proposizione precedente mostra che ogni generatore del gruppo ciclico $\mathbb{F}^*_{p^n}$ è anche un generatore del campo $\mathbb{F}_{p^n}$ come ampliamento semplice di $\mathbb{F}_p$. Osserviamo però che se $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, non è detto che α generi $\mathbb{F}^*_{p^n}$ come gruppo ciclico, come è mostrato dagli esempi successivi.

Corollario 10.5 *Per ogni primo p e ogni $n \geq 1$ esiste un polinomio $p(X) \in \mathbb{F}_p[X]$ di grado n irriducibile su $\mathbb{F}_p$. Inoltre il campo $\mathbb{F}_{p^n}$ è isomorfo al campo $\frac{\mathbb{F}_p[X]}{\langle p(X)\rangle}$.*

Dimostrazione: Se $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, il polinomio minimo di α su $\mathbb{F}_p$ è irriducibile su $\mathbb{F}_p$ e ha grado n. Se inoltre $p(X)$ è un polinomio di grado n irriducibile su $\mathbb{F}_p$, il campo

$$K := \frac{\mathbb{F}_p[X]}{\langle p(X)\rangle} = \left\{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}\,;\; c_i \in \mathbb{F}_p\,,\; p(\alpha) = 0\right\}$$

ha p^n elementi. Per il Teorema 10.3, K è dunque isomorfo a $\mathbb{F}_{p^n}$.

Esempi

10.1. Il campo $\mathbb{F}_8$ è stato costruito nell'Esempio 8.3 come un campo di spezzamento del polinomio $p(X) := X^3 + X + 1 \in \mathbb{F}_2[X]$, che è irriducibile

su $\mathbb{F}_2$. Abbiamo visto che, se α è una radice di $p(X)$, le altre radici di $p(X)$ sono α^2 e $\alpha + \alpha^2 = \alpha^4$. Questi elementi hanno tutti grado 3 su $\mathbb{F}_2$ e perciò generano $\mathbb{F}_8$ su $\mathbb{F}_2$. Ma poiché il gruppo $\mathbb{F}_8^*$ ha 7 elementi, esso ha 6 generatori e quindi ha altri tre elementi di grado 3 su $\mathbb{F}_2$, precisamente

$$\alpha^3 = \alpha + 1\,, \quad \alpha^5 = \alpha^2 + \alpha + 1\,, \quad \alpha^6 = \alpha^2 + 1.$$

Questi devono essere le radici di un altro polinomio monico di grado 3 irriducibile su $\mathbb{F}_2$ e un semplice calcolo mostra che tale polinomio è $q(X) := X^3 + X^2 + 1$. Per finire osserviamo che $p(X)$ e $q(X)$ sono gli unici polinomi di grado 3 irriducibili su $\mathbb{F}_2$, perché le loro radici esauriscono $\mathbb{F}_8 \setminus \mathbb{F}_2$.

Se β è una qualsiasi radice di $q(X)$ in $\mathbb{F}_8$ risulta anche $\mathbb{F}_8 = \mathbb{F}_2(\beta)$ e le radici di $p(X)$ e $q(X)$ si possono esprimere in funzione di β. Ad esempio, se $\beta = \alpha^3 = \alpha + 1$, le radici di $p(X)$ sono:

$$\alpha = \beta + 1 = \beta^5\,, \quad \alpha^2 = \beta^2 + 1 = \beta^3\,, \quad \alpha^4 = \beta + \beta^2 = \beta^6$$

mentre le radici di $q(X)$ sono

$$\alpha^3 = \beta\,, \quad \alpha^5 = \alpha^2 + \alpha + 1 = \beta^4\,, \quad \alpha^6 = \alpha^2 + 1 = \beta^2.$$

10.2. Il campo $\mathbb{F}_9$ è stato costruito nell'Esempio 8.5. come un campo di spezzamento del polinomio $f(X) := (X^2 + 1)(X^2 + 2X + 2) \in \mathbb{F}_3[X]$. Abbiamo visto che, posto $p(X) := X^2 + 1$ e $q(X) := X^2 + 2X + 2$, si ha che $p(X)$ e $q(X)$ sono irriducibili su $\mathbb{F}_3$. Dunque, se α è una radice di $p(X)$ e β è una radice di $q(X)$, risulta $\mathbb{F}_9 = \mathbb{F}_3(\alpha) = \mathbb{F}_3(\beta)$.

Le radici di $p(X)$ in $\mathbb{F}_9$ sono α e $2\alpha = \alpha^3$. Osserviamo che α ha ordine moltiplicativo uguale a 4, infatti risulta

$$\alpha^2 = 2\,, \quad \alpha^3 = 2\alpha\,, \quad \alpha^4 = 1.$$

Dunque α non genera il gruppo $\mathbb{F}_9^*$, che ha ordine 8, mentre genera il campo $\mathbb{F}_9$ su $\mathbb{F}_3$. Una radice di $q(X)$ è $\beta = \alpha + 2$. Poiché

$$\beta^2 = \alpha\,, \quad \beta^3 = 2\alpha + 2\,, \quad \beta^4 = 2 \neq 1,$$

allora β ha ordine moltiplicativo uguale a 8 e genera $\mathbb{F}_9^*$ come gruppo ciclico. Gli altri generatori del gruppo $\mathbb{F}_9^*$ sono

$$\beta^3 = 2\alpha + 2\,, \quad \beta^5 = 2\alpha + 1\,, \quad \beta^7 = \alpha + 1.$$

Tra questi, l'altra radice di $q(X)$ è β^3; mentre β^5 e β^7 sono radici del polinomio $s(X) := X^2 + X + 2$.

Poiché le radici di $p(X)$, $q(X)$, $s(X)$ esauriscono tutti gli elementi di $\mathbb{F}_9 \setminus \mathbb{F}_3$, non ci sono altri polinomi di grado 2 irriducibili su $\mathbb{F}_3$.

10.3. Il campo $\mathbb{F}_{64}$ è stato costruito nell'Esempio 8.4 come un campo di spezzamento su $\mathbb{F}_2$ del polinomio $f(X) = (X^2 + X + 1)(X^3 + X + 1)$.

Se α è una radice di $X^2 + X + 1$ e β è una radice di $X^3 + X + 1$, si ha $\mathbb{F}_{64} = \mathbb{F}_2(\alpha, \beta)$. Esiste tuttavia un elemento $\theta \in \mathbb{F}_{64}$ di grado 6 su $\mathbb{F}_2$ tale che $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$. Procedendo come nell'Esempio 7.7, non è difficile vedere che $\theta := \alpha + \beta$ è un tale elemento (vedi anche il successivo Esempio 16.5).

La successiva Proposizione 10.7 ci fornisce un metodo per determinare tutti i polinomi di grado fissato d irriducibili su $\mathbb{F}_p$.

Lemma 10.6 *Sia F un campo. Il polinomio $X^d - 1$ divide il polinomio $X^n - 1$ in $F[X]$ se e soltanto se d divide n.*

Dimostrazione: Se $n = qd + r$, in $F[X]$ risulta:

$$(X^n - 1) = (X^d - 1)(X^{n-d} + X^{n-2d} + \cdots + X^{n-qd}) + (X^{n-qd} - 1).$$

Perciò $X^d - 1$ divide $X^n - 1$ se e soltanto se $X^{n-qd} - 1 = 0$, se e soltanto se $n - qd = 0$, ovvero d divide n.

Proposizione 10.7 *Tutti e soli i polinomi irriducibili su $\mathbb{F}_p$ di grado uguale a un divisore di n sono i fattori irriducibili del polinomio $f_{p^n}(X) := X^{p^n} - X$. In particolare, $\mathbb{F}_{p^n}$ è un campo di spezzamento di ogni polinomio di grado n irriducibile su $\mathbb{F}_p$.*

Dimostrazione: Sia $p(X)$ un polinomio irriducibile su $\mathbb{F}_p$ di grado d. Se $p(X)$ divide $f_{p^n}(X)$, esso ha una radice α in $\mathbb{F}_{p^n}$. Perciò risulta

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)][\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)]d.$$

Ne segue che d divide n.

Viceversa, supponiamo che d divida n. Per il Lemma 10.6, allora il polinomio $X^d - 1$ divide il polinomio $X^n - 1$. Calcolando in p, si ottiene che $p^d - 1$ divide $p^n - 1$. Ma allora anche $X^{p^d-1} - 1$ divide $X^{p^n-1} - 1$ ed infine $X^{p^d} - X$ divide $X^{p^n} - X$.

Se $p(X)$ è irriducibile di grado d su $\mathbb{F}_p$, il campo $K := \frac{F_p[X]}{\langle p(X) \rangle}$ ha p^d elementi; perciò questi elementi sono esattamente le radici del polinomio $X^{p^d} - X$ (Teorema 10.3). Poiché d'altra parte $p(X)$ ha una radice in K, i polinomi $p(X)$ e $X^{p^d} - X$ hanno un fattore comune non costante in $\mathbb{F}_p[X]$ (Proposizione 9.4). Ma poiché $p(X)$ è irriducibile su $\mathbb{F}_p$, allora $p(X)$ divide $X^{p^d} - X$ in $\mathbb{F}_{p^n}[X]$ e perciò divide anche $f_{p^n}(X) := X^{p^n} - X$. In particolare $p(X)$ si spezza in fattori lineari su $\mathbb{F}_{p^n}$. Infine, poiché il campo di spezzamento di $p(X)$ contiene il campo K, se $p(X)$ ha grado n, esso contiene $\mathbb{F}_{p^n}$ e dunque coincide con esso.

Corollario 10.8 *Se d è un divisore positivo di n, il polinomio $f_{p^d}(X) := X^{p^d} - X$ divide il polinomio $f_{p^n}(X) := X^{p^n} - X$ in $\mathbb{F}_p[X]$.*

Dimostrazione: Basta osservare che, per la Proposizione 10.7, ogni fattore irriducibile di $f_{p^d}(X)$ è anche un fattore irriducibile di $f_{p^n}(X)$ in $\mathbb{F}_p[X]$.

Corollario 10.9 *Indicando con* $\mathrm{Irr}(p,m)$ *l'insieme dei polinomi monici di grado* m *irriducibili su* $\mathbb{F}_p$*, risulta*

$$X^{p^n} - X = \prod_{d>0, d|n} \{f(X)\,;\ \ f(X) \in \mathrm{Irr}(p,d)\}\,.$$

Esempi

10.4. Siano $p = 2, n = 2$. La fattorizzazione di $f_4(X)$ in fattori irriducibili su $\mathbb{F}_2$ è:

$$f_4(X) := X^4 - X = X(X+1)(X^2+X+1).$$

Allora X^2+X+1 è l'unico polinomio irriducibile di grado 2 su $\mathbb{F}_2$ e $\mathbb{F}_4$ è il suo campo di spezzamento.

10.5. Siano $p = 3, n = 2$. La fattorizzazione di $f_9(X)$ in fattori irriducibili su $\mathbb{F}_3$ è:

$$f_9(X) := X^9 - X = X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

Dunque gli unici polinomi monici di grado 2 irriducibili su $\mathbb{F}_3$ sono

$$X^2+1\,, \quad X^2+X+2\,, \quad X^2+2X+2$$

e ognuno di questi ha tutte le sue radici in $\mathbb{F}_9$ (Esempio 10.2).

10.6. Siano $p = 2, n = 3$. La fattorizzazione di $f_8(X)$ in fattori irriducibili su $\mathbb{F}_2$ è

$$f_8(X) := X^8 - X = X(X-1)(X^3+X+1)(X^3+X^2+1).$$

Allora esistono esattamente 2 polinomi di grado 3 irriducibili su $\mathbb{F}_2$, precisamente

$$X^3+X+1\,, \quad X^3+X^2+1$$

e $\mathbb{F}_8$ contiene tutte le loro radici (Esempio 10.1).

10.7. Siano $p = 2, n = 4$. Il polinomio $f_{16}(X)$ è diviso in $\mathbb{F}_2[X]$ dal polinomio $f_4(X)$ per il Corollario 10.8. Quindi si ha

$$f_{16}(X) := X^{16} - X = X(X+1)(X^2+X+1)g(X).$$

Inoltre i fattori irriducibili di $g(X)$ devono avere grado uguale a 4 e perciò sono in numero di 3. Si vede facilmente che i polinomi X^4+X^3+1 e

X^4+X+1 sono irriducibili su $\mathbb{F}_2$, perché non hanno radici e non sono divisi da X^2+X+1 in $\mathbb{F}_2[X]$. A conti fatti risulta

$$f_{16}(X) = X(X+1)(X^2+X+1)(X^4+X^3+1)(X^4+X+1)(X^4+X^3+X^2+X+1).$$

Quindi i polinomi irriducibili di grado 4 su $\mathbb{F}_2$ sono

$$X^4+X^3+1\,, \quad X^4+X+1\,, \quad X^4+X^3+X^2+X+1.$$

Notiamo che F_{16}^* ha ordine 15 e perciò ha $\varphi(15) = \varphi(3)\varphi(5) = 8$ generatori. Ne segue che non tutte le radici di questi tre polinomi generano il gruppo F_{16}^*, mentre tutte generano il campo F_{16} su $\mathbb{F}_2$.

10.8. Siano $p = 2$, $n = 6$. Il polinomio $f_{64}(X)$ è diviso in $\mathbb{F}_2[X]$ dai polinomi $f_4(X)$ e $f_8(X)$ (Corollario 10.8). Quindi si ha

$$f_{64}(X) = X(X+1)(X^2+X+1)(X^3+X+1)(X^3+X^2+1)g(X),$$

dove $g(X)$ ha grado 54. Poiché ogni fattore irriducibile di $g(X)$ deve avere grado 6, ci sono esattamente 9 polinomi di grado 6 irriducibili su $\mathbb{F}_2$. Anche in questo caso, ognuna delle radici di $g(X)$ genera il campo $\mathbb{F}_{64}$ su $\mathbb{F}_2$, mentre i generatori del gruppo $\mathbb{F}_{64}^*$ sono $\varphi(63) = \varphi(7)\varphi(9) = 36$.

10.9. Il numero $|\mathrm{Irr}(p,n)|$ dei polinomi monici di grado n irriducibili su $\mathbb{F}_p$ si può calcolare usando la *funzione di Möbius*. Questa è la funzione aritmetica $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ definita nel segente modo:

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1; \\ (-1)^k, & \text{se } n \text{ è prodotto di } k \text{ numeri primi distinti;} \\ 0 & \text{altrimenti, cioè se } n \text{ ha fattori quadratici.} \end{cases}$$

Se $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ sono due funzioni aritmetiche tali che

$$f(n) = \sum_{d>0, d|n} g(d),$$

allora sussiste la *formula di inversione di Möbius*

$$g(n) = \sum_{d>0, d|n} f(d)\mu\left(\frac{n}{d}\right) = \sum_{d>0, d|n} f\left(\frac{n}{d}\right)\mu(d).$$

Poiché, per il Corollario 10.9, si ha

$$p^n = \sum_{d>0, d|n} d\,|\mathrm{Irr}(p,d)|\,,$$

per $f : \mathbb{N} \longrightarrow \mathbb{N}$ definita da $f(n) = p^n$ e $g : \mathbb{N} \longrightarrow \mathbb{N}$ definita da $g(n) = n\,|\mathrm{Irr}(p,n)|$, la formula di inversione fornisce

$$n\,|\mathrm{Irr}(p,n)| = \sum_{d>0, d|n} p^d \mu\left(\frac{n}{d}\right),$$

da cui

$$|\mathrm{Irr}(p,n)| = \frac{1}{n}\sum_{d>0,d|n} p^d \mu\left(\frac{n}{d}\right) = \frac{1}{n}\sum_{d>0,d|n} p^{\frac{n}{d}}\mu(d).$$

Ad esempio, il numero dei polinomi di grado 6 irriducibili su $\mathbb{F}_2$ è:

$$\begin{aligned}\frac{1}{6}\sum_{d>0,d|6} 2^{\frac{6}{d}}\mu(d) &= \frac{1}{6}(2^6\mu(1) + 2^3\mu(2) + 2^2\mu(3) + 2\mu(6)) \\ &= \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = \frac{1}{6}(66 - 12) = 9\end{aligned}$$

in accordo con quanto visto nel precedente Esempio 10.8.

Descriviamo ora tutti i sottocampi di $\mathbb{F}_{p^n}$.

Proposizione 10.10 *Tutti e soli i sottocampi del campo $\mathbb{F}_{p^n}$ sono i campi F_{p^d} dove d è un divisore positivo di n.*

Dimostrazione: Sia L un sottocampo di $\mathbb{F}_{p^n}$ di grado d su $\mathbb{F}_p$. Allora L ha p^d elementi (Proposizione 10.1). Inoltre si ha

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : L][L : \mathbb{F}_p] = [\mathbb{F}_{p^n} : L]d$$

Dunque d divide n.

Viceversa, se d divide n, allora il polinomio $f_{p^d}(X)$ divide $\mathbb{F}_{p^n}(X)$ (Corollario 10.8). Dunque esso ha tutte le sue radici in $\mathbb{F}_{p^n}$. L'insieme di queste radici forma un sottocampo di $\mathbb{F}_{p^n}$ di ordine p^d (Teorema 10.3).

Terminiamo questo paragrafo calcolando il gruppo degli automorfismi del campo finito $\mathbb{F}_{p^n}$.

Per quanto visto finora, si può scrivere $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, dove il polinomio minimo di α su $\mathbb{F}_p$ è un divisore di grado n del polinomio $X^{p^n} - X$ e perciò ha esattamente n radici distinte in $\mathbb{F}_{p^n}$. Il Corollario 9.3. ci permette allora di affermare che $\mathbb{F}_{p^n}$ ha esattamente $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ automorfismi.

Notiamo che, se K è un campo di caratteristica positiva p, l'applicazione $\Phi : K \longrightarrow K$ definita da $a \mapsto a^p$ è un omomorfismo di campi non nullo. Infatti per il Lemma 10.1, si ha $(a+b)^p = a^p + b^p$ ed inoltre $(ab)^p = a^p b^p$, per ogni $a, b \in K$. Questo omomorfismo si chiama l'*omomorfismo di Fröbenius.*

Nel caso in cui $K := \mathbb{F}_{p^n}$ sia un campo finito, l'omomorfismo di Fröbenius è un automorfismo. Infatti Φ è sempre iniettivo, ma poiché $\mathbb{F}_{p^n}$ è finito, in questo caso esso è anche suriettivo.

Teorema 10.11 *Il gruppo* $\mathrm{Aut}(\mathbb{F}_{p^n})$ *è ciclico di ordine n, generato dall'automorfismo di Fröbenius.*

Dimostrazione: Poiché $\mathrm{Aut}(\mathbb{F}_{p^n})$ ha ordine n (Corollario 9.3), basta far vedere che l'automorfismo di Fröbenius Φ ha ordine n.

Sia α un generatore del gruppo $\mathbb{F}_{p^n}^*$. Poiché $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ (Proposizione 10.4), allora $\Phi^k = id$ se e soltanto se $\Phi^k(\alpha) = (\dots((\alpha^p)^p)\dots)^p = \alpha^{p^k} = \alpha$. Ma, poiché α ha ordine $p^n - 1$, il minimo intero k per cui questo avviene è $k = n$.

Esempi

10.10. Poiché $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, dove α è una radice del polinomio irriducibile $p(X) := X^2 + 1 \in \mathbb{F}_3[X]$ (Esempio 10.2), il campo $\mathbb{F}_9$ ha 2 automorfismi. Essi sono l'identità e l'automorfismo di Fröbenius

$$\Phi : \mathbb{F}_9 \longrightarrow \mathbb{F}_9\,, r(\alpha) \mapsto r(\alpha^3),$$

per ogni polinomio $r(X) \in \mathbb{F}_3[X]$ (di grado al più uguale a uno).

10.11. Poiché $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, dove α è una radice del polinomio irriducibile $p(X) := X^3 + X + 1 \in \mathbb{F}_2[X]$(Esempio 10.1), il campo $\mathbb{F}_8$ ha esattamente 3 automorfismi. Essi formano un gruppo ciclico generato dall'automorfismo Φ di Fröbenius e sono definiti rispettivamente da:

$$\Phi : r(\alpha) \mapsto r(\alpha^2)\,; \quad \Phi^2 : r(\alpha) \mapsto r(\alpha^4)\,; \quad id : r(\alpha) \longrightarrow r(\alpha),$$

per ogni polinomio $r(X) \in \mathbb{F}_2[X]$ (di grado al più uguale a due).

10.12. Il campo $\mathbb{F}_{64}$ ha 6 automorfismi, che sono stati calcolati nell'Esempio 9.5. È facile verificare che essi coincidono con gli automorfismi

$$\Phi^k : \mathbb{F}_{64} \longrightarrow \mathbb{F}_{64}\,,\ a \mapsto a^{p^k}\,, \quad \text{per } a \in \mathbb{F}_{64}\,,\ \ k = 0, \dots, 5.$$

ESERCIZI

10.1. Fattorizzare il polinomio $X^{32} - X \in \mathbb{F}_2[X]$ in polinomi irriducibili su $\mathbb{F}_2$.

10.2. Descrivere la struttura del campo $\mathbb{F}_{81}$ e dei suoi sottocampi. Stabilire se esistono polinomi di grado 2, 3, 4 irriducibili su $\mathbb{F}_3$ che hanno radici in $\mathbb{F}_{81}$ e, in caso affermativo, determinarne almeno uno.

10.3. Determinare due differenti polinomi $p(X)$, $q(X) \in \mathbb{F}_5[X]$ di grado 2 irriducibili su $\mathbb{F}_5$. Se α è una radice di $p(X)$, costruire il campo $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$ e verificare che $q(X)$ ha tutte le sue radici in $\mathbb{F}_{25}$; inoltre, se β è una radice di $q(X)$, esprimere α in funzione β. Determinare infine i generatori di $\mathbb{F}_{25}^*$ in funzione di α e β.

10.4. Sia $f(X) \in \mathbb{F}_p[X]$ un polinomio irriducibile di grado n e sia α una sua radice (in $\mathbb{F}_{p^n}$). Mostrare che tutte e sole le radici di $f(X)$ sono gli elementi α, α^p, $\alpha^{p^2}, \dots, \alpha^{p^{n-1}}$.

10.5. Sia $f(X) \in \mathbb{F}_p[X]$ e sia K un suo campo di spezzamento su $\mathbb{F}_p$. Mostrare che K ha p^m elementi, dove m è il minimo comune multiplo dei gradi dei fattori irriducibili di $f(X)$.

10.6. Stabilire se esistono polinomi di grado 2, 3, 4 irriducibili su $\mathbb{F}_2$ che si fattorizzano su $\mathbb{F}_{16}$. In caso affermativo, determinarne almeno uno.

10.7. Determinare il numero dei polinomi di grado 2 irriducibili su $\mathbb{F}_p$.

10.8. Mostrare che esistono infiniti polinomi irriducibili su $\mathbb{F}_p$.

10.9. Sia p un numero primo e sia $n \geq 1$. Mostrare che n divide $\varphi(p^n - 1)$.

10.10. Siano p e p' due numeri primi. Mostrare che il polinomio $X^p - X$ si spezza linearmente su $\mathbb{F}_{p'}$ se e soltanto se $p - 1$ divide $p' - 1$.

11 Ampliamenti Ciclotomici

Sia F un campo e si consideri il polinomio $X^n - 1 \in F[X]$, dove $n \geq 0$. Se F ha caratteristica prima p e $n = p^h m$, $h \geq 1$, allora risulta $X^n - 1 = (X^m - 1)^{p^h}$ (Lemma 10.2); perciò le radici del polinomio $X^n - 1$ in un suo campo di spezzamento su F sono tutte multiple, con molteplicità uguale a una potenza di p. Ci possiamo allora limitare a considerare il caso in cui la caratteristica del campo F non divida n.

Proposizione 11.1 *Se la caratteristica del campo F non divide n, le radici del polinomio $X^n - 1$ in un suo campo di spezzamento su F sono tutte distinte e formano un gruppo ciclico (di ordine n).*

Dimostrazione: Se $n = 1$, il teorema è banalmente vero. Sia perciò $n \geq 2$. La derivata formale del polinomio $X^n - 1$ è nX^{n-1}. Poiché la caratteristica di F non divide n, tale derivata non è nulla e perciò il polinomio $X^n - 1$ ha tutte radici distinte (Corollario 9.6). Queste radici formano un sottogruppo (finito) di K^*, perché se $\alpha^n = \beta^n = 1$, anche $(\alpha\beta^{-1})^n = 1$. Allora tale gruppo è ciclico per la Proposizione 1.2.

Se la caratteristica del campo F non divide n, le radici del polinomio $X^n - 1$ (in un suo campo di spezzamento su F) si dicono le *radici n-sime dell'unità su F*. I generatori del gruppo ciclico delle radici n-sime dell'unità su F si dicono le *radici primitive* n-sime dell'unità. Il loro numero è $\varphi(n)$, dove $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ denota la funzione di Eulero. Infatti, se ξ è una radice n-sima primitiva, tutte le altre radici primitive sono le radici ξ^k con $\mathrm{MCD}(n, k) = 1$.

Notiamo che, per $n = 1$, l'unica radice (primitiva) è $\xi = 1$ e, per $n = 2$, l'unica radice primitiva è $\xi = -1$.

Esempi

11.1. Le radici n-sime dell'unità su $\mathbb{Q}$ sono le potenze del numero complesso

$$\xi_n := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$$

ed esplicitamente esse sono i numeri complessi

$$\xi_n^k = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}), \quad k = 0, \ldots, n-1.$$

Le radici primitive sono i numeri complessi ξ_n^k con $\mathrm{MCD}(n,k) = 1$ (Esempio 1.5).

11.2. Se p è un numero primo, il gruppo delle radici $(p-1)$-sime dell'unità su $\mathbb{F}_p$ è $\mathbb{F}_p^*$. più generalmente, il gruppo delle radici (p^n-1)-sime dell'unità su $\mathbb{F}_p$ è il gruppo $\mathbb{F}_{p^n}^*$ e le radici n-sime primitive su $\mathbb{F}_p$ sono i generatori di $\mathbb{F}_{p^n}^*$; il loro polinomio minimo è un fattore di grado n del polinomio $X^{p^n} - X$ (Paragrafo 10).

11.3. Cerchiamo le radici seste dell'unità su $\mathbb{F}_5$. Poiché la fattorizzazione del polinomio $X^6 - 1$ in polinomi irriducibili su $\mathbb{F}_5$ è:

$$X^6 - 1 = (X^3-1)(X^3+1) = (X-1)(X+1)(X^2-X+1)(X^2+X+1),$$

un campo di spezzamento di $X^6 - 1$ su $\mathbb{F}_5$ è $K = \mathbb{F}_{25}$. Applicando le formule risolutive per le equazioni di secondo grado, otteniamo che le radici del polinomio $X^2 - X + 1$ in K sono $3 + 3\alpha$ e $3 + 2\alpha$, mentre le radici del polinomio $X^2 + X + 1$ sono $2 + 3\alpha$ e $2 + 2\alpha$, dove $\alpha \in K$ è tale che $\alpha^2 = 2$.

Il numero delle radici seste primitive è $\varphi(6) = 2$. Poiché si ha

$$(3+3\alpha)^2 = 2 + 3\alpha, \quad (3+3\alpha)^3 = 4 \neq 1,$$

allora $\xi = 3 + 3\alpha$ è una radice primitiva. L'unica altra radice sesta primitiva è $\xi^5 = 3 + 2\alpha$.

Proposizione 11.2 *Supponiamo che la caratteristica del campo F non divida n. Se K è un campo di spezzamento del polinomio $X^n - 1$ su F e $\xi \in K$ è una radice n-sima primitiva dell'unità su F, allora $K = F(\xi)$.*

Dimostrazione: Poiché ogni radice n-sima dell'unità su F è una potenza di ξ (Proposizione 10.1), allora $F(\xi)$ contiene K. Poiché chiaramente vale anche l'inclusione opposta, si ha l'uguaglianza.

Notiamo che per $n = 1$, 2 si ha $F(\xi) = F$.

Se $F = \mathbb{Q}$ e $n \geq 3$, le radici complesse n-sime dell'unità corrispondono nel piano di Gauss ai vertici di un poligono regolare di n lati con un vertice in 1. Perciò esse tagliano la circonferenza centrata nell'origine e di raggio unitario in n archi uguali.

Per questo motivo, se la caratteristica di F non divide n e ξ è una radice n-sima primitiva dell'unità su F, il campo $F(\xi)$ si dice l'*n-simo ampliamento ciclotomico* di F (la parola "ciclotomico" deriva dal greco e significa"che taglia il cerchio").

Il polinomio monico che ha per radici tutte e sole le radici primitive n-sime dell'unità su F si dice l'n-simo polinomio ciclotomico su F e si indica con $\Phi_n(X)$. Dunque risulta

$$\Phi_n(X) := \prod_{\mathrm{MCD}(n,k)=1} (X - \xi^k).$$

Il grado di $\Phi_n(X)$ è $\varphi(n)$.

Se $n = p$ è un numero primo e la caratteristica di F è diversa da p, esistono radici p-sime diverse da 1 e queste hanno tutte ordine p, perciò sono tutte primitive. Ne segue che

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

e

$$X^p - 1 = \Phi_1(X)\Phi_p(X).$$

In generale, per $n \geq 1$, poiché il gruppo delle radici n-sime dell'unità è ciclico, per ogni divisore positivo d di n esistono radici n-sime di ordine d ed esse sono tutte e sole le radici primitive d-sime. Allora si ha che

$$X^n - 1 = \prod_{0 \leq k \leq n-1} (X - \xi^k) = \prod_{d>0, d|n} \Phi_d(X).$$

Proposizione 11.3 *Supponiamo che la caratteristica di F non divida n. Per ogni $n \geq 1$, i coefficienti dell'n-simo polinomio ciclotomico $\Phi_n(X)$ su F appartengono all sottocampo fondamentale $\mathbb{F}$ di F. Se inoltre $\mathbb{F} = \mathbb{Q}$, i coefficienti di $\Phi_n(X)$ appartengono a $\mathbb{Z}$.*

Dimostrazione: Sia ξ una radice primitiva n-sima dell'unità su F. Procediamo per induzione su n. Se $n = 1$, allora $\Phi_1(X) = X - 1 \in \mathbb{F}[X]$.

Supponiamo che $\Phi_m(X) \in \mathbb{F}[X]$ per $m < n$. Se

$$h(X) := \prod_{n>d>0, d|n} \Phi_d(X),$$

allora per l'ipotesi induttiva $h(X) \in \mathbb{F}[X]$ e $X^n - 1 = h(X)\Phi_n(X)$. Quindi $\Phi_n(X)$ divide $X^n - 1$ in $\mathbb{F}(\xi)[X]$. Ma, poiché $h(X)$, $X^n - 1 \in \mathbb{F}[X]$, allora $\Phi_n(X) \in \mathbb{F}[X]$.

Se inoltre $\mathbb{F} = \mathbb{Q}$, poiché $\Phi_1(X) = X - 1$ ha coefficienti interi, per ipotesi induttiva possiamo supporre che anche $h(X)$ abbia coefficienti interi. Poiché $X^n - 1 \in \mathbb{Z}[X]$, per il Lemma di Gauss otteniamo che $\Phi_n(X) \in \mathbb{Z}[X]$.

La formula

$$X^n - 1 = \prod_{d>0, d|n} \Phi_d(X)$$

permette di costruire induttivamente $\Phi_n(X)$. Infatti risulta:

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{n>d>0, d|n} \Phi_d(X)}.$$

Ad esempio

$$\Phi_1(X) = X - 1;$$
$$\Phi_2(X) = \frac{X^2 - 1}{X - 1} = X + 1;$$
$$\Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1;$$
$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_1(X)\Phi_2(X)} = \frac{X^4 - 1}{(X - 1)(X + 1)} = X^2 + 1;$$
$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = \frac{X^6 - 1}{(X^2 - 1)(X^2 + X + 1)} = X^2 - X + 1;$$
$$\Phi_8(X) = \frac{X^8 - 1}{\Phi_1(X)\Phi_2(X)\Phi_4(X)} = \frac{X^8 - 1}{(X^2 - 1)(X^2 + 1)} = X^4 + 1;$$

e così via.

Esempi

11.4. Sia p un numero primo diverso dalla caratteristica di F e sia $r \geq 1$. Allora risulta:

$$\Phi_{p^r}(X) = \frac{X^{p^r - 1}}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1.$$

Infatti, per ogni $h \geq 0$ si ha:

$$X^{p^h} - 1 = \prod_{d>0, d|p^h} \Phi_d(X) = \prod_{0 \leq j \leq h} \Phi_{p^j}(X);$$

quindi tutte le radici p^r-sime non primitive dell'unità sono le radici del polinomio $X^{p^{r-1}}$ - 1.

11.5. Se p, q sono numeri primi distinti diversi dalla caratteristica di F, dall'uguaglianza

$$X^{pq} - 1 = \Phi_1(X)\Phi_p(X)\Phi_q(X)\Phi_{pq}(X)$$

otteniamo la *formula di Möbius-Dedekind*:

$$\Phi_{pq}(X) = \frac{(X^{pq}-1)(X-1)}{(X^q-1)(X^p-1)} = \frac{\Phi_p(X^q)}{\Phi_p(X)}$$
$$= \frac{X^{q(p-1)} + X^{q(p-2)} + \cdots + X^q + 1}{X^{p-1} + X^{p-2} + \cdots + X + 1}.$$

Ad esempio:

$$\Phi_{15}(X) = \frac{X^{10} + X^5 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1;$$
$$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1.$$

11.6. Se p, q sono numeri primi distinti, i coefficienti non nulli del polinomio $\Phi_{pq}(X)$ su $\mathbb{Q}$ possono assumere soltanto i valori 1 e -1 (A. Migotti, 1883). Il più piccolo intero positivo n per cui $\Phi_n(X)$ ha qualche coefficiente non nullo con modulo diverso da 1 è 105. Infatti si ha

$$\Phi_{105}(X) = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - \ldots$$

Tuttavia J. Suzuki (1987) ha dimostrato che ogni numero intero è un coefficiente di qualche polinomio ciclotomico.

Il polinomio $\Phi_n(X)$ non è sempre irriducibile su $\mathbb{F}_p$, ad esempio $\Phi_4(X) = (X^2+1) = (X+2)(X+3)$ su $\mathbb{F}_5$. Tuttavia, come mostreremo ora, $\Phi_n(X)$ è sempre irriducibile su $\mathbb{Q}$.

L'irriducibilità di $\Phi_p(X)$ su $\mathbb{Q}$, per p primo, è stata dimostrata per la prima volta da da F. Gauss (1801). Questa dimostrazione è stata successivamente semplificata da L. Kronecker, nel 1845, ed una dimostrazione diversa è stata poi data da F. G. Eisenstein nel 1850, per fornire un'applicazione del suo Criterio di Irriducibilità. Infine, la prova dell'irriducibilità di $\Phi_n(X)$ su $\mathbb{Q}$, per ogni intero $n \geq 1$, è stata ottenuta da R. Dedekind nel 1857.

Notiamo che, poiché $\Phi_n(X)$ è monico ed ha coefficienti interi (Proposizione 1.11.3), per il Lemma di Gauss, dimostrare la sua irriducibilità su $\mathbb{Q}$ equivale a dimostrare la sua irriducibilità su $\mathbb{Z}$.

Illustriamo ora il metodo di Kronecker dimostrando l'irriducibilità di $\Phi_n(X)$ su $\mathbb{Q}$ quando $n := p^r$ è una potenza di un numero primo.

Proposizione 11.4 *Se $n := p^r$, con p primo e $r \geq 1$, il polinomio $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$.*

Dimostrazione: Sia $n := p^r$. Supponiamo che $\Phi_n(X) = g(X)h(X)$, con $g(X)$, $h(X) \in \mathbb{Z}[X]$ monici di grado positivo. Dalla formula dimostrata nell'Esempio 11.4, otteniamo che $\Phi_n(1) = g(1)h(1) = p$. Dunque uno dei due fattori, ad esempio $g(1)$, vale ± 1. Le radici di $g(X)$, annullando anche $\Phi_n(X)$

sono radici n-sime dell'unità diverse da 1; perciò, se ξ è una qualsiasi radice primitiva, si ha $g(\xi)g(\xi^2)\dots g(\xi^{n-1}) = 0$. Ne segue che il polinomio $f(X) := g(X)g(X^2)\dots g(X^{n-1})$ si annulla in ogni radice primitiva ξ e perciò, avendo coefficienti interi, è diviso in $\mathbb{Z}[X]$ dal polinomio $\Phi_n(X)$, ovvero $f(X) = \Phi_n(X)k(X)$, con $k(X) \in \mathbb{Z}[X]$. Poiché inoltre $f(X)$ e $\Phi_n(X)$ sono entrambi monici, anche $k(X)$ è monico. Calcolando ancora in 1, otteniamo $\pm 1 = \Phi_n(1)k(1) = p$. Poiché $k(1) \in \mathbb{Z}$, questa è una contraddizione e perciò $\Phi_n(X)$ è irriducibile.

L'irriducibilità su $\mathbb{Q}$ dell'n-simo polinomio ciclotomico si può provare a questo punto mostrando che, se $n = rs > 1$ con $\mathrm{MCD}(r, s) = 1$ e se $\Phi_r(X)$ e $\Phi_s(X)$ sono irriducibili su $\mathbb{Q}$, allora anche $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$. Poiché ogni intero $n \geq 2$ è prodotto di potenze di numeri primi distinti, da questo fatto, usando la Proposizione 11.4, si ottiene che $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$, per ogni $n \geq 2$.

Diamo ora una dimostrazione dell'irriducibilità di $\Phi_n(X)$ su $\mathbb{Q}$ che non dipende dalla Proposizione 11.4.

Teorema 11.5 *Per ogni $n \geq 1$, il polinomio $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$.*

Dimostrazione: Supponiamo che $\Phi_n(X) = f(X)g(X)$, dove $f(X)$ e $g(X)$ sono polinomi a coefficienti interi (Lemma di Gauss) e $g(X)$ è di grado positivo irriducibile su $\mathbb{Z}$. Vogliamo mostrare che $\Phi_n(X) = \pm g(X)$. Per questo basta verificare che ogni radice n-sima primitiva dell'unità annulla $g(X)$. Poiché $g(X)$ ha grado positivo, esso è annullato da una radice n-sima primitiva ξ. Facciamo vedere che, se $\mathrm{MCD}(n, k) = 1$, allora ξ^k è ancora una radice di $g(X)$.

Cominciamo mostrando che, se p è un primo che non divide n, allora ξ^p è ancora una radice di $g(X)$. Per questo, poiché $\Phi_n(\xi^p) = f(\xi^p)g(\xi^p)$, basta mostrare che $f(\xi^p) \neq 0$. Sia per assurdo $f(\xi^p) = 0$. Allora ξ è radice del polinomio $f(X^p)$ e i polinomi $g(X)$ e $f(X^p)$ hanno una radice in comune. Ne segue che $\mathrm{MCD}(g(X), f(X^p))$ ha grado positivo e allora è uguale a $g(X)$, perché $g(X)$ è irriducibile. Ne segue che $g(X)$ divide $f(X^p)$ in $\mathbb{Q}[X]$ e anche in $\mathbb{Z}[X]$ (Lemma di Gauss). Sia $f(X^p) = g(X)h(X)$, con $h(X)$ a coefficienti interi. Riducendo modulo p, in $\mathbb{F}_p[X]$ risulta $\overline{f}(X^p) = (\overline{f}(X))^p = \overline{g}(X)\overline{h}(X)$ (Esercizio 2.3) e perciò $\overline{f}(X)$ e $\overline{g}(X)$ hanno un fattore comune in $\mathbb{F}_p[X]$. Poiché $X^n - 1 = \Phi_n(X)q(X) = f(X)g(X)q(X)$, il polinomio $X^n - 1 = \overline{f}(X)\overline{g}(X)\overline{q}(X) \in \mathbb{F}_p[X]$ ha un fattore multiplo e dunque esso ha una radice multipla nel suo campo di spezzamento. Questo non è possibile per la Proposizione 11.1. Ne segue che $f(\xi^p) \neq 0$ e perciò $g(\xi^p) = 0$.

Sia ora $k \geq 1$ tale che $\mathrm{MCD}(n, k) = 1$. Se $k = p_1 \dots p_s$ è la fattorizzazione di k in numeri primi (non necessariamente tutti distinti), Allora p_i non divide n per ogni $i = 1, \dots, s$. Perciò, ripetendo l'argomento sopra esposto, si ottiene che ξ^k è una radice di $g(X)$.

Corollario 11.6 *Se ξ è una radice complessa n-sima primitiva dell'unità, il polinomio minimo di ξ su $\mathbb{Q}$ è $\Phi_n(X)$. In particolare $\mathbb{Q}(\xi)$ ha grado $\varphi(n)$ su $\mathbb{Q}$.*

Dimostrazione: $\Phi_n(X)$ è il polinomio minimo di ξ su $\mathbb{Q}$, perché ha coefficienti razionali ed è irriducibile su $\mathbb{Q}$ (Teorema 11.5). Poiché $\Phi_n(X)$ ha grado $\varphi(n)$, allora $\mathbb{Q}(\xi)$ ha grado $\varphi(n)$ su $\mathbb{Q}$ (Proposizione 7.1).

Corollario 11.7 *La decomposizione del polinomio $X^n - 1$ in fattori monici irriducibili su $\mathbb{Q}$ è:*

$$X^n - 1 = \prod_{d>0, d|n} \Phi_d(X).$$

ESERCIZI

11.1. Mostrare che, per ogni $n \geq 1$,

$$n = \sum_{d>0, d|n} \varphi(d) \quad \text{e dunque} \quad \varphi(n) = \sum_{d>0, d|n} \mu(d)\frac{n}{d},$$

dove μ è la funzione di Möbius. (*Suggerimento*: Usare la formula di inversione di Möbius (Esempio 10.9))

11.2. Calcolare $\Phi_n(X)$ per $1 \leq n \leq 20$.

11.3. Mostrare che, se $\varphi(n) = 2$, allora il polinomio $X^n - 1$ si spezza completamente sul suo campo di definizione F oppure il suo campo di spezzamento ha grado 2 su F.

11.4. Sia ζ una radice primitiva quinta dell'unità su $\mathbb{F}_3$. Determinare il polinomio minimo di ζ su $\mathbb{F}_3$.

11.5. Sia ζ una radice primitiva ottava dell'unità su $\mathbb{F}_5$. Determinare il polinomio minimo di ζ su $\mathbb{F}_5$. Inoltre, se n è il grado di ζ su $\mathbb{F}_5$, esprimere esplicitamente ζ^k come un polinomio in ζ, di grado al più uguale a $n-1$, per $8 > k \geq 0$.

11.6. Siano $\zeta_1, \ldots, \zeta_n$ le radici complesse n-sime dell'unità e sia $k \geq 1$. Mostrare che:

$$\zeta_1^k + \cdots + \zeta_n^k = \begin{cases} 0, & \text{se } n \text{ non divide } k \\ n, & \text{se } n \text{ divide } k \end{cases}; \quad \zeta_1^k \cdots \zeta_n^k = (-1)^{k(n-1)}.$$

11.7. Sia ζ una radice primitiva n-sima dell'unità sul campo F e sia d un divisore positivo di n. Mostrare che ζ^k è una radice primitiva d-sima dell'unità se e soltanto se $\mathrm{MCD}(n,k) = \frac{n}{d}$.

11.8. Mostrare con un esempio che le $\varphi(n)$ radici primitive n-sime dell'unità possono non costituire una base su $\mathbb{Q}$ dell'n-simo ampliamento ciclotomico.

11.9. Sia $\xi_n := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, $n \geq 1$. Mostrare che, se r, s sono due interi positivi e $m := \mathrm{mcm}(r, s)$, allora $\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_r, \xi_s) = \mathbb{Q}(\xi_r\xi_s)$. In particolare, se $\mathrm{MCD}(r, s) = 1$, allora $\mathbb{Q}(\xi_{rs}) = \mathbb{Q}(\xi_r, \xi_s) = \mathbb{Q}(\xi_r\xi_s)$.

11.10. Sia $\xi_n := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, $n \geq 1$. Mostrare che, per ogni numero primo p dispari, risulta $\mathbb{Q}(\xi_p) = \mathbb{Q}(\xi_{2p})$. Esprimere inoltre ξ_p in funzione di ξ_{2p}.

11.11. Sia ξ una radice primitiva settima dell'unità. Determinare il grado su $\mathbb{Q}$ di:

$$\xi + \xi^5\,; \quad \xi^3 + \xi^4\,; \quad \xi^3 + \xi^5 + \xi^6.$$

11.12. Usando il Criterio di Irriducibilità di Eisenstein, dimostrare che, se p è un numero primo, allora $\Phi_p(X)$ è irriducibile su $\mathbb{Z}$, e quindi su $\mathbb{Q}$ (*Suggerimento*: Applicare il Criterio di Irriducibilità di Eisenstein al polinomio $\Phi_p(X + 1)$). Generalizzare poi questo procedimento per mostrare che $\Phi_{p^r}(X)$ è irriducibile su $\mathbb{Q}$, per ogni $r \geq 1$.

11.13. Dimostrare direttamente che, se p, q sono numeri primi distinti, allora $\Phi_{pq}(X)$ è irriducibile su $\mathbb{Q}$. (*Suggerimento*: Usare la formula di Möbius-Dedekind (Esempio 11.5) e gli Esercizi 7.14 e 11.9).

11.14. Mostrare che, se $n := p^r q^s$, con p, q numeri primi distinti, allora

$$\Phi_n(X) = \frac{\Phi_{p^r}(X^{q^s})}{\Phi_{p^r}(X^{q^{s-1}})} = \frac{(X^n - 1)(X^{\frac{n}{pq}} - 1)}{(X^{\frac{n}{p}} - 1)(X^{\frac{n}{q}} - 1)}.$$

Usando questa formula, procedere poi come nell'esercizio precedente per mostrare direttamente che in questo caso $\Phi_n(X)$ è irriducibile su $\mathbb{Q}$.

11.15. Poniamo $\Phi_n(X) = X^s + c_{s-1}X^{s-1} + \cdots + c_0$, con $n \geq 3$ e $s := \varphi(n)$. Mostrare che s è pari e $c_i = c_{s-i}$, per $i = 0, \ldots, s$. (*Suggerimento*: Notare che, per ogni radice ξ di $\Phi_n(X)$, anche ξ^{-1} è una radice.)

11.16. Scomporre $\Phi_n(X)$ in polinomi irriducibili su $\mathbb{R}$.

12 Ampliamenti Algebrici e Chiusura Algebrica

Si dice che l'ampliamento di campi $F \subseteq K$ è *un ampliamento algebrico*, oppure che K è *algebrico su* F, se ogni elemento $\alpha \in K$ è algebrico su F. Un campo di numeri algebrico su $\mathbb{Q}$ si dice semplicemente un *campo algebrico*.

Esempi

12.1. $\mathbb{C}$ è un ampliamento algebrico di $\mathbb{R}$. Infatti ogni numero complesso non reale è radice di un polinomio (di secondo grado) a coefficienti reali (Esempio 5.12).

12.2. $\mathbb{R}$ non è un ampliamento algebrico di $\mathbb{Q}$, perché contiene i numeri reali trascendenti.

Il seguente teorema mostra in particolare che ogni ampliamento finito è algebrico. Vedremo tuttavia che non è vero il viceversa.

Teorema 12.1 *Sia $F \subseteq K$ un ampliamento di campi. Le seguenti proprietà sono equivalenti:*

(*i*) *K è finito su F;*

(*ii*) *K è algebrico e finitamente generato su F;*

(*iii*) *$K = F(\alpha_1, \ldots, \alpha_n)$, dove α_i è algebrico su F per $i = 1, \ldots n$.*

Dimostrazione: (*i*) $\Rightarrow$ (*ii*). Sia $[K : F] = n$. Allora, se $\alpha \in K$, gli $n + 1$ elementi $1, \alpha_1, \ldots, \alpha_n$ sono linearmente dipendenti su F. Dunque α è radice di un polinomio di grado n a coefficienti in F e perciò è algebrico su F.

Sia poi $\{\beta_1, \ldots, \beta_n\}$ una base di K su F. Allora $K \subseteq F(\beta_1, \ldots, \beta_n)$ e, poiché vale anche l'inclusione opposta, si ha l'uguaglianza.

(*ii*) $\Rightarrow$ (*iii*) è evidente.

(*iii*) $\Rightarrow$ (*i*). Sia $K = F(\alpha_1, \ldots, \alpha_n)$ e si consideri la successione di ampliamenti

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_n := F_{n-1}(\alpha_n) = K.$$

Poiché α_i è algebrico su F, esso è algebrico anche su F_{i-1}. Inoltre, se r_i è il grado di α_i su F_{i-1}, risulta:

$$[K : F] = [K : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F] = r_n \ldots r_1$$

(Proposizione 7.3). Perciò $[K : F]$ è finito.

Come immediata conseguenza del risultato precedente riotteniamo la caratterizzazione degli ampliamenti algebrici semplici vista nel Paragrafo 7.

Un teorema di grande importanza teorica, che mostreremo in seguito, asserisce che ogni ampliamento finito di un campo di caratteristica zero è semplice (vedi il successivo Corollario 13.9).

Corollario 12.2 *Siano $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Le seguenti proprietà sono equivalenti:*

(*i*) $[F(\alpha) : F]$ *è finito;*

(*ii*) $F(\alpha)$ *è algebrico su* F*;*

(*iii*) α *è algebrico su* F*;*

(*iv*) α *appartiene a un sottocampo di* K *finito su* F*.*

Inoltre, se queste proprietà sono soddisfatte, $[F(\alpha) : F]$ *è uguale al grado di* α *su* F*.*

Esempi

12.3. Se $\alpha := i\sqrt{\sqrt[3]{2} - 1}$, $\mathbb{Q}(\alpha)$ è un ampliamento algebrico di $\mathbb{Q}$. Infatti risulta $\alpha^6 - 3\alpha^4 + 3\alpha^2 + 1 = 0$.

12.4. $\mathbb{Q}(\pi)$ non è un ampliamento algebrico di $\mathbb{Q}$ ma è un ampliamento algebrico di $\mathbb{Q}(\pi^2)$. Infatti π è trascendente su $\mathbb{Q}$, ma annulla il polinomio $X^2 - \pi^2$ a coefficienti in $\mathbb{Q}(\pi^2)$.

12.5. Il campo di spezzamento di un polinomio $f(X) \in F[X]$ è un ampliamento algebrico di F (Paragrafo 8).

12.6. Ogni campo finito è un ampliamento algebrico di $\mathbb{F}_p$, per un opportuno primo p (Paragrafo 10).

Proposizione 12.3 *Sia* $F \subseteq K$ *un ampliamento di campi. L'insieme degli elementi di* K *algebrici su* F *è un sottocampo di* K*.*

Dimostrazione: Siano $\alpha, \beta \in K$ algebrici su F. Allora l'ampliamento $F(\alpha, \beta)$ di F è finito su F per la Proposizione 12.1. Poiché $\alpha - \beta \in F(\alpha, \beta)$ e $\alpha\beta^{-1} \in F(\alpha, \beta)$, per $\beta \neq 0$, questi elementi sono algebrici su F per il Corollario 12.2. Allora possiamo concludere per la Proposizione 1.3.

Mostriamo ora che esistono campi di numeri che sono algebrici ma non finitamente generati, ovvero non finiti, su $\mathbb{Q}$.

Proposizione 12.4 *Il campo dei numeri reali algebrici e il campo dei numeri complessi algebrici sono ampliamenti algebrici e non finiti di* $\mathbb{Q}$*.*

Dimostrazione: Sia $\gamma_n = \sqrt[n]{2}$, $n \geq 2$. Poiché il polinomio $X^n - 2$ è irriducibile su $\mathbb{Q}$ (Criterio di Eisenstein), allora $[\mathbb{Q}(\gamma_n) : \mathbb{Q}] = n$. Se il campo dei numeri reali algebrici avesse grado finito m su $\mathbb{Q}$, allora m sarebbe diviso da ogni $n \geq 2$, il che è impossibile. Poiché il campo dei numeri complessi algebrici contiene il campo dei numeri reali algebrici, anche questo campo non può essere finito su $\mathbb{Q}$.

Nel caso in cui il campo K sia finitamente generato su F, la proposizione seguente deriva dalla Proposizione 7.3 e dal Teorema 12.1.

Proposizione 12.5 *Siano $F \subseteq L \subseteq K$ ampliamenti di campi. Allora K è algebrico su F se e soltanto se K è algebrico su L e L è algebrico su F.*

Dimostrazione: Se K è algebrico su F esso è chiaramente algebrico su L. Inoltre, ogni elemento di L, essendo in K, è algebrico su F. Perciò L è algebrico su F.

Viceversa, se K è algebrico su L, ogni suo elemento α è radice di un polinomio $f(X) := c_0 + c_1X + \cdots + c_nX^n$, a coefficienti in L. Consideriamo il campo $F' := F(c_0, c_1, \ldots, c_n)$. Si ha che $f(X) \in F'[X]$ e $F \subseteq F' \subseteq F'(\alpha) \subseteq K$. Poiché L è algebrico su F, ogni elemento c_i è algebrico su F; dunque F' è un ampliamento finito di F (Teorema 12.1). D'altra parte, α è algebrico su F', perciò $F'(\alpha)$ è un ampliamento finito di F' (Corollario 12.2). Ne segue che $F'(\alpha)$ è un ampliamento finito di F e allora α è algebrico su F (Corollario 12.2).

Dato un ampliamento di campi $F \subseteq K$, il campo intermedio formato dagli elementi di K algebrici su F si dice la *chiusura algebrica di F in K* (Proposizione 12.3). Esso è il più grande ampliamento algebrico di F contenuto in K.

Esempi

12.7. Il campo $A(\mathbb{R})$ dei numeri reali algebrici e il campo $A(\mathbb{C})$ dei numeri complessi algebrici sono la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{R}$ e $\mathbb{C}$ rispettivamente.

Un campo F si dice *algebricamente chiuso in K* se esso coincide con la sua chiusura algebrica in K, ovvero se ogni elemento di K algebrico su F appartiene ad F. Inoltre F si dice *algebricamente chiuso* se esso è algebricamente chiuso in ogni suo ampliamento; ciò equivale a dire che ogni estensione algebrica di F coincide con F.

Proposizione 12.6 *Se $F \subseteq K$ è un ampliamento di campi, la chiusura algebrica di F in K è algebricamente chiusa in K.*

Dimostrazione: Sia L la chiusura algebrica di F in K e sia $\alpha \in K$ algebrico su L. Allora $L(\alpha)$ è algebrico su L e L è algebrico su F. Ne segue che α è algebrico su F (Proposizione 12.5) e dunque $\alpha \in L$.

Tuttavia la chiusura algebrica di F in K non è necessariamente un campo algebricamente chiuso.

Esempi

12.8. Il campo $A(\mathbb{R})$ dei numeri reali algebrici è algebricamente chiuso in $\mathbb{R}$, ma non è algebricamente chiuso perché non lo è in $\mathbb{C}$. Infatti ad esempio l'unità immaginaria i è un numero algebrico su $A(\mathbb{R})$ (perché lo è su $\mathbb{R}$), ma non appartiene ad $A(\mathbb{R})$.

12.9. Il *Teorema Fondamentale dell'Algebra* afferma che il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso. Già nel 1629 A. Girard aveva affermato ciò che con linguaggio attuale si può esprimere dicendo che ogni polinomio di grado n a coefficienti reali ha sempre n radici in qualche ampliamento di $\mathbb{R}$ (*L'invention en algébre*). Successivamente L. Euler, dando per scontato che tali radici esistessero, aveva sostenuto che esse sono sempre numeri complessi (*Recherches sur les racines imaginaires des équations*, 1749). La dimostrazione di Euler era corretta nel caso in cui $n \leq 6$, ma lacunosa in generale. Alcuni punti di questa dimostrazione furono successivamente corretti da J. L. Lagrange, che usò a questo scopo i suoi risultati sui gruppi delle permutazioni delle radici di un polinomio (*Sur la forme des racines imaginaires des équations*, 1772). Un'altra dimostrazione, basata sulle proprietà del discriminante, fu poi data da P. S. de Laplace (1795). Il primo ad osservare che era necessario dimostrare l'esistenza delle radici di un polinomio reale nel campo complesso fu C. F. Gauss nel 1797. Egli diede quattro dimostrazioni di questo fatto, la prima delle quali fu inclusa nella sua Tesi di Dottorato, pubblicata nel 1799. In seguito sono state date moltissime altre dimostrazioni del Teorema Fondamentale dell'Algebra, con l'impiego delle tecniche più diverse: la più elementare è forse quella di R. Argand (*Réflexions sur la nouvelle théorie d'analyse*, 1814), poi perfezionata da A. L. Cauchy (*Sur les racines imaginaires des équations*, 1820), che fa uso del così detto *Teorema del Minimo*. Nell'ultima dimostrazione, del 1849, Gauss considerò poi più generalmente polinomi a coefficienti complessi.

Proposizione 12.7 *Le seguenti condizioni sono equivalenti per il campo K.*

(*i*) *K è algebricamente chiuso;*

(*ii*) *Ogni polinomio non costante $f(X) \in K[X]$ ha almeno una radice in K;*

(*iii*) *Ogni polinomio non costante $f(X) \in K[X]$ ha tutte le sue radici in K;*

(*iv*) *Ogni polinomio non costante $f(X) \in K[X]$ si fattorizza in polinomi di primo grado in $K[X]$;*

(*v*) *I soli polinomi di $K[X]$ irriducibili su K sono i polinomi di primo grado.*

Dimostrazione: $(i) \Rightarrow (iii)$. Ogni radice di $f(X)$ è un elemento algebrico su K. Dunque essa appartiene a K.

$(ii) \Rightarrow (iii)$. Se α è una radice di $f(X)$ in K, allora per il Teorema di Ruffini si ha $f(X) = (X - \alpha)g(X)$ con $g(X) \in K[X]$. Dunque si può concludere per induzione sul grado di $f(X)$.

$(iii) \Rightarrow (ii)$, $(iii) \Rightarrow (iv)$ e $(iv) \Rightarrow (v)$ sono evidenti.

$(v) \Rightarrow (i)$. Sia $K \subseteq K'$ un ampliamento di campi e sia $\alpha \in K'$. Se α è algebrico su K, il suo polinomio minimo su K, essendo irriducibile su K, deve avere grado uguale a 1. Quindi $\alpha \in K$.

Proposizione 12.8 *Sia K algebricamente chiuso e $F \subseteq K$. Allora la chiusura algebrica di F in K è un campo algebricamente chiuso.*

Dimostrazione: Sia L la chiusura algebrica di F in K e sia $f(X) := c_0 + c_1X + \cdots + c_nX^n \in L[X] \subseteq K[X]$. Poiché K è algebricamente chiuso, ogni radice α di $f(X)$ appartiene a K (Proposizione 12.7); mostriamo che essa appartiene a in L. Se $L' := F(c_0, c_1, \ldots, c_n)$, allora L' è algebrico su F, perché $L' \subseteq L$. Inoltre α è algebrico su L', perché $f(X) \in L'[X]$. Considerando gli ampliamenti $F \subseteq L' \subseteq L'(\alpha)$, ne segue che α è algebrico su F (Proposizione 12.5). Perciò $\alpha \in L$.

Un ampliamento L di F si dice una *chiusura algebrica di F* se esso è algebrico su F ed è algebricamente chiuso.

Il seguente corollario è immediato.

Corollario 12.9 *Sia K algebricamente chiuso e sia $F \subseteq K$. Se L è la chiusura algebrica di F in K, allora L è una chiusura algebrica di F.*

Esempi

12.10. Poiché $\mathbb{C}$ è algebricamente chiuso ed è algebrico su $\mathbb{R}$, esso è una chiusura algebrica di $\mathbb{R}$.

12.11. Il campo $A(\mathbb{R})$ dei numeri reali algebrici non è una chiusura algebrica di $\mathbb{Q}$, perché esso non è algebricamente chiuso.

12.12. Il campo $A(\mathbb{C})$ dei numeri complessi algebrici è algebricamente chiuso, perché è la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Dunque esso è una chiusura algebrica di $\mathbb{Q}$ ed anche di ogni ampliamento algebrico F di $\mathbb{Q}$. In particolare $A(\mathbb{C})$ è una chiusura algebrica di $A(\mathbb{R})$.

Dato un campo F, l'esistenza di una sua chiusura algebrica è garantita dal *Lemma di Zorn*, che asserisce che ogni insieme parzialmente ordinato in cui ogni catena ammette un maggiorante ha almeno un elemento massimale. Una formulazione equivalente è l'*Assioma di Zermelo*, che asserisce che ogni insieme è bene ordinabile.

Teorema 12.10 (E. Steinitz, 1910) *Ogni campo F possiede una chiusura algebrica.*

Dimostrazione: Nel caso in cui F sia *contabile*, cioè finito o numerabile, si può costruire una chiusura algebrica di F senza usare il Lemma di Zorn.

Infatti, se F è contabile, l'insieme dei polinomi $F[X]$ è numerabile come unione numerabile di insiemi contabili (*primo procedimento diagonale di Cantor*). Perché, per ogni $n \geq 0$, l'insieme P_n dei polinomi di grado n su F può essere messo in corrispondenza biunivoca con l'insieme contabile F^{n+1}, associando ad ogni polinomio la $(n+1)$-pla dei suoi coefficienti, ed inoltre $F[X] = \bigcup_{n\geq 0} P_n \cup \{0\}$. Allora possiamo scrivere $F[X] = \{f_i(X); i \geq 1\}$.

Posto $K_0 := F$, per ogni $i \geq 1$, sia K_i un campo di spezzamento del polinomio $f_i(X)$ sul campo K_{i-1}. In questo modo si ottiene induttivamente una successione di campi (non necessariamente distinti)

$$K_0 := F \subseteq K_1 \subseteq \ldots \subseteq K_{i-1} \subseteq K_i \subseteq \ldots$$

L'unione di questi campi è un campo K algebrico su F ed inoltre ogni polinomio di $F[X]$ ha tutte le sue radici in K. Perciò K è una chiusura algebrica di F (Proposizione 12.7).

Nel caso in cui F non sia contabile, si può procedere in modo simile a quello dell'esempio precedente, facendo uso dell'*Assioma di Zermelo* e del *Principio di Induzione Transfinita.*

Infatti possiamo scrivere $F[X] = \{f_\lambda(X); \lambda \in \Lambda\}$, dove Λ è un insieme bene ordinato con primo elemento λ_0 (Assioma di Zermelo). Per induzione transfinita su Λ, definiamo $K_0 := F$ e, supposto noto K_ν per $\nu < \lambda$, definiamo K_λ come il campo di spezzamento di $f_\lambda(X)$ sul campo $\bigcup_{\nu<\lambda} K_\nu$. In questo modo, si ottiene ancora che $K := \bigcup_{\lambda\in\Lambda} K_\lambda$ è una chiusura algebrica di F.

Il nostro prossimo obiettivo è quello di dimostrare che due chiusure algebriche di un campo F sono isomorfe.

Teorema 12.11 (E. Steinitz, 1910) *Siano $F \subseteq L \subseteq K_1$ e $L \subseteq K_2$ ampliamenti di campi.*

(1) Se K_1 è algebrico su L e K_2 è algebricamente chiuso, ogni F-isomorfismo di L in K_2 si può estendere a un F-isomorfismo di K_1 in K_2.

(2) Se K_1 e K_2 sono due chiusure algebriche di L, ogni F-isomorfismo di L in K_2 si può estendere a un F-isomorfismo suriettivo tra K_1 e K_2.

Dimostrazione: (1). Sia φ un F-isomorfismo di L in K_2. Consideriamo l'insieme di tutte le coppie (N, σ) dove $L \subseteq N \subseteq K_1$ e $\sigma : N \longrightarrow K_2$

estende φ. Questo insieme è non vuoto, contenendo la coppia (L, φ), ed è parzialmente ordinato secondo la relazione

$$(N_1, \sigma_1) \leq (N_2, \sigma_2) \Leftrightarrow N_1 \subseteq N_2 \text{ e } \sigma_2 \text{ estende } \sigma_1.$$

Inoltre ogni catena $\{(N_\lambda, \sigma_\lambda)\}_{\lambda \in \Lambda}$ ammette un maggiorante, dato dalla coppia (N, σ), dove

$$N := \bigcup_{\lambda \in \Lambda} N_\lambda \subseteq K_1 \text{ e } \sigma : N \longrightarrow K_2 \text{ è tale che } \sigma(x) = \sigma_\lambda(x) \text{ se } x \in N_\lambda.$$

Dunque per il Lemma di Zorn, esiste una coppia massimale (M, μ).

Mostriamo che $M = K_1$. Sia $\alpha \in K_1$ e sia $m(X)$ il suo polinomio minimo su M. Consideriamo il polinomio $\mu^*(m(X)) \in K_2[X]$, i cui coefficienti sono le immagini secondo μ dei coefficienti di $m(X)$. Poiché K_2 è algebricamente chiuso, $\mu^*(m(X))$ ha una radice in K_2. Allora μ si può estendere a un F-isomorfismo $\nu : M(\alpha) \longrightarrow K_2$ (Proposizione 9.2). Dunque $(M, \mu) \leq (M(\alpha), \nu)$ e, per la massimalità della coppia (M, μ), deve risultare $\alpha \in M$, ovvero $M = K_1$.

(2). Siano poi K_1 e K_2 due chiusure algebriche di L. Per il punto (1), ogni F-isomorfismo $\varphi : L \longrightarrow K_2$ si può estendere ad un F-isomorfismo massimale $\mu : K_1 \longrightarrow K_2$. Facciamo vedere che μ è suriettivo. Sia $\beta \in K_2$, con polinomio minimo $q(X)$ su $\varphi(L)$. Il polinomio $p(X) = (\varphi^{-1})^*(q(X)) \in L[X]$ è irriducibile su L perché lo è $q(X)$ su $\varphi(L)$ (Lemma 9.1). Se $\alpha \in K_1$ è una radice di $p(X)$, poiché $\varphi^*(p(X)) = q(X)$ e β è una radice di $q(X)$, allora φ si può estendere a un isomorfismo $\psi : L(\alpha) \longrightarrow K_2$ in cui $\psi(\alpha) = \beta$ (Proposizione 9.2). Ma essendo $(L(\alpha), \psi) \leq (K_1, \mu)$, deve risultare $\mu(\alpha) = \psi(\alpha) = \beta$.

Corollario 12.12 *Due chiusure algebriche di un campo sono isomorfe.*

Dimostrazione: Siano K_1 e K_2 due chiusure algebriche del campo F. Per il Teorema 12.11 (2), l'immersione di F in K_2 si estende a un isomorfismo tra K_1 e K_2.

Corollario 12.13 *Sia $F \subseteq L$ un ampliamento di campi e sia K una chiusura algebrica di L. Ogni F-automorfismo di L si può estendere a un F-automorfismo di K.*

Dimostrazione: Segue dal Teorema 12.11 (2) per $K_1 = K = K_2$.

Se K è una chiusura algebrica di F, allora K deve essere algebrico su F e contenere un campo di spezzamento di ogni polinomio di $F[X]$. Il risultato successivo mostra che è vero anche il viceversa.

Proposizione 12.14 *Sia $F \subseteq K$ un ampliamento algebrico di campi. Se ogni polinomio (irriducibile) di $F[X]$ si fattorizza in polinomi di primo grado in $K[X]$, allora K è una chiusura algebrica di F.*

Dimostrazione: Sia K' un ampliamento algebrico di K e sia $\alpha \in K'$. Allora α è algebrico su F e per ipotesi il polinomio minimo di α su F si spezza linearmente in $K[X]$. Ne segue che $\alpha \in K$ e $K' = K$. Dunque K è algebricamente chiuso.

Esempi

12.13. La seguente costruzione di una chiusura algebrica è dovuta ad E. Artin.

Sia $F := K_0$ un campo e sia $\mathcal{I} := \{p_\lambda(X); \lambda \in \Lambda\}$ l'insieme dei polinomi irriducibili di $F[X]$. Sia $\mathbf{X} := \{X_\lambda; \lambda \in \Lambda\}$ un insieme di indeterminate algebricamente indipendenti su F e consideriamo l'anello di polinomi $F[\mathbf{X}]$. Per ogni $\lambda \in \Lambda$ sia $p_\lambda(X_\lambda) \in F[\mathbf{X}]$ il polinomio ottenuto da $p_\lambda(X)$ sostituendo l'indeterminata X con X_λ e sia $I := \langle p_\lambda(X_\lambda)\rangle$ l'ideale di $F[\mathbf{X}]$ generato da tutti i polinomi $p_\lambda(X_\lambda)$. Allora I è un ideale proprio di $F[\mathbf{X}]$. Infatti se $1 \in I$, esisterebbero in $F[\mathbf{X}]$ polinomi $p_i := p(X_{\lambda_i})$ e $f_i(\mathbf{X})$, $i = 1, \ldots, n$ tali che $1 = \sum_i p_i f_i$. Il che è impossibile perché questa relazione è una relazione di dipendenza algebrica tra tutte le variabili che compaiono in essa (che sono in numero finito).

Sia M un ideale massimale di $F[\mathbf{X}]$ contenente I (qui si usa il Lemma di Zorn). Allora l'anello quoziente $K := F[\mathbf{X}]/M$ è un campo contenente F. Poiché $p_\lambda(X_\lambda) \in I \subseteq M$, per ogni $\lambda \in \Lambda$, si ha un F-isomorfismo

$$\frac{F[X]}{\langle p_\lambda(X)\rangle} \longrightarrow \frac{F[\mathbf{X}]}{I} \longrightarrow K := \frac{F[\mathbf{X}]}{M},$$

definito da

$$f(X) + \langle p_\lambda(X)\rangle \mapsto f(X_\lambda) + I \mapsto f(X_\lambda) + M.$$

Dunque ogni polinomio $p_\lambda(X)$ ha una radice in $K_1 := K$, precisamente la classe di X_λ.

Possiamo allora costruire, per induzione su $i \geq 0$, un campo K_i in cui tutti i polinomi irriducibili su K_{i-1} hanno almeno una radice. Posto $L := \bigcup_{i\geq 0} K_i$, si vede facilmente che L è un campo algebricamente chiuso. Infatti ogni polinomio non nullo di $L[X]$ appartiene a qualche anello $K_n[X]$; perciò si spezza linearmente su K_{n+1} e quindi anche su L. Ne segue che la chiusura algebrica di F in L è una chiusura algebrica di F (Corollario 12.9).

12.14. Se F è un campo numerabile e K è una sua chiusura algebrica, anche K è numerabile. Infatti, come visto nella dimostrazione del Teorema 12.10, una chiusura algebrica di F si può ottenere come unione numerabile di campi di spezzamento di polinomi su F ed ogni tale campo di spezzamento è

numerabile, avendo grado finito su F. Ad esempio, il campo $A(\mathbb{C})$ dei numeri complessi algebrici, essendo una chiusura algebrica di $\mathbb{Q}$, è numerabile.

Poiché ogni ampliamento algebrico è contenuto in una chiusura algebrica, vediamo che ogni ampliamento algebrico di un campo numerabile è numerabile. Più generalmente si può dimostrare che un campo infinito ha la stessa cardinalità di ogni suo ampliamento algebrico.

Nel seguito denoteremo con $\overline{F}$ una fissata chiusura algebrica di F e, fissata una immersione di F in $\overline{F}$, supporremo che ogni ampliamento algebrico di F sia contenuto in $\overline{F}$ tramite l'estensione di questa immersione. Per quanto abbiamo appena visto, questa ipotesi non è restrittiva. Notiamo che F è algebricamente chiuso se e soltanto se $F = \overline{F}$.

Come accade nel caso numerico (Esempio 9.3), se K è un ampliamento finito di F, gli F-isomorfismi di K in $\overline{F}$ sono finiti e possono essere costruiti per induzione sui generatori. Precisamente si ha il seguente risultato.

Proposizione 12.15 *Siano F un campo e $K := F(\alpha_1, \ldots, \alpha_n)$ un ampliamento finito di F. Allora gli F-isomorfismi di K in $\overline{F}$ sono in numero finito. Precisamente essi sono al più $[K : F]$ e sono esattamente $[K : F]$ se i polinomi minimi di $\alpha_1, \ldots, \alpha_n$ su F hanno tutte radici distinte.*

Dimostrazione: Consideriamo la catena di ampliamenti:

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_n := F_{n-1}(\alpha_n) = K.$$

Se α_i ha grado r_i su F_{i-1}, allora

$$[K : F] = [F_1 : F][F_2 : F_1] \ldots [F_{n-1} : F_{n-2}][K : F_{n-1}] = r_1 \ldots r_n.$$

Gli F-isomorfismi di $F_1 := F(\alpha_1)$ in $\overline{F}$ sono al più r_1 e sono esattamente r_1 se il polinomio minimo di α_1 su F ha tutte radici distinte (Corollario 9.3). Ognuno di questi F-isomorfismi si estende al più a r_2 F-isomorfismi di $F_2 := F_1(\alpha_2)$ in $\overline{F}$ (Proposizione 9.2). Inoltre, se il polinomio minimo di α_2 su F ha tutte radici distinte, anche il polinomio minimo di α_2 su F_1 ha tutte radici distinte (perché divide il precedente). In questo caso le estensioni a F_2 di un F-isomorfismo di F_1 in $\overline{F}$ sono esattamente r_2. Così proseguendo, si ottengono al più $[K : F] = r_1 \ldots r_n$ F-isomorfismi di K in $\overline{F}$ ed esattamente $[K : F]$ se i polinomi minimi di $\alpha_1, \ldots, \alpha_m$ su F hanno tutte radici distinte.

Notiamo che, se $F \subseteq L \subseteq \overline{F}$ e $\overline{L}$ è la chiusura algebrica di L in $\overline{F}$, allora $\overline{L}$ è una una chiusura algebrica di L (Corollario 12.9). Inoltre, poiché ogni elemento di $\overline{F}$ è anche algebrico su L, risulta $\overline{F} = \overline{L}$. Infine, il campo di spezzamento di un polinomio $f(X) \in F[X]$ è univocamente determinato in $\overline{F}$. Il seguente risultato segue allora subito dal Teorema 12.11(1).

Proposizione 12.16 *Siano $F \subseteq L \subseteq K$ ampliamenti algebrici. Allora ogni F-isomorfismo di L in $\overline{F}$ si può estendere a un F-ismorfismo di K in $\overline{F}$.*

ESERCIZI

12.1. Sia $F \subseteq K$ un ampliamento di campi e sia S un sottoinsieme di K (eventualmente infinito) i cui elementi siano tutti algebrici su F. Mostrare che $F(S)$ è algebrico su F.

12.2. Sia $F \subseteq K$ un ampliamento algebrico di campi e sia A un anello tale che $F \subseteq A \subseteq K$. Mostrare che A è un campo.

12.3. Mostrare che, se $F \subseteq K$ è un ampliamento finito di campi, allora K è contenuto nel campo di spezzamento su F di un opportuno polinomio $f(X) \subseteq F[X]$.

12.4. Mostrare che $a+bi$ è un numero complesso algebrico se e soltanto se a e b sono numeri reali algebrici. Dedurne che, se x è algebrico, allora $\sin(x)$ e $\cos(x)$ sono trascendenti (*Suggerimento*: Ricordare la formula di Euler $e^{ix} = \cos(x)+i\sin(x)$ ed usare il Teorema di Lindemann citato nell'Esercizio 5.4).

12.5. Mostrare che $1 + 11\sqrt{2} - 17\sqrt{3}$ è un numero algebrico.

12.6. Mostrare che le radici del polinomio $X^{10} - \sqrt[5]{2}X^5 + \sqrt{5}X^2 - \sqrt[10]{10} \in \mathbb{R}[X]$ sono algebriche su $\mathbb{Q}$.

12.7. Siano a, $b \in \mathbb{R}$. Mostrare che, se $a + b$ e ab sono numeri algebrici, allora anche a e b lo sono.

12.8. Sia F un campo numerico. Mostrare che una chiusura algebrica di F è costituita esattamente dai numeri complessi algebrici su F.

12.9. Mostrare che i polinomi irriducibili su un campo F sono infiniti.

12.10. Mostrare che un campo finito non può essere algebricamente chiuso.

12.11. Mostrare che esistono campi infiniti algebrici su $\mathbb{F}_p$.

12.12. Sia K l'unione dei campi $\mathbb{F}_{p^n}$, $n \geq 1$. Mostrare che K è una chiusura algebrica di $\mathbb{F}_p$.

12.13. Mostrare che il campo $F(X)$ delle funzioni razionali in una indeterminata X sul campo F non è algebricamente chiuso.

12.14. Mostrare che, se $F \subseteq K$ è un ampliamento di campi, allora, a meno di isomorfismi, $\overline{F} \subseteq \overline{K}$. Mostrare inoltre con un esempio che può essere $\overline{F} \neq \overline{K}$.

13 Separabilità. Il Teorema dell'Elemento Primitivo

Sia $\overline{F}$ una fissata chiusura algebrica di F. Un elemento $\alpha \in \overline{F}$ si dice *separabile su* F se il suo polinomio minimo su F non ha radici multiple e un polinomio $f(X) \in F[X]$ si dice *separabile* se le sue radici sono tutte separabili. Un polinomio che non è separabile si dice anche *inseparabile*.

Secondo questa definizione, un polinomio separabile ma non irriducibile può avere radici multiple. Infatti, se $p(X)$ è irriducibile e separabile, allora il polinomio $p(X)^m$ è separabile per ogni $m \geq 2$, ma ogni sua radice è multipla, con molteplicità uguale a m. Tuttavia, ogni polinomio separabile ha lo stesso campo di spezzamento di un polinomio senza radici multiple. Infatti, se $f(X) = p_1(X)^{k_1} \dots p_s(X)^{k_s} \in F[X]$, dove $p_1(X), \dots, p_s(X)$ sono polinomi distinti irriducibili su F e $k_i \geq 1$, allora i polinomi $f(X)$ e $p_1(X) \dots p_s(X)$ hanno lo stesso campo di spezzamento in $\overline{F}$ (Esercizio 8.3).

Come abbiamo visto nella Proposizione 9.7, ogni polinomio a coefficienti in un campo di caratteristica zero è separabile. Tuttavia in caratteristica positiva possono esistere polinomi inseparabili.

Proposizione 13.1 *Sia F un campo e $q(X) \in F[X]$ un polinomio irriducibile su F. Allora:*

(a) *Se F ha caratteristica zero, $q(X)$ è separabile su F;*

(b) *Se F ha caratteristica prima uguale a p, $q(X)$ è inseparabile su F se e soltanto se $q(X) = c_0 + c_1 X^p + \dots + c_r X^{p^r}$, per un opportuno $r \geq 1$.*

Dimostrazione: Per il Corollario 9.6, $q(X)$ è separabile su F se e soltanto se $q'(X) \neq 0$. Poiché $q(X)$ è non costante, se F ha caratteristica zero, risulta $q'(X) \neq 0$ e perciò $q(X)$ è separabile su F.

Supponiamo che F abbia caratteristica positiva p e sia $q(X) := a_0 + a_{k_1} X^{k_1} + \dots + a_{k_n} X^{k_n}$ con $a_{k_i} \neq 0$ per $i = 1, \dots, n$. Allora $q'(X) = 0$ se e soltanto se p divide tutti i coefficienti $k_i a_{k_i}$ di $q'(X)$. Poiché p non divide a_{k_i}, ciò equivale a dire che p divide k_i, per $i = 1, \dots, n$. Ma, se $k_i = ps_i$, allora:

$$q(X) := a_0 + a_{k_1} X^{ps_1} + \dots + a_{k_n} X^{ps_n} = c_0 + c_1 X^p + \dots + c_r X^{p^r},$$

con $r = s_n$.

Corollario 13.2 *Siano F un campo di caratteristica prima uguale a p e $q(X) \in F[X]$ un polinomio di grado n irriducibile su F. Se p non divide n, allora $q(X)$ è separabile su F.*

Nella Proposizione 13.1 (b), l'ipotesi di irriducibilità è necessaria. Infatti, se F ha caratteristica prima uguale a p e $q(X) \in F[X]$ è separabile, allora $f(X) := q(X)^p = g(X^p)$ è ancora separabile (Lemma 10.2).

Per dare un esempio di un polinomio irriducibile e inseparabile, dimostriamo prima il seguente lemma.

Lemma 13.3 *Sia F un campo di caratteristica prima uguale a p e sia $f(X) := X^p - a \in F[X]$, $h \geq 1$. Allora sono possibili soltanto i due casi seguenti:*

(a) *Il polinomio $f(X)$ è irriducibile su F.*

(b) *Il polinomio $f(X)$ ha una radice $\alpha \in F$. In questo caso in $F[X]$ risulta $f(X) = (X-\alpha)^p$; in particolare α è l'unica radice di $f(X)$, con molteplicità uguale a p.*

Dimostrazione: Sia $\alpha \in \overline{F}$ una radice del polinomio $f(X) := X^p - a$. Poiché $\overline{F}$ ha caratteristica p, in $\overline{F}[X]$ risulta $(X-\alpha)^p = X^p - \alpha^p = X^p - a =: f(X)$ (Lemma 10.2). Dunque un eventuale fattore proprio di $f(X)$ in $F[X]$ deve essere del tipo $h(X) := (X-\alpha)^r$, con $r < p$ (Proposizione 9.4). Poiché $\mathrm{MCD}(r,p) = 1$, esistono due interi u, v tali che $ur + vp = 1$ (Identità di Bezout). Allora $\alpha = \alpha^{ur+vp} = (\alpha^r)^u a^v$. Poiché α^r è il termine noto di $h(X)$, si ha che $\alpha^r \in F$ e dunque anche $\alpha \in F$. Ne segue che, se $f(X)$ è riducibile, allora $f(X)$ ha una radice α in F e $f(X) = (X-\alpha)^p$ in $F[X]$.

Esempi

13.1. Un polinomio irriducibile e inseparabile in caratteristica p. Sia τ una indeterminata su $\mathbb{F}_p$ e sia $F := \mathbb{F}_p(\tau)$. Il polinomio $p(X) := X^p - \tau \in F[X]$ è irriducibile e inseparabile su F.

Per la Proposizione 13.1(b), basta mostrare che $p(X)$ è irriducibile su F. Se $p(X)$ non è irriducibile su F, allora τ ha una radice p-esima in F (Lemma 14.3). Sia tale radice $\alpha := \frac{f(\tau)}{g(\tau)}$, con $g(\tau) \neq 0$. Allora, poiché $\alpha^p = \tau$, si ha $f(\tau)^p - \tau g(\tau)^p = 0$. Questo è un polinomio in τ a coefficienti in $\mathbb{F}_p$; dunque deve essere il polinomio nullo, perché τ è trascendente su $\mathbb{F}_p$. Ma questo è impossibile, perché $g(\tau) \neq 0$ e allora il termine di massimo grado di $\tau g(\tau)^p$ non si può cancellare con nessun termine di $f(\tau)^p$. Ne segue che $p(X)$ è irriducibile su F.

Un ampliamento algebrico $F \subseteq K$ si dice *separabile* se ogni elemento di K è separabile su F. Inoltre il campo F si dice *perfetto* se ogni suo ampliamento algebrico è separabile. La seguente proposizione discende immediatamente dalle definizioni.

Proposizione 13.4 *Le seguenti proprietà sono equivalenti per un campo F:*

(*i*) *F è perfetto;*

(*ii*) *Ogni polinomio irriducibile di $F[X]$ è separabile su F;*

(*iii*) *Una chiusura algebrica $\overline{F}$ di F è un ampliamento separabile di F.*

Proposizione 13.5 *Sia F un campo.*

(*a*) *Se F ha caratteristica zero, allora F è perfetto.*

(*b*) *Se F ha caratteristica prima uguale a p, F è perfetto se e soltanto se, per ogni $a \in F$, il polinomio $X^p - a$ ha una radice in F (equivalentemente ogni elemento $a \in F$ è una potenza p-esima).*

Dimostrazione: (*a*) Se F ha caratteristica zero, ogni polinomio $f(X) \in F[X]$ è separabile (Proposizione 14.1(a)). Dunque F è perfetto.

(*b*) Supponiamo che F abbia caratteristica prima uguale a p. Se per qualche $a \in F$ il polinomio $X^p - a$ non ha radici in F, allora esso è irriducibile su F per il Lemma 14.3 e dunque è anche inseparabile su F per la Proposizione 14.1(b). Ne segue che F non è perfetto.

Supponiamo viceversa ogni elemento di F sia una potenza p-esima e sia $p(X) \in F[X]$ irriducibile su F. Se $p(X)$ è inseparabile su F, allora $p(X) = c_0 + c_1X^p + \cdots + c_rX^{pr}$, per un opportuno $r \geq 0$ (Proposizione 14.1(b)). Posto $c_i = a_i^p$, allora risulta

$$p(X) = a_0^p + a_1^pX^p + \cdots + a_r^pX^{pr} = (a_0 + a_1X + \cdots + a_rX^r)^p.$$

Questa è una contraddizione perché $p(X)$ è irriducibile su F. Dunque $p(X)$ è separabile e perciò F è perfetto.

Ricordiamo che, se F è un campo di caratteristica positiva p, l'applicazione $\Phi : F \longrightarrow F$ definita da $a \mapsto a^p$ è un omomorfismo non nullo di campi, detto omomorfismo di Fröbenius (Paragrafo 10). Il seguente corollario è del tutto evidente.

Corollario 13.6 *Un campo F di caratteristica p è perfetto se e soltanto se l'omomorfismo di Fröbenius $\Phi : F \longrightarrow F$ è suriettivo, equivalentemente Φ è un automorfismo di F.*

Corollario 13.7 *Ogni campo finito è perfetto, in particolare $\mathbb{F}_p$ è perfetto per ogni numero primo p.*

Dimostrazione: Se F è un campo finito, esso ha caratteristica positiva p. Essendo un omomorfismo non nullo di campi, $\Phi : F \longrightarrow F$ è sempre iniettivo. Poiché F è finito, allora Φ è anche suriettivo.

Esempi

13.2. Per ogni primo p, se τ è una indeterminata su $\mathbb{F}_p$, il campo $\mathbb{F}_p(\tau)$ non è perfetto. Infatti abbiamo visto nel precedente Esempio 14.1 che il polinomio $X^p - \tau$ è irriducibile e inseparabile su $\mathbb{F}_p(\tau)$.

Se K è finito su F e $K := F(\alpha)$, allora α si dice un *elemento primitivo di K su F*. Per questo motivo il teorema seguente, che ha grande utilità teorica, va sotto il nome di *Teorema dell'Elemento Primitivo*; nel caso numerico esso fu dimostrato per la prima volta da E. Galois nel 1830.

Teorema 13.8 (Teorema dell'Elemento Primitivo) *Sia* $K := F(\alpha_1, \ldots, \alpha_n)$ *un ampliamento finito di* F. *Se almeno* $n-1$ *elementi tra gli* $\alpha_1, \ldots, \alpha_n$ *sono separabili, allora* K *è un ampliamento semplice di* F.

Dimostrazione: Se F è un campo finito, anche K, avendo grado finito su F, lo è. Allora il teorema è vero per la Proposizione 10.4.

Supponiamo che F sia infinito e procediamo per induzione su n.

Se $n = 1$ il risultato è evidente. Se $n \geq 2$, possiamo supporre che α_n sia separabile. Poiché almeno $n-2$ elementi tra $\alpha_1, \ldots, \alpha_{n-1}$ sono separabili, se il teorema è vero per $k = n-1$, allora esiste $\beta \in K$ tale che $F(\alpha_1, \ldots, \alpha_{n-1}) = F(\beta)$. Posto $\alpha_n := \gamma$, dobbiamo allora dimostrare che l'ampliamento $F(\beta, \gamma)$ di F è semplice.

Siano $p(X)$ e $q(X)$ i polinomi minimi su F di β e γ rispettivamente e siano $\beta := \beta_1, \ldots, \beta_r$, $\gamma := \gamma_1, \ldots, \gamma_s$ le radici distinte di $p(X)$ e $q(X)$ in $\overline{F}$. Poiché gli elementi $c_{ij} := \frac{\beta - \beta_i}{\gamma_j - \gamma} \in \overline{F}$, con $i = 1, \ldots, r$ e $j = 2, \ldots, s$, sono finiti e F è infinito, allora esiste $c \in F$ tale che $c \neq c_{ij}$, equivalentemente tale che $\beta + c\gamma \neq \beta_i + c\gamma_j$, per ogni i e ogni $j \neq 1$. Posto $\theta := \beta + c\gamma$, mostriamo che $F(\beta, \gamma) = F(\theta)$.

Consideriamo il polinomio $h(X) := p(\theta - cX) \in F(\theta)[X] \subseteq \overline{F}[X]$. Allora risulta $h(\gamma) = p(\beta) = 0$ e $h(\gamma_j) = p(\beta + c(\gamma - \gamma_j)) \neq 0$ per $j = 2, \ldots, s$, perché $\beta + c(\gamma - \gamma_j) \neq \beta_i$ per ogni $i = 1, \ldots, r$ e le uniche radici di $p(X)$ sono $\beta := \beta_1, \ldots, \beta_r$. Poiché $\alpha_n := \gamma$ è separabile su F, allora γ non è una radice multipla di $q(X)$ e dunque in $\overline{F}[X]$ risulta $\mathrm{MCD}(h(X), q(X)) = (X - \gamma)$. Questo è anche il massimo comune divisore di $h(X)$ e $q(X)$ in $F(\theta)[X]$ (Proposizione 9.4 (c)) e dunque $\gamma \in F(\theta)$. Ne segue che anche $\beta = \theta - c\gamma \in F(\theta)$ e allora $F(\beta, \gamma) = F(\theta)$.

Corollario 13.9 *Ogni ampliamento di campi finito e separabile è semplice.*

Corollario 13.10 *Ogni ampliamento finito di un campo perfetto, in particolare di un campo di caratteristica zero, è semplice.*

Esempi

13.3. Ogni radice n-sima primitiva dell'unità sul campo F è un elemento primitivo dell'n-simo ampliamento ciclotomico di F (Paragrafo 11).

13.4. Se F è un campo di caratteristica diversa da 2, ogni polinomio irriducibile su F di grado uguale a 2 o 4 è separabile (Proposizione 13.1). Allora, ogni ampliamento biquadratico $K := F(\alpha, \beta)$ di F è separabile e un elemento primitivo per K su F è $\theta = \alpha + \beta$ (Esempio 7.6).

13.5. Un elemento primitivo per $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ su $\mathbb{Q}$ è $\theta := \sqrt{3} + \sqrt[3]{2}$ (Esempio 7.7).

13.6. Un ampliamento finitamente generato che è non semplice. Sia $K := F(X,Y)$ il campo delle funzioni razionali in due indeterminate algebricamente indipendenti sul campo F. Se $K = F(\theta)$, con $\theta = \frac{f(X,Y)}{g(X,Y)}$, allora dalla relazione $X = \frac{u(\theta)}{v(\theta)}$ si otterrebbe una relazione di dipendenza algebrica tra X e Y. Dunque K non può essere un ampliamento semplice di F.

Il seguente teorema dà una condizione più generale per l'esistenza di un elemento primitivo.

Teorema 13.11 *Un ampliamento finito è semplice se e soltanto se ha un numero finito di campi intermedi.*

Dimostrazione: Sia $F \subseteq K$ un ampliamento finito. Se F è un campo finito, anche K lo è. Dunque K è un ampliamento semplice di F (Teorema 10.4) ed inoltre ci sono evidentemente un numero finito di campi intermedi tra F e K. Supponiamo dunque che F sia infinito.

Sia $K = F(\alpha_1, \ldots, \alpha_n)$, $n \geq 1$ (Teorema 12.1). Supponiamo che l'ampliamento $F \subseteq K$ abbia un numero finito di campi intermedi e mostriamo che K è un ampliamento semplice di F. Poiché anche l'ampliamento $F \subseteq F(\alpha_1, \ldots, \alpha_{n-1})$ ha un numero finito di campi intermedi, per induzione su n, basta considerare il caso in cui $K = F(\alpha, \beta)$.

Poiché i campi del tipo $F(\alpha + c\beta)$, al variare di $c \in F$, sono in numero finito, esistono c_1, $c_2 \in F$ tali che $F(\alpha + c_1\beta) = F(\alpha + c_2\beta) =: L$. Mostriamo che $F(\alpha, \beta) = L$. Chiaramente $F(\alpha, \beta) \subseteq L$. Viceversa, poiché $\alpha + c_1\beta, \alpha + c_2\beta \in L$, allora $\beta = \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} \in L$ e anche $\alpha = (\alpha + c_1\beta) - c_1\beta \in L$. Perció $F(\alpha, \beta) \subseteq L$.

Viceversa, mostriamo che ogni ampliamento algebrico semplice $K := F(\alpha)$ ha un numero finito di campi intermedi. Sia $m(X)$ il polinomio minimo di α su F. Se L è un campo intermedio, il polinomio minimo $p_L(X)$ di α su L divide $m(X)$ in $L[X]$, e dunque anche in $K[X]$. Quindi possiamo definire tra l'insieme dei campi intermedi dell'ampliamento $F \subseteq K$ e l'insieme dei polinomi di $K[X]$ che dividono $m(X)$ l'applicazione che associa al campo L il polinomio $p_L(X)$. Osserviamo che i divisori di $m(X)$ in $K[X]$ sono in numero finito; infatti K è contenuto in un campo di spezzamento di $m(X)$ e su tale campo $m(X)$ si fattorizza in un numero finito di polinomi di primo grado.

Per concludere, mostriamo che questa applicazione è iniettiva. Sia L' il sottocampo di L generato su F dai coefficienti di $p_L(X)$. Si ha $F \subseteq L' \subseteq L \subseteq K$. Poiché $p_L(X) \in L'[X] \subseteq L[X]$ e $p_L(X)$ è irriducibile su L, allora $p_L(X)$ è anche irriducibile su L'. Dunque $p_L(X) = p_{L'}(X)$ è anche il polinomio minimo di α su L'. Ne segue che $K = F(\alpha) = L'(\alpha) = L(\alpha)$ ha lo stesso grado sia su L che su L' e perció $L = L'$ (Corollario 7.4). In conclusione, il campo intermedio L è univocamente determinato dai coefficienti di $p_L(X)$ e perció l'applicazione che associa ad L il polinomio $p_L(X)$ è iniettiva.

Notiamo che un ampliamento con un numero finito di campi intermedi è necessariamente algebrico. Infatti, se α è trascendente su F, i campi intermedi $F(\alpha^n)$ dell'ampliamento $F \subseteq F(\alpha)$ sono tutti distinti per $n \geq 1$.

Corollario 13.12 *Ogni ampliamento finito e separabile ha un numero finito di campi intermedi.*

Dimostrazione: Segue dal Teorema 13.10, perché un ampliamento finito e separabile è semplice (Corollario 13.9).

Esempi

13.7. Un ampliamento finito che è non semplice. Siano τ, ω due indeterminate algebricamente indipendenti su $\mathbb{F}_p$. Poniamo $F := \mathbb{F}_p(\tau^p, \omega^p)$ e $K := \mathbb{F}_p(\tau, \omega)$. Notiamo che τ^p e ω^p sono ancora indeterminate algebricamente indipendenti su $\mathbb{F}_p$, perché lo sono τ e ω. Procedendo come nell'Esempio 13.1, possiamo allora vedere che il polinomio $X^p - \tau^p \in F[X]$ è irriducibile su F, perché la sua unica radice è τ e $\tau \notin F$. Dunque τ ha grado p su F. Analogamente anche ω ha grado p su $F(\tau) = \mathbb{F}_p(\tau, \omega^p)$, con polinomio minimo $X^p - \omega^p$. Ne segue che $K := F(\tau, \omega)$ è finito di grado p^2 su F. Notiamo che sia τ che ω sono inseparabili su F.

L'ampliamento $F \subseteq K$ non è semplice perché ha un numero infinito di campi intermedi. Infatti, essendo τ e ω algebricamente indipendenti su $\mathbb{F}_p$, per ogni $c \in F$, il campo $F(\tau + c\omega)$ è propriamente compreso tra F e K. Inoltre, se $c \neq c' \in F$, risulta $F(\tau + c\omega) \neq F(\tau + c'\omega)$, altrimenti $\tau, \omega \in F$ e $F = K$. Poiché F è infinito, ci sono infiniti campi intermedi tra F e K.

Vogliamo ora approfondire lo studio degli ampliamenti separabili dal punto di vista degli F-isomorfismi.

Teorema 13.13 *Sia $F \subseteq K$ un ampliamento finito. Allora le seguenti proprietà sono equivalenti:*

(*i*) *L'ampliamento $F \subseteq K$ è separabile;*

(*ii*) *$K = F(\alpha)$ e α è separabile su F;*

(*iii*) *$K := F(\alpha_1, \ldots, \alpha_n)$ e α_i è separabile su F per $i = 1, \ldots, n$;*

(*iv*) *Gli F-isomorfismi distinti di K in $\overline{F}$ sono esattamente $[K : F]$.*

Dimostrazione: (*i*) $\Rightarrow$ (*ii*) per il Teorema dell'Elemento Primitivo (Corollario 13.9).

(*ii*) $\Rightarrow$ (*iii*) è ovvia.

(*iii*) $\Rightarrow$ (*iv*) segue dalla Proposizione 12.14.

$(iv) \Rightarrow (i)$. Poiché K è finito su F, allora $K = F(\alpha_1, \ldots, \alpha_n)$,, con $n \geq 1$. Sia $\alpha_0 \in K$ inseparabile su F. Allora $K = F(\alpha_1, \ldots, \alpha_n) = F(\alpha_0, \alpha_1, \ldots, \alpha_n)$. Consideriamo la catena di campi:

$$F \subseteq F_0 := F(\alpha_0) \subseteq F_1 := F_0(\alpha_1) \subseteq \ldots \subseteq F_i := F(\alpha_0, \alpha_1, \ldots, \alpha_i) \subseteq \ldots \subseteq K$$

Sia $r_0 := [F_0 : F]$ e $r_i := [F_i : F_{i-1}]$ per $i = 1, \ldots, n$.

Per il Corollario 9.3, gli F-isomorfismi di F_0 in $\overline{F}$ sono in numero strettamente minore di r_0. Inoltre, per $i = 1, \ldots, n$, gli F-isomorfismi di F_i in $\overline{F}$ che estendono un fissato F-isomorfismo di F_{i-1} in $\overline{F}$ sono al più r_i (Proposizione 9.2). Ne segue che gli F-isomorfismi di K in $\overline{F}$ sono in numero strettamente minore di $[K : F] = r_0 r_1 \ldots r_n$.

Se K è un ampliamento finito di F, il numero degli F-isomorfismi distinti di K in $\overline{F}$ si dice il *grado di separabilità di K su F* e si indica con $[K : F]_s$. Il seguente corollario è immediato.

Corollario 13.14 *Un ampliamento finito $F \subseteq K$ è separabile se e soltanto se $[K : F]_s = [K : F]$.*

Se $p(X) \in F[X]$ è un polinomio irriducibile su F e α è una sua radice, il grado di separabilità di $F(\alpha)$ su F si dice anche il *grado di separabilità di α* o ancora il *grado di separabilità di $p(X)$*.

Per determinare il grado di separabilità del polinomio $p(X)$, si può procedere nel modo seguente.

Il numero degli F-isomorfismi distinti di $F(\alpha)$ in $\overline{F}$ è uguale al numero delle radici distinte di $p(X)$ (Corollario 9.3). Se $p(X)$ è separabile, tale numero è uguale a $[F(\alpha) : F]$. Se $p(X)$ non è separabile, per quanto visto nella Proposizione 13.1, F ha caratteristica prima p e $p(X) = q(X^{p^h})$ per qualche $h \geq 1$. Se scegliamo h massimale, allora, posto $Y = X^{p^h}$, non è possibile scrivere $q(Y)$ come un polinomio in Y^p; dunque, ancora per la Proposizione 13.1, il polinomio $q(Y)$ è (irriducibile e) separabile su F.

Osserviamo ora che, per ogni radice α di $p(X)$, allora α^{p^h} è una radice di $q(Y)$. Viceversa, poiché siamo in caratteristica p, per ogni $\beta \in \overline{F}$, esiste un unico elemento $\alpha \in \overline{F}$ tale che $\beta = \alpha^{p^h}$ ed inoltre, se β è una radice di $q(Y)$, allora α è una radice di $p(X)$. In definitiva, se $\beta_1, \ldots, \beta_m$ sono le radici di $q(Y)$ e $\beta_i = \alpha_i^{p^h}$, $i = 1, \ldots, m$, le radici distinte di $p(X)$ sono esattamente $\alpha_1, \ldots, \alpha_m$, tutte con molteplicità p^h. Infatti,

$$p(X) = q(X^{p^h}) = \prod_{1 \leq i \leq m} (X^{p^h} - \beta_i) = \prod_{1 \leq i \leq m} (X^{p^h} - \alpha_i^{p^h}) = \prod_{1 \leq i \leq m} (X - \alpha_i)^{p^h}.$$

Ne segue che $[F(\alpha) : F]_s = \deg(q(Y))$ ed inoltre

$$[F(\alpha) : F] = \deg(p(X)) = \deg(q(Y))p^h = [F(\alpha) : F]_s p^h.$$

Notiamo che $[F(\alpha) : F]_s = 1$ se e soltanto se $p(X) = X^{p^h} - a$, ovvero $\alpha^{p^h} = a \in F$, per un opportuno $h \geq 0$.

Lemma 13.15 *Sia $F \subseteq L$ un ampliamento algebrico e sia $\alpha \in \overline{F}$. Allora ogni F-isomorfismo di L in $\overline{F}$ si estende a $[L(\alpha) : L]_s$ F-isomorfismi distinti di $L(\alpha)$ in $\overline{F}$.*

Dimostrazione: Sia φ un F-isomorfismo di L in $\overline{F}$. Se $p(X)$ è il polinomio minimo di α su L, il numero degli F-isomorfismi distinti di $L(\alpha)$ in $\overline{F}$ che estendono φ è uguale al numero delle radici distinte del polinomio $\varphi^*(p(X))$ (Proposizione 9.2).

D'altra parte, se $K \subseteq \overline{F}$ è il campo di spezzamento di $p(X)$ su L, φ si può estendere ad un F-isomorfismo ψ di K in $\overline{F}$ (Corollario 12.14). Fattorizzando $p(X)$ in fattori lineari su K, si vede facilmente che $p(X)$ e $\psi^*(p(X)) = \varphi^*(p(X))$ hanno lo stesso numero di radici distinte in $\overline{F}$. Tale numero è per definizione uguale al grado di separabilità $[L(\alpha) : L]_s$.

Proposizione 13.16 *Siano $F \subseteq L \subseteq K$ ampliamenti finiti di campi. Allora*

$$[K : F]_s = [K : L]_s [L : F]_s.$$

Dimostrazione: Poiché L e K sono ampliamenti algebrici finitamente generati, possiamo supporre che $L = F(\alpha_1, \ldots, \alpha_m)$ e $K = F(\alpha_1, \ldots, \alpha_n)$ con $n \geq m \geq 1$. Consideriamo la catena di ampliamenti:

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_{n-1}(\alpha_n) =: K,$$

dove $L = F_m$. Applicando il Lemma 13.15, per induzione su $i \geq 1$ si ottiene

$$[K : F]_s = \prod_{1 \leq i \leq n} [F_{i-1}(\alpha_i) : F_{i-1}]_s = [K : L]_s [L : F]_s.$$

Proposizione 13.17 *Siano $F \subseteq L \subseteq K$ ampliamenti algebrici di campi. Allora l'ampliamento $F \subseteq K$ è separabile se e soltanto se gli ampliamenti $F \subseteq L$ e $L \subseteq K$ sono separabili.*

Dimostrazione: Supponiamo che l'ampliamento $F \subseteq K$ sia separabile. Sia $\alpha \in K$ con polinomio minimo $m(X)$ su F e $p(X)$ su L. Poiché $m(X)$ non ha radici multiple in $\overline{F}$ e $p(X)$ divide $m(X)$ in $L[X] \subseteq \overline{F}[X]$, allora anche $p(X)$ non ha radici multiple in $\overline{F}$. Ne segue che α è separabile su L. Infine è chiaro che se K è separabile su F, anche L lo è.

Viceversa, supponiamo che gli ampliamenti $F \subseteq L$ e $L \subseteq K$ siano separabili. Sia $\alpha \in K$ con polinomio minimo $p(X) := c_0 + c_1 X + \cdots + c_n X^n$ su L e si consideri il campo $L' = F(c_0, \ldots, c_n)$. Poiché L è separabile su F e $L' \subseteq L$, anche L' è separabile su F. Inoltre, poiché $p(X) \in L'[X]$ e α è separabile su L, allora α è separabile anche su L'. Considerando gli

ampliamenti finiti $F \subseteq L' \subseteq L'(\alpha)$, per il Corollario 13.14 e la Proposizione 13.16, si ha

$$[L'(\alpha) : F] = [L'(\alpha) : L'][L' : F] = [L'(\alpha) : L']_s[L' : F]_s = [L'(\alpha) : F]_s.$$

Dunque l'ampliamento $F \subseteq L'(\alpha)$ è separabile, ancora per il Corollario 13.14, ed in particolare α è separabile anche su F.

Corollario 13.18 *Sia $F \subseteq K$ un ampliamento separabile finito e sia L un campo intermedio. Allora gli F-isomorfismi di L in $\overline{F}$ sono $[L : F]$ e ogni tale isomorfismo si estende a $[K : L]$ F-isomorfismi distinti di K in $\overline{F}$.*

Dimostrazione: Gli ampliamenti $F \subseteq L$ e $L \subseteq K$ sono separabili (Proposizione 13.17). Allora gli F-isomorfismi di L in $\overline{F}$ sono $[L : F]$ per il Teorema 13.13. Inoltre $[K : L] = [K : L]_s$ e, per il Teorema dell'Elemento Primitivo, si ha $K = L(\alpha)$. Dunque ogni F-isomorfismo di L in $\overline{F}$ si estende a $[K : L]$ F-isomorfismi distinti di K per il Lemma 13.15.

Si dice che un elemento $\alpha \in \overline{F}$ è *puramente inseparabile su F* se $[F(\alpha) : F]_s = 1$. Come visto precedentemente, questo avviene se e soltanto se F ha caratteristica positiva p e il polinomio minimo di α su F è del tipo $X^{p^h} - a$, ovvero se $\alpha^{p^h} = a \in F$, per un opportuno $h \geq 0$. Un ampliamento algebrico $F \subseteq K$ si dice *puramente inseparabile* se ogni elemento di $K \setminus F$ è puramente inseparabile su F.

Teorema 13.19 *Sia $F \subseteq K$ un ampliamento finito di campi. Allora:*

(*a*) *$[K : F] = p^h[K : F]_s$, per un opportuno primo p e $h \geq 0$;*

(*b*) *K è puramente inseparabile su F se e soltanto se $[K : F]_s = 1$.*

Dimostrazione: Sia $K = F(\alpha_1, \ldots, \alpha_n)$ e consideriamo la catena di ampliamenti:

$$F_0 := F \subseteq F_1 := F(\alpha_1) \subseteq \ldots \subseteq F_i := F_{i-1}(\alpha_i) \subseteq \ldots \subseteq F_{n-1}(\alpha_n) =: K.$$

Per la Proposizione 13.16, si ha $[K : F]_s = \prod_{1 \leq i \leq n} [F_{i-1}(\alpha_i) : F_{i-1}]_s$.

(*a*) Se F ha caratteristica zero, allora F è perfetto e basta prendere $h = 0$ (Corollario 13.14). Altrimenti, sia F di caratteristica positiva p. Per quanto osservato precedentemente per gli ampliamenti semplici, per ogni $i = 1, \ldots, n$, si ha

$$[F_{i-1}(\alpha_i) : F_{i-1}] = p^{h_i}[F_{i-1}(\alpha_i) : F_{i-1}]_s, \ h_i \geq 0.$$

Dunque

$$[K : F] = \prod_{1 \leq i \leq n} [F_{i-1}(\alpha_i) : F_{i-1}] = p^h \prod_{1 \leq i \leq n} [F_{i-1}(\alpha_i) : F_{i-1}]_s = p^h[K : F]_s.$$

per un opportuno $h \geq 0$.

(b) Sia $\alpha \in K$. Poiché $[F(\alpha) : F]_s$ divide $[K : F]_s$ (Proposizione 13.16), se $[K : F]_s = 1$ risulta $[F(\alpha) : F]_s = 1$ per ogni $\alpha \in K \setminus F$. Viceversa, se $[F(\alpha_i) : F]_s = 1$ per ogni $i \leq n$, allora

$$[K : F]_s = \prod_{1 \leq i \leq n} [F_{i-1}(\alpha_i) : F_{i-1}]_s \leq \prod_{1 \leq i \leq n} [F(\alpha_i) : F]_s = 1.$$

Quindi $[K : F]_s = 1$.

Se K è un ampliamento finito di F, il numero $[K : F]_i := \frac{[K:F]}{[K:F]_s}$ si dice il *grado di inseparabilità* di K su F. Riformulando in questi termini il teorema precedente, otteniamo:

Corollario 13.20 *Sia $F \subseteq K$ un ampliamento finito di campi. Se $[K : F]_i \neq 1$, allora F ha caratteristica prima p e $[K : F]_i$ è una potenza di p. Inoltre K è puramente inseparabile su F se e soltanto se $[K : F] = [K : F]_i$.*

Terminiamo questo paragrafo mostrando che ogni ampliamento algebrico di F si può spezzare in un ampliamento separabile e un ampliamento puramente inseparabile.

Teorema 13.21 *Sia $F \subseteq K$ un ampliamento algebrico e sia K_s l'insieme degli elementi di K separabili su F. Allora:*

(a) *K_s è un campo;*

(b) *L'ampliamento $F \subseteq K_s$ è separabile;*

(c) *Se $K_s \neq K$, l'ampliamento $K_s \subseteq K$ è puramente inseparabile.*

Dimostrazione: (a) Se α, $\beta \in K$ sono separabili su F, allora $F(\alpha, \beta)$ è un ampliamento separabile di F (Teorema 13.13). Poiché $\alpha - \beta \in F(\alpha, \beta)$ e $\alpha\beta^{-1} \in F(\alpha, \beta)$ per $\beta \neq 0$, essi sono separabili su F.

(b) segue immediatamente dalla definizione.

(c) Se $K_s \neq K$, allora F ha caratteristica positiva p. Sia $\alpha \in K \setminus K_s$ e sia $p(X)$ il suo polinomio minimo su K_s. Allora esiste $h \geq 1$ tale che $p(X) = q(X^{p^h})$ e il polinomio $q(Y) \in K_s[Y]$ è separabile su K_s. La radice α^{p^h} di $q(Y)$ è separabile su K_s e allora, poiché K_s è separabile su F, per la Proposizione 13.17 essa è anche separabile su F. Ne segue che $\alpha^{p^h} \in K_s$ e dunque α è puramente inseparabile su F.

ESERCIZI

13.1. Sia $K := F(\alpha_1, \ldots, \alpha_n)$ un ampliamento finito e separabile di F. Mostrare che $\alpha := x_1\alpha_1 + \ldots, x_n\alpha_n$ è un elemento primitivo di K su

F, eccetto che per un numero finito di n-ple $(x_1, \ldots, x_n)$ di elementi di F (*Suggerimento.* Seguire la dimostrazione del Teorema 13.8).

13.2. Determinare un elemento primitivo per i seguenti ampliamenti di $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2});\ \mathbb{Q}(\sqrt{2}, \sqrt[4]{2});\ \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5});\ \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5});\ \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt[3]{2}).$$

13.3. Siano $\alpha := \sqrt[3]{2}$, $\xi \in \mathbb{C}$ una radice primitiva terza dell'unità e $K := \mathbb{Q}(\alpha, \xi)$. Mostrare che $\alpha - \alpha\xi$ è un elemento primitivo per K su $\mathbb{Q}$ mentre $\alpha + \alpha\xi$ non lo è.

13.4. Sia $f(X) \in F[X]$ e sia $d(X) := \mathrm{MCD}(f(X), f'(X))$. Mostrare che il polinomio $\frac{f(X)}{d(X)}$ è separabile su F.

13.5. Stabilire quali tra i seguenti polinomi sono separabili su $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_3$:

$$X^3 + 1;\ X^2 - 2X + 1;\ 6X^2 + X - 1;\ X^5 + X^4 + X^3 + X^2 + 1;\ X^9 + X^3 + 1.$$

13.6. Costruire un ampliamento finito semplice e non separabile del campo $\mathbb{F}_p(\tau)$, dove τ è una indeterminata su $\mathbb{F}_p$ (*Suggerimento.* Usare il polinomio $X^p - \tau$ considerato nell'Esempio 13.1).

13.7. Dare un esempio esplicito di un polinomio separabile su $\mathbb{F}_p$ la cui derivata formale è nulla.

13.8. Mostrare che ogni ampliamento algebrico di un campo perfetto è perfetto.

13.9. Mostrare che un campo algebricamente chiuso è perfetto.

13.10. Sia p un numero primo e sia τ una indeterminata su $\mathbb{F}_p$. Verificare che l'omomorfismo di Fröbenius $\Phi : \mathbb{F}_p(\tau) \longrightarrow \mathbb{F}_p(\tau)$, definito da $x \mapsto x^p$, non è suriettivo (Esercizio 3.3).

13.11. Siano $F \subseteq L \subseteq K$ ampliamenti finiti di campi. Mostrare che

$$[K : F]_i = [K : L]_i [L : F]_i.$$

14 Ampliamenti Normali

Sia $\overline{F}$ una fissata chiusura algebrica di F. Due elementi $\alpha, \beta \in \overline{F}$ si dicono *coniugati su* F se essi hanno lo stesso polinomio minimo su F, equivalentemente se esiste un F-isomorfismo φ di $F(\alpha)$ in $\overline{F}$ tale che $\varphi(\alpha) = \beta$ (Corollario 9.3). In questo caso anche i campi $F(\alpha)$ e $F(\beta) = \varphi(F(\alpha))$ si dicono coniugati. più generalmente, due campi L, M algebrici su F si dicono *coniugati su* F *in* $\overline{F}$ se esiste un F-isomorfismo φ di L in $\overline{F}$ tale che $\varphi(L) = M$. Se $\varphi(L) = L$, per ogni F-isomorfismo φ, allora L si dice anche *autoconiugato.*

Proposizione 14.1 *Siano $F \subseteq L \subseteq K$ ampliamenti algebrici. Allora:*

(*a*) *I campi coniugati a L su F sono esattamente i campi $\varphi(L)$, al variare di φ tra gli F-isomorfismi di K in $\overline{F}$.*

(*b*) *Se $F \subseteq K$ è un ampliamento finito e separabile di grado n, $\varphi_1, \ldots, \varphi_n$ sono gli F-isomorfismi di K in $\overline{F}$ e $[K : L] = m$, allora i campi coniugati a L su F sono i campi $\varphi_1(L), \ldots, \varphi_n(L)$, ognuno contato $\frac{n}{m}$ volte.*

In particolare, se $\alpha \in K$ ha grado m su F, allora il polinomio minimo di α su F ha radici $\varphi_1(\alpha), \ldots, \varphi_n(\alpha)$, ognuna contata $\frac{n}{m}$ volte.

Dimostrazione: (*a*) Ogni F-isomorfismo di L in $\overline{F}$ si estende a un F-isomorfismo di K in $\overline{F}$ (Corollario 12.14). Viceversa è evidente che la restrizione a L di un F-isomorfismo di K in $\overline{F}$ è ancora un F-isomorfismo.

(*b*) Per il Corollario 13.18, essendo $n = [K : F] = [K : L][L : F] = [K : L]m$, ci sono esattamente $\frac{n}{m}$ isomorfismi distinti di K in $\overline{F}$ che estendono un fissato isomorfismo di L in $\overline{F}$, cioè che coincidono su L. Ne segue che ci sono $\frac{n}{m}$ campi distinti coniugati a L su F.

Se in particolare $L = F(\alpha)$, allora i campi coniugati a L sono tutti e soli i campi $F(\beta)$ al variare di β tra le radici distinte del polinomio minimo di α su F. Ma tali radici sono esattamente i valori distinti tra $\varphi_1(\alpha), \ldots, \varphi_n(\alpha)$ (Corollario 9.3).

Se $F \subseteq K$ è un ampliamento separabile di grado n, la proposizione precedente ci fornisce un modo per determinare il polinomio minimo $m(X)$ su F di un elemento $\alpha \in K$ una volta che si conoscano gli F-isomorfismi $\varphi_1, \ldots, \varphi_n$ di K in $\overline{F}$. Infatti, se $\varphi_1(\alpha), \ldots, \varphi_d(\alpha)$ sono i valori distinti tra i $\varphi_i(\alpha)$, allora

$$m(X) = (X - \varphi_1(\alpha)) \ldots (X - \varphi_d(\alpha)).$$

Esempi

14.1. Sia F un campo numerico reale e sia $K := F(\sqrt{a}, \sqrt{b})$ un suo ampliamento biquadratico. Per quanto visto nell'Esempio 9.2 (d), per ogni $\alpha := h(\sqrt{a}, \sqrt{b}) \in K$, le radici del polinomio minimo di α su F sono i numeri complessi distinti tra

$$h(\sqrt{a}, \sqrt{b}),\ h(\sqrt{a}, -\sqrt{b}),\ h(-\sqrt{a}, \sqrt{b}),\ h(-\sqrt{a}, -\sqrt{b}).$$

Ad esempio, se $\alpha = \sqrt{a} + \sqrt{b}$, allora si ottengono i valori distinti:

$$\alpha = \sqrt{a} + \sqrt{b},\ \sqrt{a} - \sqrt{b},\ -\sqrt{a} + \sqrt{b},\ -\sqrt{a} - \sqrt{b},$$

da cui il polinomio minimo di α su F è:

$$m(X) = X^4 - 2(a + b)X^2 + (a - b)^2$$

(Esempio 7.6).

Se invece $\alpha = \sqrt{a}\sqrt{b}$, si ottengono i valori distinti $\sqrt{ab}$, $-\sqrt{ab}$, da cui, come deve essere,

$$m(X) = X^2 - ab.$$

14.2. Sia $p(X) := X^3 - 3X + 1 \in \mathbb{Q}[X]$. Se α è una radice reale di $p(X)$, allora le altre radici di $p(X)$ in $\mathbb{C}$ sono $\beta := \alpha^2 - 2$ e $\gamma := -\alpha^2 - \alpha + 2$ e sono anche esse reali. Dunque gli F-isomorfismi di $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ (che sono tutti automorfismi) sono definiti rispettivamente da

$$\psi_1 := id : r(\alpha) \mapsto r(\alpha)\ ;\ \psi_2 : r(\alpha) \mapsto r(\beta)\ ;\ \psi_3 : r(\alpha) \mapsto r(\gamma),$$

per ogni $r(X) \in \mathbb{Q}[X]$ di grado al più uguale a 2 (Esempio 9.3(a)).

Poiché ogni elemento $\zeta \in \mathbb{Q}(\alpha)\backslash\mathbb{Q}$ ha grado 3 su $\mathbb{Q}$, allora il suo polinomio minimo su $\mathbb{Q}$ è:

$$m(X) = (X - \zeta)(X - \psi_2(\zeta))(X - \psi_3(\zeta)).$$

Se ad esempio $\zeta = \alpha - 2$, allora risulta $\psi_2(\zeta) = \alpha^2 - 4$ e $\psi_3(\zeta) = -(\alpha^2 + \alpha)$. Per cui il polinomio minimo di ζ è:

$$m(X) = (X - \alpha + 2)(X - \alpha^2 + 4)(X + \alpha^2 + \alpha) = X^3 + 6X^2 + 9X + 3.$$

Notiamo che anche il polinomio $m(X)$ ha tutte radici reali.

14.3. Sia p un numero primo e $n \geq 1$. Posto $q := p^n$, ogni isomorfismo di $\mathbb{F}_q$ in una sua chiusura algebrica è un automorfismo. Inoltre $\mathrm{Aut}(\mathbb{F}_q)$ è ciclico di ordine n, generato dall'automorfismo di Fröbenius $\Phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ definito da $x \mapsto x^p$ (Teorema 10.11). Se $\alpha \in \mathbb{F}_q$ ha grado m su $\mathbb{F}_p$, allora le radici del suo polinomio minimo su $\mathbb{F}_p$ sono:

$$\alpha,\ \Phi(\alpha) = \alpha^p,\ \Phi^2(\alpha) = \alpha^{p^2},\ \ldots,\ \Phi^{n-1}(\alpha) = \alpha^{p^{n-1}}.$$

Tra queste, soltanto m sono distinte.

Un ampliamento algebrico $F \subseteq K$ si dice *normale*, oppure K si dice *normale su* F se, per ogni $\alpha \in K$, tutti i coniugati di α su F appartengono a K.

La seguente proposizione discende dalle definizioni e dal Corollario 9.3.

Proposizione 14.2 *Sia $F \subseteq K$ un ampliamento algebrico. Le seguenti proprietà sono equivalenti:*

(*i*) *L'ampliamento $F \subseteq K$ è normale;*

(*ii*) *Ogni polinomio irriducibile $f(X) \in F[X]$ che ha una radice in K si spezza linearmente su K;*

(*iii*) *Per ogni F-isomorfismo $\varphi : K \longrightarrow \overline{F}$, $\varphi(K) \subseteq K$;*

(*iv*) *Ogni F-isomorfismo φ di K in $\overline{F}$ è un automorfismo di K;*

(*v*) *K è autoconiugato su F.*

Proposizione 14.3 *Siano $F \subseteq K$ un ampliamento algebrico. Le seguenti proprietà sono equivalenti:*

(*i*) *L'ampliamento $F \subseteq K$ è normale e finito;*

(*ii*) *$K = F(\alpha_1, \ldots, \alpha_n)$ e K contiene i coniugati di α_i per $i = 1, \ldots, n$;*

(*iii*) *K è un campo di spezzamento su F di un polinomio $f(X) \in F[X]$.*

Dimostrazione: (*i*) $\Rightarrow$ (*ii*) Se K è un ampliamento finito di F, allora risulta $K = F(\alpha_1, \ldots, \alpha_n)$ per opportuni $\alpha_1, \ldots, \alpha_n \in K$ (Teorema 12.1). Se inoltre K è normale su F, per definizione esso contiene tutti gli elementi coniugati ad α_i, per $i = 1, \ldots, n$.

(*ii*) $\Rightarrow$ (*iii*) Sia $m_i(X)$ il polinomio minimo di α_i su F, per $i = 1, \ldots, n$. Poiché per ipotesi $m_i(X)$ ha tutte le sue radici in K, il polinomio $f(X) := m_1(X) \ldots m_n(X) \in F[X]$ si spezza linearmente su K. D'altra parte, essendo K generato su F da alcune radici di $f(X)$, allora K è il campo di spezzamento di $f(X)$ su F.

(*iii*) $\Rightarrow$ (*i*) Sia $K \subseteq \overline{F}$ il campo di spezzamento su F del polinomio $f(X) \in F[X]$. Allora $K = F(\alpha_1, \ldots, \alpha_n)$ con $f(\alpha_i) = 0$, $i = 1, \ldots, n$. E' chiaro che K è un ampliamento finito di F. Se φ è un F-isomorfismo di K in $\overline{F}$, risulta $\varphi(f(\alpha_i)) = f(\varphi(\alpha_i)) = 0$. Dunque $\varphi(\alpha_i) \in K$, per ogni i, e $\varphi(K) = F(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) \subseteq K$. Ne segue che K è normale su F.

Esempi

14.4. Se F è un campo finito, ogni suo ampliamento algebrico K è normale. Infatti, per ogni $\alpha \in K$, il campo $F(\alpha)$ è un campo di spezzamento del polinomio minimo di α su $\mathbb{F}_p$ (Proposizione 10.7). Ma allora $F(\alpha)$ è anche un campo di spezzamento del polinomio minimo di α su F.

14.5. Ogni ampliamento quadratico o biquadratico è normale. Infatti un polinomio di secondo grado che ha una radice in un campo K si spezza linearmente su K.

14.6. Ogni ampliamento ciclotomico è normale, essendo il campo di spezzamento di un polinomio (Proposizione 11.2).

14.7. Un campo di caratteristica zero può avere ampliamenti algebrici che non sono normali. Ad esempio, se $\alpha := \sqrt[3]{2}$, il campo $K := \mathbb{Q}(\alpha)$ non è un ampliamento normale di $\mathbb{Q}$. Infatti il polinomio minimo di α su $\mathbb{Q}$, che è il polinomio $m(X) := X^3 - 2$, non ha tutte le sue radici in $\mathbb{Q}(\alpha)$. Invece il

campo di spezzamento di $m(X)$ su $\mathbb{Q}$ è normale: esso è il campo $\mathbb{Q}(\sqrt[3]{2}, \xi)$, dove $\xi \in \mathbb{C}$ è una radice primitiva terza dell'unità (Esempio 7.8(b)).

Questo esempio mostra anche che un campo intermedio di un ampliamento normale non è necessariamente normale.

Proposizione 14.4 *Sia $F \subseteq K$ un ampliamento algebrico normale. Allora l'ampliamento $L \subseteq K$ è normale per ogni campo intermedio L.*

Dimostrazione: Sia $\alpha \in K$ con polinomio minimo $m(X)$ su F. Poiché $m(X)$ ha tutte le sue radici in K e il polinomio minimo di α su L divide $m(X)$, anche questo polinomio ha tutte le sue radici in K.

Mostriamo ora che, dato un ampliamento algebrico $F \subseteq K$, esiste un campo, univocamente determinato in $\overline{F}$, che è minimale rispetto alle proprietà di contenere K ed essere normale su F.

Proposizione 14.5 *Sia $F \subseteq K$ un ampliamento algebrico. Allora esiste un campo $N \subseteq \overline{F}$ contenente K tale che:*

(*a*) *L'ampliamento $F \subseteq N$ è normale;*

(*b*) *Se $M \subseteq \overline{F}$ è un ampliamento normale di F contenente K, allora $N \subseteq M$.*

Inoltre il campo N è unicamente determinato in $\overline{F}$ ed è generato su F dai campi coniugati di K.

Dimostrazione: Sia N il sottocampo di $\overline{F}$ generato dai campi coniugati a K su F. Se $L = \varphi(K) \subseteq N$ è uno di questi campi coniugati, con φ un F-isomorfismo di K in $\overline{F}$, e ψ è un F-isomorfismo di N in $\overline{F}$, allora $\psi(L) = \psi(\varphi(K)) = \psi\varphi(K)$ è un campo coniugato a K su F, perché $\psi\varphi : K \longrightarrow \overline{F}$ è un F-isomorfismo (Esercizio 9.1). Perciò $\psi(L)$ è contenuto in N. Ne segue che ogni F-isomorfismo ψ di N in $\overline{F}$ porta tutti i coniugati di K in N. Allora $\psi(N) \subseteq N$ e perciò N è normale su F.

Sia poi $M \subseteq \overline{F}$ un ampliamento normale di F contenente K. Se $\alpha \in K$, allora M deve contenere tutti i coniugati di α su F. Ne segue che M deve contenere tutti i coniugati di K e dunque deve contenere N.

Per finire, osserviamo che il campo N è unicamente determinato in $\overline{F}$ per la proprietà (*b*).

Con le notazioni della proposizione precedente, il campo N si chiama *la chiusura normale di K su F in $\overline{F}$*.

È evidente che K è normale su F se e soltanto se esso coincide con la sua chiusura normale in $\overline{F}$. Inoltre, per costruzione, se K è separabile su F, anche la sua chiusura normale in $\overline{F}$ lo è.

Esempi

14.8. Sia $F \subseteq F(\alpha)$ un ampliamento algebrico semplice e sia $m(X)$ il polinomio minimo di α su F. Se $\varphi_1, \ldots, \varphi_m$ sono gli F-isomorfismi di $F(\alpha)$ in $\overline{F}$, le radici distinte di $m(X)$ sono esattamente $\varphi_1(\alpha), \ldots, \varphi_m(\alpha)$ e la chiusura normale di $F(\alpha)$ in $\overline{F}$ è

$$N = \varphi_1(F(\alpha)) \ldots \varphi_m(F(\alpha)) = F(\varphi_1(\alpha), \ldots, \varphi_m(\alpha));$$

ovvero N è il campo di spezzamento in $\overline{F}$ del polinomio $m(X)$.

Ad esempio, la chiusura normale di $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{C}$ è il campo di spezzamento del polinomio $X^3 - 2$, cioè $\mathbb{Q}(\sqrt[3]{2}, \xi)$, dove $\xi \in \mathbb{C}$ è una radice primitiva terza dell'unità.

14.9. Se $K := F(\alpha_1, \ldots, \alpha_n)$ è finito su F e $\varphi_1, \ldots, \varphi_m$ sono gli F-isomorfismi di K in $\overline{F}$, allora N è il composto in $\overline{F}$ dei campi $\varphi_1(K), \ldots, \varphi_m(K)$ ed è generato su F da tutti i coniugati $\varphi_1(\alpha_i), \ldots, \varphi_m(\alpha_i)$ di α_i in $\overline{F}$, per $i = 1, \ldots n$.

Se $m_i(X)$ è il polinomio minimo di α_i su F, allora N è il campo di spezzamento in $\overline{F}$ del polinomio $f(X) := m_1(X) \ldots m_n(X)$ su F.

14.10. Un ampliamento $F \subseteq K$ finito e separabile è un ampliamento semplice (Corollario 13.9). In questo caso, come visto nel precedente Esempio 14.8, la sua chiusura normale in $\overline{F}$ è generata dai coniugati di un suo elemento primitivo.

ESERCIZI

14.1. Determinare i campi coniugati a $\mathbb{Q}(\sqrt[n]{2})$, $n \geq 2$, e la chiusura normale di $\mathbb{Q}(\sqrt[n]{2})$ in $\mathbb{C}$.

14.2. Sia $\alpha = \sqrt{3} + \sqrt[3]{2}$. Determinare i campi coniugati a $\mathbb{Q}(\alpha)$ e la chiusura normale di $\mathbb{Q}(\alpha)$ in $|C$.

14.3. Stabilire quali tra i seguenti ampliamenti di $\mathbb{Q}$ sono normali e, nei casi negativi, determinare la loro chiusura normale in $\mathbb{C}$:

$$\mathbb{Q}(\sqrt{3}, \sqrt{5});\ \mathbb{Q}(\sqrt{3}, \sqrt[3]{5});\ \mathbb{Q}(\sqrt{2} + i, \sqrt[3]{7});\ \mathbb{Q}(i\sqrt{3}, \sqrt[3]{5}).$$

14.4. Siano $p_1, \ldots, p_n$ numeri primi distinti e sia $K := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Mostrare che K è normale su $\mathbb{Q}$.

14.5. Verificare che il campo dei numeri complessi algebrici è la chiusura normale in $\mathbb{C}$ del campo dei numeri reali algebrici.

14.6. Dare un esempio di ampliamento normale non finito.

14.7. Dare un esempio di ampliamento normale non separabile.

14.8. Mostrare che la relazione di coniugio su F è una relazione di equivalenza sull'insieme dei sottocampi della chiusura algebrica $\overline{F}$ di F.

14.9. Dimostrare la Proposizione 14.2.

14.10. Mostrare che, se l'ampliamento $F \subseteq K$ è separabile, anche la chiusura normale di K su F è separabile.

14.11. Mostrare che ogni F-isomorfismo di $\overline{F}$ in $\overline{F}$ è suriettivo e dunque è un automorfismo.

15 Ampliamenti di Galois

Un ampliamento algebrico normale e separabile si chiama un *ampliamento di Galois*. Segue subito dalla definizione che un ampliamento algebrico $F \subseteq K$ è di Galois precisamente quando ogni polinomio irriducibile su F che ha una radice in K si spezza in fattori lineari distinti su K.

Se F è perfetto, in particolare se F ha caratteristica zero oppure è un campo finito, ogni suo ampliamento algebrico è separabile (Paragrafo 13). In questo caso gli ampliamenti di Galois di F coincidono con gli ampliamenti normali.

Esempi

15.1. Se F è un campo finito, ogni ampliamento algebrico $F \subseteq K$ è di Galois (Corollario 13.7 ed Esempio 14.4).

15.2. Se F è un campo di caratteristica diversa da 2, ogni ampliamento quadratico o biquadratico di F è separabile (Esempio 13.4) e normale (Esempio 14.5). Quindi è un ampliamento di Galois.

Il seguente teorema caratterizza gli ampliamenti di Galois finiti.

Teorema 15.1 *Sia $F \subseteq K$ un ampliamento finito di campi. Allora le seguenti condizioni sono equivalenti:*

(*i*) *L'ampliamento $F \subseteq K$ è di Galois (cioè è normale e separabile);*

(*ii*) *Il gruppo degli F-automorfismi di K ha ordine $[K : F]$;*

(*iii*) *$K = F(\alpha)$ è un ampliamento semplice e il polinomio minimo di α su F ha $[K : F]$ radici distinte in K;*

(*iv*) *K è il campo di spezzamento su F di un polinomio separabile $f(X) \in F[X]$;*

(*v*) *K è il campo di spezzamento su F di un polinomio $p(X) \in F[X]$ irriducibile e separabile su F.*

Dimostrazione: (*i*) $\Leftrightarrow$ (*ii*) Poiché K è finito su F, allora K è separabile su F se e soltanto se gli F-isomorfismi di K in una sua chiusura algebrica $\overline{F}$ sono esattamente $[K : F]$ (Teorema 13.13). Inoltre K è normale su F

se e soltanto se ogni tale F-isomorfismo è un F-automorfismo (Proposizione 14.2).

$(i) \Rightarrow (iii)$ Poiché K è un ampliamento finito e separabile di F, per il Teorema dell'Elemento Primitivo (Corollario 13.9), allora $K = F(\alpha)$, con α separabile su F. Se K è anche normale, tutte le radici del polinomio minimo di α su F (necessariamente tutte distinte) appartengono a K.

$(iii) \Rightarrow (v)$ Il polinomio minimo $m(X)$ di α su F è irriducibile e separabile su F. Poiché K contiene tutte le radici di $m(X)$ ed inoltre $[K : F] = \deg m(X)$, allora K è il campo di spezzamento di $m(X)$ su F.

$(v) \Rightarrow (iv)$ è evidente.

$(iv) \Rightarrow (i)$ Sia $K = F(\alpha_1, \ldots, \alpha_n)$ il campo di spezzamento di $f(X)$ su F, dove $\alpha_1, \ldots, \alpha_n$ sono le radici distinte di $f(X)$. Poiché $\alpha_1, \ldots, \alpha_n$ sono elementi separabili su F, allora K è separabile su F (Teorema 13.13). Inoltre K è normale su F per il Teorema 14.3.

Esempi

15.3. Se la caratteristica di F non divide n, l'n-simo ampliamento ciclotomico di F è un ampliamento di Galois (Paragrafo 11).

15.4. Un ampliamento di terzo grado $F \subseteq F(\alpha)$ è di Galois se e soltanto se il polinomio minimo di α su F ha tre radici distinte in $F(\alpha)$ (Esempio 7.8).

Proposizione 15.2 *Sia $F \subseteq K$ un ampliamento di Galois e L un suo campo intermedio. Allora l'ampliamento $L \subseteq K$ è di Galois.*

Dimostrazione: L'ampliamento $L \subseteq K$ è separabile per la Proposizione 13.17 e normale per la Proposizione 14.14.

Se $F \subseteq K$ è un ampliamento di Galois e L è un campo intermedio, l'ampliamento $F \subseteq L$ è separabile (Proposizione 13.17) ma può non essere normale (Esempio 14.7) e dunque può non essere di Galois. Il minimo ampliamento di Galois di F in K contenente L è la chiusura normale di L su F. In questo contesto, tale chiusura normale si dice anche la *chiusura di Galois di L in K*.

Se $F \subseteq K$ è un ampliamento di Galois, il gruppo degli F-automorfismi di K si chiama il *gruppo di Galois di K su F* e si indica con $\mathrm{Gal}_F(K)$.

Proposizione 15.3 *Siano $F \subseteq L \subseteq K$ ampliamenti algebrici. Se $F \subseteq K$ è un ampliamento di Galois, la chiusura normale di L su F in $\overline{F}$ è generata dai campi $\varphi(L)$, al variare di φ in $\mathrm{Gal}_F(K)$. In particolare essa è contenuta in K ed è il minimo ampliamento di Galois di F in K contenente L.*

Dimostrazione: Se l'ampliamento $F \subseteq K$ è di Galois, per normalità, gli F-isomorfismi di K in $\overline{F}$ sono esattamente gli F-automorfismi di K, ovvero

gli elementi di $\mathrm{Gal}_F(K)$. I campi coniugati a L su F sono allora tutti e soli i campi $\varphi(L)$, al variare di φ in $\mathrm{Gal}_F(K)$ (Proposizione 14.1), e la chiusura normale di L su F è il campo N generato dai campi $\varphi(L)$ (Proposizione 14.5). Poiché L è separabile su F (Proposizione 13.17), anche N è separabile su F. Perciò N è un ampliamento di Galois di F. Inoltre, ogni ampliamento di Galois di F in $\overline{F}$ contenente L, essendo normale, contiene N.

Corollario 15.4 *Sia $F \subseteq K$ un ampliamento di Galois. Se L è un campo intermedio, le seguenti proprietà sono equivalenti:*

(*i*) *L'ampliamento $F \subseteq L$ è di Galois;*

(*ii*) *L'ampliamento $F \subseteq L$ è normale;*

(*iii*) *$\varphi(L) \subseteq L$ per ogni $\varphi \in \mathrm{Gal}_F(K)$;*

(*iv*) *$\varphi(L) = L$ per ogni $\varphi \in \mathrm{Gal}_F(K)$.*

Dimostrazione: (*i*) $\Leftrightarrow$ (*ii*) Se l'ampliamento $F \subseteq K$ è di Galois, allora L è separabile su F (Proposizione 13.17). Perciò l'ampliamento $F \subseteq L$ è di Galois se e soltanto se è normale.

(*ii*) $\Leftrightarrow$ (*iv*) L è normale su F se e soltanto se è autoconiugato. Quindi possiamo concludere per il punto (b) della proposizione precedente.

(*iii*) $\Leftrightarrow$ (*iv*) segue dal fatto che $\mathrm{Gal}_F(K)$ è un gruppo.

Se $F \subseteq K$ è un ampliamento di Galois finito e L è un campo intermedio, l'ampliamento $F \subseteq L$, essendo finito e separabile, è semplice (Corollario 13.9). Se $L = F(\alpha)$, allora la chiusura di Galois di L su F è

$$N = \varphi_1(F(\alpha)) \dots \varphi_n(F(\alpha)) = F(\varphi_1(\alpha), \dots, \varphi_n(\alpha)),\ \varphi_i \in \mathrm{Gal}_F(K),$$

cioè N è il campo di spezzamento del polinomio minimo di α su F (Esempio 14.10).

ESERCIZI

15.1. Stabilire quali tra i seguenti campi sono ampliamenti di Galois di $\mathbb{Q}$:

$\mathbb{Q}(\sqrt{3})$; $\mathbb{Q}(\sqrt{2}, i)$; $\mathbb{Q}(\sqrt{3}, \sqrt{5})$; $\mathbb{Q}(\sqrt[5]{3})$; $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$; $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{5})$; $\mathbb{Q}(\sqrt{2}+i, \sqrt[3]{7})$.

15.2. Siano $p_1, \dots, p_n$ numeri primi distinti e sia $K := \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. Mostrare che l'ampliamento $\mathbb{Q} \subseteq K$ è di Galois.

15.3. Mostrare che, se F è un campo di caratteristica zero, ogni ampliamento finito di F è contenuto in un ampliamento di Galois.

16 Ampliamenti Puramente Trascendenti

Sia $F \subseteq K$ un ampliamento di campi e siano $\alpha_1, \ldots, \alpha_n \in K$. Allora, come nel Paragrafo 4, posto $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ possiamo considerare l'omomorfismo di anelli

$$v_{\boldsymbol{\alpha}} : F[\mathbf{X}] := F[X_1, \ldots, X_n] \longrightarrow K \text{ definito da } f(\mathbf{X}) \mapsto f(\boldsymbol{\alpha}).$$

Gli elementi $\alpha_1, \ldots, \alpha_n$ si dicono *algebricamente indipendenti su* F se $\mathrm{Ker}(v_{\boldsymbol{\alpha}}) = (0)$. Altrimenti essi si dicono *algebricamente dipendenti*. In altre parole, $\alpha_1, \ldots, \alpha_n$ sono algebricamente dipendenti su F se esiste un polinomio di grado positivo $f(X_1, \ldots, X_n) \in F[\mathbf{X}]$ tale che $f(\alpha_1, \ldots, \alpha_n) = 0$. In questo caso l'uguaglianza $f(\alpha_1, \ldots, \alpha_n) = 0$ si dice una *relazione algebrica su* $\alpha_1, \ldots, \alpha_n$ (a coefficienti in F). È chiaro dalla definizione che se n elementi di K sono algebricamente indipendenti su F, lo sono anche s elementi comunque scelti tra questi.

Un sottoinsieme S di K si dice *algebricamente indipendente su* F se ogni suo sottoinsieme finito è costituito da elementi algebricamente indipendenti su F.

Se $\alpha_1, \ldots, \alpha_n$ sono algebricamente indipendenti su F, essi non annullano in particolare nessun polinomio di primo grado a coefficienti non tutti nulli $c_1X_1 + \cdots + c_nX_n \in F[\mathbf{X}]$. Perciò $\alpha_1, \ldots, \alpha_n$ sono anche linearmente indipendenti su F. Tuttavia elementi linearmente indipendenti possono essere algebricamente dipendenti. Ad esempio $\sqrt{2}$ e $\sqrt{3}$ sono linearmente indipendenti su $\mathbb{Q}$, ma, se $f(X_1, X_2) := 3X_1^2 - 2X_2^2$, allora $f(\sqrt{2}, \sqrt{3}) = 0$. Dunque $\sqrt{2}$ e $\sqrt{3}$ sono algebricamente dipendenti su $\mathbb{Q}$.

Applicando la definizione al caso $n = 1$, si ha che α è algebricamente indipendente su F se e soltanto se esso è trascendente su F. Quindi elementi algebricamente indipendenti su F sono trascendenti. Tuttavia, se $\alpha_1, \ldots, \alpha_n$ sono trascendenti su F, essi possono essere algebricamente dipendenti. Ad esempio π e π^2 sono entrambi trascendenti su $\mathbb{Q}$, ma se $f(X_1, X_2) := X_1^2 - X_2$ risulta $f(\pi, \pi^2) = 0$. Dunque π e π^2 sono algebricamente dipendenti su $\mathbb{Q}$. Non è noto se i due numeri trascendenti π ed e siano algebricamente indipendenti su $\mathbb{Q}$.

Proposizione 16.1 *Sia $F \subseteq K$ un ampliamento di campi. Gli elementi $\alpha_1, \ldots, \alpha_n \in K$ sono algebricamente indipendenti su F se e soltanto se α_1 è trascendente su F e α_i è trascendente su $F(\alpha_1, \ldots, \alpha_{i-1})$ per $i = 2, \ldots, n$.*

Dimostrazione: Basta osservare che α_i è algebrico su $F(\alpha_1, \ldots, \alpha_{i-1})$ se e soltanto se esiste un polinomio di grado positivo $f(X) \in F(\alpha_1, \ldots, \alpha_{i-1})[X]$ annullato da α_i. Ma ciò equivale a dire che esiste un polinomio di grado positivo $f(X_1, \ldots, X_i) \in F[X_1, \ldots, X_i]$ tale che $f(\alpha_1, \ldots, \alpha_i) = 0$, ovvero che $\alpha_1, \ldots, \alpha_i$ sono algebricamente dipendenti su F.

Proposizione 16.2 *Sia $F \subseteq K$ un ampliamento di campi. Gli elementi $\alpha_1, \ldots, \alpha_n \in K$ sono algebricamente indipendenti su F se e soltanto se l'applicazione*

$$v'_{\boldsymbol{\alpha}} : F(X_1, \ldots, X_n) \longrightarrow F(\alpha_1, \ldots, \alpha_n), \quad \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \mapsto \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

è un F-isomorfismo.

Dimostrazione: Per definizione $\alpha_1, \ldots, \alpha_n$ sono algebricamente indipendenti su F se e soltanto se l'omomorfismo $v_{\boldsymbol{\alpha}} : F[\mathbf{X}] \longrightarrow K$ è iniettivo, ovvero se la sua immagine $F[\boldsymbol{\alpha}] := \{f(\boldsymbol{\alpha}); f(\mathbf{X}) \in F[\mathbf{X}]\}$ è un anello isomorfo a $F[\mathbf{X}]$. In questo caso $v_{\boldsymbol{\alpha}}$, si estende ad un F-isomorfismo $v'_{\boldsymbol{\alpha}} : F(X_1, \ldots, X_n) \longrightarrow F(\alpha_1, \ldots, \alpha_n)$ ponendo $v'_{\boldsymbol{\alpha}}(\frac{f(\mathbf{X})}{g(\mathbf{X})}) = \frac{f(\boldsymbol{\alpha})}{g(\boldsymbol{\alpha})}$ (Esercizio 3.5). Viceversa, se $v'_{\boldsymbol{\alpha}}$ è un isomorfismo, allora $\alpha_1, \ldots, \alpha_n$ non possono annullare nessun polinomio di grado positivo in $X_1, \ldots, X_n$. Altrimenti $\mathrm{Ker}(v'_{\boldsymbol{\alpha}}) \neq (0)$

Si dice che l'ampliamento $F \subseteq K$ è *puramente trascendente*, oppure che K è *puramente trascendente su* F, se $K = F(S)$ per qualche sottoinsieme S di K algebricamente indipendente su F. In particolare, un ampliamento finitamente generato $F(\alpha_1, \ldots, \alpha_n)$ è puramente trascendente se gli elementi $\alpha_1, \ldots, \alpha_n$ sono algebricamente indipendenti su F, ovvero se $F(\alpha_1, \ldots, \alpha_n)$ è isomorfo al campo delle funzioni razionali $F(X_1, \ldots, X_n)$ (Proposizione 16.2). Un ampliamento semplice $F(\alpha)$ di F o è algebrico oppure è puramente trascendente su F e questa seconda eventualità si verifica esattamente quando α è trascendente su F. In quest'ultimo caso si usa semplicemente dire che $F(\alpha)$ è un *ampliamento (semplice) trascendente di* F.

Questa terminologia è giustificata dal fatto che, se $K := F(S)$ è puramente trascendente su F, allora ogni $\beta \in K \setminus F$ è trascendente su F. Infatti, scriviamo $\beta = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$ con $\alpha_i \in S$ e $g(\mathbf{X}) \neq 0$; se esistessero degli elementi non tutti nulli $c_0, c_1, \ldots, c_n \in F$ tali che $c_0 + c_1\beta + \cdots + c_n\beta^n = 0$, eliminando i denominatori, si otterrebbe una relazione algebrica su $\alpha_1, \ldots, \alpha_n$.

Dato un ampliamento di campi $F \subseteq K$, un sottoinsieme S di K si dice una *base di trascendenza di K su F* se l'ampliamento $F(S)$ è puramente trascendente ed inoltre K è algebrico su $F(S)$. In particolare, se $K = F(S)$ è un ampliamento puramente trascendente, allora S è una base di trascendenza di K su F.

Se K non è algebrico su F, l'esistenza di una base di trascendenza di K su F è garantita dal Lemma di Zorn. Infatti, l'insieme di tutti i sottoinsiemi di K algebricamente indipendenti su F è parzialmente ordinato per inclusione ed ogni catena di questo insieme ammette un maggiorante, dato dall'unione degli insiemi della catena. Dunque esiste un sottoinsieme S di K massimale rispetto alla proprietà di essere algebricamente indipendente su F e questo è una base di trascendenza di K su F, perché K è algebrico su $F(S)$.

Esempi

16.1. Ogni estensione semplice propria di un campo algebricamente chiuso è puramente trascendente.

16.2. L'insieme $\mathbf{X} := \{X_i\}_{i\in I}$ è una base di trascendenza del campo delle funzioni razionali $F(\mathbf{X})$ su F.

16.3. Se $K := \mathbb{Q}(e, \sqrt{3})$, allora K è algebrico su $\mathbb{Q}(e)$ ed e è trascendente su $\mathbb{Q}$. Perciò una base di trascendenza di K su $\mathbb{Q}$ è $\{e\}$.

16.4. I numeri π e $\sqrt{\pi+2}$ sono algebricamente dipendenti su $\mathbb{Q}$, perché $\pi - (\sqrt{\pi+2})^2 + 2 = 0$. Inoltre

$$\mathbb{Q} \subsetneq \mathbb{Q}(\pi) \subsetneq \mathbb{Q}(\pi, \sqrt{\pi+2}) = \mathbb{Q}(\sqrt{\pi+2})$$

e $\mathbb{Q}(\sqrt{\pi+2})$ è algebrico su $\mathbb{Q}(\pi)$. Sia

$$K := \mathbb{Q}(\pi, \sqrt{\pi+2}, \sqrt{2}) = \mathbb{Q}(\sqrt{\pi+2}), \sqrt{2}).$$

Poiché $\sqrt{2}$ è algebrico su $\mathbb{Q}(\sqrt{\pi+2})$ (perché lo è su $\mathbb{Q}$), si ha che K è algebrico sia su $\mathbb{Q}(\pi)$ che su $\mathbb{Q}(\sqrt{\pi+2})$. D'altra parte, sia π che $\sqrt{\pi+2}$ sono trascendenti, perciò sia $\{\pi\}$ che $\{\sqrt{\pi+2}\}$ sono basi di trascendenza di K su $\mathbb{Q}$.

Il seguente teorema ha un ben noto analogo per l'indipendenza lineare.

Teorema 16.3 (E. Steinitz, 1910) *Sia $F \subseteq K$ un ampliamento di campi e supponiamo che K abbia una base di trascendenza finita $\{\beta_1, \ldots, \beta_n\}$ su F. Se $\alpha_1, \ldots, \alpha_m \in K$ sono algebricamente indipendenti su F, allora $m \leq n$ e si può completare l'insieme $\{\alpha_1, \ldots, \alpha_m\}$ ad una base di trascendenza di K su F aggiungendo al più $n - m$ elementi di $\{\beta_1, \ldots, \beta_n\}$. In particolare, il numero degli elementi di una base di trascendenza di K su F è il massimo numero di elementi di K algebricamente indipendenti su F.*

Dimostrazione: Se $\{\beta_1, \ldots, \beta_n\}$ è una base di trascendenza di K su F, allora α_1 è algebrico su $L := F(\beta_1, \ldots, \beta_n)$. Quindi esiste un polinomio a coefficienti non tutti nulli $f(X) := c_0 + c_1X + \cdots + c_sX^s \in L[X]$ tale che $f(\alpha_1) = 0$. Questa è una relazione algebrica tra α_1 e gli elementi di $\{\beta_1, \ldots, \beta_n\}$ che compaiono nei coefficienti di $f(X)$ (che non sono tutti in F perché α_1 è trascendente su F). Allora α_1 è algebrico su $L' := F(\alpha_1, \beta_2, \ldots, \beta_n)$. Consideriamo la catena di campi $L' \subseteq L'(\beta_1) = L(\alpha_1) \subseteq K$. Poiché $L'(\beta_1)$ è algebrico su L' e K è algebrico su $L(\alpha_1)$ (perché lo è su L), allora K è algebrico su $L' := F(\alpha_1, \beta_2, \ldots, \beta_n)$ (Proposizione 12.15). Se $m \leq n$, così proseguendo si ottiene che K è algebrico su $F(\alpha_1, \ldots, \alpha_m, \beta_{m+1}, \ldots, \beta_n)$. D'altra parte, non può essere $m > n$, altrimenti α_{n+1} sarebbe algebrico su $F(\alpha_1, \ldots, \alpha_n)$, in contraddizione col fatto che $\alpha_1, \ldots, \alpha_m$ sono algebricamente indipendenti su F (Proposizione 16.1).

Corollario 16.4 *Sia $F \subseteq K$ un ampliamento di campi. Allora, se esiste una base di trascendenza finita di K su F, due basi di trascendenza hanno lo stesso numero di elementi.*

Il corollario precedente ci permette di definire il *grado di trascendenza* di una estensione di campi $F \subseteq K$ nel seguente modo:

- Se K è algebrico su F, il suo grado di trascendenza su F è zero;
- Se K ha una base di trascendenza finita su F, il suo grado di trascendenza su F è il numero degli elementi di tale base (ovvero il massimo numero di elementi di K algebricamente indipendenti su F);
- Se K ha una base di trascendenza infinita su F, il suo grado di trascendenza su F è infinito.

Anche nel caso infinito si può dimostrare che due basi di trascendenza hanno la stessa cardinalità. Quindi in ogni caso si può definire il grado di trascendenza di un ampliamento $F \subseteq K$ come la cardinalità di una (qualsiasi) base di trascendenza di K su F.

Notiamo anche che, se S è una base di trascendenza di K su F, allora K e $F(S)$ hanno la stessa cardinalità, perché K è algebrico su $F(S)$ (Paragrafo 12).

Se $F \subseteq K$ indichiamo con $\mathrm{trdeg}_F(K)$ il grado di trascendenza di K su F. Dalla Proposizione 16.2 segue immediatamente che, se $F \subseteq K$ è un ampliamento puramente trascendente, allora $\mathrm{trdeg}_F(K) = n$ se e soltanto se K è F-isomorfo a $F(X_1, \ldots, X_n)$.

Esempi

16.5. Il grado di trascendenza di $F(X)$ su F è uguale a uno. Quindi due qualsiasi funzioni razionali distinte sono algebricamente dipendenti su F.

16.6. Se $K := F(\alpha)$ è un qualsiasi ampliamento semplice di F e $\beta \in F(\alpha) \setminus F$, allora K è algebrico su $F(\beta)$. Infatti, se α è algebrico su F, questo è chiaro. Se α non è algebrico su F, allora K è un ampliamento puramente trascendente di F. Quindi β è trascendente su F. Poiché il grado di trascendenza di K su F è uguale a uno, allora K è algebrico su $F(\beta)$.

16.7. Se K è il campo delle funzioni razionali sul campo F nelle infinite indeterminate $\{X_\lambda\}_{\lambda \in \Lambda}$, allora K ha grado di trascendenza infinito su F, uguale alla cardinalità di Λ.

Siamo ora in grado di classificare gli ampliamenti finitamente generati di un campo F.

Teorema 16.5 *Sia $K := F(\alpha_1, \ldots, \alpha_n)$ un ampliamento finitamente generato del campo F. Allora si possono presentare due sole possibilità:*

(a) *K è algebrico, ovvero finito su F.*

(b) *Per un opportuno $r \leq n$, il campo $L := F(\alpha_{i_1}, \ldots, \alpha_{i_r})$ è un ampliamento puramente trascendente di F e K è algebrico su L.*

Dimostrazione: K è algebrico su F se e soltanto se esso è finito su F (Teorema 12.1). Supponiamo che $K := F(\alpha_1, \ldots, \alpha_n)$ non sia algebrico su F. Allora, sempre per il Teorema 12.1, almeno uno degli α_i è trascendente su F. A meno dell'ordine possiamo supporre che tale elemento sia α_1. Se K non è algebrico su $F(\alpha_1)$, possiamo allora supporre che α_2 sia trascendente su $F(\alpha_1)$. Iterando questo procedimento, otteniamo che, per un opportuno $r \leq n$, gli elementi $\alpha_1, \ldots, \alpha_r$ sono algebricamente indipendenti su F (Proposizione 16.1) e K è algebrico su $F(\alpha_1, \ldots, \alpha_r)$.

Il teorema precedente dimostra in particolare che, se K è finitamente generato e non algebrico su F, allora una base di trascendenza di K su F esiste. Inoltre gli elementi di una tale base possono essere scelti tra i generatori di K su F.

Corollario 16.6 *Siano $F \subseteq L \subseteq K$ ampliamenti di campi finitamente generati. Se K è algebrico su L, allora K e L hanno lo stesso grado di trascendenza su F.*

Terminiamo questo paragrafo dimostrando che ogni campo intermedio di un ampliamento trascendente semplice è ancora un ampliamento trascendente semplice. Questo risultato è di particolare importanza nello studio delle curve algebriche.

Lemma 16.7 *Sia X una indeterminata sul campo F e sia $K := F(X)$. Se $\theta := \frac{g(X)}{h(X)} \in K \setminus F$, con $\mathrm{MCD}(g(X), h(X)) = 1$, allora X è algebrico su $F(\theta)$ e il suo grado su $F(\theta)$ è uguale al massimo tra i gradi di $g(X)$ e $h(X)$.*

Dimostrazione: Il polinomio $m(Z) := g(Z) - \theta h(Z) \in (F[\theta])[Z]$ è annullato da X ed ha grado $m := \max\{\deg(g(Z), \deg(h(Z)\}$ in Z. Mostriamo che $m(Z)$ è un polinomio minimo di X su $F(\theta)$ facendo vedere che esso è irriducibile su $F(\theta)$. Poiché θ è trascendente su F, esso si comporta come una indeterminata su F. Poiché inoltre $m(Z) \in (F[\theta])[Z]$ ed è primitivo su $F[\theta]$ (cioè i suoi coefficienti non hanno fattori comuni in $F[\theta]$), per il Lemma di Gauss, $m(Z)$ è irriducibile su $F(\theta)$ se soltanto se lo è su $F[\theta]$. Sia $f(\theta, Z) \in (F[\theta])[Z]$ un divisore di $m(Z)$ di grado positivo in Z. Allora $m(\theta, Z) = f(\theta, Z)q(\theta, Z)$ con $q(\theta, Z) \in (F[\theta])[Z] = F[Z, \theta]$. Leggiamo questa uguaglianza in $(F[Z])[\theta]$. Poiché $m(\theta, Z)$ è di primo grado in θ e i suoi

coefficienti sono coprimi in $F[Z]$, esso è irriducibile in $(F[Z])[\theta]$. Dunque uno dei suoi fattori è una costante invertibile di $F[Z]$ e perciò appartiene a F. Poiché $f(\theta, Z)$ ha grado positivo in Z, allora $q(\theta, Z) = q \in F$. Ne segue che $m(\theta, Z)$ e $f(\theta, Z)$ sono associati in $(F[\theta])[Z]$ e perciò $m(Z)$ è irriducibile su $F[\theta]$.

Teorema 16.8 (J. Lüroth) *Sia X una indeterminata sul campo F e sia $K := F(X)$. Se L è un campo tale che $F \subseteq L \subseteq K$, allora esiste un elemento (trascendente) $\theta \in K$ tale che $L = F(\theta)$.*

Dimostrazione: Se $\beta \in L \setminus F$, K è algebrico su $F(\beta)$ per il Lemma 16.7. Poiché $F(\beta) \subseteq L$, allora K è algebrico su L (Proposition 12.15). Sia $m(Z) := c_0 + c_1 Z + \cdots + Z^n \in L[Z]$ il polinomio minimo di X su L. Se $c_i \neq 0$, si ha $c_i = \frac{g_i(X)}{h_i(X)}$, con $g_i(X), h_i(X) \in F[X]$ non nulli e $\mathrm{MCD}(g_i(X), h_i(X)) = 1$. Inoltre, poiché X è trascendente su F, almeno uno dei coefficienti di $m(Z)$ non appartiene a F. Sia un tale coefficiente $\theta := \frac{g(X)}{h(X)}$. Vogliamo mostrare che $L = F(\theta)$.

Moltiplicando $m(Z)$ per il minimo comune denominatore dei coefficienti, si ottiene un polinomio $f(X, Z) \in (F[X])[Z]$ che è primitivo su $F[X]$ (cioè i cui coefficienti non hanno fattori comuni in $F[X]$). Consideriamo il polinomio $p(Z) := g(Z) - \theta h(Z) \in F(\theta)[Z] \subseteq F(X)[Z]$. Questo è un polinomio minimo di X su $F(\theta)$ (Dimostrazione del Lemma 16.7); dunque esso è diviso da $m(Z)$ in $F(\theta)[Z]$ e perciò anche in $F(X)[Z]$. Allora il polinomio $k(X, Z) := h(X)g(Z) - g(X)h(Z)$ è diviso da $f(X, Z)$ in $F(X)[Z]$. Poiché $f(X, Z)$ è primitivo su $F[X]$, per il Lemma di Gauss, si ha $k(X, Z) = f(X, Z)q(X, Z)$, dove $q(X, Z) \in F[X, Z]$.

Il polinomio $k(X, Z)$ è simmetrico in X, Z; quindi esso ha stesso grado m sia rispetto a X che a Z. Tale grado è il grado di $p(Z)$ e perciò $m = \max\{\deg(g(X), \deg(h(X)\}$. Ora m è al più uguale al grado di $f(X, Z)$ in X, perché $h(X)$ divide $f(X, Z)$ e $g(X)$ divide un suo termine in $F[X, Z]$. Ma poiché $f(X, Z)$ divide $k(X, Z)$, i gradi di $k(X, Z)$ e $f(X, Z)$ rispetto a X devono risultare uguali. Ma allora $q(X, Z) = q(Z) \in F[Z]$. Inoltre $q(Z)$ è addirittura una costante di F, infatti, essendo $\mathrm{MCD}(g(X), h(X)) = 1$, $k(X, Z)$ è primitivo su $F[Z]$. Ne segue che $k(X, Z)$ e $f(X, Z)$ hanno entrambi stesso grado $m = n$, sia rispetto a X che a Z. Per la proprietà moltiplicativa del grado di un ampliamento, si ha $[F(X) : L][L : F(\theta)] = [F(X) : F(\theta)]$. Ma $[F(X) : L] = n = m = [F(X) : F(\theta)]$, dunque $L = F(\theta)$.

Il Teorema di Lüroth non si può estendere al caso di 2 o più indeterminate. Infatti in generale non è vero che se $F \subsetneq L \subseteq F(X_1, \ldots, X_n)$, $n \geq 2$, allora L è un ampliamento puramente trascendente di F.

ESERCIZI

16.1. Se $\alpha := \frac{f(X)}{g(X)} \in F(X)$ con $\mathrm{MCD}(f(X), g(X)) = 1$, definiamo il grado di α come il massimo tra i gradi di $f(X)$ e $g(X)$. Mostrare che, se α ha grado $m \geq 1$, allora ogni elemento di $F(X)$ si può scrivere come un polinomio di $F(\alpha)[X]$ di grado al più uguale a m.

16.2. Sia $\alpha \in F(X)$. Mostrare che $F(\alpha) = F(X)$ se e soltanto se $\alpha = \frac{a+bX}{c+dX}$, con a, b, c, $d \in F$ e $ad - bc \neq 0$.

16.3. Sia F un campo. Mostrare che, se $F(\alpha_1, \ldots, \alpha_n) = F(X_1, \ldots, X_n)$, gli elementi $\alpha_1, \ldots, \alpha_n$ sono algebricamente indipendenti su F.

16.4. Determinare una base di trascendenza di $\mathbb{C}(X, X + \frac{1}{X})$ su $\mathbb{C}$, dove X è una indeterminata su $\mathbb{C}$.

16.5. Mostrare che, se F ha caratteristica zero, ogni ampliamento finitamente generato di F è un ampliamento algebrico semplice di F oppure di un ampliamento puramente trascendente di F.

16.6. Mostrare che un ampliamento di campi $F \subseteq K$ che ha grado di trascendenza almeno uguale a 2 non può essere semplice.

16.7. Siano $F \subseteq L \subseteq K$ ampliamenti di campi. Mostrare che, se $\mathrm{trdeg}_F(K)$ è finito, allora $\mathrm{trdeg}_F(K) = \mathrm{trdeg}_L(K) + \mathrm{trdeg}_F(L)$.

16.8. Mostrare che due ampliamenti puramente trascendenti di F sono isomorfi se e soltanto se hanno lo stesso grado di trascendenza su F.

16.9. Sia $F(S)$ un ampliamento puramente trascendente di F. Mostrare che ogni automorfismo φ di F si può estendere a un automorfismo ψ di $F(S)$ ponendo $\psi(a) = \varphi(a)$ per ogni $a \in F$ e $\psi(s) = s$ per ogni $s \in S$ (*Suggerimento.* Generalizzare il Lemma 9.1(a) e usare l' Esercizio 4.8).

16.10. Sia $F(S)$ un ampliamento puramente trascendente di F. Mostrare che ogni applicazione biunivoca $\beta : S \longrightarrow S$, si può estendere in modo unico a un automorfismo ψ di $F(S)$ ponendo $\psi(a) = a$ per ogni $a \in F$ e $\psi(s) = \beta(s)$ per ogni $s \in S$ (*Suggerimento.* Usare l'Esercizio 4.8).

16.11. Sia $F(S)$ un ampliamento puramente trascendente di F. Mostrare che $F(S)$ è isomorfo al campo delle funzioni razionali $F(\mathbf{X})$, dove $\mathbf{X} = \{X_s\}_{s \in S}$ è un insieme di indeterminate algebricamente indipendenti su F. (*Suggerimento.* Usare l'Esercizio 4.8 e la Proposizione 16.2).

17 Gli Automorfismi del Campo Complesso

Siano S una base di trascendenza di $\mathbb{C}$ su $\mathbb{Q}$ (Paragrafo 16) e $\mathbf{X} := \{X_s; s \in S\}$ un insieme di indeterminate algebricamenti indipendenti su $\mathbb{Q}$. Se

$$\mathbb{Q}(S) := \left\{ \frac{f(S)}{g(S)}; f(\mathbf{X}), g(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}], g(\mathbf{X}) \neq 0 \right\},$$

per ogni applicazione biunivoca $\eta : S \longrightarrow S$, l'applicazione

$$\varphi_\eta : \mathbb{Q}(S) \longrightarrow \mathbb{Q}(S) \, , \frac{f(s_1, \ldots, s_n)}{g(t_1, \ldots, t_m)} \mapsto \frac{f(\eta(s_1), \ldots, \eta(s_n))}{g(\eta(t_1), \ldots, \eta(t_m))}$$

è ben posta ed è un automorfismo di $\mathbb{Q}(S)$ (Esercizio 16.11).

Proposizione 17.1 *Se S è una base di trascendenza di $\mathbb{C}$ su $\mathbb{Q}$, ogni applicazione biunivoca di S si estende a un automorfismo di $\mathbb{C}$.*

Dimostrazione: Come abbiamo appena visto, ogni applicazione biunivoca di S in sé si estende ad un automorfismo di $\mathbb{Q}(S)$. Poiché $\mathbb{C}$ è algebrico su $\mathbb{Q}(S)$, per la Proposizione 12.13, ogni tale automorfismo si estende ad un automorfismo di $\mathbb{C}$.

Vogliamo ora dimostrare che il gruppo degli automorfismi di $\mathbb{C}$ ha la cardinalità dell'insieme delle parti di $\mathbb{C}$. Notiamo però che gli unici automorfismi continui di $\mathbb{C}$ sono l'identità il coniugio, perché l'identità è l'unico automorfismo di $\mathbb{R}$ (Esempio 3.5).

Cominciamo con l'osservare che ogni base di trascendenza S di $\mathbb{C}$ su $\mathbb{Q}$ ha la cardinalità del continuo. Infatti $\mathbb{C}$ ha la cardinalità del continuo ed è algebrico su $\mathbb{Q}(S)$. Quindi anche $\mathbb{Q}(S)$ ha la cardinalità del continuo, come visto nell'Esempio 12. 12. Poiché $\mathbb{Q}$ è numerabile, S deve avere la cardinalità del continuo.

Lemma 17.2 *Sia S un insieme che ha la cardinalità del continuo $\mathfrak{c}$. Allora l'insieme delle corrispondenze biunivoche di S in se stesso ha cardinalità $2^{\mathfrak{c}}$.*

Dimostrazione: Basta far vedere che le corrispondenze biunivoche di $\mathbb{R}$ in $\mathbb{R}$ sono $2^{\mathfrak{c}}$. Cominciamo con l'osservare che ogni corrispondenza di $\mathbb{R}$ in $\mathbb{R}$ è determinata in modo univoco dal suo grafo, ovvero da un sottoinsieme di $\mathbb{R} \times \mathbb{R}$. Poiché l'insieme $\mathbb{R} \times \mathbb{R}$ ha la cardinalità del continuo, l'insieme di tutti i grafi, ovvero di tutte le corrispondenze di $\mathbb{R}$ in $\mathbb{R}$, sono $2^{\mathfrak{c}}$. Ne segue che le corrispondenze biunivoche di $\mathbb{R}$ in $\mathbb{R}$ sono al più $2^{\mathfrak{c}}$.

Mostriamo ora che tali corrispondenze sono almeno $2^{\mathfrak{c}}$. Per ogni sottoinsieme A dell'intervallo aperto $I := (0, 1)$ consideriamo il sottoinsieme $B_A := A \cup (-\infty, 0]$ di $\mathbb{R}$ ed il suo complementare $C_A := \mathbb{R} \setminus B_A$. Entrambi questi insiemi hanno cardinalità $\mathfrak{c}$, dunque esistono una corrispondenza biunivoca tra B_A e la semiretta $(-\infty, 0]$ ed una corrispondenza biunivoca tra C_A e la semiretta aperta $(0, -\infty)$. Incollando queste due corrispondenze biunivoche, si ottiene per ogni A una corrispondenza biunivoca di $\mathbb{R}$ in $\mathbb{R}$. Poiché l'intervallo $I := (0, 1)$ ha ancora la cardinalità del continuo, l'insieme dei suoi sottoinsiemi A ha cardinalità $2^{\mathfrak{c}}$. Dunque in questo modo si ottengono $2^{\mathfrak{c}}$ corrispondenze biunivoche di $\mathbb{R}$ in $\mathbb{R}$.

Proposizione 17.3 *Il gruppo degli automorfismi di $\mathbb{C}$ ha cardinalità $2^{\mathfrak{c}}$.*

Dimostrazione: Sia S una base di trascendenza di $\mathbb{C}$ su $\mathbb{Q}$. Poiché S ha la cardinalità del continuo ed ogni corrispondenza biunivoca di S in sé induce un automorfismo di $\mathbb{C}$ (Proposizione 17.1), allora gli automorfismi di $\mathbb{C}$ sono

almeno $2^{\mathfrak{c}}$ per il Lemma 17.3. D'altra parte, poiché anche $\mathbb{C}$ ha la cardinalità del continuo, tali automorfismi, essendo corrispondenze biunivoche, sono al più $2^{\mathfrak{c}}$ per lo stesso lemma.

ESERCIZI

17.1. Mostrare che gli unici automorfismi continui di $\mathbb{C}$ sono l'identità e il coniugio. (*Suggerimento*: Notare che, poiché $\mathbb{Q}$ è denso in $\mathbb{R}$, ogni automorfismo continuo di $\mathbb{C}$ deve essere l'identità su $\mathbb{R}$.)

17.2. Mostrare che esistono infiniti isomorfismi di $\mathbb{R}$ in $\mathbb{C}$. (*Suggerimento*: Sia S una base di trascendenza di $\mathbb{R}$ su $\mathbb{Q}$. Osservare che una corrispondenza biunivoca di S in sé induce un isomorfismo di $\mathbb{Q}(S)$ in $\mathbb{C}$ ed usare il Teorema 12.11.)

17.3. Mostrare che $\mathbb{C}$ ha infiniti automorfismi che scambiano i e $-i$ (*Suggerimento*: Usare l'esercizio precedente e la Proposizione 9.2.)

17.4. Sia φ un automorfismo di $\mathbb{C}$. Mostrare che la restrizione di φ ad ogni ampliamento ciclotomico di $\mathbb{Q}$ è un automorfismo. Tuttavia non è vero che, se $\alpha \in \mathbb{C}$ ha modulo uguale a 1, allora $\varphi(\alpha)$ ha necessariamente modulo uguale a 1 (*Suggerimento*: Ricordare che esistono numeri trascendenti di modulo uguale a 1 (Esercizio 5.6).)

17.5. Mostrare che ogni automorfismo di $\mathbb{C}$ è l'identità su uno dei seguenti campi: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$. (*Suggerimento*: Notare che ogni automorfismo di $\mathbb{C}$ è un automorfismo dell'ottavo ampliamento ciclotomico.)