VI - TEORIA DEI CAMPI

1 Estensioni di campi

Siano F, E campi. E si dice *estensione* di F (e si scrive $E|F$) se esiste un omomorfismo iniettivo di campi (detto immersione):

$$\phi \ : \ F \ \longrightarrow \ E.$$

In tal caso, l'immagine $\phi(F)$ è un sottocampo di E *isomorfo* ad F. Risulta allora spesso più agevole pensare di identificare ogni elemento a di F con la sua immagine $\phi(a)$, e di vedere quindi F "contenuto" in E come suo sottocampo.

Esempi fondamentali di estensioni di campi sono $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{R}$ e $\mathbb{C}|\mathbb{Q}$ (con le immersioni naturali - ovvero la restrizione dell'identità).
Un altro esempio che è utile tener presente è il seguente. Se F è un campo, allora l'anello dei polinomi $F[x]$ è un dominio d'integrità. Denotiamo con $F(x)$ il campo delle frazioni di $F[x]$. Quindi

$$F(x) = \left\{ \ \frac{f}{g} \ | \ f, g \in F[x], \ g \neq 0 \ \right\}$$

si chiama *campo delle frazioni algebriche* su F. Allora $F(x)|F$ è un'estensione di campi (l'immersione è quella che associa ad ogni elemento a di F il polinomio "costante" a).

Ancora, sia F un campo, e I un ideale massimale di $F[x]$; allora $E = F[x]/I$ è un campo, e $E|F$ è una estensione mediante l'omomorfismo (definito da F in E)

$$a \ \mapsto \ a + I.$$

(Ricordo che se $I \neq \{0\}$ è un ideale di $F[x]$ (con F un campo) allora, per quanto visto in precedenza, I è principale e $I = (f)$, dove f è un polinomio di grado minimo tra i polinomi non nulli contenuti in I. Inoltre I è massimale se e soltanto se f è irriducibile in $F[x]$.)

Inffine, osserviamo che se $E|F$ e $L|E$ sono estensioni di campi ottenute mediante, rispettivamente, gli omomorfismi ϕ e ψ, allora $L|F$ è un'estensione, ottenibile mediante l'omomorfismo composto $\psi \circ \phi$.

Grado di una estensione.

Sia F un sottocampo del campo E (o più in generale, sia $E|F$ un'estensione di campi). Allora è possibile vedere in modo naturale E come uno spazio vettoriale su F (ovvero su $\phi(F)$): i vettori sono gli elementi di E, gli scalari quelli di F e il prodotto di un vettore per uno scalare è effettuato mediante la moltiplicazione dei due elementi nel campo E. Si verifica facilmente che tutti gli assiomi di spazio vettoriale sono soddisfatti.

Definizione. Sia $E|F$ un'estensione di campi. La *dimensione* di E come spazio vettoriale su F si chiama **grado** di E su F, e si denota con $[E : F]$.

Ad esempio, ogni numero complesso si scrive in modo unico nella forma $a + ib = a1 + bi$ con $a, b \in \mathbb{R}$, cioè come combinazione lineare (a coefficienti nel campo degli scalari $\mathbb{R}$) di 1 e i (visti come vettori). Quindi $\{1, i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$ e dunque $[\mathbb{C} : \mathbb{R}] = 2$ (mentre $[\mathbb{R} : \mathbb{Q}] = \infty$, come sarà chiaro più avanti).
Osserviamo anche che $[E : F] = 1$ se e solo se $E = F$.

Questo semplice punto di vista è di fatto molto utile. Ecco una prima applicazione.

Proposizione 1.1 *Sia L un campo finito. Allora $|L| = p^n$ con p un numero primo e $1 \leq n \in \mathbb{N}$.*

Dimostrazione. Poichè L è un campo ed è finito la sua caratteristica deve essere un numero primo p (Proposizione 7.2 Cap. IV). Quindi, se F è il suo sottoanello fondamentale, allora $F \simeq \mathbb{Z}_p$ è un campo, e possiamo vedere L come estensione di F. Sia $[L : F] = n$ il grado di questa estensione. Allora L è uno spazio vettoriale su F di dimensione n; quindi, *come spazio vettoriale*, L è isomorfo allo spazio $F^{(n)}$ delle n-uple a coefficienti in F. In particolare, $|L| = |F^{(n)}| = |F|^n = p^n$. ■

Dimostreremo più avanti che per ogni primo p ed ogni $n \geq 1$ esiste un campo di ordine p^n, e che due campi finiti dello stesso ordine sono isomorfi.

Ricordiamo (Proposizione 8.2, Cap. IV) che se F è un campo, e $I = (f)$ un ideale massimale dell'anello dei polinomi $F[x]$ con $n = \deg f$, allora ogni elemento del campo $E_f = F[x]/I$ si scrive in modo unico nella forma

$$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + I = a_0 \cdot 1 + a_1 \cdot (x + I) + \ldots + a_{n-1} \cdot (x^{n-1} + I)$$

con $a_0, a_1, \ldots, a_{n-1} \in F$. Ne segue che l'insieme di elementi di E_f:

$$1,\ x + I,\ x^2 + I, \ldots, x^{n-1} + I$$

è una base di E_f come spazio vettoriale su F, e quindi $[E_f : F] = n = \deg f$.

Vediamo ora un importante strumento per lo studio dei gradi di un'estensione.

Teorema 1.2 (Formula dei Gradi) *Siano F, L, M campi con $F \leq L \leq M$. Allora $[M : F] = [M : L][L : F]$.*

Dimostrazione. Il fatto è ovvio se $[M : L] = \infty$ oppure $[L : F] = \infty$ (qui, adottiamo la convenzione $\infty \cdot n = \infty \cdot \infty = \infty$). Quindi assumiamo che $[M : L] = n,\ [L : F] = m$ siano entrambi finiti.
Sia $a_1, a_2, \ldots, a_n$ una base di M su L, e sia $b_1, b_2, \ldots, b_m$ una base di L su F. Proviamo che gli elementi $b_j a_i$ $(1 \leq j \leq m,\ 1 \leq i \leq n)$ costituiscono una base di M su F.
(generazione). Sia $u \in M$, allora esistono $x_1, x_2, \ldots, x_n$ in L tali che

$$u = x_1 a_1 + x_1 a_2 + \ldots + x_n a_n = \sum_{i=1}^{n} x_i a_i \ .$$

Ora ogni $x_i \in L$ è a sua volta una combinazione a coefficienti in F della base (b_j):

$$x_i = y_{1i} b_1 + y_{2i} b_2 + \ \ldots \ + y_{mi} b_m = \sum_{j=1}^{m} y_{ji} b_j \ .$$

Quindi

$$u = \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i)$$

quindi ogni $u \in M$ è combinazione a coefficienti in F degli elementi $b_j a_i$.
(indipendenza). Proviamo ora che il sistema $(b_j a_i)$ è linearmente indipendente. Sia $I = \{1, \ldots, m\} \times \{1, \ldots, n\}$ e siano, per $(j, i) \in I$, $y_{ji} \in F$ tali che

$$\sum_{(j,i) \in I} y_{ji} b_j a_i = 0 \ .$$

Allora

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{ji} b_j a_i) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} y_{ji} b_j \right) a_i$$

dove, per ogni $1 \leq i \leq n$, $\sum_{j=1}^{m} y_{ji} b_j \in L$. Poichè gli elementi a_i sono linearmente indipendenti su L, si ha, per ogni $1 \leq i \leq n$,

$$\sum_{j=1}^{m} y_{ji} b_j = 0$$

e, poichè gli elementi b_j sono indipendenti su F, si conclude che $y_{ji} = 0$ per ogni $(j, i) \in I$, provando così l'indipendenza del sistema $(b_j a_i)$.
Dunque $(b_j a_i)_{(j,i) \in I}$ è una base di M come spazio vettoriale su F e quindi

$$[M : F] = nm = [M : L][L : F] \ . \qquad \blacksquare$$

Elementi algebrici e trascendenti.

Sia F un sottocampo del campo E (se $E|F$ è estensione, F è identificato con la sua copia isomorfa in E), e sia $b \in E$. Denotiamo con

– $F[b]$ il minimo *sottoanello* di E che contiene $F \cup \{b\}$;

– $F(b)$ il minimo *sottocampo* di E che contiene $F \cup \{b\}$ (come al solito, esso esiste perché l'intersezione di sottocampi di E è un sottocampo). Chiaramente $F[b] \subseteq F(b)$.

Ricordo (limitandolo ai campi) il contenuto del Teorema 8.3 (Cap. IV):

Sia $E|F$ un'estensione di campi, e sia $b \in E$. Allora

$$F[b] = \left\{ \sum_{i=0}^{n} a_i b^i \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in F \right\} .$$

E, in generale, $F(b)$ risulterà isomorfo al campo delle frazioni di $F[b]$.
Queste notazioni si estendono nella maniera naturale. Siano $b_1, b_2, \ldots, b_n$ elementi di E; allora $F[b_1, b_2, \ldots, b_n]$ è il minimo sottoanello di E che contiene $F \cup \{b_1, b_2, \ldots, b_n\}$; mentre $F(b_1, b_2, \ldots, b_n)$ è il minimo sottocampo di E che contiene $F \cup \{b_1, b_2, \ldots, b_n\}$. Risulta immediato verificare che

$$F(b_1, b_2, \ldots, b_n) = (F(b_1, \ldots, b_{n-1}))(b_n) = F(b_1) \ldots (b_{n-1})(b_n).$$

In particolare

$$F(b_1)(b_2) = F(b_1, b_2) = F(b_2)(b_1).$$

Definizione. Sia $E|F$ un'estensione di campi, e sia $b \in E$.

(1) b si dice **algebrico** su F se esiste un polinomio $f \neq 0$ in $F[x]$ tale che $f(b) = 0$.

(2) b si dice **trascendente** su F se per ogni polinomio $f \neq 0$ in $F[x]$ si ha $f(b) \neq 0$.

Esempi. 1) Per ogni $n, m \in \mathbb{N}$, con $m \geq 1$, $\sqrt[m]{n}$ è un numero reale algebrico su $\mathbb{Q}$, essendo radice del polinomio $x^m - n \in \mathbb{Q}[x]$. Similmente, $i \in \mathbb{C}$ è algebrico su $\mathbb{Q}$ essendo radice del polinomio $x^2 + 1$.

2) Esistono numeri reali che sono trascendenti su $\mathbb{Q}$. Esempi sono i numeri π ed e. La dimostrazione di questo fatto è stata ottenuta da F. Lindemann nel 1882, ed è piuttosto complicata. Tuttavia, non è difficile provare che l'insieme dei numeri reali che sono algebrici su $\mathbb{Q}$ è un insieme numerabile; poichè l'insieme dei reali non è numerabile, da ciò segue che devono esistere numeri reali trascendenti su $\mathbb{Q}$ (anzi, che l'insieme di essi è più che numerabile).

3) L'elemento $x \in F(x)$ è trascendente su F (nell'estensione $F(x)|F$). Più in generale, si provi per esercizio che ogni $f/g \in F(x) \setminus F$ (con f, g polinomi su F, $g \neq 0$) è trascendente su F.

Esercizio. Si provi che $u = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$.

Soluzione. Occorre trovare un polinomio non nullo in $\mathbb{Q}[x]$ che ammette u come radice. Cominciamo con elevare u al quadrato

$$u^2 = 2 - 2\sqrt{2}\sqrt{3} + 3 = 5 - 2\sqrt{6}$$

da cui $2\sqrt{6} = 5 - u^2$ ed elevando ancora al quadrato

$$24 = u^4 - 10u^2 + 25$$

quindi u è radice del polinomio $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ e dunque è algebrico su $\mathbb{Q}$.

Osserviamo i seguente fatti banali. 1) Se $b \in F$ allora b è algebrico su F (è radice del polinomio $x - b \in F[x]$).

2) Siano $F \leq E \leq L$ campi, e sia $b \in L$: se b è algebrico su F, allora b è algebrico su E; mentre se b è trascendente su E allora è trascendente su F.

Veniamo ora ad una osservazione fondamentale. Sia $E|F$ un'estensione di campi, e sia $b \in E$. Abbiamo allora l'omomorfismo di sostituzione

$$\begin{array}{rccc} \sigma_b: & F[x] & \to & E \\ & f & \mapsto & f(b) \end{array}$$

la cui immagine è $F[b]$ ed il cui nucleo è $I_b = \ker(\sigma_b) = \{\ f \in F[x] \mid f(b) = 0\ \}$. Dal Teorema fondamentale di omomorfismo discende allora che

$$F[b] \simeq \frac{F[x]}{I_b}\ .$$

Vale dunque il seguente importante risultato.

Teorema 1.3 *Sia $E|F$ un'estensione di campi, e sia $b \in E$. Allora $F[b] \simeq F[x]/I_b$, dove $I_b = \{f \in F[x] \mid f(b) = 0\}$.*

Supponiamo che l'elemento $b \in E$ sia trascendente su F; allora, per definizione, l'ideale $I_b = \{f \in R[x] \mid f(b) = 0\}$ coincide con $\{0\}$; dunque, in questo caso, l'omomorfismo di sostituzione σ_b è iniettivo. Quindi $F[b]$ è isomorfo all'anello dei polinomi $F[x]$ (e non è un campo).

Se invece b è algebrico su F, per definizione esiste almeno un polinomio non nullo a coefficienti in F che ammette b come radice. Dunque l'ideale $\ker(\sigma_b) = I_b$ non è l'ideale nullo. Poiché F è un campo, I_b è un ideale principale, e sappiamo che un generatore f di I_b è un polinomio di grado *minimo* tra i polinomi non nulli di I_b. Fra i generatori di I_b ne esiste dunque uno e uno solo *monico* (ovvero con coefficiente direttivo uguale a 1): esso è detto **polinomio minimo** di b (su F).

Chiamiamo f il polinomio minimo di b su F ($b \in E$ algebrico su F), e supponiamo che f si fattorizzi in $F[x]$ come il prodotto di due polinomi, cioè che $f = gh$ con $g, h \in F[x]$ (ed, essendo $f \neq 0$, è anche $g \neq 0 \neq h$). Allora, applicando l'omomorfismo di sostituzione:

$$0 = f(b) = g(b)h(b)\ ;$$

poiché E è un campo, si deve avere $g(b) = 0$ oppure $h(b) = 0$. Sia $g(b) = 0$, allora, poiché $g \neq 0$, deve essere $\deg g = \deg f$, quindi $\deg h = 0$, che significa $h \in F^*$; similmente, se $h(b) = 0$ si ha $\deg h = \deg f$ e $g \in F^*$. Abbiamo quindi concluso che il polinomio f è **irriducibile** (vedi la Proposizione 8.6 del Cap. IV e gli esempi che seguono). [Viceversa, se $f \in F[x]$ è un polinomio monico irriducibile che ammette b come radice nel campo K, allora f è il polinomio minimo di b su F; infatti il polinomio minimo g di b divide f e quindi $\deg g = \deg f$ da cui $g = f$ (essendo entrambi monici).]

Ora, poiché f è irriducibile, per una proprietà fondamentale dei P.I.D. (e $F[x]$ è tale), $I_b = (f)$ è un ideale massimale, e pertanto $F[b] \simeq F[x]/(f)$ è un campo (Teorema 8.7 del Cap. IV).

Ricapitolando, se $b \in E$ è **algebrico** su F, allora $F[b]$ è un campo; quindi, in questo caso $F(b) = F[b]$.

Se invece b è **trascendente** su F, allora $F[b]$ è isomorfo all'anello dei polinomi $F[x]$. Poiché $F(b)$ è un campo che contiene $F[b] \simeq F[x]$, per la proprietà del campo delle frazioni, esiste un campo $K \simeq F(x)$ tale che $F[b] \leq K \leq F(b)$; ma $F(b)$ è il minimo sottocampo di E che contiene $F \cup \{b\}$ e quindi $K = F(b)$. In conclusione, abbiamo dunque provato il seguente risultato.

Teorema 1.4 *Sia $E|F$ un'estensione di campi e sia $b \in E$. Allora*

(1) *Se b è algebrico su F, allora $F(b) = F[b] \simeq F[x]/(f)$, dove f è il polinomio minimo di b su F. Inoltre, $[F[b] : F] = \deg f$.*

(2) *Se b è trascendente su F, allora $F(b) \simeq F(x)$. In tal caso $[F(b) : F] = \infty$.*

Corollario 1.5 *Sia $E|F$ un'estensione di campi e sia $b \in E$. Allora b è trascendente su F se e soltanto se $F(b) \neq F[b]$.*

In effetti, dobbiamo ancora chiarire compiutamente l'ultima affermazione al punto (1) del Teorema 1.4.
Sia $b \in E$ un elemento algebrico su F, e $f \in F[x]$ il suo polinomio minimo. Allora per quanto ricordato a proposito degli elementi dell'anello quoziente $F[x]/(f)$, e mediante l'isomorfismo $F[x]/(f) \to F[b]$ (dato da $g + (f) \mapsto g(b)$), otteniamo infatti la seguente descrizione degli elementi di $F[b]$.

Proposizione 1.6 *Sia $E|F$ un'estensione di campi, $b \in E$ un elemento algebrico su F, e $f \in F[x]$ il suo polinomio minimo. Allora ogni elemento di $F[b]$ si scrive in modo unico nella forma*

$$a_0 + a_1 b + \ldots + a_{n-1} b^{n-1}$$

dove $n = \deg f$ e $a_0, a_1, \ldots, a_{n-1} \in F$.

Da ciò segue che $(1, b, b^2, \ldots, b^{n-1})$ è una base di $F[b]$ come spazio vettoriale su F, e che quindi $[F[b] : F] = \dim_F(F[b]) = n = \deg f$.

Esempio. Abbiamo visto che $b = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$, e il suo polinomio minimo è $f = x^4 - 10x^2 + 1$; quindi $\mathbb{Q}[b] = \mathbb{Q}(b)$ è un campo di grado 4 su $\mathbb{Q}$. Troviamo l'espressione di $(b^2 + b - 1)^{-1} \in \mathbb{Q}(b)$ come combinazione a coefficienti razionali di $1, b, b^2, b^3$. Si può procedere brutalmente determinando i coefficienti $a_i \in \mathbb{Q}$ con l'imporre l'uguaglianza

$$(b^2 + b - 1)(a_0 + a_1 b + a_2 b^2 + a_3 b^3) = 1,$$

oppure si pone $g = x^2 + x - 1$ e poiché $(g, f) = 1$ (dato che f è irriducibile) mediante l'algoritmo di Euclide si determinano $h, t \in \mathbb{Q}[x]$ tali che $hg + tf = 1$; a questo punto, sostituendo b, si ha $1 = h(b)g(b) + t(b)f(b) = h(b)(b^2 + b - 1)$, per cui $b^{-1} = h(b)$. Così procedendo si trova che

$$1 = -\frac{x+2}{7} \cdot f + \frac{x^3 + x^2 - 10x - 9}{7} \cdot g$$

e pertanto $b^{-1} = \frac{1}{7}(b^3 + b^2 - 10b - 9)$.

Estensioni semplici.

Un'estensione $E|F$ di campi si dice si dice **estensione semplice** se esiste $b \in E$ tale che $E = F(b)$. In tal caso, b si dice un *elemento primitivo* di $E|F$. Ad esempio, $\mathbb{C} = \mathbb{R}[i]$ è una estensione semplice di $\mathbb{R}$. Il Teorema 1.4 fornisce una descrizione delle estensioni semplici. In particolare, notiamo il fatto seguente.

Proposizione 1.7 *Sia $E|F$ un'estensione semplice di campi. Allora $[E : F]$ è finito, oppure $E \simeq F(x)$.*

Esempi. 1) Sia $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$; allora $L|\mathbb{Q}$ è una estensione semplice. Proviamo infatti che $L = \mathbb{Q}[\sqrt{2} - \sqrt{3}]$. L'inclusione $\mathbb{Q}[\sqrt{3} - \sqrt{2}] \subseteq L$ è ovvia. Viceversa, osserviamo che

$$\sqrt{3} + \sqrt{2} = (\sqrt{3} - \sqrt{2})^{-1} \in \mathbb{Q}[\sqrt{3} - \sqrt{2}],$$

e quindi $\sqrt{2} = \frac{1}{2}[(\sqrt{3} + \sqrt{2}) - (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}[\sqrt{3} - \sqrt{2}]$. Analogamente $\sqrt{3} \in \mathbb{Q}[\sqrt{3} - \sqrt{2}]$, e dunque $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} - \sqrt{3}]$.

2) $\mathbb{Q}(\pi, \sqrt{2})$ non è un'estensione semplice di $\mathbb{Q}$. Infatti, poiché π è trascendente su $\mathbb{Q}$, $[\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}] = \infty$, e dunque $\mathbb{Q}(\pi, \sqrt{2})$ non può essere un'estensione di $\mathbb{Q}$ ottenuta mediante l'aggiunzione di un elemento algebrico. Se fosse $\mathbb{Q}(\pi, \sqrt{2}) \simeq \mathbb{Q}(x)$, allora (vedi esercizio 1) ogni elemento di $\mathbb{Q}(\pi, \sqrt{2}) \setminus \mathbb{Q}$ sarebbe trascendente su $\mathbb{Q}$, e ciò è in contraddizione con il fatto che $\sqrt{2} \in \mathbb{Q}(\pi, \sqrt{2}) \setminus \mathbb{Q}$ è algebrico su $\mathbb{Q}$.

Osservazione. $\mathbb{R}$ non è una estensione semplice di $\mathbb{Q}$. Questo si può provare dimostrando che ogni estensione semplice di un campo numerabile è numerabile. Poichè $\mathbb{R}$ non è numerabile, non può essere una estensione semplice di $\mathbb{Q}$.

Citaimo, senza dimostrarlo, il seguente risultato di Steinitz.

Teorema 1.8 *Sia $E|F$ un'estensione di grado finito. Allora $E|F$ è semplice se e solo se il numero di campi intermedi tra F ed E è finito.*

Estensioni algebriche.

Un'estensione di campi $E|F$ si dice **algebrica** se ogni elemento di E è algebrico su F.

Proposizione 1.9 *Sia $E|F$ una estensione di campi di grado finito n. Allora ogni elemento di E è algebrico su F, e di grado $\leq n$ (e quindi $E|F$ è algebrica).*

Dimostrazione. Sia $E|F$ estensione con $[E : F] = n < \infty$, e sia $b \in E$. Ora, E è uno spazio vettoriale di dimensione n su F. Quindi gli $n + 1$ elementi $1, b, b^2, b^3, \ldots, b^n$ di E sono linearmente *dipendenti* su F, cioè esistono $a_0, a_1, a_2, \ldots, a_n$ in F non tutti nulli tali che

$$a_0 \cdot 1 + a_1 b + a_2 b^2 + \ldots + a_n b^n = 0$$

e dunque b è radice del polinomio non nullo $f = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$. Quindi, b è algebrico su F, ed il suo polinomio minimo divide f e pertanto ha grado al più $\deg f \leq n$. ∎

Corollario 1.10 *Sia $E|F$ un'estensione di campi, e sia $b \in E$ algebrico su F. Allora $F[b]$ è estensione algebrica di F*

DIMOSTRAZIONE. Sia $f \in F[x]$ il polinomio minimo di b su F, e sia $n = \deg f$. Allora $[F[b] : F] = n$, e si applica la Proposizione precedente. ∎

Un estensione $E|F$ tale che $[E : F] < \infty$ si dice estensione **finita**.

Proposizione 1.11 *Sia $E|F$ una estensione di campi. Allora $E|F$ è finita se e solo se esistono elementi $b_1, \ldots, b_m \in E$, algebrici su F, tali che $E = F[b_1, \ldots, b_m]$.*

DIMOSTRAZIONE. Sia $E = F[b_1, \ldots, b_m]$. Allora $b_1, \ldots, b_m$ sono algebrici su F (dire perché). Una ripetuta applicazione del punto (1) del Teorema 1.4 e della formula dei gradi porta a $[E : F] < \infty$; infatti:

$$\begin{aligned} [E : F] &= [F[b_1, \ldots, b_{n-1}][b_n] : F[b_1, \ldots, b_{n-1}]] \ldots\ldots [F[b_1][b_2] : F[b_1]]\, [F[b_1] : F] \leq \\ &\leq [F[b_n] : F] \cdot \ldots \cdot [F[b_2] : F] \cdot [F[b_1] : F] < \infty. \end{aligned}$$

Viceversa, sia $[E : F] = n < \infty$, e procediamo per induzione su n. Se $n = 1$, $E = F$ e non c'è nulla da provare. Sia $n \geq 2$, e sia $b_1 = b \in E \setminus F$. Allora $2 \leq [F(b) : F] = k \leq n$ per la Proposizione 1.9. Se $F(b) = E$ siamo a posto; altrimenti, applichiamo la formula dei gradi $n = [E : F] = [E : F(b)][F(b) : F]$, e quindi $[F(b) : F] = n/k < n$. Per ipotesi induttiva, esistono $b_2, \ldots, b_m \in E$ tali che $E = F(b)(b_2, \ldots, b_m)$, e quindi $E = F(b_1, b_2, \ldots, b_m)$ e abbiamo concluso. ∎

Teorema 1.12 *Sia $E|F$ una estensione di campi. Allora l'insieme degli elementi di E algebrici su F è un sottocampo di E (che ovviamente contiene F).*

DIMOSTRAZIONE. Siano $a, b \in E$ algebrici su F. Allora $[F(a) : F] = n$ e $[F(b) : F] = m$ con $1 \leq n, m \in \mathbb{N}$. Sia f il polinomio minimo di b su F. Allora, in particolare, $0 \neq f \in F(a)[x]$, e $f(b) = 0$. Pertanto b è algebrico su $F(a)$ e si ha $[F(a, b) : F(a)] \leq \deg f = m$. Quindi, per la formula dei gradi

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] \leq nm < \infty.$$

Dunque, per il Lemma 1.9, ogni elemento di $F(a, b)$ è algebrico su F. In particolare, sono quindi algebrici su F gli elementi $a - b,\ ab, a^{-1},\ b^{-1}$. Dunque somme, prodotti e inversi di elementi algebrici sono ancora elementi algebrici, provando così l'asserto. ∎

Se $E|F$ è una estensione di campi, il campo costituito da tutti gli elementi algebrici di E su F si chiama **chiusura algebrica** di F in E (la denoteremo con $\overline{F}_E$). Un caso molto importante, è quello dell'estensione $\mathbb{C}|\mathbb{Q}$. I numeri complessi che sono algebrici su $\mathbb{Q}$ si chiamano *numeri algebrici* e l'insieme di essi (ovvero la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$), che denotiamo con $\overline{\mathbb{Q}}$, si chiama il **campo dei numeri algebrici**. Osserviamo che $\mathbb{R} \not\subseteq \overline{\mathbb{Q}}$, infatti $\mathbb{R}$ contiene elementi trascendenti su $\mathbb{Q}$ (ad esempio $\pi \notin \overline{\mathbb{Q}}$).

Proposizione 1.13 $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$.

DIMOSTRAZIONE. Per ogni intero $n \geq 2$, sia $\delta_n = \sqrt[n]{2}$. δ_n è algebrico su $\mathbb{Q}$, ed il suo polinimio minimo è $x^n - 2$ (che è irriducibile per il Criterio di Eisenstein - Ccriterio 2 del Cap. IV). Dunque $\overline{\mathbb{Q}}$ contiene elementi il cui grado su $\mathbb{Q}$ è grande quanto si vuole, e dunque, per la Proposizione 1.9, $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$. ∎

Quest'ultimo fatto riconferma, in particolare, che il grado di $\mathbb{R}$ su $\mathbb{Q}$ è ∞.
Usando metodi del genere, possiamo infine fare la seguente osservazione.

Proposizione 1.14 *Siano $E|F$ e $L|E$ estensioni algebriche di campi. Allora l'estensione $L|F$ è algebrica.*

DIMOSTRAZIONE. Siano $E|F$ e $L|E$ estensioni algebriche, e sia $b \in L$. Poiché b è algebrico su E esistono elementi non tutti nulli $a_0, a_1, \ldots, a_m$ di E tali che

$$a_0 + a_1 b + \ldots + a_m b^m = 0.$$

Quindi b è algebrico su $K = F(a_1, a_2, \ldots, a_m)$, e $[K(b) : K] \leq m$. Poiché ciascun a_1 $(i = 1, 2, \ldots, m)$ è algebrico su F, K ha grado finito su F. Dunque

$$[K(b) : F] = [K(b) : K][K : F] < \infty.$$

Dalla Proposizione 1.9 segue che b è algebrico su F, così provando che l'estensione $L|F$ è algebrica. ∎

Commenti e trucchi.

$\mathbb{R}$ *contiene elementi trascendenti su* $\mathbb{Q}$. Iniziamo osservando che $\mathbb{Q}[x]$ è numerabile: infatti, se denotiamo con P_n l'insieme di tutti polinomi razionali di grado n, allora P_n è numerabile; poiché $\mathbb{Q}[x] = \bigcup_{n\in\mathbb{N}} P_n$, $\mathbb{Q}[x]$ è un'unione numerabile di insiemi numerabili, ed è pertanto numerabile. Ora, ogni elemento di $\mathbb{R}$ che sia algebrico su $\mathbb{Q}$ è radice di qualche polinomio non nullo in $\mathbb{Q}[x]$. Poiché un polinomio non nullo ha al più un numero finito di radici, l'insieme degli elementi di $\mathbb{R}$ algebrici su $\mathbb{Q}$ (la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{R}$) è unione numerabile di insiemi finiti, ed è dunque numerabile. Siccome $\mathbb{R}$ non è numerabile, questo significa che esistono elementi di $\mathbb{R}$ che non sono algebrici su $\mathbb{Q}$. (Osserviamo che ciò implica, in particolare, che $\mathbb{R}$ contiene un sottocampo isomorfo a $\mathbb{Q}(x)$.)

Formula dei gradi. La formula dei gradi risulta molto utile per eliminare i conti in diverse situazioni. Vediamo alcuni esempi.

1) Sia $F \leq L$ una estensione di campi. Proviamo che se $b \in L$ è algebrico su F di grado dispari allora $F[b] = F[b^2]$. Poichè b è algebrico, $F[b]$ e $F[b^2]$ sono campi. L'inclusione $F[b^2] \subseteq F[b]$ è ovvia. Supponiamo per assurdo $F[b] \not\subseteq F[b^2]$; ciò equivale a $b \notin F[b^2]$. Ora, b è radice del polinomio $g = x^2 - b^2 \in F[b^2][x]$, e siccome $b \notin F[b^2]$, g è il polinomio minimo di b sul campo $F[b^2]$. Poichè chiaramente $F[b^2, b] = F[b]$ si ha allora $[F[b] : F[b^2]] = 2$ e quindi, per la formula dei gradi,

$$[F[b] : F] = [F[b] : F[b^2]][F[b^2] : F] = 2[F[b^2] : F]$$

contro l'ipotesi che $[F[b] : F]$ sia dispari.

2) Calcolare il grado di $L = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]$ su $\mathbb{Q}$. $\sqrt[3]{3}$ è algebrico su $\mathbb{Q}$ ed il suo polinomio minimo su $\mathbb{Q}$ è $x^3 - 3$. Quindi $\mathbb{Q}[\sqrt[3]{3}]$ è un campo e $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = 3$. Ora, $\sqrt{2} \notin \mathbb{Q}[\sqrt[3]{3}]$, perché, se così fosse, allora $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{3}]$ e per la formula dei gradi si avrebbe la conclusione assurda che $2 = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$ divide $[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}] = 3$. Dunque $x^2 - 2$ è il polinomio minimo di $\sqrt{2}$ anche sul campo $\mathbb{Q}(\sqrt[3]{3})$. Applicando ancora la formula dei gradi si ha in conclusione

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

3) Siano $\zeta, \omega \in \mathbb{C}$, rispettivamente, una radice 7-ima ed una radice quinta dell'unità, diverse da 1. Proviamo che $\omega \notin \mathbb{Q}[\zeta]$. Infatti (vedi la Proposizione 4.7 del Cap. IV ed il commento seguente) i polinomi minimi su $\mathbb{Q}$ di ζ e ω sono, rispettivamente

$$x^6 + x^5 + \ldots + x + 1 \quad \text{e} \quad x^4 + x^3 + x^2 + x + 1.$$

Quindi $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 6$ e $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$; se fosse $\omega \in \mathbb{Q}[\zeta]$ allora $\mathbb{Q}[\omega] \subseteq \mathbb{Q}[\zeta]$ che, applicando la formula dei gradi come negli esempi precedenti, conduce ad una contraddizione.

Esercizio. Sia $f = x^3 - x + 1 \in \mathbb{Q}[x]$, e sia $b \in \mathbb{C}$ una radice di f. Si provi che $\mathbb{Q}(b)$ non contiene altre radici di f. Il facile studio del grafico della funzione reale $y = x^3 - x + 1$ associata al polinomio f, mostra che esso interseca l'asse delle ascisse in un solo punto. Dunque, f ha una sola radice reale α, e due radici complesse e non reali ζ e $\bar{\zeta}$, tra loro coniugate. Se $b = \alpha$, allora $\mathbb{Q}(b) \subseteq \mathbb{R}$, e dunque $\zeta \notin \mathbb{Q}(b)$ e $\bar{\zeta} \notin \mathbb{Q}(b)$. Sia allora $b = \zeta$. Poiché f è irriducibile su $\mathbb{Q}$ (è monico di terzo grado e non ha radici intere), esso è il polinomio minimo di ogni sua radice in $\mathbb{C}$. In particolare

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg f = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Se fosse $\alpha \in \mathbb{Q}(\zeta)$, allora $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$, e dunque, per la formula dei gradi $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$. Ciò è assurdo perché $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, mentre $\zeta \in \mathbb{C} \setminus \mathbb{R}$. Si osservi anche che $\bar{\zeta} \notin \mathbb{Q}(\zeta)$.

ESERCIZI

1. Sia F un campo e $F(x)$ il campo delle frazioni algebriche su F. Si provi che ogni elemento in $F(x) \setminus F$ è trascendente su F.

2. Calcolare $[\mathbb{Q}(\sqrt{5}, \sqrt{11}) : \mathbb{Q}]$.

3. Calcolare $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ con $\alpha \in \mathbb{C}$ tale che $\alpha^7 = 2$. Stessa domanda con α tale che $\alpha^6 = 4$.

4. Sia $a = \sqrt[3]{3} + 1313$. Qual è il grado del polinomio minimo di a su $\mathbb{Q}$? Qual è il grado del polinomio minimo di $a + i$ su $\mathbb{Q}$?

5. Siano $a, b \in \mathbb{C}$ elementi algebrici su $\mathbb{Q}$ tali che $[\mathbb{Q}(a) : \mathbb{Q}] = n$, $[\mathbb{Q}(b) : \mathbb{Q}] = m$ con $(n, m) = 1$. Si provi che $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$.

6. Sia $E = \mathbb{Q}(\sqrt[3]{2})$. Si provi che il polinomio $x^2 + x + 1$ è irriducibile in $E[x]$.

7. provare che i campi $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{5})$ non sono isomorfi.

8. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^3 - x + 1$, e in $\mathbb{Q}(\alpha)$ si consideri l'elemento $\beta = 2 - 3\alpha + 2\alpha^2$. Si provi che β è algebrico su $\mathbb{Q}$ e si trovi il suo polinomio minimo.

9. Sia $E|F$ un'estensione di grado finito e tale che per ogni coppia F_1, F_2 di campi intermedi tra F ed E si ha $F_1 \subseteq F_2$ oppure $F_2 \subseteq F_1$. Provare che $E|F$ è un'estensione semplice.

10. Sia A il campo dei numeri algebrici. Provare che ogni $z \in \mathbb{C} \setminus A$ è trascendente su A. Assumendo quindi il fatto che $\mathbb{C}$ è algebricamente chiuso, provare che A è un campo algebricamente chiuso.

11. Sia $E|F$ un'estensione algebrica. Si provi che se R è un sottoanello di E contenente F, allora R è un campo.

12. Siano $a, b \in \mathbb{C}$ algebrici su $\mathbb{Q}$, con $[\mathbb{Q}(a) : \mathbb{Q}] = p$, $[\mathbb{Q}(b) : \mathbb{Q}] = q$, p, q primi distinti e $p > q$. Sia f il polinomio minimo di a su $\mathbb{Q}$, e h il polinomio minimo di $a + b$ su $\mathbb{Q}$.

1) Provare che $[\mathbb{Q}(a, b) : \mathbb{Q}] = pq$.

2 Provare che f è il polinomio minimo di a su $\mathbb{Q}(b)$.

3) Provare che $\deg h \geq p$ e che $\deg h | pq$.

4) Sia, per assurdo, $\deg h = p$. Posto $h_1 = h(x + b) \in \mathbb{Q}(b)[x]$, provare che $h_1 = f \in \mathbb{Q}[x]$, e confrontando i coefficienti di grado $p - 1$ arrivare ad una contraddizione.

5) Concludere che $\deg h = pq$, e quindi che $\mathbb{Q}(a, b) = \mathbb{Q}(a + b)$.

2 Campi di spezzamento

Un omomorfismo iniettivo è detto **monomorfismo**.

Sia $f = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio irriducibile sul campo F. Allora l'ideale (f) di $F[x]$ è massimale; quindi $E = F[x]/(f)$ è un campo, ed è in modo naturale (mediante il monomorfismo definita da $a \mapsto a + (f)$, per ogni $a \in F$) un'estensione di F. Identificando gli elementi di F con le loro immagini in E, il polinomio f può essere visto come un polinomio a coefficienti in E. In E sia $\alpha = x + (f)$; allora

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \ldots + a_n\alpha^n = a_0 + a_1(x + (f)) + \ldots + a_n(x + (f))^n = \\ &= a_0 + (a_1 x + (f)) + \ldots + (a_n x^n + (f)) = \\ &= a_0 + a_1 x + \ldots + a_n x^n + (f) = f + (f) = (f) = 0_E. \end{aligned}$$

Dunque E è un'estensione di F che *contiene una radice di* f (e osserviamo che risulta $E = F[\alpha]$). Abbiamo dunque provato il seguente fatto fondamentale.

Proposizione 2.1 *Sia f un polinomio irriducibile sul campo F. Allora esiste un'estensione E di F che contiene una radice α di F, ed è tale che $E = F[\alpha]$.*

La situazione descritta da questa proposizione si chiama "aggiunzione" ad F di una radice di f.

Definizione. Sia F un campo, e $0 \neq f \in F[x]$. Un'estensione E di F si dice **campo di spezzamento** per f su F, se esistono elementi $a_1, \ldots, a_n \in E$ tali che

1) $f = a(x - a_1) \cdots (x - a_n)$ in $E[x]$ (dove a è il coefficiente direttivo di f);

2) $E = F[a_1, \ldots, a_n]$.

In altre parole, un campo di spezzamento per f su F è una estensione di F che contiene tutte le radici di f, ed è da queste generata su F. Il risultato che segue mostra come, in sostanza mediante aggiunzione successiva di radici, sia sempre possibile estendere F ad un campo di spezzamento per f.

Teorema 2.2 *Sia F un campo, e $0 \neq f \in F[x]$, con $\deg f = n$. Allora esiste un campo di spezzamento E per f su F, tale che $[E : F]$ divide $n!$.*

DIMOSTRAZIONE. Sia F un campo, e $0 \neq f \in F[x]$, con $\deg f = n$. Procediamo per induzione su n. Se $n = 1$ allora F è esso stesso campo di spezzamento. Sia $n \geq 2$. Supponiamo che f sia riducibile in $F[x]$. Dunque $f = f_1 f_2$ con $f_1, f_2 \in F[x]$ e, ponendo $d = \deg f_1$, $1 \geq d \leq n-1$ e $\deg f_2 = n - d < n$. Per ipotesi induttiva, esistono allora un campo di spezzamento E_1 per f_1 su F, ed un campo di spezzamento E per f_2 su E_1, inoltre $[E - 1 : F]$ divide $d!$ e $[E : E_1]$ divide $(n-d)!$. Si verifica facilmente dalla definizione che E è un campo di spezzamento per f su F; infine per la formula dei gradi si ha che $[E : F] = [E : E_1][E_1 : E]$ divide $d!(n-d)!$ che, a sua volta, divide $n!$. Supponiamo quindi che f si irriducibile in $F[x]$. Per la Proposizione 2.1, esiste allora un'estensione E_1 di F tale che $E_1 = F[\alpha]$ con α radice di f; inoltre, per il Teorema 1.4, $[E_1 : E] = n$. Ora, in $E_1[x]$, f si fattorizza come $(x-\alpha)g$, con $\deg g = n-1$. Per ipotesi induttiva, esiste un campo di spezzamento E per g su E_1, con $[E : E_1] | (n-1)!$. Come sopra, E è un campo di spezzamento per f su F, e si ha che $[E : F] = [E : E_1][E_1 : F]$ divide $(n-1)!n = n!$. ∎

Esempi. 1) Sia $1 \leq n \in \mathbb{N}$, e sia $\omega \in \mathbb{C}$ una radice *primitiva* n-esima dell'unità (quindi, $\omega = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$, con $0 \leq k \leq n-1$ e $(k, n) = 1$); sia $f = x^n - 1$. Allora, le radici in $\mathbb{C}$ di f sono tutte e sole le potenze ω^t con $t = 0, 1, \ldots, n-1$. Quindi $E = \mathbb{Q}(\omega) = \mathbb{Q}(1, \omega, \omega^2, \ldots, \omega^{n-1})$ è un campo di spezzamento per f su $\mathbb{Q}$. In $E[x]$,

$$x^n - 1 = (x-1)(x-\omega)\cdots(x-\omega^{n-1}).$$

Inoltre, se $n = p$ è un primo, allora sappiamo (come applicazione del criterio di Eisenstein) che il polinomio minimo di ω su $\mathbb{Q}$ è $1 + x + \ldots + x^{p-1}$, e pertanto $[E : \mathbb{Q}] = p - 1$. Se n non è un primo si può provare (lo vedremo più avanti) che $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$, dove ϕ è la funzione di Eulero (ed anche il numero di radici primitive n-esime dell'unità distinte).

2) Sia $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Nell'esercizio a pag. 9 abbiamo osservato che f ha in $\mathbb{C}$ una redice reale α e due radici complesse e non reali ζ e $\bar{\zeta}$, tra loro coniugate. Abbiamo anche provato che l'aggiunzione a $\mathbb{Q}$ di una sola di queste radici non dà luogo ad un campo di spezzamento per f su $\mathbb{Q}$. Quindi un tale campo di spezzamento è dato da $E = \mathbb{Q}(\alpha, \zeta, \bar{\zeta}) = \mathbb{Q}(\alpha, \zeta)$. Ora, poiché f è irriducibile su $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. In $\mathbb{Q}(\alpha)[x]$ si ha $f = (x-\alpha)g$, dove g è un polinomio irriducibile di grado 2 (se g fosse riducibile allora $\mathbb{Q}(\alpha)$ conterrebbe tutte le radici di f) che ammette ζ e $\bar{\zeta}$ come radici. Dunque $[\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)] = 2$ e, per la formula dei gradi

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!.$$

Estensioni normali.

Siano $E|F$ e $M|\overline{F}$ estensioni di campi, e supponiamo che sia dato un isomorfismo di campi $^- : F \to \overline{F}$ (con $a \mapsto \bar{a}$ per ogni $a \in F$). Ci chiediamo sotto quali condizioni sia possibile estendere tale isomorfismo a un monomorfismo $E \to M$.
Osserviamo in primo luogo che è possibile estendere in modo canonico l'isomorfismo $^- : F \to \overline{F}$ ad un isomorfismo (che denoteremo ancora con $^-$) dall'anello dei polinomi $F[x]$ in $\overline{F}[x]$; definito da, se $g = a_0 + a_1x + \ldots + a_nx^n \in F[x]$,

$$\bar{g} = \bar{a}_0 + \bar{a}_1x + \ldots + \bar{a}_nx^n.$$

Lemma 2.3 *Sia $^- : F \to \overline{F}$ ad un isomorfismo di campi. Sia E estensione di F tale che $E = F[b]$ con b algebrico su F, e sia f il polinomio minimo di b. Sia M un'estensione di $\overline{F}$. Allora l'isomorfismo $^-$ si estende ad un monomorfismo $E \to M$ se e solo se M contiene qualche radice di $\bar{f}$. Inoltre, se c è una radice in M di $\bar{f}$, allora esiste un unico monomorfismo $\phi : E \to M$ che estende $^-$ e tale che $\phi(b) = c$; e si ha $\phi(E) = \overline{F}[c]$.*

Dimostrazione. Supponiamo che esista un monomorfismo $\phi : E \to M$ che estende l'isomorfismo $^-$ (cioè tale che $\phi(a) = \bar{a}$ per ogni $a \in F$). Allora, se $f = a_0+a_1x+\ldots+a_n$,

$$\bar{f}(\phi(b)) = \bar{a}_0 + \ldots + \bar{a}_n\phi(b)^n = \phi(a_0) + \ldots + \phi(a_n)\phi(b)^n = \phi(f(b)) = 0$$

e dunque $\phi(b) \in M$ è una radice di $\bar{f}$.
Viceversa, sia $c \in M$ una radice di $\bar{f}$, e ricordiamo che ogni elemento di $E = F[b]$ si scrive in modo unico nella forma $a_0 + a_1b + a_{n-1}b^{n-1}$, con $a_0, a_1, \ldots, a_n \in F$. Allora l'applicazione $\phi : E \to M$ definita da, per ogni $u = a_0 + a_1b + a_{n-1}b^{n-1} \in E$,

$$\phi(u) = \bar{a}_0 + \bar{a}_1c + \bar{a}_{n-1}c^{n-1},$$

definisce un monomorfismo da E in M che chiaranente estende $^-$. Infatti, l'isomorfismo $F[x] \to \overline{F}[x]$ (che manda f in $\bar{f}$, che quindi è il polinomio minimo di c su $\overline{F}$) manda l'ideale (f) nell'ideale $(\bar{f})$. Ne segue che $F[x]/(f)$ è isomorfo a $\overline{F}[x]/(\bar{f})$ (mediante l'applicazione $g + (f) \mapsto \bar{g} + (\bar{f})$). L'applicazione ϕ definita sopra è la composizione dei tre isomorfismi

$$E = F[b] \to \frac{F[x]}{(f)} \to \frac{\overline{F}[x]}{(\bar{f})} \to \overline{F}[c],$$

con l'inclusione di $\overline{F}[c]$ in M. ϕ è quindi un monomorfismo da E in M. Infine, è chiaro che ϕ è l'unico monomorfismo da E in M che estende $^-$ e manda b in c. ∎

Vediamo subito una applicazione del Lemma 2.3, che stabilisce l'unicità (a meno di isomorfismo) del campo di spezzamento di un polinomio.

Teorema 2.4 *Sia $^- : F \to \overline{F}$ ad un isomorfismo di campi, e $0 \neq f \in F[x]$. Siano, rispettivamente, E un campo di spezzamento per f su F, e M un campo di spezzamento per $\bar{f}$ su $\overline{F}$. Allora l'isomorfismo $^-$ si estende ad un isomorfismo $E \to M$.*

Dimostrazione. Procediamo per induzione su $[E : F]$. Se $[E : F] = 1$, allora $E = F$ e di conseguenza f si fattorizza in $F[x]$ come prodotto di polinomi lineari; ne segue che anche $\bar{f}$ si fattorizza in $\overline{F}[x]$ come prodotto di polinomi lineari e quindi $M = \overline{F}$.
Sia quindi $[E : F] \geq 2$. Allora, in $F[x]$, $f = gh$ dove g è un fattore irriducibile e non lineare. Di conseguenza, in $\overline{F}[x]$, $\bar{f} = \bar{g}\bar{h}$. Siano, rispettivamente, $b \in E$ una radice di g,

e $c \in M$ una radice di $\bar{g}$. Per il Lemma 2.3, l'isomorfismo $F \to \overline{F}$ si estende ad un unico isomorfismo $\eta : F[b] \to \overline{F}[c]$ tale che $\eta(b) = c$. Ora, E è un campo di spezzamento per f su $F[b]$ e M è un campo di spezzamento per $\bar{f}$ su $\overline{F}[c]$. D'altra parte

$$[E : F] = [E : F[b]][F[b] : F] = [E : F[b]](\deg g) \geq [E : F[b]] \cdot 2,$$

e quindi $[E : F[b]] < [E : F]$. Per ipotesi induttiva esiste dunque un isomorfismo $\bar{\eta} : E \to M$ che estende η. Chiaramente, $\bar{\eta}$ estende anche l'isomorfismo $F \to \overline{F}$. ∎

Abbiamo enunciato e provato il Lemma 2.3 ed il Teorema 2.4 in forma generale, a partire cioè da un arbitrario isomorfismo $F \to \overline{F}$, questo (in particolare per il Teorema) per poter applicare con maggior facilità l'induzione; in molti casi (ma non sempre), saremo in seguito interessati alla situazione in cui $\overline{F} = F$ e l'isomorfismo di partenza è l'identità. Si tratta di un caso importante, che giustifica la seguente definizione.

Definizione. Siano E e M estensioni del medesimo campo F. Allora un monomorfismo $\phi : E \to M$ tale che $\phi(a) = a$ per ogni $a \in F$ si dice **F-monomorfismo**. Se ϕ è un isomorfismo, si chiama **F-isomorfismo**.

Corollario 2.5 *Sia F un campo, $0 \neq f \in F[x]$, e siano E e M campi di spezzamento per f su F. Allora esiste un F-isomorfismo di E in M.*

Dimostrazione. È un caso particolare del Teorema 2.4. ∎

Proviamo ora un'altra importante proprietà dei campi di spezzamento.

Proposizione 2.6 *Sia E un campo di spezzamento su F per il polinomio $f \in F[x]$, e sia g un polinomio irriducibile in $F[x]$ che ha una radice in E. Allora E contiene un campo di spezzamento per g su F.*

Dimostrazione. Poiché E è campo di spezzamento di f, $E = F(a_1, \ldots, a_n)$, dove $a_1, \ldots, a_n$ sono le radici di f. Sia g un polinomio irriducibile in $F[x]$ che abbia una radice $b \in E$. Sia M un campo di spezzamento per g su E.
Sia $b_1 \in M$ una radice di g. Ora, $E_1 = F(b_1, a_1, \ldots, a_n) = E(b_1)$ è un campo di spezzamento per f su $F(b_1)$, mentre $E = F(b, a_1, \ldots, a_n)$ è un campo di spezzamento per f su $F(b)$. Poiché g è il polinomio minimo su F sia di b che di b_1, per il Lemma 2.3 esiste un F-isomorfismo $\eta : F(b) \to F(b_1)$ tale che $\eta(b) = b_1$. Siccome g ha coefficienti in F, $\eta(g) = g$. Dunque, per il Teorema 2.4, η si può estendere ad un F-isomorfismo $\eta_1 : E \to E_1$. Siccome η_1 fissa F, si ha $[E : F] = [E_1 : F]$. Ma $E_1 \supseteq E$ e quindi, per la formula dei gradi, $[E_1 : E] = 1$, cioè $E_1 = E$. Questo implica che $b_1 \in E$. Poiché ciò vale per ogni radice b_1 di g in M, e M è generato su E da tali radici, si conclude che $M = E$ e pertanto che E contiene un campo di spezzamento per g su F. ∎

Un'estensione algebrica di campi $E|F$ che soddisfa la conclusione della Proposizione precedente si chiama estensione normale.

Definizione. Un'estensione algebrica di campi $E|F$ si dice **normale** se E contiene un campo di spezzamento di ogni polinomio irriducibile in $F[x]$ che ha almeno una radice in E.

La proposizione 2.6 viene completata col seguente risultato.

Teorema 2.7 *Sia $E|F$ un'estensione di campi. Allora sono equivalenti*

(1) $E|F$ è finita e normale;

(2) E è un campo di spezzamento per qualche polinomio in $F[x]$.

DIMOSTRAZIONE. (2) $\Rightarrow$ (1) : è la Proposizione 2.6.
(1) $\Rightarrow$ (2). Sia E un'estensione finita e normale del campo F. Poiché $E|F$ è finita, per la Proposizione 1.11, esistono elementi $b_1, \ldots, b_n$ di E (algebrici su F) tali che $E = F[b_1, \ldots, b_n]$. Per ciascun $i = 1, \ldots, n$ sia $f_i \in F[x]$ il polinomio minimo di b_i su F, e poniamo $f = f_1 f_2 \ldots f_n$. Poiché $E|F$ è un'estensione normale, E contiene un campo di spezzamento su F per ciascuno dei polinomi f_i. Ne segue che E contiene un campo di spezzamento per f. Siccome poi E è generato su F da radici di f, si conclude che E è un campo di spezzamento per f su F. ∎

Radici multiple.

Sia F campo, $0 \neq f \in F[x]$, E un campo di spezzamento per f, e $\alpha \in E$ una radice di f. Allora dal teorema di Ruffini segue che, in $E[x]$, $(x-\alpha)$ divide f. Si chiama **molteplicità** (algebrica) della radice α il massimo intero positivo m_α tale che $(x-\alpha)^{m_\alpha}$ divide f (chiaramente, essa non dipende dal particolare campo di spezzamento). La radice α si dice radice *semplice* se $m_\alpha = 1$, e radice *multipla* se $m_\alpha \geq 2$.
Osserviamo che, ancora per il Teorema di Ruffini, α è una radice semplice se e soltanto se, in $E[x]$, $f = (x-\alpha)g$ con $g(\alpha) \neq 0$.

Ricordiamo ora la definizione di polinomio *derivato*: sia $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ un polinomio a coefficienti nel campo F. Il suo polinomio derivato f' è:

$$f' = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

Le seguenti regole di derivazione sono di immediata verifica.

Siano $f, g \in F[x]$. Allora

$$(f+g)' = f' + g'$$
$$(fg)' = f'g + g'f.$$

Lemma 2.8 *Sia F campo, $0 \neq f \in F[x]$, e α una radice di f (in un campo di spezzamento E). Allora α è una radice multipla se e solo se $f'(\alpha) = 0$.*

DIMOSTRAZIONE. Siano f ed α come nelle ipotesi. Supponiamo che α sia radice multipla di f; quindi, in $E[x]$, $f = (x-\alpha)^2 g$ (con $g \in E[x]$) e dunque, applicando la regola di derivazione riportata sopra,

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

da cui segue che $f'(\alpha) = 0$.

Viceversa, sia α radice semplice di f. Allora, in $E[x]$, $f = (x-\alpha)g$ e $g(\alpha) \neq 0$. Dunque

$$f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(\alpha) = g(\alpha) \neq 0$$

concludendo la dimostrazione. ■

Nella situazione che stiamo considerando, supponiamo che il polinomio monico $f \in F[x]$ sia irriducibile. Allora f è il polinomio minimo di ogni sua radice in qualche estensione di F. In particolare è il polinomio minimo della radice $\alpha \in E$. Poiché $f' \in F[x]$ e $\deg f' = degf - 1$, si osserva dunque che α è radice anche di f' (e quindi è radice multipla di f) se e soltanto se $f' = 0$. Assumiamo ulteriormente che $char(F) = 0$; allora, si verifica facilmente che, se f è un polinomio di grado ≥ 1 (non necessariamente irriducibile) in $F[x]$, si ha $f' \neq 0$.
Mettendo insieme queste due osservazioni abbiamo dunque la seguente

Proposizione 2.9 *Sia F un campo di caratteristica 0, e sia $f \in F[x]$ un polinomio irriducibile. Allora tutte le radici di f, in un campo di spezzamento E, sono semplici (quindi, se $\deg f = n$, f ha n radici distinte in E).*

I campi di caratteristica 0 non sono i soli a godere della proprietà stabilita dalla Proposizione precedente (tali campi sono detti *perfetti*). Ad esempio, essa sussiste anche per i campi finiti. Ma non tutti i campi sono perfetti. Ad esempio si consideri il campo delle frazioni algebriche su $\mathbb{Z}_p$ (p un primo), ovvero $F = \mathbb{Z}_p(t)$ (abbiamo chiamato t l'ideterminata per riservare x a denotare un'indeterminata su F). Nell'anello dei polinomi $F[x]$ si consideri $f = x^p - t$. Si può provare che f è irriducibile in $F[x]$, mentre d'altra parte $f' = px^{p-1} = 0$ (dato che, in un campo di caratteristica p moltiplicare per p dà sempre 0). Quindi, per il Lemma 2.8, le radici di f in un campo di spezzamento sono multiple (si può anche provare che, se α è una radice di f in E, allora, in $E[x]$, $f = (x-\alpha)^p$).

Un polinomio a coefficienti nel campo F si dice *separabile* se ogni suo fattore irriducibile ha tutte radici semplici in un suo campo di spezzamento (dunque, se $char(F) = 0$ ogni polinomio $0 \neq f \in F[x]$ è separabile).
Un'estensione di campi $E|F$ si dice **separabile** se è algebrica e per ogni $b \in E$ il polinomio minimo di b in $F[x]$ è separabile. Un'immediata conseguenza della Proposizione 2.9 è il seguente fatto

Teorema 2.10 *Sia F un campo di caratteristica 0. Allora ogni estensione algebrica $E|F$ è separabile.*

ESERCIZI

1. Sia F un campo, e siano $a \in F$ e $1 \leq n \in \mathbb{N}$, tali che il polinomio $f = x^n - a$ è irriducibile in $F[x]$. Sia u una radice di F in un'opportune estensione di F, e sia $m \geq 1$, $m|n$. Si provi che il grado di u^m su F è n/m, e si determini il polinomio minimo di u^m su F.

2. Sia F campo con $char(F) \neq 2$, e sia $f \in F[x]$ un polinomio irriducibile di grado 2. Sia E campo di spezzamento per f, ed $a \in E$ una radice di f. Si provi che $E = F[a]$, e che esiste $d \in E$ tale che $E = F[d]$ e $d^2 \in F$.

3. Si provi che $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ è il campo di spezzamento su $\mathbb{Q}$ di $x^3 - 2$.

4. Per ciascuno dei seguenti polinomi razionali si determini un campo di spezzamento contenuto in $\mathbb{C}$, e se ne calcoli il grado su $\mathbb{Q}$:

- $f = x^5 - 2$.
- $g = x^4 - x^2 + 4$.

5. Sia $E|F$ un'estensione normale, e sia L campo intermedio ($F \leq L \leq E$): si provi che $E|L$ è un'estensione normale.

6. Sia F un campo e sia $E|F$ estensione tale che $[E : F] = 2$. Si provi che $E|F$ è un'estensione normale.

7. Si provi che $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ è un'estensione normale.

8. Si provi che le estensioni $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ sono normali, mentre l'estensione $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ non lo è.

9. Sia E campo di spezzamento per un polinomio f sul campo F, e sia K un campo tale che $F \leq K \leq E$. Si provi che ogni F-monomorfiamo $K \to E$ si può estendere ad un F-automorfismo di E.

10. Sia F, e $0 \neq f \in F[x]$. Si provi che tutte le radici di f in un campo di spezzamento sono semplici se e solo se (in $F[x]$) $(f, f') = 1$.

11. In una opportuna estensione di $\mathbb{Z}_3$, si trovino le eventuali radici multiple del polinomio $x^7 + x^5 + x^4 - x^3 - x^2 - x + 1$.

12. Sia $E|F$ un'estensione separabile, e sia L un campo intermedio: si provi che $E|L$ e $L|F$ sono estensioni separabili.

3 Gruppo di Galois

Sia $E|F$ un'estensione di campi, e siano ψ, ϕ F-automorfismi di E (ovvero automorfismi del campo E che lasciano fisso ogni elemento del sottocampo F); è chiaro allora che anche ϕ^{-1} e $\phi \circ \psi$ sono F-automorfismi di di E. Dunque l'insieme degli F-automorfismi di E è un sottogruppo del gruppo degli automorfismi di E: esso viene chiamato **Gruppo di Galois** dell'estensione $E|F$, e si denota con $Gal(E|F)$.

Esempi. 1) Sia F un campo di caratteristica diversa da 2, ed $E = F[b]$ dove $b \in E$ è tale che $b \notin F$ e $b^2 \in F$. Allora, il polinomio minimo di b su F è $x^2 - b^2$, le cui radici in E sono b e $-b$ (che sono distinte perché $\mathrm{char}(F) \neq 2$). Poiché E è generato su F dall'elemento b (più esplicitamente: gli elementi di E sono tutti del tipo $a_0 + a_1 b$, con $a_0, a_1 \in F$), un F-automorfismo di E è univocamente determinato dall'immagine di b tramite esso. Dunque, segue dal Lemma 2.3, che $Gal(E|F) = \{\iota_E, \phi\}$ dove ϕ è l'unico F-automorfismo di E tale che $\phi(b) = -b$. Precisamente, ϕ è dato da $\phi(a_0 + a_1 b) = a_0 - a_1 b$, per ogni $a_0 + a_1 b \in E$.
In particolare, questo si applica al caso di $\mathbb{C} = \mathbb{R}(i)$, per cui deduciamo che $Gal(\mathbb{C}|\mathbb{R})$ è costituito dall'identità e dall'automorfismo di coniugio di $\mathbb{C}$.

2) $Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{\iota\}$. Infatti, sempre per il Lemma 2.3, se ϕ è un $\mathbb{Q}$-automorfismo di $\mathbb{Q}(\sqrt[3]{2})$, allora $\phi(\sqrt[3]{2})$ deve di necessità essere una radice del polinomio minimo $g = x^3 - 2$ di $\sqrt[3]{2}$ su $\mathbb{Q}$; ma $\mathbb{Q}(\sqrt[3]{2})$ non contiene radici di g diverse da $\sqrt[3]{2}$, dato che queste ultime non sono reali mentre $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Dunque ogni $\mathbb{Q}$-automorfismo di $\mathbb{Q}(\sqrt[3]{2})$ deve mandare $\sqrt[3]{2}$ in se stesso. Poiché $\mathbb{Q}(\sqrt[3]{2})$ è generato su $\mathbb{Q}$ da $\sqrt[3]{2}$, si conclude che l'identità è l'unico elemento del gruppo di Galois di $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$.

3) Siano p un numero primo positivo, $\omega \in \mathbb{C}$ una radice primitiva p-esima dell'unità, e poniamo $E = \mathbb{Q}(\omega)$. Gli automorfismi di E che fissano i razionali sono chiaramente determinati dall'immagine di ω. Se σ è un tale $\mathbb{Q}$-automorfismo, allora $\sigma(\omega)$ deve essere una radice dell'unità diversa da 1, quindi $\sigma(\omega) = \omega^k$ per un $1 \leq k \leq p-1$, e pertanto $|Gal(E|\mathbb{Q})| \leq p-1$. D'altra parte, per ogni $1 \leq k \leq p-1$ si ha che $E = \mathbb{Q}(\omega^k)$, e ω^k (così come ω) è radice del polinomio irriducibile $1+x+\ldots+x^{p-1}$. Per il Lemma 2.3 esiste dunque un $\mathbb{Q}$-automorfismo σ_k di E tale che $\sigma_k(\omega) = \omega^k$. Dunque $Gal(E|\mathbb{Q}) = \{\iota = \sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$. In particolare, $|Gal(E|\mathbb{Q})| = p - 1 = [E : \mathbb{Q}]$ (osserviamo che, in questo esempio, E è un campo di spezzamento su $\mathbb{Q}$).

4) $Gal(\mathbb{R}|\mathbb{Q}) = \{\iota\}$. Infatti, l'identità è il solo automorfismo (di campo!) di $\mathbb{R}$. Sia ϕ automorfismo di $\mathbb{R}$, allora da $\phi(1) = 1$ segue che $\phi(z) = z$ per ogni $z \in \mathbb{Z}$, e da ciò che $\phi(u) = u$ per ogni $u \in \mathbb{Q}$ (lo si dimostri per bene). Inoltre se $0 \leq r \in \mathbb{R}$, allora $0 \leq \phi(r)$: infatti se $r \geq 0$, esiste $a \in \mathbb{R}$ tale che $r = a^2$ e, quindi, poiché ϕ è omomorfismo, $\phi(r) = \phi(a^2) = \phi(a)^2 \geq 0$. Supponiamo, per assurdo, che esista $r \in \mathbb{R}$ tale che $\phi(r) \neq r$; possiamo assumere che $\phi(r) > r$ (il ragionamento nel caso opposto è identico). Allora. per la densità dei razionali nei reali, esiste $u \in \mathbb{Q}$ con $r < u < \phi(r)$, e quindi, per quanto osservato sopra,

$$0 > \phi(u - r) = \phi(u) - \phi(r) = u - \phi(r) < 0,$$

che è una contraddizione. Quindi $\phi = \iota_{\mathbb{R}}$.

Sia $G = Gal(E|F)$ il gruppo di Galois dell'estensione di campi $E|F$, e sia H un sottogruppo di G. Si pone

$$Inv_E(H) = \{\ b \in E \mid \sigma(b) = b \ \text{ per ogni } \sigma \in H\ \}.$$

Dalle definizioni date, e mediante semplici verifiche, segue ora facilmente la seguente ossevazione.

Lemma 3.1 *Sia $E|F$ un'estensione di campi. Allora*

(1) se L è un campo intermedio (cioè $F \leq L \leq E$) allora $Gal(E|L) \leq Gal(E|F)$;

(2) se $H \leq Gal(E|F)$ allora $Inv_E(H)$ è un sottocampo di E contenente F.

Dimostrazione. Per esercizio. ∎

Questo Lemma mostra che il funtore $Gal(E|\ \cdot\ )$ associa ad ogni campo intermedio dell'estensione $E|F$ un sottogruppo di $Gal(E|F)$; e viceversa il funtore $Inv_E(\ \cdot\ )$ associa

ad ogni sottogruppo di $Gal(E|F)$ un campo intermedio dell'estensione $E|F$. Il teorema fondamentale della Teoria di Galois afferma che per certe estensioni (in particolare per i campi di spezzamento su $\mathbb{Q}$ di polinomi razionali), questi due funtori sono l'uno l'inverso dell'altro, e che vi è pertanto una corrispondenza biunivoca tra l'insieme dei sottogruppi di $Gal(E|F)$ e quello dei campi intermedi dell'estensione $E|F$.

Teorema 3.2 *Sia F un campo, ed E campo di spezzamento su F per il polinomio $0 \neq f \in F[x]$. Se le radici di f in E sono tutte semplici allora $|Gal(E|F)| = [E : F]$.*

Dimostrazione. Procediamo per induzione su $[E : F]$. Se $[E : F] = 1$ allora $E = F$ e non c'è nulla da provare.
Sia quindi $[E : F] > 1$. Allora, in $F[x]$, f ha un fattore irriducibile g di grado $n = \deg g$ almeno 2. Per ipotesi, E contiene n radici distinte di g: $b = b_1, b_2, \ldots, b_n$. Per il Lemma 2.3, per ogni $i = 1, 2, \ldots, n$, esiste un unico F-isomorfismo $\tau_i : F[b] \to F[b_i]$ tale che $\tau_i(b) = b_i$. Ora, E è un campo di spezzameno per il polinomio f sia su $F[b]$ che su $F[b_i]$, e quindi, per il Teorema 2.4, ciascun τ_i $(i = 1, 2, \ldots, n)$ può essere esteso ad un isomorfismo $\eta_i : E \to E$. È chiaro che gli η_i sono F-automorfismi di E, cioè $\eta_i \in Gal(E|F)$ per ogni $i = 1, 2, \ldots, n$ (osserviamo che possiamo scegliere $\eta_1 = \iota_E$).
Sia ora $H = Gal(E|F[b])$. Per il Lemma 3.1, H è un sottogruppo di $G = Gal(E|F)$. Proviamo che G è l'unione disgiunta

$$G = \eta_1 H \cup \eta_2 H \cup \ldots \cup \eta_n H \tag{1}$$

(ovvero che $\{\eta_1, \eta_2, \ldots, \eta_n\}$ è un sistema di rappresentanti delle classi laterali sinistre di G modulo H). Proviamo innanzi tutto che tali classi sono distinte. Siano $1 \leq i, j \leq n$ tali che $\eta_i H = \eta_j H$; allora $\eta_j^{-1}\eta_i = \sigma \in H$, quindi $\eta_i = \eta_j \sigma$, e dunque

$$b_i = \eta_i(b) = \eta_j\sigma(b) = \eta_j(\sigma(b)) = \eta_j(b) = bj$$

da cui segue $i = j$. Proviamo ora che l'unione è tutto G. Sia $\alpha \in G$; poiché α fissa ogni elemento di F, $\alpha(b)$ deve essere una radice di g, dunque $\alpha(b) = b_i$, per un unico $i = 1, 2, \ldots, n$. Ne segue che $\eta_i^{-1}\alpha(b) = b$, e dunque che $\eta_i^{-1}\alpha \in Gal(E|F[b]) = H$, cioè $\alpha \in \eta_i H$, provando così l'uguaglianza (1). Dunque, applicando l'ipotesi induttiva $|H| = [E : F[b]]$ (che sussiste perché E è campo di spezzamento per f su $F[b]$), si ha

$$|G| = |H|n = [E : F[b]] \deg g = [E : F[b]][F[b] : F] = [E : F],$$

e la dimostrazione è completa. ∎

Definizione. Un'estensione di campi $E|F$ che sia *finita, normale e separabile* si dice **estensione di Galois**.

Segue quindi dai Teoremi 2.7 e 2.10 che se F è un campo di caratteristica 0, ed E è un campo di spezzamento per un polinomio $0 \neq f \in F[x]$, allora l'estensione $E|F$ è un'estensione di Galois.

Teorema 3.3 *Se $E|F$ è un'estensione di Galois allora $|Gal(E|F)| = [E : F]$.*

DIMOSTRAZIONE. Sia $E|F$ un'estensione di Galois. Poiché $[E : F] < \infty$, esistono $b_1, \ldots, b_n \in E$ tali che $E = F[b_1, \ldots, b_n]$. Per ogni $i = 1, 2, \ldots, n$, sia $f_i \in F[x]$ il polinomio minimo di b_i su F, e sia $f \in F[x]$ il prodotto degli f_i distinti. Poiché $E|F$ è normale, E contiene un campo di spezzamento per ciascuno degli f_i e quindi contiene un campo di spezzamento per f su F; ma $b_1, \ldots, b_n$ sono tutti radici di f, e dunque E è un campo di spezzamento per f. Ora, poiché $E|F$ è separabile, ciascun f_i ha solo radici semplici. Siccome polinomi monici irriducibili distinti non possono avere radici comuni, concludiamo che le radici di f sono tutte semplici. Dunque, per il Teorema 3.2, $|Gal(E|F)| = [E : F]$. ∎

Come esempio, determiniamo il gruppo di Galois dell'estensione $E|\mathbb{Q}$ dove E è il campo di spezzamento del polinomio $f = x^3 - x + 1$. Abbiamo visto che, in $\mathbb{C}$, f ha tre radici $\alpha, \zeta, \bar{\zeta}$, di cui α è reale e $\zeta, \bar{\zeta}$ sono complesse coniugate. Quindi, un campo di spezzamento per f è $E = \mathbb{Q}(\alpha, \zeta, \bar{\zeta}) = \mathbb{Q}(\alpha, \zeta)$ e, come abbiamo visto, $[E : F] = 6$. Sia $\Omega = \{\alpha, \zeta, \bar{\zeta}\}$, e sia $G = Gal(E|F)$. Se $\sigma \in G$, allora σ manda radici di f in radici di f, e dunque induce una permutazione dell'insieme Ω. Pertanto è possibile definire (semplicemente mediante restrizione) un'azione di G su Ω. Se $\sigma \in G$ fissa tutti gli elementi di Ω, allora, poiché E è da questi generato su F, σ deve essere l'identità su E. Dunque l'azione di G su Ω è fedele e pertanto G è isomorfo ad un sottogruppo di $Sym(\Omega) \simeq S_3$. Ma, per il Teorema 3.2, $|G| = [E : F] = 6$. Quindi $G \simeq S_3$. Descriviamo ora i campi degli invarianti $Inv_E(H)$ dei sottogruppi H di G. Osserviamo innanzi tutto che ogni $\sigma \in G$ è univocamente determinato dalla permutazione che esso induce sull'insieme Ω delle radici di f, e che (in questo caso! dato che $G \simeq S_3$) ogni permutazione di Ω è indotta da un elemento di G. Osserviamo anche (lo si provi usando la formula dei gradi) che $E \cap \mathbb{R} = \mathbb{Q}[\alpha]$. Chiaramente, $Inv_E(\{\iota\}) = E$. Sia $\tau_0 \in G$ tale che induce su Ω la permutazione che fissa α e scambia tra loro ζ e $\bar{\zeta}$; $H_0 = \langle \tau_0 \rangle$ è un sottogruppo di ordine 2 di G. Ora, τ_0 è la restrizione a E dell'automorfismo di coniugio, e quindi $Inv_E(H_0) = E \cap \mathbb{R} = \mathbb{Q}[\alpha]$. Sia $\tau_1 \in G$ tale che τ_1 fissa ζ e scambia α e $\bar{\zeta}$, e sia $H_1 = \langle \tau_1 \rangle$. Allora, chiaramente, $\mathbb{Q}[\zeta] \leq Inv_E(H_1)$; se fosse $Q[\zeta] < Inv_E(H_1)$ allora, per la formula dei gradi, $Inv_E(H_1) = E$, ma ciò non è perché $\alpha \notin Inv_E(H_1)$: dunque $Inv_E(H_1) = Q[\zeta]$. Allo stesso modo si prova che, posto $H_2 = \langle \tau_2 \rangle$, dove $\tau_2 \in G$ è tale che fissa $\bar{\zeta}$ e scambia α con ζ, allora $Inv_E(H_2) = Q[\bar{\zeta}]$. A questo punto, osserviamo che

$$Inv_E(G) \leq Inv_E(H_0) \cap Inv_E(H_1) = \mathbb{Q}[\alpha] \cap \mathbb{Q}[\zeta] = \mathbb{Q}$$

e dunque $Inv_E(G) = \mathbb{Q}$.
Infine, sia $\gamma \in G$ tale che $\gamma(\alpha) = \zeta,\ \gamma(\zeta) = \bar{\zeta},\ \gamma(\bar{\zeta}) = \alpha$. Allora $A = \langle \gamma \rangle = \{\iota, \gamma, \gamma^{-1}\}$ è un sottogruppo di ordine 3 di G (che corrisponde al sottogruppo alterno A_3 di S_3). Sia

$$d = (\alpha - \zeta)(\zeta - \bar{\zeta})(\bar{\zeta} - \alpha).$$

Allora $\gamma(d) = (\zeta - \bar{\zeta})(\bar{\zeta} - \alpha)(\alpha - \zeta) = d$, e dunque $d \in Inv_E(A)$. Ora, $d \notin \mathbb{Q}$, infatti: $\tau_0(d) = (\alpha - \bar{\zeta})(\bar{\zeta} - \zeta)(\zeta - \alpha) = -d$. Quindi $\mathbb{Q} < \mathbb{Q}[d] \leq Inv_E(A)$; e siccome $Inv_E(A) \neq E$, si deduce che $Inv_E(A) = \mathbb{Q}[d]$. Osserviamo che da $\tau_0(d) = -d$ segue $\tau_0(d^2) = d^2$, e similmente si verifica che $\tau_1(d^2) = d^2$; quindi $d^2 \in Inv_E(\tau_0) \cap Inv_E(\tau_1) = \mathbb{Q}[\alpha] \cap \mathbb{Q}[\zeta] = \mathbb{Q}$. Con un po' di conti, tenendo conto che $a^3 = \alpha - 1$ e delle identità fornite dal confronto dei coefficienti in

$$x^3 - x + 1 = (x - \alpha)(x - \zeta)(x - \bar{\zeta})$$

si trova che $d^2 = -23$. In particolare, $[\mathbb{Q}[d] : \mathbb{Q}] = 2$. Ricapitolando abbiamo trovato che

$$Inv_E(\{\iota\}) = E, \quad Inv_E(G) = \mathbb{Q}, \quad Inv_E(A) = \mathbb{Q}[i\sqrt{23}],$$

$$Inv_E(H_0) = Q[\alpha], \quad Inv_E(H_1) = Q[\zeta], \quad Inv_E(H_2) = Q[\bar{\zeta}]$$

Notiamo come per ogni sottogruppo H di G si abbia $[Inv_E(H) : \mathbb{Q}] = [G : H]$. Questo non è un caso, come vedremo più avanti col teorema fondamentale della teoria di Galois. Quello stesso

Teorema garantisce che, poiché quelli che abbiamo esaminato sono tutti i sottogruppi di $G \simeq S_3$, i campi di invarianti che abbiamo trovato sono tutti i campi intermedi nell'estensione $E|\mathbb{Q}$.

Permutazioni delle radici. Concludiamo questo paragrafo col formalizzare esplicitamente un'osservazione che abbiamo già fatto nel corso dello svolgimento di alcuni degli esempi, che è semplice, ma fondamentale nella pratica.
Sia $E|F$ un'estensione di campi, sia $G = Gal(E|F)$, e $f \in F[x]$. Se $b \in E$ è una radice di f, allora, per ogni $\alpha \in G$, si ha (poiché α fissa i coefficienti di F),

$$f(\alpha(b)) = \alpha(f(b)) = \alpha(0) = 0.$$

Quindi, *gli elementi di $Gal(E|F)$ trasformano le radici in E di ciascun polinomio f a coefficienti in F in radici di f*. In altri termini, per ogni $f \in F[x]$, $Gal(E|F)$ opera come un gruppo di permutazioni sull'insieme delle radici di f in E. Particolarmente significativo è il caso in cui E è il campo di spezzamento di $f \in F[x]$. In questo caso, E è generato da F e dall'insieme $\mathbb{R} = \{b_1, \ldots, b_n\}$ delle radici di f. $G = Gal(E|F)$ oper su R come un gruppo di permutazioni; inoltre, poiché E è generato da R, un F-automorfismo di E che fissa ogni elemento di R è l'identità, pertanto l'azione di G su R è fedele, e quindi G è isomorfo ad un sottogruppo di $Sym(R) = S_n$. Osserviamo infine che se $f \in F[x]$ è irriducibile, F separabile, ed E è un campo di spezzamento, allora $Gal(E|F)$ opera transitivamente sull'insieme R delle radici in E di f; in generale, per campi di spezzamento, le orbite di $Gal(E|F)$ su R sono costituiscono gli insiemi delle radici dei fattori irriducibili di f (in $F[x]$).

ESERCIZI

1. Sia F un campo, ed E campo di spezzamento su F per il polinomio $0 \neq f \in F[x]$. Si provi che $|Gal(E|F)| \leq [E : F]$.

2. Se K e L sono sottocampi del medesimo campo E, denotiamo con $K \vee L$ il minimo sottocampo di E contenete $K \cup L$. Sia $E|F$ un'estensione di campi. Provare che:

i) Se K e L sono campi intermedi di $E|F$, allora $\mathrm{Gal}(E|K) \cap \mathrm{Gal}(E|L) = \mathrm{Gal}(E|K \vee L)$;

ii) Se H e T sono sottogruppi di $Gal(E|F)$, allora $\mathrm{Inv}_E(H) \cap \mathrm{Inv}_E(T) = \mathrm{Inv}_E(\langle H, T\rangle)$.

3. Sia F un campo infinito, e $F(x)$ il suo campo delle frazioni algebriche. Si provi che $\mathrm{Gal}(F(x)|F)$ è infinito.

4. Sia $E = \mathbb{Q}(\sqrt{35}, \sqrt[3]{5})$. Dire se l'estensione $E|\mathbb{Q}$ è normale.

5. Provare che l'estensione $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ è di Galois, e provare che il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})$ è isomorfo al prodotto diretto di due gruppi ciclici di ordine 2.

6. Sia $E = \mathbb{Q}(r)$, dove $r \in \mathbb{C}$ è una radice del polinomio $g = x^3 + x^2 - 2x - 1$. Verificare che anche $r' = r^2 - 2$ è radice di g. Determinare quindi $\mathrm{Gal}(E|\mathbb{Q})$, e provare che $E|\mathbb{Q}$ è un'estensione normale.

7. Sia E il campo di spezzamento del polinomio $f = x^3+3x^2+3$ su $\mathbb{Q}$. Provare che $\mathrm{Gal}(E|\mathbb{Q}) \simeq S_3$.

8. Sia E il campo di spezzamento di $f = x^4 - 7x^3 + 2x - 14$ su $\mathbb{Q}$. Determinare l'ordine del gruppo di Galois $\mathrm{Gal}(E|\mathbb{Q})$. Stessa domanda con $f = x^4 + 2x^2 - 2$.

9. Determinare il gruppo $\mathrm{Gal}(E|\mathbb{Q})$, dove E è campo di spezzamento su $\mathbb{Q}$ per il polinomio $f = x^4 + 1$.

10. Determinare il gruppo $\mathrm{Gal}(E|\mathbb{Q})$, dove E è campo di spezzamento su $\mathbb{Q}$ per il polinomio $f = (x^3 - 2)(x^2 - 3)$.

11. Sia $f \in \mathbb{Q}[x]$, con $\deg f \geq 2$, e sia E campo di spezzamento per f su $\mathbb{Q}$, e sia $G = \mathrm{Gal}(E|\mathbb{Q})$. Provare che $|G| \leq n!$, e che se f non è irriducibile allora $|G| \leq (n-1)!$.

4 Campi finiti

In questo paragrafo descriveremo brevemente le principali caratteristiche dei campi finiti. Iniziamo col ricordare un'utile proprietà numerica dei coefficienti binomiali.
Sia p un primo (positivo) e sia $1 \leq i \leq p-1$. Allora p divide il numeratore ma non il denominatore di

$$\binom{p}{i} = \frac{p(p-1)(p-2)\dots(p-i+1)}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (i-1) \cdot i}$$

e quindi p divide $\binom{p}{i}$.

Lemma 4.1 *Sia F un campo di caratteristica prima p. Allora l'applicazione $\Phi : F \to F$ definita da $\Phi(a) = a^p$, per ogni $a \in F$, è un monomorfismo (di campi).*

Dimostrazione. Constatato che $\Phi(0) = 0$ e $\Phi(1) = 1$, siano $a, b \in F$. Allora, poiché F è commutativo, $\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$. Applicando lo sviluppo di Newton della potenza di un binomio (che vale ancora perché F è commutativo), si ha

$$\Phi(a+b) = (a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Per quanto osservato sopra a proposito dei coefficienti binomiali, e ricordando che, in un anello di caratteristica p, i multipli $p \cdot a$ si annullano, si ricava che, per ogni $i = 1, \dots, p-1$, $\binom{p}{i} a^i b^{p-i} = 0$, e dunque

$$\Phi(a+b) = a^p + b^p = \Phi(a) + \Phi(b)$$

provando pertanto che Φ è un omomorfismo. Poiché F è un campo, $\ker(\Phi) = \{0\}$, e quindi Φ è iniettivo (cioè è un monomorfismo). ∎

Il monomorfismo Φ descritto nel Lemma precedente si chiama *endomorfismo di Frobenius* di F. Se F è finito allora Φ è biettiva (infatti è una applicazione iniettiva da un insieme finito in sé, ed è quindi suriettiva) e pertanto è un automorfismo di F. Osserviamo inoltre che per ogni $k \geq 0$, ed ogni $a \in F$

$$\Phi^k(a) = a^{p^k}.$$

Sia ora p un primo fissato e $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ il campo con p elementi. Per $1 \leq n \in \mathbb{N}$ denotiamo con $GF(p^n)$ il campo di spezzamento su $\mathbb{Z}_p$ del polinomio

$$f = x^{p^n} - x$$

(GF sta per Galois Field). Sia $D \subseteq GF(p^n)$ l'insieme delle radici di f. Ricordando che per il Teorema di Eulero-Fermat, $a^p = a$ per ogni $a \in \mathbb{Z}_p$, si osserva subito che $\mathbb{Z}_p \subseteq D$. Inoltre, poiché

$$f' = p^n x^{p^n-1} - 1 = -1$$

(infatti anche la caratteristica di $\mathbb{Z}_p[x]$ è p), il Lemma 2.8 assicura che le radici di f sono tutte semplici e dunque, per il teorema di Ruffini, $|D| = p^n$. Siano ora $a, b \in D$, con $b \neq 0$; allora, per il lemma 4.1 (opportunamente reiterato)

$$f(ab^{-1}) = (ab^{-1})^{p^n} - ab^{-1} = a^{p^n}(b^{-1})^{p^n} - ab^{-1} = ab^{-1} - ab^{-1} = 0$$

$$f(a-b) = (a-b)^{p^n} - (a-b) = a^{p^n} - b^{p^n} - (a-b) = (a^{p^n} - a) - (b^{p^n} - b) = 0.$$

Dunque, ab^{-1} e $a-b$ appartengono a D, e pertanto D è un sottocampo di $GF(p^n)$. Poiché $GF(p^n)$ è il campo generato da $\mathbb{Z}_p$ e da D, si conclude che $D = GF(p^n)$. In particolare, $|GF(p^n)| = p^n$. Abbiamo così provato la prima parte del seguente risultato.

Teorema 4.2

(1) Sia p un primo e sia $1 \leq n \in \mathbb{N}$. Allora esiste un campo di ordine p^n.

(2) Due campi finiti dello stesso ordine sono isomorfi.

Dimostrazione. Rimane da dimostrare il punto (2). Poiché (Proposizione 1.1) ogni campo finito ha ordine una potenza di un primo, è sufficiente provare che ogni campo F di ordine p^n (p primo e $1 \leq n \in \mathbb{N}$) è isomorfo a $GF(p^n)$. Innanzi tutto, poiché il sottoanello fondamentale di F è il campo $\mathbb{Z}_p$, si ha che F è un'estensione di $\mathbb{Z}_p$. Ora, il gruppo moltiplicativo F^* degli elemento non nulli di F ha ordine $|F| - 1 = p^n - 1$. Ricordando che se G è un gruppo finito e $g \in G$ allora $g^{|G|} = 1$, si ha $a^{p^n-1} = 1$ per ogni $a \in F^*$, e quindi (tenendo conto che $0^{p^n} = 0$),

$$a^{p^n} = a$$

per ogni $a \in F$. Quindi gli elementi di F sono tutti radici del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$. Poiché $|F| = p^n$ si conclude che F è un campo di spezzamento su $\mathbb{Z}_p$ per $x^{p^n} - x$, e dunque è isomorfo a $GF(p^n)$. ∎

Ci proponiamo ora di dire qualcosa a proposito dell'estensione $E|\mathbb{Z}_p$, dove $E = GF(p^n)$. Innanzi tutto, osserviamo che

$$[GF(p^n) : \mathbb{Z}_p] = n.$$

Infatti se $d = [GF(p^n) : \mathbb{Z}_p]$, allora $GF(p^n)$ *come spazio vettoriale su* $\mathbb{Z}_p$ è isomorfo a $\mathbb{Z}_p^{(d)}$ (l'insieme delle d-uple ordinate a coefficienti in $\mathbb{Z}_p$) e dunque, confrontando gli ordini, si ha $d = n$.
Sia Φ l'automorfismo di Frobenius di $E = GF(p^n)$. Poiché, per il Teorema di Eulero-Fermat, $\Phi(a) = a^p = a$ per ogni $a \in \mathbb{Z}_p$, Φ è un $\mathbb{Z}_p$-automorfismo, cioè $\Phi \in Gal(E|\mathbb{Z}_p)$. Ora, come abbiamo osservato sopra, per ogni $b \in E$,

$$\Phi^n(b) = b^{p^n} = b$$

e quindi $\Phi^n = \iota_E$. Mentre, se $1 \leq k < n$, esiste almeno un $b \in E$ tale che $\Phi^k(b) = b^{p^k} \neq b$ (dato che il polinomio $x^{p^k} - x$ ha al più p^k radici in E), e quindi $\Phi^k \neq \iota$. Dunque, nel gruppo $Gal(E|\mathbb{Z}_p)$, $|\langle\Phi\rangle| = n$.
D'altra parte, per il Teorema 3.2, $|Gal(E|\mathbb{Z}_p)| = [E : \mathbb{Z}_p] = n$. Quindi

$$Gal(E|\mathbb{Z}_p) = \langle\Phi\rangle = \{\iota, \Phi, \Phi^2, \ldots, \Phi^{n-1}\}.$$

La dimostrazione dell'esistenza di campi finiti di ordine p^n che abbiamo dato è abbastanza concettuale. Di fatto, per costruire un campo di tale ordine si procede nel modo seguente. Si trova un polinomio *irriducibile* $f \in \mathbb{Z}_p[x]$ di grado n, e uno c'è senz'altro tra i fattori irriducibili di $x^{p^n} - x$ (questa affermazione verrà chiarita tra poco). Quindi si considera il campo $E = \mathbb{Z}_p[x]/(f)$. Poiché gli elementi di E si scrivono tutti in modo unico nella forma

$$a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + (f) \qquad (a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_p)$$

si conclude che $|E| = p^n$.

Esempio. Poichè il polinomio $x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ non ha radici in $\mathbb{Z}_5$, esso non ha fattori di grado 1 in $\mathbb{Z}_5[x]$, e quindi è irriducibile in $\mathbb{Z}_5[x]$. Dunque

$$E = \frac{\mathbb{Z}_5[x]}{(x^3 + x + \overline{1})}$$

è un campo di ordine $5^3 = 125$ (e pertanto coincide col campo di spezzamento del polinomio $x^{125} - x$ su $\mathbb{Z}_5$).

Gruppo moltiplicativo di un campo.

In questo paragrafo dimostriamo la seguente importante proprietà del gruppo moltiplicativo degli elementi non nulli di un campo.

Teorema 4.3 *Ogni sottogruppo* **finito** *del gruppo moltiplicativo di un campo è ciclico.*

Per la dimostrazione di questo Teorema abbiamo biosogna di una caratterizzazione dei gruppi ciclici, che è fornita dal seguente Lemma.

Lemma 4.4 *Sia G un gruppo commutativo finito di ordine n. Se per ogni divisore d di n, G ha al più un sottogruppo di ordine d, allora G è ciclico.*

DIMOSTRAZIONE. Sia G un gruppo di ordine n che soddisfa alle ipotesi del Lemma. Allora $G = P_1 \times P_2 \times \cdots \times P_s$, dove i P_i è (l'unico) p_i-sottogruppo di Sylow di G per ogni divisore primo p_i di n. Chiaramente ogni P_i soddisfa le ipotesi del Lemma e poichè il prodotto di gruppi ciclici di ordine coprimo è ciclico, è sufficiente provare il Lemma nel caso in cui G è un p-gruppo per un primo p. In tal caso, sia $g \in G$ un elemento del massimo ordine possibile $|g| = p^m$. Sia $y \in G$, con $|y| = p^s$; per la scelta di g si ha $s \leq m$. Ora $T =< g^{p^{m-s}} >$ è un sottogruppo di $< g >$ e quindi di G di ordine p^s. Poiché, per ipotesi, G ha un unico sottogruppo di ordine p^s, deve essere $T =< y >$ e quindi $y \in < g >$. Dunque $G =< g >$ è un gruppo ciclico, e il Lemma è provato. ∎

DIMOSTRAZIONE DEL TEOREMA 4.3. Sia F un campo, e sia G un sottogruppo finito del gruppo moltiplicativo F^*. Sia $|G| = n$; proviamo che G soddisfa le ipotesi del Lemma 4.4. G è commutativo perchè tale è il gruppo moltiplicativo di un campo. Sia d un divisore di n e sia $T \leq G$ con $|T| = d$. Allora, per ogni $a \in T$ si ha $a^d = 1$. Quindi ogni $a \in T$ è una radice in F del polinomio $x^d - 1 \in F[x]$. Poichè F è un campo, il numero di radici di tale polinomio è al più $d = |T|$. Quindi T coincide con l'insieme delle radici in F del polinomio $x^d - 1$. Questo prova che G ha al più un sottogruppo di ordine d. Per il Lemma 4.4, G è ciclico. ∎

Esempio 1. Sia $n \geq 2$ e sia U_n l'insieme delle radici complesse n-esime dell'unità. Allora U_n è un sottogruppo del gruppo moltiplicativo $\mathbb{C}^*$ e contiene esattamente n elementi. Dunque U_n è un gruppo ciclico di ordine n (rispetto alla moltiplicazione). Per quanto sappiamo sui gruppi ciclici, il numero di generatori di U_n è $\phi(n)$ dove ϕ è la funzione di Eulero. I generatori di U_n si sono le radici n-esime **primitive** dell'unità, ovvero i numeri complessi

$$cos\frac{2k\pi}{n} + i \cdot sin\frac{2k\pi}{n}$$

con $1 \leq k \leq n-1$ e $(k, n) = 1$.

Esempio 2. Consideriamo il campo di ordine 125

$$E = \frac{\mathbb{Z}_5[x]}{(x^3 + x + \overline{1})}$$

costruito in un precedente esempio. Il suo gruppo moltiplicativo E^* è un gruppo ciclico di ordine $124 = 4 \cdot 31$. Sia α un suo generatore; dunque $E^* =< \alpha >= \{1, \alpha, \alpha^2, \ldots, \alpha^{123}\}$. Notiamo che posto $\beta = \alpha^{31}$ allora $\langle\beta\rangle$ è un sottogruppo di E^* di ordine 4 e quindi i suoi elementi sono radici del polinomio $x^4 - 1$; d'altra parte, per il teorema di Fermat, ogni elemento non nullo $a \in \mathbb{Z}_5$ è tale che $a^4 = 1$; quindi si ha $\langle\beta\rangle = \mathbb{Z}_5 \setminus \{0\}$.

Naturalmente, l'esempio 2 si generalizza ad un qualsiasi campo finito. Se p è un primo e $E = GF(p^n)$, allora il gruppo moltiplicativo E^* degli elementi non nulli di E è ciclico ed ha ordine $p^n - 1$. I suoi generatori (ce ne sono in numero di $\phi(p^n - 1)$) si chiamano

elementi primitivi del campo finito E. Se α è un tale elemento primitivo, gli elementi non nulli di E sono quindi tutti potenze di α, e questo procura una rappresentazione degli elementi di E particolarmente utile in alcune applicazioni computazionali (ma, computazionalmente, trovare α non è una cosa facile).
Osserviamo infine che se α è un elemento primitivo del campo $GF(p^n)$, allora chiaramente $GF(p^n) = \mathbb{Z}_p(\alpha)$. Siccome $[GF(p^n) : \mathbb{Z}_p] = n$, il polinomio minimo f di α su $\mathbb{Z}_p$ ha grado n. Poiché α (in quanto elemento di $GF(p^n)$) è anche una radice di $g = x^{p^n} - x$, si ha che f divide g. Dunque, come avevamo già sostenuto in precedenza, $x^{p^n} - x$ ammette un fattore irriducibile di grado n.

Anche l'esempio 1 si può considerare a partire da un qualsiasi campo F. Sia $n \geq 1$, e supponiamo inoltre, se $charF = p$, che n sia coprimo con p. Allora le radici del polinomio $f = x^n - 1_F$ in un suo campo di spezzamento E sono tutte semplici, dato che $f' = nx^{n-1} \neq 0$ non ha radici in comune con f, e costituiscono un sottogruppo U di ordine n del gruppo moltiplicativo di E. Per il Teorema 4.3, U è un gruppo ciclico. I suoi generatori si chiamano *radici primitive n-esime* sul campo F.

ESERCIZI

1. Si determini il numero di fattori irriducibili di $x^{125} - x$ in $\mathbb{Z}_5$[x].

2. Dire quanti sono i polinomi irriducibili di grado 2 in $\mathbb{Z}_p[x]$ (p un primo).

3. Si costruiscano campi di ordine 8, 27, 81 e 121.

4. Siano $1 \leq m \leq n \in \mathbb{N}$, e sia p un numero primo. Si provi che esiste un monomorfismo $GF(p^m) \to GF(p^n)$ se e solo se $m|n$.

5. Sia E un campo di ordine p^n e sia $g \in \mathbb{Z}_p[x]$ un polinomio irriducibile di grado m, con $m|n$. Si provi che g ha una radice in E.

6. Si provi che ogni estensione di campi finiti è normale.

7. Sia E un campo di ordine 125. Dire quante radici hanno in E i seguenti polinomi:
$x^3 - 1,\ x^4 - 1,\ x^{31} - 1,\ x^7 - 1$. Provare che $x^2 + x + 1$ è irriducibile in $E[x]$.

8. Sia F un campo finito di caratteristica p, e sia $f \in F[x]$. Si provi che $f' = 0$ se e solo se $f \in F[x^p]$. Ricordando che se F è finito allora il suo endomorfismo di Frobenius è un automorfismo, e che quindi $F = F^p = \{a^p \mid a \in F\}$, dedurre che se $f \in F[x]$ ha grado almeno 1 e $f' = 0$, allora esiste $g \in F[x]$ tale che $f = g^p$. Concludere che se F è un campo finito ogni polinomio di $F[x]$ è separabile.

9. Sia F un campo di caratteristica p, e sia $a \in F$. Si provi che se $a \notin F^p$, allora $x^p - a$ è irriducibile in $F[x]$, ma ha un'unica radice in un suo campo di spezzamento. Si deduce che se $F = \mathbb{Z}_p(t)$ è il campo delle frazioni algebriche su $\mathbb{Z}_p$, allora $x^p - t \in F[x]$ è un polinomio irriducibile ma non separabile.

10. Sia F un campo finito di ordine $q = p^n$. Si provi che

i) se $p = 2$, ogni elemento di F è un quadrato;

ii) se $p > 2$, allora F contiene esattamente $\frac{q+1}{2}$ elementi che sono quadrati ;

iii) se $p > 2$, allora gli elementi di F che sono quadrati sono tutte e sole le radici del polinomio $x^{(q+1)/2} - x$. [sugg.: si studi la applicazione $F \to F$ definita da $a \mapsto a^2$ per ogni $a \in F$].

11. Si provi che in un campo finito ogni elemento é somma di due quadrati.

5 Connessione di Galois

In questo capitolo dimostreremo il teorema fondamentale della Teoria di Galois. Iniziamo con un risultato tecnico ma utile.

Lemma 5.1 (Lemma di Artin) *Sia G un gruppo finito di automorfismi del campo E, e sia $F = \mathrm{Inv}_E(G)$. Allora $[E : F] \leq |G|$.*

Dimostrazione. Sia $|G| = n$, e sia $G = \{g_1 = \iota, g_2, \ldots, g_n\}$. Siano $x_1, x_2, \ldots, x_{n+1}$ elementi di E, e consideriamo il sistema di equazioni lineari su E

$$\begin{cases} g_1(x_1)t_1 + g_1(x_2)t_2 + \ldots + g_1(x_{n+1})t_{n+1} = 0 \\ g_2(x_1)t_1 + g_2(x_2)t_2 + \ldots + g_2(x_{n+1})t_{n+1} = 0 \\ \cdot \\ \cdot \\ g_n(x_1)t_1 + g_n(x_2)t_2 + \ldots + g_n(x_{n+1})t_{n+1} = 0 \end{cases} \tag{2}$$

che è un sistema omogeneo con n equazioni e $n + 1$ incognite. Per la teoria generale dei sistemi di equazioni lineari (che vale sopra un campo qualunque), tale sistema ammette soluzione non nulla $(y_1, y_2, \ldots, y_{n+1}) \neq (0, 0, \ldots, 0)$ ad elementi in E. Tra queste soluzioni ne scegliamo una $(b_1, b_2, \ldots, b_{n+1})$ con il massimo numero possibile di zeri; osservando che, eventualmente riordinando gli x_i, possiamo suppore $b_1 \neq 0$, e moltiplicando poi per b^{-1} (dato che il sistema è omogeneo) possiamo supporre che $b_1 = 1$. Quindi, per ogni $1 \leq j \leq n$,

$$g_j(x_1)b_1 + g_j(x_2)b_2 + \ldots + g_j(x_{n+1})b_{n+1} = 0.$$

Sia $g \in G$. Applicando g all'identità di sopra

$$gg_j(x_1)g(b_1) + gg_j(x_2)g(b_2) + \ldots + gg_j(x_{n+1})g(b_{n+1}) = 0. \tag{3}$$

per ogni $1 \leq j \leq n$. Poiché G è un gruppo, $\{gg_1, gg_2, \ldots, gg_n\} = G$, e quindi le identità (3) significano che la $(n+1)$-upla di elementi di E $(g(b_1), g(b_2), \ldots, g(b_n))$ è una soluzione del sistema (2). Dunque, anche

$$(g(b_1) - b_1,\ g(b_2) - b_2,\ \ldots,\ g(b_{n+1}) - b_{n+1}) \tag{4}$$

è soluzione di (2). Ora, poiché g è isomorfismo di E, se $b_i = 0$ si ha $g(b_i) - b_i = 0$, e inoltre $g(b_1) - b_1 = g(1) - 1 = 1 - 1 = 0$. Dunque, la soluzione (4) ha un numero di zeri maggiore di $(b_1, \ldots, b_{n+1})$ e quindi, per la scelta di quest'ultima, la (4) deve essere la soluzione nulla; cioè, per ogni $i = 1, \ldots, n+1$,

$$g(b_i) = b_1.$$

Ciò vale per ogni $g \in G$, e quindi $b_i \in F = \mathrm{Inv}_E(G)$ per ogni $i = 1, \ldots, n+1$. Ricordando che avevamo posto $g_1 = \iota$ la prima equazione del sistema (2) dà allora

$$x_1 b_1 + x_2 b_2 + \ldots + x_{n+1} b_{n+1} = 0$$

con i $b_i \in F$ non tutti nulli. Questo prova che gli $n+1$ elementi $x_1, x_2, \ldots, x_{n+1}$ di E sono linearmente dipendenti su F. Quindi, come spazio vettoriale su F, la dimensione di E è al più n, ovvero $[E : F] \leq n$. ∎

Ricordiamo che un'estensione di campi $E|F$ si dice di Galois se è finita, normale e separabile. In particolare se $char(F) = 0$ ed E è un campo di spezzamento per un polinomio su F, allora $E|F$ è un'estensione di Galois.

Lemma 5.2 *Sia $E|F$ un'estensione di Galois e $F \leq L \leq E$ un campo intermedio. Allora $E|L$ è un'estensione di Galois.*

Dimostrazione. Sia $E|F$ di Galois e L campo con $F \leq L \leq E$. Poiché $[E : F] < \infty$, anche $[E : L] < \infty$. Sia $g \in L[x]$ un polinomio irriducibile monico che ha una radice $b \in E$. Sia $f \in F[x]$ il polinomio minimo di b su F. Poiché g è il polinomio minimo di b su L si ha che, in $L[x]$, g divide f. Siccome $E|F$ è normale, E contiene un campo di spezzamento per f su F, e quindi contiene un campo di spezzamento per g su L. Ciò prova che $E|L$ è un'estensione normale.
Infine, sia $u \in E$ e sia $g \in L[x]$ il polinomio minimo di u su L; mostriamo che g è separabile (cioè che ha tutte radici semplici in un suo campo di spezzamento). Come prima, sia f il polinomio minimo di u su F. Allora, in $L[x]$, $g|f$. Poiché $E|F$ è separabile, f è separabile, e di conseguenza g è separabile. Dunque $E|L$ è un'estensione separabile, e pertanto è un'estensione di Galois. ∎

Proposizione 5.3 *Sia $E|F$ un'estensione finita di campi, e sia $G = \mathrm{Gal}(E|F)$ un gruppo finito. Allora sono equivalenti*

(i) *$E|F$ è un'estensione di Galois;*

(ii) *$F = \mathrm{Inv}_E(G)$.*

Dimostrazione. (i) $\Rightarrow$ (ii). Sia $E|F$ estensione di Galois. Allora, per il Teorema 3.3, si ha $|G| = [E : F]$. D'altra parte, per definizione di F-isomorfismo, F è contenuto in $\mathrm{Inv}_E(G)$, e chiaramente $\mathrm{Gal}(E|\mathrm{Inv}_E(G)) = G$. Per il Lemma 5.2, anche $E|\mathrm{Inv}_E(G)$ è un'estensione di Galois, e quindi $[E : \mathrm{Inv}_E(G)] = |\mathrm{Gal}(E|\mathrm{Inv}_E(G))| = |G|$. Dunque $[E : F] = [E : \mathrm{Inv}_E(G)]$, e pertanto $\mathrm{Inv}_E(G) = F$.

(ii) $\Rightarrow$ (i). Sia $F = \mathrm{Inv}_E(G)$, e sia $G = \{\eta_1 = \iota_E, \eta_2, \ldots, \eta_n\}$. Sia $g \in F[x]$ un polinomio monico irriducibile su F che ha una radice $b \in E$. Consideriamo il polinomio

$$f = (x - \eta_1(b))(x - \eta_2(b)) \ldots (x - \eta_n(b)) \in E[x].$$

Per ogni $\eta \in G$, la moltiplicazione a sinistra per η è una permutazione di G, e quindi (considerando l'estensione canonica di η a $E[x]$,

$$\eta(f) = (x - \eta\eta_1(b))(x - \eta\eta_2(b)) \ldots (x - \eta\eta_n(b)) = f.$$

Dunque i coefficienti di f sono tutti elementi di E fissati da η; ciò vale per ogni $\eta \in G$, per cui i coefficienti di f appartengono a $\mathrm{Inv}_E(G) = F$, cioè $f \in F[x]$. Ma f ammette $b = \eta_1(b)$ come radice e dunque il polinomio minimo g di b divide f. Da ciò segue che g si fattorizza in $E[x]$ come prodotto di fattori lineari, e quindi che E contiene un campo di spezzamento per g. Pertanto $E|F$ è un'estensione normale.
Similmente procediamo per provare la separabilità. Sia $b \in E$, e sia $g \in F[x]$ il suo polinomio minimo. Per ogni $\eta \in G$, $g(\eta(b)) = \eta(g(b)) = 0$, cioè $\eta(b)$ è un radice di g. Sia $A = \{b = b_1, b_2, \ldots, b_k\}$ l'insieme di tutte le radici *distinte* di g che si ottengono come immagine di b tramite un elemento di G. Allora, per ogni $\eta \in G$, $\eta(A) \subseteq A$, e poiché η è iniettivo, $\eta(A) = A$. Poniamo $f = (x - b_1)(x - b_2) \ldots (x - b_k) \in E[x]$. Per il teorema di Ruffini $f|g$ in $E[x]$ e, per quanto osservato sopra, $\eta(f) = f$ per ogni $\eta \in G$. Dunque, come prima, i coefficienti di f sono invarianti per ogni $\eta \in G$, e quindi $f \in F[x]$. Siccome f ammette $b = b_1$ come radice si ha che $g|f$. Pertanto $g = f$, e dunque le radici di g sono semplici, provando così che $E|F$ è separabile. Poiché $E|F$ è finita per ipotesi, si conclude che $E|F$ è un'estensione di Galois. ∎

Teorema 5.4 (Fondamentale della Teoria di Galois) *Sia $E|F$ un'estensione di Galois, e sia $G = \mathrm{Gal}(E|F)$. Siano $\mathcal{S}$ l'insieme di tutti i sottogruppi di G, e $\mathcal{F}$ l'insieme di tutti i campi L con $F \leq L \leq E$. Allora le applicazioni:*

$$\begin{array}{rccc} \mathrm{Gal}(E, \cdot): & \mathcal{F} & \to & \mathcal{S} \\ & L & \mapsto & \mathrm{Gal}(E|L) \end{array} \qquad \begin{array}{rccc} \mathrm{Inv}_E: & \mathcal{S} & \to & \mathcal{F} \\ & H & \mapsto & \mathrm{Inv}_E(H) \end{array}$$

sono l'una l'inversa dell'altra. Inoltre, valgono le seguenti proprietà per ogni $H, K \in \mathcal{S}$,

(1) $H \leq K$ se e solo se $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$;

(2) $|H| = [E : \mathrm{Inv}_E(H)]$ e $[G : H] = [\mathrm{Inv}_E(H) : F]$;

(3) H è normale in G se e solo se $\mathrm{Inv}_E(H)|F$ è un'estensione normale. In tal caso, $\mathrm{Gal}(\mathrm{Inv}_E(H)|F) \simeq G/H$.

Dimostrazione. Sia H un sottogruppo di $G = \mathrm{Gal}(E|F)$, allora $\mathrm{Inv}_E(H) \in \mathcal{F}$. Poniamo $H' = \mathrm{Gal}(E|\mathrm{Inv}_E(H))$. Poiché, per definizione, ogni automorfismo in H fissa ogni elemento di $Inv_E(H)$, si ha $H \leq H'$. Ora, poiché per il Lemma 5.2, $E|\mathrm{Inv}_E(H)$ è un'estensione di Galois, dal Teorema 3.3 segue $|H'| = [E : \mathrm{Inv}_E(H)]$; d'altra parte, per il Lemma di Artin, $[E : \mathrm{Inv}_E(H)] \leq |H|$. Quindi $|H'| \leq |H|$, e siccome $H \leq H'$ si conclude che $H' = H$.

Sia ora L un campo intermedio di $E|F$, allora $\mathrm{Gal}(E|L) \leq G$. Sia $L' = \mathrm{Inv}_E(\mathrm{Gal}(E|L))$. Per definizione di $\mathrm{Gal}(E|L)$ si ha chiaramente $L \subseteq L'$. Ma, per il punto precedente,

$\mathrm{Gal}(E|L') = \mathrm{Gal}(E|L)$. Poiché $E|L$ ed $E|L'$ sono entrambe estensioni di Galois, per il Teorema 3.3 si ha $[E : L] = |\mathrm{Gal}(E|L)| = |\mathrm{Gal}(E|L')| = [E : L']$; dunque $[L' : L] = 1$, cioè $L' = L$.

Abbiamo così provato che le applicazioni $\mathrm{Gal}(E, \cdot\ )$ e Inv_E sono l'una l'inversa dell'altra, e quindi che esse stabiliscono una corrispondenza biunivoca tra gli insiemi $\mathcal{S}$ e $\mathcal{F}$. Proviamo ora gli altri punti dell'enunciato.

(1) Siano $H, K \leq G$. Se $H \leq K$ allora chiaramente $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$. Viceversa, sia $\mathrm{Inv}_E(H) \supseteq \mathrm{Inv}_E(K)$; allora $\mathrm{Gal}(E|\mathrm{Inv}_E(H)) \leq \mathrm{Gal}(E|\mathrm{Inv}_E(K))$, e per quanto provato sopra

$$H = \mathrm{Gal}(E|\mathrm{Inv}_E(H)) \leq \mathrm{Gal}(E|\mathrm{Inv}_E(K)) = K.$$

(2) Sia $H \leq G$. Per quanto già provato: $|G| = [E : F]$, $H = \mathrm{Gal}(E|\mathrm{Inv}_E(H))$ e quindi (poiché $E|\mathrm{Inv}_E(H)$ è di Galois) $|H| = [E : \mathrm{Inv}_E(H)]$. Applicando la formula dei gradi ed il Teorema di Lagrange per l'ordine dei sottogruppi di un gruppo finito si ha

$$[G : H] = \frac{|G|}{|H|} = \frac{[E : F]}{[E : \mathrm{Inv}_E(H)]} = [\mathrm{Inv}_E(H) : F].$$

(3) Sia N un sottogruppo normale di G, e poniamo $L = \mathrm{Inv}_E(N)$. Allora, per ogni $\eta \in N$ ed ogni $\sigma \in G$, si ha $\sigma^{-1}\eta\sigma \in N$. Quindi, se $b \in L$, $b = \sigma^{-1}\eta\sigma(b)$, da cui, applicando σ, si deduce che, per ogni $b \in L$ ed ogni $\eta \in N$, $\sigma(b) = \eta(\sigma(b))$, ovvero $\sigma(b) \in L$, e quindi $\sigma(L) \subseteq L$. Poiché, allo stesso modo, $\sigma^{-1}(L) \subseteq L$, si ha $\sigma(L) = L$. Dunque, la restrizione definisce un'applicazione

$$\begin{array}{rccc} \Phi: & G & \to & \mathrm{Gal}(L|F) \\ & \sigma & \mapsto & \sigma_{|L} \end{array}$$

che facilmente si verifica essere un omomorfismo di gruppi. Ora

$$\ker(\Phi) = \{\sigma \in G \mid \sigma_{|L} = \iota_L\} = \mathrm{Gal}(E|L) = \mathrm{Gal}(E|\mathrm{Inv}_E(N)) = N.$$

Per il teorema di omomorfismo per gruppi, si ha quindi $G/N \simeq Im(\Phi)$. Inoltre,

$$\mathrm{Inv}_L(\mathrm{Gal}(L|F)) \subseteq \mathrm{Inv}_L(\Phi(G)) = L \cap \mathrm{Inv}_E(G) = L \cap F = F,$$

quindi $\mathrm{Inv}_L(\mathrm{Gal}(L|F)) = F$, e per la Proposizione 5.3 si deduce che $L|F$ è un'estensione di Galois. In particolare è normale e

$$|\mathrm{Gal}(L|F)| = [L : F] = \frac{[E : F]}{[E : L]} = \frac{|\mathrm{Gal}(E|F)|}{|\mathrm{Gal}(E|L)|} = \frac{|G|}{|N|} = |G/Ker(\Phi))|$$

da cui segue che Φ è suriettiva, e $\mathrm{Gal}(L|F) \simeq G/N$.

Viceversa, sia $H \leq G$ tale che $L = \mathrm{Inv}_E(H)$ è estensione normale di F. Allora $L|F$ è di Galois dato che è sicuramente separabile, essendo L contenuto in E. Siano $\gamma \in G$ e $b \in L$. Sia $f \in F[x]$ il polinomio minimo di b su F. Poiché $L|F$ è normale L contiene un campo di spezzamento per f su F; in particolare contiene tutte le radici di f che appartengono ad E. Ora, essendo γ un F-isomorfismo, $f(\gamma(b)) = \gamma(f(b)) = 0$. Dunque, per quanto osservato sopra $\gamma(b) \in L$, e ciò vale per ogni $b \in L$. Pertanto, come prima, la restrizione $\gamma \mapsto \gamma_{|L}$ è un omomorfismo Φ del gruppo G nel gruppo $Gal(L|F)$, e chiaramente $H \leq Ker(\Phi)$; posto $K = Ker(\Phi)$, gli elementi di K sono gli automorfismi

di E che inducono l'identità su L, quindi per il punto (1), $L \subseteq \mathrm{Inv}_E(K) \subseteq \mathrm{Inv}_E(H) = L$. Dunque $L = \mathrm{Inv}_E(K)$ e, di conseguenza, $H = \mathrm{Gal}(E|L) = \mathrm{Gal}(E|\mathrm{Inv}_E(K)) = K$ che è un sottogruppo normale di G. ∎

Esempio 1. Sia $\omega \in \mathbb{C}$ una radice primitiva 11-esima dell'unità (e.g. $\omega = \cos\frac{2\pi}{11} + i\sin\frac{2\pi}{11}$), e sia $U = \{\omega^k \mid 0 \leq k \leq 10\}$ l'insieme di tutte le radici 11-esime dell'unità. U è un sottogruppo ciclico del gruppo moltiplicativo $\mathbb{C}^*$. Ora, il polinomio minimo di ω su $\mathbb{Q}$ è il polinomio *ciclotomico*

$$\Phi_{11}(x) = x^{10} + x^9 + \ldots + x^2 + x + 1.$$

Sia $E \leq \mathbb{C}$ il suo campo di spezzamento. Allora $E|\mathbb{Q}$ è un'estensione di Galois (detta estensione ciclotomica di grado 11); sia $G = \mathrm{Gal}(E|\mathbb{Q})$ il suo gruppo di Galois. Poiché l'insieme di tutte le radici complesse di $\Phi_{11}(x)$ è $U \setminus \{1\}$, si ha $E = \mathbb{Q}[\omega]$, e quindi

$$|G| = [E : \mathbb{Q}] = [\mathbb{Q}[\omega] : \mathbb{Q}] = \deg \Phi_{11}(x) = 10.$$

Se $\alpha \in G$, allora $\alpha(U) = U$, e quindi (essendo un automorfismo di campo), α induce un automorfismo $a_{|U}$ del gruppo ciclico U (che, come gruppo, è isomorfo a $\mathbb{Z}/11\mathbb{Z}$). Inoltre, è chiaro che α è univocamente individuato dall'immagine $\alpha(\omega) \in U \setminus \{1\}$. Siccome $|G| = 10 = |U \setminus \{1\}|$, concludiamo che per ogni $1 \leq k \leq 10$, esiste uno ed un solo $\eta_k \in G$ tale che $\eta_k(\omega) = \omega^k$ (cosa che si poteva anche direttamente dedurre dal Lemma 2.3).
Poniamo $\eta = \eta_2$ (ovvero l'automorfismo di E tale che $\omega \mapsto \omega^2$). Ora per $t \geq 1$,

$$\eta^t(\omega) = \omega^{2^t}.$$

Quindi, $\eta^n = \iota = 1_G$ se e solo se $\omega^{2^n} = 1$, ovvero se e solo se $2^n \equiv 1 \pmod{11}$. Poiché il minimo intero $n \geq 1$ per cui ciò si verifica è $n = 10$, concludiamo che l'ordine di η nel gruppo G è 10. Quindi $G = \langle\eta\rangle$, e G è un gruppo ciclico.
Per quanto conosciamo sui gruppi ciclici, per ogni divisore d di 10, G ammette uno ed un solo sottogruppo di ordine d. Precisamente, i sottogruppi di $G = \langle\eta\rangle$ sono

$$G_1 = G = \langle\eta\rangle \qquad G_2 = \langle\eta^2\rangle \qquad G_3 = \langle\eta^5\rangle \qquad G_4 = \{\iota\},$$

di ordine, rispettivamente, 10, 5, 2 e 1. Siano $F_i = \mathrm{Inv}_E(G_i)$ $(i = 1, 2, 3, 4)$ i corrispondenti campi degli invarianti. Per il Teorema 5.4, questi sono tutti e soli i campi intermedi dell'estensione $E|\mathbb{Q}$. Abbiamo poi, per ogni i,

$$[F_i : \mathbb{Q}] = [\mathrm{Inv}_E(G_i) : \mathbb{Q}] = [G : G_i] = 10/|G_i|.$$

In particolare $[F_2 : \mathbb{Q}] = 2$. In E sia

$$a = \omega + \omega^4 + \omega^5 + \omega^9 + \omega^3 = \omega + \eta^2(\omega) + \eta^4(\omega) + \eta^6(\omega) + \eta^8(\omega).$$

Per come è definito, $\eta^2(a) = a$, e quindi $a \in \mathrm{Inv}_E(\langle\eta^2\rangle) = F_2$. D'altra parte $a \notin \mathbb{Q}$ (altrimenti ω sarebbe radice del polinomio razionale $x^9 + x^5 + x^4 + x^3 + x - a$), e dunque (dato che $[F_2 : \mathbb{Q}]$ è un numero primo) $F_2 = \mathbb{Q}[a]$. Similmente, sia

$$b = \omega + \eta^5(\omega) = \omega + \omega^{10} = \omega + \omega^{-1} = \omega + \overline{\omega}.$$

Allora $b \in \mathrm{Inv}_E(\langle\eta^5\rangle) = F_3$, $b \notin \mathbb{Q}$ e, poiché $[F_3 : \mathbb{Q}] = 5$, $F_3 = \mathbb{Q}[b]$.
Concludendo, se ω è una radice primitiva 11-esima, i campi intermedi dell'estensione ciclotomica $\mathbb{Q}(\omega)|\mathbb{Q}$ di grado 11 sono

$$\mathbb{Q} \qquad \mathbb{Q}(\omega + \omega^3 + \omega^4 + \omega^5 + \omega^9) \qquad \mathbb{Q}(\omega + \omega^{-1}) \qquad \mathbb{Q}(\omega).$$

Osserviamo infine che, poiché in questo caso $Gal(\mathbb{Q}(\omega)|\mathbb{Q})$ è un gruppo abeliano, e quindi tale che ogni suo sottogruppo è normale, per il punto (3) del Teorema 5.4 i campi che abbiamo elencato sopra sono estensioni normali di $\mathbb{Q}$.

Esempio 2. Determinaimo il gruppo di Galois G di $E|\mathbb{Q}$, dove $E \leq \mathbb{C}$ è il campo di spezzamento su $\mathbb{Q}$ del polinomio $f = x^5 - 2$. Innanzi tutto f è irriducibile per il criterio di Eisenstein; in particolare le sue radici in E sono tutte distinte. Inoltre, f ha una radice reale $a = \sqrt[5]{2}$, e

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5.$$

In particolare 5 divide $[E : \mathbb{Q}] = |G|$. Sia $\omega = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ una radice primitiva quinta dell'unità. Allora le radici di f sono

$$a, \quad \omega a, \quad \omega^2 a, \quad \omega^3 a, \quad \omega^4 a \tag{5}$$

e quindi $E = \mathbb{Q}(a, \omega)$. Ora, il polinomio minimo di ω su $\mathbb{Q}$ è $g = x^4 + x^3 + x^2 + x + 1$. Poiché $\mathbb{Q}(\omega)$ è il campo di spezzamento di g su $\mathbb{Q}$, l'estensione $\mathbb{Q}(\omega)|\mathbb{Q}$ è normale, e quindi, per il punto (3) del Teorema 5.4, $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$ è un sottogruppo normale di G, e

$$G/N \simeq \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$$

è un gruppo ciclico di ordine 4 (questo si vede anlalogamente a quanto fatto nell'esempio precedente con una radice 11-esima). In particolare 4 divide $|G|$, e quindi $5 \cdot 4 = 20$ divide $|G| = [E : \mathbb{Q}]$. Ora,

$$[E : \mathbb{Q}] = [\mathbb{Q}(\omega, a) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] \leq [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] \leq 5 \cdot 4 = 20.$$

Dunque, $|G| = [E : \mathbb{Q}] = 20$, e inoltre $[E : \mathbb{Q}(\omega)] = 5$. Pertanto $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$ ha ordine 5. Sia $H = \mathrm{Gal}(E|\mathbb{Q}(a))$; allora $|H| = [E : \mathbb{Q}(a)] = 4$. Quindi $N \cap H = \{1\}$, e $NH = G$. Per il secondo teorema di isomorfismo per gruppi,

$$\frac{G}{N} = \frac{NH}{N} = \frac{H}{N \cap H} = H,$$

e dunque H è un gruppo ciclico. Osserviamo che H non è normale in G; infatti, $\mathrm{Inv}_E(H) = \mathbb{Q}(a)$ che non è un'estensione normale di $\mathbb{Q}$ (dato che $\mathbb{Q}(a)$ contiene una sola radice del polinomio irriducibile f). Di fatto (lo si completi per esercizio) in G il sottogruppo H ha cinque coniugati distinti, che corrispondo ai campi intermedi $\mathbb{Q}(a)$, $\mathbb{Q}(\omega a)$, $\mathbb{Q}(\omega^2 a)$, $\mathbb{Q}(\omega^3 a)$, $\mathbb{Q}(\omega^4 a)$.
Possiamo ora descrivere piuttosto esplicitamente gli elementi di G. Innanazi tutto, osserviamo che un $\mathbb{Q}$-automorfismo di $E = \mathbb{Q}(a, \omega)$ è univocamente determinato dalle immagini di $a = \sqrt[5]{2}$ e di ω. Consideriamo per primo il sottogruppo $N = \mathrm{Gal}(E|\mathbb{Q}(\omega))$; esso è ciclico di ordine 5, sia σ un suo generatore; poiché $\mathrm{Inv}_E(N) = \mathbb{Q}(\omega)$, si ha $\sigma(\omega) = \omega$. Ora, ogni elemento di G manda radici di f in radici di f, ovvero induce una permutazione degli elementi in (5), e dunque $\sigma(a) = \omega^k a$ per qualche $1 \leq k \leq 4$; rimpiazzando eventualmente σ con una sua potenza, possiamo assumere $\sigma(a) = \omega a$. Prendiamo ora in esame $H = \mathrm{Gal}(E|\mathbb{Q}(a))$; anch'esso è ciclico, per cui sia η un suo generatore; allora η ha ordine 4, e poiché $\mathrm{Inv}_E(H) = \mathbb{Q}(a)$, $\eta(a) = a$. Ne segue che η "muove" ω, e siccome $\eta(\omega a) = \omega^t a$ per qualche $1 \leq t \leq 4$, si ha $\eta(\omega) = \omega^t$. Dal fatto che $|\eta| = 4$ segue $t = 2, 3$, e dunque, sostituendo eventualmente η con η^{-1}, possiamo porre $\eta(\omega) = \omega^2$. Poiché $G = NH$ concludiamo che gli elementi di G sono tutti del tipo $\sigma^u\eta^v$ con $0 \leq u \leq 4$ e $0 \leq v \leq 3$, dove

$$\sigma^u\eta^v(\sqrt[5]{2}) = \omega\sqrt[5]{2}$$
$$\sigma^u\eta^v(\omega) = \omega^{2^u}$$

Notiamo anche che $\sigma^\eta = \eta^{-1}\sigma\eta = \sigma^3$. Di passaggio, consideriamo a questo punto l'elemento $b = \sqrt[5]{2} + \omega \in E$, ed osserviamo che nessun $1 \neq \alpha \in G$ fissa b; da ciò segue che $E = \mathbb{Q}(b)$: infatti se fosse $\mathbb{Q}(b) < E$, allora $\mathbb{Q}(b)$ dovrebbe essere il campo degli invarianti di qualche sottogruppo non banale di G, il che non è.
Proviamo infine, a mo' di illustrazione della forza della connessione di Galois, come nell'estensione $E|\mathbb{Q}$ ci sia una sola estensione intermedia di grado 2 su $\mathbb{Q}$. Ciò corrisponde a provare che G ha un solo sottogruppo di indice 2. Sia T un tale sottogrupoo; allora T ha ordine 10 e dunque

contiene un sottogruppo di ordine 5; ma N è l'unico sottogruppo di ordine 5 di G (dato che N è un 5-sottogruppo di Sylow normale di G); dunque $N \leq T$; ma allora T/N è un sottogruppo di ordine 2 di G/N: poiché G/N è ciclico esiste un solo tale sottogruppo, e dunque T è unico (si provi che $T = N\langle\eta^2\rangle$). $L = \mathrm{Inv}_E(T)$ è quindi il solo campo intermedio in $E|\mathbb{Q}$ che ha grado 2 su $\mathbb{Q}$. Ancora $L \leq \mathbb{Q}(\omega)$, da cui segue facilmente che $L = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{5})$.

Gruppo di Galois di un polinomio.

Proposizione 5.5 *Sia F un campo, $f \in F[x]$, e E un campo di spezzamento per f su F. Se f è un polinomio separabile allora $E|F$ è un'estensione di Galois.*

Dimostrazione. Sia $f_1 \in F[x]$ il polinomio ottenuto moltiplicando i fattori irriducibili distinti di f in $F[x]$. Chiaramente, E è un campo di spezzamento per f_1 su F. Poiché f è separabile, e polinomi irriducibili distinti non possono avere radici comuni, le radici di f_1 sono tutte semplici e quindi, per il Teorema 3.2, $|\mathrm{Gal}(E|F)| = [E : F]$. Ma E è anche campo di spezzamento per f su $L = \mathrm{Inv}_E(G)$, e dunque $[E : L] = |\mathrm{Gal}(E|L)|$. Ma chiaramente $G = \mathrm{Gal}(E|L)$; dunque $[E : F] = [E : L]$, e quindi $F = L = \mathrm{Inv}_E(G)$. Poiché $E|F$ è finita, per la Proposizione 5.3 $E|F$ è un'estensione di Galois. ∎

Sia F un campo, $f \in F[x]$ un polinomio separabile ed E un suo campo di spezzamento su F. Allora $\mathrm{Gal}(E|F)$ si chiama **gruppo di Galois del polinomio** f. Ovviamente, esso non dipende dal particolare campo di spezzamento. Come abbiamo già più volte avuto modo di osservare, gli elementi di $G = \mathrm{Gal}(E|F)$ permutano le radici di f, e si verifica subito che ciò definisce un'azione di G sull'insieme Ω delle radici di f; ora, se $\sigma \in G$ fissa tutte le radici di f, siccome fissa anche tutti gli elementi di F, ed E è generato su F dall'aggiunzione delle radici di f, si conclude che σ è l'identità di E. Quindi l'azione di G sull'insieme Ω è un'azione fedele, e pertanto G è isomorfo ad un sottogruppo del gruppo simmetrico $\mathrm{Sym}(\Omega)$, Se $\deg f = n$, allora $|\Omega| \leq n$, e dunque G è isomorfo ad un sottogruppo di S_n.
Supponiamo a questo punto che il polinomio f sia irriducibile su F di grado n. Essendo separabile, le sue n radici nel cammpo di spezzamento E sono distinte. Siano a e b due di tali radici; allora, per il Lemma 2.3 esiste un F-isomorfismo $F[a] \to F[b]$ che manda a in b. Poiché E è campo di spezzamento per f sia su $F[a]$ che su $F[b]$, il Teorema 2.4 assicura che tale isomorfismo può essere esteso ad un F-isomorfismo η di E, cioè ad un elemento $\eta \in Gal(E|F)$. Dunque esiste η nel gruppo di Galois G di f su F tale che $\eta(a) = b$. Pertanto, come gruppo di permutazioni dell'insieme delle radici di f, G è transitivo. Dunque: *il gruppo di Galois di un polinomio irriducibile e separabile di grado n è isomofo ad un sottogruppo transitivo di S_n.*

Nel seguito di questa sezione, daremo un'idea di come trovare, fissato un primo p, polinomi a coefficienti razionali il cui gruppo di Galois (su $\mathbb{Q}$) sia isomorfo al gruppo simmetrico S_p. Iniziamo con un lemma sui gruppi di permutazioni.

Lemma 5.6 *Sia p un numero primo. Sia G un sottogruppo di S_p che contiene un ciclo di ordine p ed una trasposizione. Allora $G = S_p$.*

DIMOSTRAZIONE. Possiamo chiaramente supporre che G contenga la trasposizione $\tau = (1\,2)$. Sia σ un ciclo di ordine p contenuto in G; allora esiste una sua opprtuna potenza $\gamma = \sigma^k$ (con $1 \leq k \leq p-1$) tale che $\gamma(1) = 2$. Ora, poiché p è primo, γ è anch'essa un ciclo di ordine p, sia $\gamma = (1\,2\,i_3 \ldots\, i_p)$ (dove $\{i_3, i_4, \ldots\, i_p\} = \{3, 4, \ldots, p\}$). Quindi, eventualmente riordinando i punti $\{3, 4, \ldots, p\}$, possiamo supporre che $\gamma = (1\,2\,3\,\ldots\,p)$. Ora $\gamma^{-1}\tau\gamma = (2\,3)$, $\gamma^{-1}(2\,3)\gamma = (3\,4)$, e così via, portando a concludere che G contiene tutte le trasposizioni del tipo $(k\,k+1)$ (con $k = 1, \ldots, p-1$). Ma ancora, $(1\,2)(2\,3)(1\,2) = (1\,3)$, da cui iterando segue che G contiene tutte le trasposizioni del tipo $(1\,k)$. Ma allora, per ogni $1 \leq i, j \leq p$, $i \neq j$, si ha $(i\;j) = (1\,i)(1\,j)(1\,i) \in G$. Poiché le trasposizioni generano tutto S_p si conclude che $G = S_p$. ∎

Proposizione 5.7 *Sia p un primo, e f un polinomio irriducibile in $\mathbb{Q}[x]$ di gardo p. Supponiamo che f abbia esattamente due radici non reali nel campo $\mathbb{C}$. Allora il gruppo di Galois di f su $\mathbb{Q}$ è isomorfo a S_p.*

DIMOSTRAZIONE. Sia $E \leq \mathbb{C}$ il campo di spezzamento per f su $\mathbb{Q}$, e denotiamo con G il suo gruppo di Galois, che interpretiamo come un gruppo di permutazioni sull'insieme delle p radici (che sono tutte distinte) di f in E, dunque come sottogruppo del gruppo simmetrico S_p. Sia b una di tali radici; poiché f è irriducibile, $[\mathbb{Q}[b] : \mathbb{Q}] = \deg f = p$. Quindi

$$|G| = [E : \mathbb{Q}] = [E : \mathbb{Q}[b]][\mathbb{Q}[b] : \mathbb{Q}] = [E : \mathbb{Q}[b]] \cdot p.$$

Dunque p divide l'ordine di G, e pertanto (per il teorema di Sylow) G contiene un elemento γ di ordine p. Poiché l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti, si ha che γ (come permutazione delle radici di f) è un ciclo di ordine p. Siano ora u e v le sole due radici non reali di f. Allora $v = \bar{u}$ è il coniugato complesso di u (e $u = \bar{v}$). Dunque l'automorfismo di coniugio in $\mathbb{C}$ fissa tutte le radici reali di f e scambia tra di loro le due radici non reali. Poiché E è generato su $\mathbb{Q}$ dalle radici di f, ne segue che la restrizione τ ad E del coniugio complesso è un $\mathbb{Q}$-automorfismo di E, cioè un elemento di G. Come permutazione dell'insieme delle radici di f, τ fissa tutte le radici reali e scambia u e v, e dunque è una trasposizione in S_p. Quindi G è un sottogruppo di S_p che contiene una trasposizione ed un ciclo di ordine p e pertanto, per il Lemma precedente, $G = S_p$. ∎

Consideriamo ad esempio il polinomio razionale $f = x^5 - 10x + 2$ che, per il criterio di eisenstein, è irriducibile su $\mathbb{Q}$. Per verificare che f soddisfa le ipotesi della Proposizione 5.7 studiamo il garfico della funzione polinomiale reale $y = f(x)$. Siccome il termine di grado massimo nella x è di grado dispari si ha:

$$\lim_{x\to-\infty} f(x) = -\infty \qquad\qquad \lim_{x\to+\infty} f(x) = +\infty$$

Inoltre $y' = 5x^4 - 10 = 5(x^4 - 2)$, e si trova quindi che $y = f(x)$ ha un massimo relativo per $x = -\sqrt[4]{2}$, ed un minimo relativo per $x = \sqrt[4]{2}$. Ora $f(-\sqrt[4]{2}) = -2\sqrt[4]{2} + 10\sqrt[4]{2} + 2 > 0$, e $f(\sqrt[4]{2}) = 2\sqrt[4]{2} - 10\sqrt[4]{2} + 2 < 0$. Quindi il grafico di $y = f(x)$ attraversa una volta l'asse delle x nell'intervallo $(-\sqrt[4]{2},\ \sqrt[4]{2})$, e dunque, complessivamente, incontra esattamente in tre punti l'asse delle x. Pertanto il polinomio $f = x^5 - 10x + 2$ ha esattemente tre radici reali, e di conseguenza in $\mathbb{C}$ ha altre due radici complesse coniugate. Per la Proposizione precedente si ha che il gruppo di Galois di f su $\mathbb{Q}$ è isomnorfo a S_5.

Per ogni primo p è possibile trovare esplicitamente un polinomio irriducibile razionale di grado p che soddisfa alle ipotesi della Proposizione 5.7 (vedi Jacobson: Basica Algebra I, pag. 261)

ESERCIZI

1. Sia $E|F$ un estensione di campi finiti. Si provi che $E|F$ è un'estensione di Galois, e che il suo gruppo di Galois è ciclico.

2. Sia $\omega \in \mathbb{C}$ una radice primitiva 17-esima dell'unità, e sia $E = \mathbb{Q}[\omega]$. Si provi che $E|\mathbb{Q}$ è un'estensione di Galois e si dica qual è l'indice $[E : \mathbb{Q}]$. Si provi quindi che $E|\mathbb{Q}$ ha esattamente 5 campi intermedi (inclusi $\mathbb{Q}$ ed E), e si dimostri che (rispetto all'inclusione) essi formano una catena.

3. Sia $\omega \in \mathbb{C}$ una radice primitiva ottava dell'unità, e sia $E = \mathbb{Q}(\omega)$. Si determini il polinomio minimo di ω su $\mathbb{Q}$, si descriva il gruppo di Galois $\mathrm{Gal}(E|\mathbb{Q})$, e si determinino i campi intermedi dell'estensione $E|\mathbb{Q}$.

4. Si determinino i campi intermedi dell'estensione $E|\mathbb{Q}$, dove $E \leq \mathbb{C}$ è il campo di spezzamento del polinomio $x^7 - 1$ su $\mathbb{Q}$.

5. Sia $n \geq 1$, e siano $\zeta_1, \zeta_2, \ldots, \zeta_k$ tutte le radici *primitive* n-esime dell'unità in $\mathbb{C}$. Si provi che il polinomio

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2) \ldots (x - \zeta_k)$$

è un polinomio a coefficienti razionali, è irriducibile su $\mathbb{Q}$, ed ha grado $\phi(n)$, dove ϕ è la funzione di Eulero ($\Phi_n(x)$ è detto polinomio ciclotomico n-esimo su $\mathbb{Q}$).

6. Sia $F = \mathbb{Z}_5$, sia ω una radice primitiva 13-esima dell'unità su F. Tenendo conto che $5^4 \equiv 1 \pmod{13}$, provare che $|F(\omega)| = 5^4$. Quindi descrivere il gruppo di Galois ed i campi intermedi dell'estensione $F(\omega)|F$.

7. Sia $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Si provi che $E|\mathbb{Q}$ è un'estensione di Galois, e si determinino i suoi sottocampi intermedi.

8. Trovare un polinomio in $\mathbb{Q}[x]$ tale che il suo gruppo di Galois su $\mathbb{Q}$ sia isomorfo al gruppo simmetrico S_7.

9. Sia $f \in \mathbb{Q}[x]$ un polinomio irriducibile di grado 3, e sia G il suo gruppo di Galois. Si provi che G è isomorfo a S_3 oppure ad A_3. Denotate con a, b, c le radici di f in un campo di spezzamento E per f, sia

$$d = (a - b)(b - c)(c - a).$$

Si provi che se $G \simeq S_3$ allora $d \in E \setminus \mathbb{Q}$, $\mathbb{Q}[d] = \mathrm{Inv}_E(A_3)$, e $[Q[d] : \mathbb{Q}] = 2$. Si provi che $G \simeq A_3$ se e solo se $d \in \mathbb{Q}$.

10. Si descriva il gruppo di Galois su $\mathbb{Q}$ del polinomio $f = x^4 - x^2 + 4$.

11. Si descriva il gruppo di Galois su $\mathbb{Q}$ del polinomio $f = x^4 - 2$. Si dica se, posto E il campo di spezzamento di f su $\mathbb{Q}$, l'estensione $E|\mathbb{Q}$ ammette campi intermedi che non sono estensioni normali di $\mathbb{Q}$.

12. Sia $E|F$ un'estensione di campi, con E campo di spezzamento di un polinomio irriducibile $f \in F[x]$. Siano $\alpha_1, \ldots, \alpha_n$ le radici di f in E, e si supponga che $\mathrm{Gal}(E|F)$ sia abeliano. Si provi che allora, per ogni $i = 1, \ldots, n$, $E = F[\alpha_i]$, e quindi che $[E : F] = \deg f$.

13. Sia F un campo di caratteristica 0, e sia $E|F$ un'estensione finita. Usando il Teorema di Steinitz (Teorema 1.8) si provi che $E|F$ è un'estensione semplice.

6 Epilogo

La vicenda delle idee di Galois (tra le più belle e feconde della storia della matematica) continua mostrando come le radici di un polinomio razionale f possano essere espresse, a partire dai coefficienti dello stesso, mediante radicali (ed ovviamente le usuali operazioni: si pensi alla formula risolutiva delle equazioni di secondo grado) se e soltanto se il gruppo di Galois di f su $\mathbb{Q}$ soddisfa una proprietà piuttosto restrittiva detta risolubilità. Questa è senz'altro soddisfatta se $\deg f \leq 4$ (ed infatti esistono "formule risolutive" per equazioni polinomiali di grado fino a 4), mentre per $n \geq 5$ si vede abbastanza facilmente che il gruppo simmetrico S_n non è risolubile. Poiché, come abbiamo visto, esistono polinomi razionali il cui gruppo di Galois è S_n, ne segue che le radici di un polinomio di grado 5, o maggiore, non sempre possono essere espresse mediante radicali a partire dai coefficienti del polinomio, ed in particolare che per $n \geq 5$ non esiste una "formula risolutiva" per le equazioni di grado n.
In tal modo, prima di morire all'età di ventuno anni, per un duello i cui pretesti rimangono misteriosi, Evariste Galois chiudeva un problema che per secoli aveva affascinato ed eluso molti tra i matematici migliori, e nel contempo apriva interi nuovi orizzonti alla matematica, dando vita, si può dire, a quella che sarebbe diventata l'algebra moderna.
Alla memoria di tal gigante, sopra le spalle del quale egli non solo è indegno ma anche incapace di salire, il sottoscritto dedica queste imperfette pagine.
Si capisce che ci vuole ben altro: siate felici.