

Cenni di Teoria di Galois

dispense provvisorie del corso di Algebra 1 2010-2011

Alessio Del Vigna - Giovanni Gaiffi

29 gennaio 2011

1 Ripasso sui polinomi e i campi di spezzamento: raccordo con il corso di Aritmetica.

per prima cosa abbiamo ripassato i seguenti concetti, dal corso di Aritmetica: estensione/ampliamento di campi, polinomio minimo di un elemento di una estensione, grado di una estensione, grado di una ‘torre’ di estensioni finite, elementi algebrici su un campo, estensioni algebriche e il teorema: sia K una estensione di F , allora gli elementi di K algebrici su F formano un campo.

Teorema 1.1. *Sia F un campo e $p(x)$ un polinomio irriducibile di grado $n \geq 1$ a coefficienti in F . Allora esiste un ampliamento E di F con $[E : F] = n$ nel quale $p(x)$ ha una radice.*

Dimostrazione. Dal momento che $p(x)$ è irriducibile in $F[x]$ abbiamo che $E = F[x]/(p(x))$ è un campo: sarà questo il campo che cerchiamo.

Intanto facciamo vedere che E è un’estensione di F . Consideriamo F' , l’immagine di F in E , cioè $F' = \{a + (p(x)) \mid a \in F\}$. F' è un campo isomorfo a F : sia infatti

$$\phi : F[x] \longrightarrow F[x]/(p(x))$$

l’applicazione di proiezione $\phi(f(x)) = f(x) + (p(x))$; allora la restrizione di ϕ a F induce un isomorfismo da F in F' (dimostrare). Usando questo isomorfismo possiamo identificare F con F' , e in tal senso si dice che E è un’estensione di F .

Il grado di questa estensione è n in quanto $\{x^i + (p(x)) \mid 0 \leq i \leq n-1\}$ è una base di E su F . Per comodità denotiamo con α l’elemento $\phi(x) = x + (p(x))$ nel campo E . Dato $f(x) \in F[x]$, chi è $\phi(f(x))$? Essendo ϕ un omomorfismo, se abbiamo $f(x) = \sum_{i=0}^k b_i x^i$ allora

$$\phi(f(x)) = \phi\left(\sum_{i=0}^k b_i x^i\right) = \sum_{i=0}^k \phi(b_i) \phi(x)^i,$$

e se identifichiamo b_i con $\phi(b_i)$ mediante l’isomorfismo precedente abbiamo che $\phi(f(x)) = f(\alpha)$. In particolare, allora, $0 = \phi(p(x)) = p(\alpha)$; vediamo così che $\alpha \in E$ è una radice di $p(x)$. \square

Corollario 1.1. *Sia F un campo e $f(x)$ un polinomio a coefficienti in F . Allora esiste un ampliamento finito E di F nel quale $f(x)$ ha una radice. Inoltre $[L : F] \leq \deg f(x)$.*

Dimostrazione. Sia $p(x)$ un fattore irriducibile di $f(x)$. Per il teorema precedente esiste un ampliamento finito E di F con $[E : F] = \deg p(x) \leq \deg f(x)$ nel quale $p(x)$, e quindi $f(x)$, ha una radice. \square

Anche se in realtà si tratta di un corollario del corollario appena visto, il risultato che segue è così importante che lo enunciamo come teorema:

Teorema 1.2. *Sia F un campo e $f(x)$ un polinomio a coefficienti in F di grado $n \geq 1$. Allora esiste un ampliamento finito E di F di grado al più $n!$ nel quale $f(x)$ ha n radici (una radice di molteplicità m si conta come m radici).*

Dimostrazione. Per il corollario precedente esiste un ampliamento E_0 di F con $[E_0 : F] \leq n$ in cui $f(x)$ ha una radice α , e dunque in $E_0[x]$, $f(x)$ si fattorizza in $f(x) = (x - \alpha)q(x)$, dove $q(x)$ ha grado $n - 1$. Per induzione esiste un ampliamento E di E_0 di grado al più $(n - 1)!$ nel quale $q(x)$ ha $n - 1$ radici, e poiché una radice di $f(x)$ o è α o è radice di $q(x)$, E contiene tutte le n radici di $f(x)$. Ora, $[E : F] = [E : E_0][E_0 : F] \leq (n - 1)! \cdot n = n!$. \square

Il teorema precedente afferma l'esistenza di un'estensione finita E di F nella quale il dato polinomio $f(x)$ di grado n ha n radici. Se $f(x) = \sum_{i=0}^n a_i x^i$ con $a_n \neq 0$, e se le radici sono $\alpha_1, \dots, \alpha_n \in E$ allora abbiamo in $E[x]$ la fattorizzazione

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Osservazione 1.1. Poiché $E[x]$ è un dominio a fattorizzazione unica si ha che il polinomio $f(x)$ non ha altre radici. Se $(x - \beta) \mid f(x)$ allora $(x - \beta) \mid (x - \alpha_i)$ per qualche i data l'unicità di fattorizzazione in irriducibili. Dunque $\beta = \alpha_i$ per qualche i .

Osservazione 1.2. I risultati che abbiamo dato finora valgono sui campi, ma non sui corpi. Consideriamo $x^2 + 1$ in $\mathbb{R}Q_8$ corpo dei quaternioni reali e osserviamo che ha almeno tre radici: infatti i, j, k sono radici.

Esercizio 1.1. Trovare tutte le (infinite!) radici di $x^2 + 1$ in $\mathbb{R}Q_8$.

Osservazione 1.3. Dato un anello A che non è un dominio, può accadere che un polinomio di grado n in $A[x]$ abbia più di n radici. Per esempio, se $a, b \in A$ e $ab = 0$, allora il polinomio ax ha almeno due radici...

Definizione 1.1. Se $f(x) \in F[x]$, un'estensione finita E di F si dice *campo di spezzamento* per $f(x)$ su F se su E , ma non su un sottocampo proprio di E , $f(x)$ si fattorizza nel prodotto di fattori lineari.

Con tale definizione il teorema 1.2 garantisce l'esistenza di campi di spezzamento. Si ricava inoltre immediatamente dalla costruzione usata per il teorema che, se il grado di un polinomio $f(x)$ è n , allora un campo di spezzamento di $f(x)$ avrà grado al massimo $n!$ su F . Sulla limitazione superiore al grado del campo di spezzamento non si possono fare miglioramenti, in quanto vedremo che tale limite può essere talvolta raggiunto.

Sorge subito la domanda: se abbiamo E_1 e E_2 campi di spezzamento su F di $f(x) \in F[x]$, che relazione intercorre fra loro? Ripasseremo, dal corso di Aritmetica, il teorema che afferma che E_1 e E_2 sono isomorfi.

Introduciamo intanto una notazione: quando abbiamo un isomorfismo $\phi : A \rightarrow A'$ fra due anelli, chiameremo $\tilde{\phi}$ l'isomorfismo indotto fra i corrispondenti anelli di polinomi $A[x]$, $A'[x]$:

$$\tilde{\phi} : \begin{array}{ccc} A[x] & \longrightarrow & A'[x] \\ \sum_{i=0}^n a_i x^i & \longmapsto & \sum_{i=0}^n \phi(a_i) x^i \end{array}$$

Esercizio 1.2. Fate la (facile) verifica del fatto che $\tilde{\phi}$ è un isomorfismo.

Teorema 1.3 (di estensione). *Siano $F \subseteq K$ e $F' \subseteq K'$ due estensioni di campi e $\phi : F \rightarrow F'$ un isomorfismo. Sia $a \in K$ algebrico su F e $a' \in K'$ algebrico su F' tale che se*

$$p(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$$

è il polinomio minimo di cui a è radice allora a' è radice di $\tilde{\phi}(p(x))$. Allora esiste un unico isomorfismo $\phi' : F(a) \rightarrow F'(a')$ tale che $\phi'|_F = \phi$ e $\phi'(a) = a'$.

Dimostrazione. Osserviamo che con le condizioni richieste, se ϕ' esiste allora è unico. Dato che $\tilde{\phi}$ è un isomorfismo di anelli, $\tilde{\phi}(p(x))$ è irriducibile in $F'[x]$ (e dunque, essendo monico, è il polinomio minimo di a').

Consideriamo $F[x]/(p(x))$ e $F'[x]/(\tilde{\phi}(p(x)))$, rispettivamente isomorfi a $F(a)$ e $F'(a')$. Per concludere il teorema dobbiamo mostrare che i due quozienti sono isomorfi. Consideriamo il diagramma:

$$F(a) \xrightarrow{\tau} \frac{F[x]}{(p(x))} \longrightarrow \frac{F'[x]}{(\tilde{\phi}(p(x)))} \xrightarrow{\tau'} F'(a'),$$

dove τ è l'isomorfismo che lascia fisso F e manda a in $x + (p(x))$ e τ' l'isomorfismo che lascia fisso F' e manda $x + (\tilde{\phi}(p(x)))$ in a' ¹. Dobbiamo trovare una mappa centrale che sia un isomorfismo per concludere il teorema. Osserviamo che $\tilde{\phi}$ passa al quoziente in quanto $\tilde{\phi}((p(x))) = (\tilde{\phi}(p(x)))$ e induce un isomorfismo ψ tra i due quozienti, che è quello che manda $x + (p(x))$ in $x + (\tilde{\phi}(p(x)))$.

Quindi la mappa $\tau\psi\tau'$ è un isomorfismo tra $F(a)$ e $F'(a')$; verifichiamo che ha le proprietà richieste. Sia $k \in F$, allora

$$(\tau\psi\tau')(k) = (\tau\psi)(k) = \tau(\phi(k)) = \phi(k),$$

¹Questi due isomorfismi li avete già studiati nel corso di Aritmetica e li abbiamo 'ripassati' a lezione.

e quindi $\phi'|_F = \phi$. Per quel che riguarda l'immagine di a :

$$(\tau\psi\tau')(a) = (\tau\psi)(x + (p(x))) = \tau' \left(x + \left(\tilde{\phi}(p(x)) \right) \right) = a'.$$

□

Corollario 1.2. *Sia $F \subseteq K$ una estensione di campi. Se $\alpha, \beta \in K$ sono due radici di un polinomio irriducibile $p(x) \in F[x]$ allora esiste un unico isomorfismo $F(\alpha) \rightarrow F(\beta)$ che è l'identità su F e porta α in β .*

Teorema 1.4. *Siano F e F' campi e $\phi : F \rightarrow F'$ un isomorfismo. Sia $f(x) \in F[x]$ e siano E un campo di spezzamento di $f(x)$ su F ed E' un campo di spezzamento di $\tilde{\phi}(f(x))$ su F' . Allora esiste $\phi' : E \rightarrow E'$ isomorfismo tale che $\phi'|_F = \phi$.*

Dimostrazione. Se $\deg f \leq 1$ allora non c'è niente da dimostrare poiché $E = F$ e $E' = F$ e quindi $\phi' = \phi$. Se invece $\deg f > 1$ sia $g(x)$ un fattore irriducibile di $f(x)$. Sia $a \in E$ una radice di $g(x)$ e sia $a' \in E'$ una radice di $\tilde{\phi}(g(x))$. Per il teorema precedente esiste $\theta : F(a) \rightarrow F'(a')$ isomorfismo tale che $\theta|_F = \phi$ e $\theta(a) = a'$. Allora in $F(a)$ abbiamo

$$f(x) = \frac{f(x)}{x-a}(x-a) = f_1(x)(x-a)$$

dove $f_1(x) \in F(a)[x]$. Osserviamo che E è campo di spezzamento anche di $f_1(x)$ su $F(a)$; analogamente E' è un campo di spezzamento di $\tilde{\theta}(f_1(x))$ su $F'(a')$. Inoltre $\deg f_1 = \deg f - 1$ e quindi per induzione esiste un $\phi' : E \rightarrow E'$ isomorfismo tale che $\phi'|_{F(a)} = \theta$. Dunque $\phi'|_F = \theta|_F = \phi$. □

Corollario 1.3. *Siano E ed E' campi di spezzamento di $f(x) \in F[x]$ su F . Allora E ed E' sono isomorfi.*

Dimostrazione. Basta prendere nel teorema precedente $F' = F$ e $\phi = id_F$. □

2 Derivata di un polinomio e molteplicità

Definizione 2.1. Sia F un campo, e $f(x) \in F[x]$, con $f(x) = a_0 + a_1x + \dots + a_nx^n$. Definiamo la *derivata* di $f(x)$ come il polinomio

$$f'(x) = a_1 + 2a_2x + \dots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}.$$

(con questa scrittura si intende che se $f(x) = a_0$ allora $f'(x) = 0$).

La derivata è definita in modo formale (indipendentemente dalla nozione di ‘limite’) dalla precedente espressione. Non è difficile mostrare che dalla precedente definizione seguono le ben note regole di calcolo delle derivate:

Lemma 2.1. *Siano $f(x)$ e $g(x)$ polinomi in $F[x]$, e $\alpha, \beta \in F$. Allora*

- (1) $(\alpha f(x) + \beta g(x))' = \alpha f'(x) + \beta g'(x)$;
- (2) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Dimostrazione. (1) Verifica immediata (esercizio).

(2) È sufficiente mostrare questo punto nel caso particolare $f(x) = x^i$ e $g(x) = x^j$, in virtù della (1). □

Bisogna prestare attenzione al caso in cui F è un campo a caratteristica finita. Prendiamo ad esempio un campo a caratteristica p e i polinomi in $\mathbb{Z}_p[x]$. La derivata del polinomio x^p è

$$px^{p-1} = 0$$

perché p è la caratteristica del campo. Viene quindi a cadere il familiare risultato dell’analisi secondo cui se la derivata di un polinomio è zero allora deve essere una costante.

La derivata viene introdotta a questo punto perché entra in gioco in un criterio utile per stabilire se un polinomio ha radici multiple. Lo esponiamo attraverso i due teoremi seguenti:

Teorema 2.1. *Sia $f(x) \in F[x]$, con F campo. Se $f(x)$ ha fattori (non invertibili) multipli allora il grado di $(f(x), f'(x))$ è maggiore o uguale a 1.*

Dimostrazione. Senza perdere di generalità possiamo supporre che $f(x)$ abbia un fattore non banale di molteplicità due, ossia abbiamo $f(x) = g_1^2(x)f_1(x)$. Consideriamo la sua derivata e calcoliamola grazie al lemma 2.1:

$$f'(x) = (g_1^2(x))' \cdot f_1(x) + g_1^2(x)f_1'(x) = g_1(x) (2f_1(x)g_1'(x) + g_1(x)f_1'(x)).$$

Questo calcolo mostra che $g_1(x)$ è un fattore sia di $f(x)$ che di $f'(x)$, e quindi abbiamo che $f(x)$ e $f'(x)$ hanno massimo comun divisore di grado maggiore o uguale a 1. □

Teorema 2.2. *Sia $f(x) \in F[x]$, con F campo. Se $f(x)$ non ha fattori multipli in un campo di spezzamento $E \supseteq F$ di $f(x)$ allora $(f(x), f'(x)) = 1$.²*

²Questo massimo comun divisore è fatto in $F[x]$, comunque segue subito (per es. usando il Lemma di Bezout) che $(f(x), f'(x)) = 1$ in $K[x]$ con K una qualunque estensione di F .

Dimostrazione. Sia E il campo di spezzamento di $f(x)$ su F ; se in E si ha che $f(x)$ non ha fattori multipli avremo

$$f(x) = \prod_{i=1}^n (x - \alpha_i),$$

con $\alpha_i \neq \alpha_j$ per ogni $i \neq j$. Calcolando in E la derivata di $f(x)$ abbiamo che

$$f'(x) = \sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (x - \alpha_j),$$

da cui $f'(\alpha_k) \neq 0$ per ogni $k = 1, \dots, n$ ³. Questo mostra che $f(x)$ e $f'(x)$, in E , non hanno fattori in comune. D'altra parte, un fattore comune in $F[x]$ sarebbe un fattore comune anche in $E[x]$, quindi $f(x)$ e $f'(x)$ non possono avere fattori in comune in $F[x]$. \square

3 Polinomi ed elementi separabili

Definizione 3.1. Sia F un campo. Un polinomio irriducibile $g(x) \in F[x]$ si dice *separabile* se la derivata $g'(x)$ è non nulla. Un polinomio $f(x) \in F[x]$ si dice *separabile* se è prodotto di irriducibili separabili.

Osservazione 3.1. Osserviamo che se F è a caratteristica 0 allora ogni polinomio di grado maggiore di zero è separabile. Infatti dato $g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ irriducibile si ha $g'(x) = nx^{n-1} + \sum_{i=0}^{n-1} i a_i x^{i-1}$ e quindi è non nullo.

Osservazione 3.2. Se $g(x) \in F[x]$ è irriducibile separabile allora non ha radici multiple. Infatti essendo irriducibile si ha che $(g(x), g'(x))$ o è $g(x)$ o è 1 (a meno di associati); ma $g'(x)$ ha grado minore di $g(x)$ perché la derivata è non nulla e quindi $(g(x), g'(x)) = 1$. Si conclude applicando il Teorema 2.1.

Proposizione 3.1. Sia $F \subseteq E$ un'estensione di F . Se $f(x) \in F[x]$ si spezza in E come $f(x) = \prod_{i=1}^n (x - a_i)$ con $a_i \in E$ e $a_i \neq a_j$ per $i \neq j$ allora $f(x)$ è un polinomio separabile.

Dimostrazione. Sia $g(x)$ un fattore irriducibile di $f(x)$: essendo $g(x) \mid f(x)$ si ha che, in $E[x]$, $g(x) = \prod_{j \in I} (x - a_j)$, con $\emptyset \subsetneq I \subseteq \{1, \dots, n\}$. Osserviamo che $g'(a_k) \neq 0$ per ogni $k \in I$, e quindi $g'(x)$ non può essere il polinomio nullo. Dunque $g(x)$ è irriducibile separabile e quindi $f(x)$ è separabile per definizione. \square

³Infatti $f'(\alpha_k) = \prod_{\substack{j=1 \\ j \neq k}}^n (\alpha_k - \alpha_j) \neq 0$ in quanto gli α_i sono tutti distinti.

Proposizione 3.2. *Sia $g(x) \in F[x]$ irriducibile e separabile, e sia E un campo di spezzamento di $g(x)$ su F . Sia $a \in E$ una radice di $g(x)$. Allora*

$$|\{\phi : F(a) \rightarrow E \text{ omomorfismo} \mid \phi|_F = id_F\}| = [F(a) : F].$$

Dimostrazione. Il polinomio $g(x)$, essendo separabile, ha tutte le radici distinte, e sono in numero di $\deg g(x)$. Per il Teorema 1.3 sappiamo che, se $a, b \in E$ sono due radici distinte di g allora esiste un unico isomorfismo $F(a) \cong F(b)$ che manda a in b , e quindi ci sono almeno $\deg g$ omomorfismi da $F(a)$ in E . Ma un omomorfismo $\phi : F(a) \rightarrow E$ è del tipo descritto: infatti lascia fisso il polinomio $g(x)$ perché non ne altera i coefficienti e quindi deve mandare a in una radice di $g(x)$. Quindi ci sono esattamente $\deg g = [F(a) : F]$ omomorfismi. \square

Corollario 3.1. *Sia $g(x) \in F[x]$ irriducibile e separabile, e sia E un campo di spezzamento di $g(x)$ su F . Sia $a \in E$ una radice di $g(x)$ e sia $k \in F(a) - F$. Allora esiste $\tau : F(a) \rightarrow E$ con $\tau|_F = id$ e $\tau(k) \neq k$.*

Dimostrazione. Consideriamo la torre $F \subseteq F(k) \subseteq F(a)$. Ora, a è radice di $g(x)$ su F , ma sarà anche radice di un polinomio $q(x) \in F(k)[x]$ irriducibile. Siccome $q(x) \mid g(x)$ in $F(k)[x]$ segue che $q(x)$ si fattorizza come prodotto di fattori lineari in $E[x]$ e non ha radici multiple. Dunque $q(x)$ è separabile. Per la proposizione precedente si ha

$$N = |\{\phi : F(a) \rightarrow E \text{ omomorfismo} \mid \phi|_{F(k)} = id\}| = [F(a) : F(k)].$$

Se per assurdo per ogni $\tau : F(a) \rightarrow E$ che lascia fisso F si avesse $\tau(k) = k$ allora gli insiemi $\{\phi : F(a) \rightarrow E \text{ omomorfismo} \mid \phi|_{F(k)} = id\}$ e $\{\phi : F(a) \rightarrow E \text{ omomorfismo} \mid \phi|_F = id\}$ coinciderebbero, e dunque $N = [F(a) : F]$. Ma allora

$$[F(a) : F(k)] = N = [F(a) : F] = [F(a) : F(k)][F(k) : F],$$

e dunque $[F(k) : F] = 1$, ossia $k \in F$, assurdo. \square

Corollario 3.2. *Sia $E \supsetneq F$ il campo di spezzamento di un polinomio separabile $g(x) \in F[x]$. Sia $a \in E - F$. Allora esiste $\tau : E \rightarrow E$ automorfismo tale che $\tau(a) \neq a$ e $\tau|_F = id$.*

Dimostrazione. Possiamo scrivere $E = F(a_1, \dots, a_t)$, dove a_1, a_2, \dots, a_t sono le radici di $g(x)$ in E . Dovrà essere, per qualche $1 \leq i \leq t$, che $a \notin F(a_1, \dots, a_{i-1})$ ma $a \in F(a_1, \dots, a_i)$, ossia

$$a \in F(a_1, \dots, a_{i-1})(a_i) - F(a_1, \dots, a_{i-1})$$

Sia $g_i(x)$ il polinomio irriducibile di a_i su $F(a_1, \dots, a_{i-1})$ e sia $L \subseteq E$ il campo di spezzamento di $g_i(x)$ su $F(a_1, \dots, a_{i-1})$. Essendo $g_i(x)$ separabile (perché $g_i(x) \mid g(x)$, dunque non ha radici multiple in L), esiste $\tau' : F(a_1, \dots, a_{i-1})(a_i) \rightarrow L$ con $\tau'(a) \neq a$ per il Corollario 3.1. Osserviamo che in particolare τ' soddisfa $\tau'|_F = id$. Grazie al Teorema 1.4 di estensione sui campi di spezzamento a questo punto possiamo costruire un isomorfismo di E su E la cui restrizione a $F(a_1, \dots, a_{i-1}, a_i)$ coincide con τ' . \square

Definizione 3.2. Sia $F \subseteq E$ un'estensione di campi. Un elemento $a \in E$ è *separabile* su F se è algebrico su F e se il suo polinomio minimo su F è separabile.

Osservazione 3.3. Se il campo F è a caratteristica 0 allora ogni elemento algebrico su F è separabile: infatti ogni polinomio, e quindi il polinomio irriducibile dell'elemento, è separabile.

Teorema 3.1 (dell'elemento primitivo). *Sia $F \subseteq E$ un'estensione finita di campi, e sia $E = F(\alpha, \beta_1, \dots, \beta_n)$ con i β_i separabili su F . Allora esiste $\delta \in E$ tale che $E = F(\delta)$.*

Dimostrazione. Se F è un campo finito allora E è un campo finito. Sappiamo che E^* è ciclico⁴, e quindi $E^* = (\gamma)$ per un certo γ . Ma allora $E = F(\gamma)$.

Supponiamo adesso F infinito: osserviamo che basta dimostrare l'enunciato per $n = 1$, poi la tesi generale segue per induzione. Sia dunque $E = F(\alpha, \beta)$, con α algebrico su F e β separabile. Siano $f(x)$ e $g(x)$ in $F[x]$ i polinomi irriducibili di α e β su F , e sia \tilde{E} il campo di spezzamento di $f(x)g(x)$ su F che contiene E (lo costruiamo aggiungendo a E le altre radici del polinomio prodotto). In $\tilde{E}[x]$ vale

$$f(x) = \prod_{i=1}^n (x - a_i) \quad \text{e} \quad g(x) = \prod_{k=1}^n (x - b_k),$$

e diciamo $a_1 = \alpha$ e $b_1 = \beta$. Inoltre, visto che β è separabile allora i b_k sono distinti a due a due. Consideriamo adesso l'equazione

$$a_i + xb_k = \alpha + x\beta.$$

Osserviamo che se $k \neq 1$ allora, per ogni i , l'equazione ha una sola soluzione, che è

$$x = \frac{a_i - \alpha}{\beta - b_k}$$

Essendo F infinito possiamo quindi trovare un $r \in F$ tale che $a_i + rb_k \neq \alpha + r\beta$ per ogni $k \neq 1$ e per ogni i . Affermiamo che, detto $\delta = \alpha + r\beta$, si ha $F(\delta) =$

⁴Lo avete dimostrato nel corso di Aritmetica, comunque daremo alla fine di queste dispense, nel Paragrafo 8.2, una seconda dimostrazione.

$F(\alpha, \beta)$. Essendo $\delta \in F(\alpha, \beta)$ si ha dunque $F(\delta) \subseteq F(\alpha, \beta)$; adesso mostriamo che $\alpha, \beta \in F(\delta)$, da cui seguirà l'altra inclusione che ci serve.

Ora, β è radice del polinomio $g(x)$, ed inoltre vale $f(\delta - r\beta) = f(\alpha) = 0$. Dunque $g(x)$ e $f(\delta - rx)$ hanno $x - \beta$ come fattore comune in $\tilde{E}[x]$, ed anzi affermiamo che questo è proprio il loro massimo comun divisore in $\tilde{E}[x]$. Presa infatti un'altra radice $b_k \neq \beta$ di $g(x)$, allora $f(\delta - rb_k) \neq 0$ in quanto, per la scelta di r , tra i $\delta - rb_k$ non compare alcun a_i radice di $f(x)$; inoltre $(x - \beta)^2 \nmid g(x)$ e quindi il massimo comun divisore in $\tilde{E}[x]$ è proprio $x - \beta$. Ma allora i due polinomi hanno un massimo comun divisore non banale su $F(\delta)[x]$ (se fossero primi fra loro in $F(\delta)[x]$ lo sarebbero anche in $\tilde{E}[x]$ - si vede per esempio usando Bezout), e questo deve essere un divisore di $x - \beta$: dunque tale massimo comun divisore sarà $c_0 + c_1x \in F(\delta)[x]$. Tale massimo comun divisore differisce solo per moltiplicazione per un elemento di \tilde{E}^* da $x - \beta$, dunque valutato in β deve essere nullo, pertanto

$$\beta = -\frac{c_0}{c_1} \in F(\delta).$$

Ma allora $\alpha = \delta - r\beta \in F(\delta)$. \square

Una estensione di un campo F del tipo $F(\gamma)$, ossia ottenuta 'aggiungendo' un solo elemento si chiama *estensione semplice*. Il seguente corollario è di immediata dimostrazione:

Corollario 3.3. *Ogni estensione finita di un campo F a caratteristica 0 è una estensione semplice.*

4 Elementi della teoria di Galois

Definizione 4.1. Sia $F \subseteq E$ un'estensione di campi e denotiamo con $\text{Aut}(E/F)$ l'insieme degli automorfismi ϕ di E che lasciano fisso F punto a punto (ossia $\phi|_F = id$).

È immediato dimostrare che $\text{Aut}(E/F)$ è un gruppo con la composizione di applicazioni. Poniamo

$$E' = \{h \in E \mid \phi(h) = h, \forall \phi \in \text{Aut}(E/F)\}.$$

Non è difficile vedere che E' è un campo e che, in generale, $F \subseteq E' \subseteq E$.

Definizione 4.2. Il campo E' è detto *campo fisso* di $\text{Aut}(E/F)$.

Mostriamo due esempi: nel primo $E' = F$, nel secondo $E' = E$.

Esempio 4.1. Consideriamo $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$, sappiamo che $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$. Cerchiamo gli automorfismi di $\mathbb{Q}(\sqrt{2})$ che lasciano fisso \mathbb{Q} : tali automorfismi lasceranno fisso $x^2 - 2$ e dunque devono mandare $\sqrt{2}$ in un'altra radice di $x^2 - 2$. Quindi abbiamo due possibilità: o l'automorfismo è l'identità, oppure l'automorfismo è quello che fissa \mathbb{Q} e che porta $\sqrt{2}$ in $-\sqrt{2}$ (sappiamo che esiste per il Corollario 1.2). Dunque $\mathbb{Q}(\sqrt{2})' = \mathbb{Q}$.

Esempio 4.2. Prendiamo $\mathbb{Q}(\sqrt[3]{2})$. Essendo tale campo isomorfo a $\mathbb{Q}[x]/(x^3 - 2)$ si ha che un elemento generico del campo è $\alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_2 (\sqrt[3]{2})^2$ con $\alpha_i \in \mathbb{Q}$ (questo equivale a dire che $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ è una base di $\mathbb{Q}(\sqrt[3]{2})$ su \mathbb{Q}). Sia $\tau \in \text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$: argomentando come prima si ha che $\tau(\sqrt[3]{2})$ deve essere una radice di $x^3 - 2$ (in quanto questo polinomio è lasciato fisso da τ). Quindi necessariamente $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, essendo le altre due radici complesse non reali, e allora $\tau = id$. Ma allora $\mathbb{Q}(\sqrt[3]{2})' = \mathbb{Q}(\sqrt[3]{2})$.

Definizione 4.3. Un'estensione $F \subseteq E$ si dice *estensione di Galois* se E è finita su F ⁵ e se il campo fisso è F . In tal caso $\text{Aut}(E/F)$ si chiama *gruppo di Galois* dell'estensione.

L'idea che ci accompagnerà fino agli ultimi risultati che presenteremo qui sulla teoria di Galois sarà quella di far corrispondere sottocampi delle estensioni normali con dei sottogruppi del gruppo di Galois dell'estensione.

Proposizione 4.1. *Sia $F \subseteq E$ estensione finita. Allora $\text{Aut}(E/F)$ è finito.*

Dimostrazione. Siccome E è finita avremo che sarà $F(a_1, \dots, a_n)$ per certi a_i algebrici su F . Sia $\phi \in \text{Aut}(E/F)$: lasciando fisso F esso è determinato univocamente dalle immagini degli a_i . Sia $p_i(x)$ il polinomio irriducibile di a_i su F : ϕ dovrà mandare a_i in una radice di $p_i(x)$, ma le radici di $p_i(x)$ sono finite. \square

Teorema 4.1. *Sia $F \subseteq E$ estensione di Galois. Allora ogni elemento $a \in E$ è radice di un polinomio irriducibile e separabile $f(x) \in F[x]$. Inoltre E contiene un campo di spezzamento di $f(x)$.*

Dimostrazione. Sia \mathcal{O} l'orbita di $a \in E$ sotto l'azione di $\text{Aut}(E/F)$. Definiamo il polinomio

$$f(x) = \prod_{\gamma \in \mathcal{O}} (x - \gamma) \in E[x].$$

Osserviamo che $f(x)$ viene lasciato fisso da qualsiasi automorfismo in $\text{Aut}(E/F)$; infatti preso $\sigma \in \text{Aut}(E/F)$ si ha

$$\tilde{\sigma}(f(x)) = \prod_{\gamma \in \mathcal{O}} (x - \sigma(\gamma)) = f(x)$$

⁵Non è la definizione più generale possibile: adottiamo nel corso questa condizione di finitezza e dunque considereremo solo estensioni di Galois finite.

in quanto σ compie solo una permutazione degli elementi dell'orbita \mathcal{O} . Adesso vogliamo dire di più. Sia $f(x) = \sum_{i=0}^r b_i x^i$ con $b_i \in E$: per quanto osservato $\sigma(b_i) = b_i$ per ogni i e per ogni $\sigma \in \text{Aut}(E/F)$. Dunque $b_i \in F$ per ogni i , in quanto l'estensione è di Galois. Quindi $f(x) \in F[x]$.

Ora dobbiamo mostrare che $f(x)$ ha le proprietà richieste. Intanto $f(x)$ è separabile per costruzione in quanto ha tutte le radici distinte. Adesso dobbiamo mostrare che $f(x)$ è irriducibile in $F[x]$: supponiamo che $f(x) = f_1(x)f_2(x)$ con $f_1(x), f_2(x) \in F[x]$. L'elemento a è radice di $f(x)$ per costruzione, quindi supponiamo senza perdere di generalità che $f_1(a) = 0$. Avendo $f_1(x)$ i coefficienti in F si ha che, per ogni $\sigma \in \text{Aut}(E/F)$,

$$\tilde{\sigma}(f_1(x)) = f_1(x).$$

Ma allora $\sigma(a)$, che è radice di $\tilde{\sigma}(f_1(x))$, è radice di $f_1(x)$. Siccome questo vale per ogni $\sigma \in \text{Aut}(E/F)$, otteniamo che ogni $\gamma \in \mathcal{O}$ è radice di $f_1(x)$. Ma allora $f_1(x)$ ha tutte le radici di $f(x)$, ossia $f_1(x) = kf(x)$ con $k \in F$, e quindi $f_2(x)$ ha grado 0 ed è invertibile. Da questo si conclude che $f(x)$ è irriducibile. \square

Siamo in grado adesso di dare una caratterizzazione delle estensioni di Galois:

Teorema 4.2. *Sia $F \subseteq E$ un'estensione di campi. L'estensione è di Galois se e solo se E è il campo di spezzamento su F di un polinomio di $F[x]$ separabile.*

Dimostrazione. (\implies) Sia $F \subseteq E$ un'estensione di Galois. Essendo E un'estensione finita di F avremo che sarà della forma $E = F(a_1, \dots, a_n)$ per certi a_i algebrici su F . Per il Teorema 4.1 sappiamo che tutti gli a_i sono separabili. Dunque possiamo applicare il teorema dell'elemento primitivo, e concludere che $E = F(\gamma)$, per un certo γ che, sempre in virtù del Teorema 4.1, è separabile. Costruiamo ora il polinomio irriducibile $g(x)$ di γ su F , creato come nella dimostrazione precedente. Tale polinomio è separabile e, come sappiamo dal Teorema 4.1, E contiene un suo campo di spezzamento K . Poichè però $E = F(\gamma) \subseteq K \subseteq E$ si conclude subito che E coincide con K .

(\impliedby) Sia E campo di spezzamento di un polinomio separabile su $F[x]$. Si osserva subito che $[E : F]$ è finito; studiamo il campo fisso E' di $\text{Aut}(E/F)$ e mostriamo che $E' = F$. Preso $a \in E - F$, per il Corollario 3.2, esiste un automorfismo di $\text{Aut}(E/F)$ che non lo lascia fisso: dunque il campo fisso coincide con F , e l'estensione è di Galois. \square

Corollario 4.1. *Se $F \subseteq E$ è un'estensione di Galois e L è un'estensione di E allora ogni $\sigma \in \text{Aut}(L/F)$ manda E in E .*

Dimostrazione. Intanto, come nella dimostrazione precedente, si osserva che $E = F(\gamma)$, con γ radice del polinomio separabile $g(x)$ di cui E è campo di spezzamento

su F . Sia ora $\sigma \in \text{Aut}(L/F)$: ovviamente σ lascia fisso F , ma allora $\tilde{\sigma}$ lascia fisso il polinomio $g(x)$. Dunque $\sigma(\gamma)$ deve essere una radice di $g(x)$, in particolare appartiene a E . Si conclude che E viene mandato in se stesso. \square

Abbiamo già detto che se E è un'estensione finita di F allora il gruppo $\text{Aut}(E/F)$ è finito. Se in particolare l'estensione è di Galois, caso che a noi interessa particolarmente, si può dire esattamente quanti elementi ha $\text{Aut}(E/F)$.

Corollario 4.2. *Sia $F \subseteq E$ un'estensione di Galois. Allora*

$$|\text{Aut}(E/F)| = [E : F].$$

Dimostrazione. Come sopra si osserva che $E = F(\gamma)$, con γ radice del polinomio separabile $g(x)$ di cui E è campo di spezzamento su F . Osserviamo che:

$$[E : F] = [F(\gamma) : F] = |\{\phi : F(\gamma) \rightarrow E \text{ omomorfismo} \mid \phi|_F = id\}| = |\text{Aut}(E/F)|,$$

con la seconda uguaglianza giustificata dalla proposizione 3.2, in quanto E è il campo di spezzamento di $g(x)$. \square

Esempio 4.3 (caratterizzazione delle estensioni quadratiche su campi con caratteristica diversa da 2). Sia $a \in F$ un non quadrato: ossia, per ogni $b \in F$ si ha $b^2 \neq a$. Questo significa che il polinomio $f(x) = x^2 - a$ è irriducibile in $F[x]$. Osserviamo che la derivata formale di $f(x)$ è $f'(x) = 2x$: quindi se la caratteristica di F non è 2 allora tale derivata è non nulla e $x^2 - a$ è separabile. Allora $E = F[x]/(x^2 - a)$ su F è un'estensione di Galois, in quanto E è il campo di spezzamento di un polinomio separabile su $F[x]$. Il gruppo di Galois dell'estensione ha due elementi e quindi

$$\text{Aut}(E/F) \cong \mathbb{Z}_2.$$

Viceversa, sia E un'estensione di F di grado 2, allora $E = F(\beta)$ con $\beta \in E$ che soddisfa un polinomio di grado due $f(x) = x^2 + \gamma_1 x + \gamma_0$ irriducibile su $F[x]$. Visto che $f(x)$ si fattorizza in $E[x]$, E contiene anche l'altra radice di $f(x)$, dunque è un campo di spezzamento di $f(x)$. Allora l'estensione $F \subset E$ è di Galois.

Osserviamo che con il cambiamento di variabile $x \leftarrow x - \frac{\gamma_1}{2}$ si ottiene

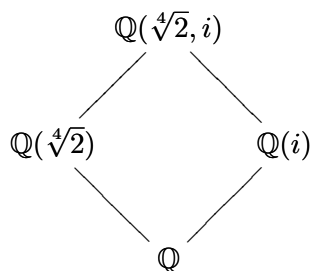
$$f\left(x - \frac{\gamma_1}{2}\right) = \left(x - \frac{\gamma_1}{2}\right)^2 + \gamma_1 \left(x - \frac{\gamma_1}{2}\right) + \gamma_0 = x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right)$$

e quindi $\alpha = \beta + \frac{\gamma_1}{2}$ soddisfa $x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right) = 0$. Ma allora possiamo scrivere

$$E = F(\beta) = F\left(\beta + \frac{\gamma_1}{2}\right) \cong F[x]/\left(x^2 - \left(\frac{\gamma_1^2}{4} - \gamma_0\right)\right).$$

Esempio 4.4. Sia $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, e sia E il suo campo di spezzamento su \mathbb{Q} . Ci chiediamo se l'estensione $\mathbb{Q} \subseteq E$ è di Galois e, in caso affermativo, vogliamo calcolarne il gruppo di Galois.

Intanto il polinomio è separabile, in quanto la caratteristica del campo è 0; quindi $E = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$ è di Galois perché è il campo di spezzamento di un polinomio separabile. La situazione è la seguente:



Calcoliamo il grado dell'estensione:

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

dove il primo grado da sinistra è 2 in quanto $x^2 + 1$ è irriducibile su $\mathbb{Q}(\sqrt[4]{2})$ visto che $i \notin \mathbb{Q}(\sqrt[4]{2})$, mentre il secondo grado è 4 in quanto $x^4 - 2$ è irriducibile in $\mathbb{Q}[x]$ (si può vedere in vari modi, fra cui il criterio di Eisenstein). Quindi il gruppo di Galois è un gruppo di ordine 8; adesso vogliamo esplicitarne la struttura. Osservando lo schema di sopra deve essere

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$$

e quindi $x^4 - 2$ è irriducibile su $\mathbb{Q}(i)$. Sia $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i)) \subseteq \text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ tale che $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ (una tale σ esiste per il Corollario 1.2, tenendo presente che $\mathbb{Q}(i)(\sqrt[4]{2}) = \mathbb{Q}(i)(\sqrt[4]{2}i)$). Sia inoltre $\tau \in \text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(\sqrt[4]{2})) \subseteq \text{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ tale che $\tau(i) = -i$ (come sopra, una tale τ esiste per il Corollario 1.2). Osserviamo che σ ha ordine 4 e τ ha ordine 2, quindi $\langle \sigma \rangle \cong \mathbb{Z}_4$ e $\langle \tau \rangle \cong \mathbb{Z}_2$. Essendo $\langle \sigma \rangle$ normale perché ha indice 2 ed essendo $\langle \sigma \rangle \cap \langle \tau \rangle = \{e\}$ (un elemento che appartiene ad entrambi i sottogruppi deve fissare sia i sia $\sqrt[4]{2}$ dunque è l'identità) si ha che il gruppo di Galois è un prodotto semidiretto $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$: le due possibilità sono un gruppo abeliano o il gruppo diedrale. Si verifica che $\tau\sigma = \sigma^{-1}\tau$ e che quindi il gruppo di Galois è D_4 .

5 Corrispondenza di Galois

Presenteremo la “corrispondenza di Galois” tra campi intermedi di un'estensione di Galois e i sottogruppi del gruppo di Galois.

Proposizione 5.1. *Sia $F \subseteq E$ un'estensione di Galois. Se H è un sottogruppo di $\text{Aut}(E/F)$ tale che il suo campo fisso $\{a \in E \mid h(a) = a \forall h \in H\}$ coincide con F allora $H = \text{Aut}(E/F)$.*

Dimostrazione. Si ha $E = F(a_1, \dots, a_n)$, dove le a_i sono le radici del polinomio separabile di cui E è campo di spezzamento. Per il teorema dell'elemento primitivo si ha che $E = F(\delta)$. Consideriamo l'orbita \mathcal{O} di δ sotto l'azione di H e costruiamo dunque

$$f(x) = \prod_{\gamma \in \mathcal{O}} (x - \gamma).$$

Ripetendo il ragionamento della dimostrazione del teorema 4.1 si ha che $f(x)$ è un polinomio a coefficienti in F , separabile e irriducibile in $F[x]$. Dunque $f(x) \in F[x]$ è il polinomio irriducibile di δ . Allora segue che

$$|H| \geq |\mathcal{O}| = \deg f(x) = [E : F] = |\text{Aut}(E/F)|,$$

ma H è un sottogruppo di $\text{Aut}(E/F)$ e dunque si deve avere l'uguaglianza. \square

Sia $F \subseteq E$ un'estensione di Galois; vogliamo associare ai campi K tali che $F \subseteq K \subseteq E$ un sottogruppo del gruppo di Galois dell'estensione. Per semplificare le notazioni scriviamo $\mathcal{C} = \{K \text{ campi} \mid F \subseteq K \subseteq E\}$ e $\mathcal{S} = \{G \mid G < \text{Aut}(E/F)\}$. Definiamo le seguenti due mappe:

$$i: \begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{S} \\ K & \longmapsto & \text{Aut}(E/K) \end{array} \quad \text{e} \quad j: \begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathcal{C} \\ G & \longmapsto & \{a \in E \mid g(a) = a \forall g \in G\} \end{array} .$$

La mappa i associa a K il sottogruppo $\text{Aut}(E/K)$ di $\text{Aut}(E/F)$ dato dagli automorfismi di E che lasciano fisso K ; la mappa j , invece, associa a G il proprio campo fisso.

Osservazione 5.1. **Se $F \subseteq E$ è un'estensione di Galois e $F \subseteq K \subseteq E$ allora anche $K \subseteq E$ è un'estensione di Galois. Infatti E è il campo di spezzamento di un polinomio separabile in $F[x]$, ma allora E sarà anche il campo di spezzamento dello stesso polinomio ma considerato a coefficienti in K (il polinomio rimane separabile).**

Teorema 5.1 (primo teorema di Galois). *Le mappe i e j sono una l'inversa dell'altra.*

Dimostrazione. Intanto per l'osservazione 5.1 si ha che $K \subseteq E$ è un'estensione di Galois; vogliamo mostrare che $j(i(K)) = K$. Basta osservare che

$$j(i(K)) = j(\text{Aut}(E/K)) = K$$

perché $\text{Aut}(E/K)$ ha come campo fisso proprio K , in quanto è di Galois. Adesso dobbiamo mostrare che $i(j(G)) = G$; per definizione

$$i(j(G)) = \text{Aut}(E/j(G)).$$

Sempre per l'osservazione che precede il teorema l'estensione $j(G) \subseteq E$ è di Galois. Ora, G è un sottogruppo di $\text{Aut}(E/j(G))$ e lascia fissi esattamente gli elementi di $j(G)$, e quindi per la proposizione 5.1 $G = \text{Aut}(E/j(G))$. \square

Teorema 5.2 (secondo teorema di Galois). *Sia $F \subseteq E$ un'estensione di Galois e sia $F \subseteq K \subseteq E$. Allora $F \subseteq K$ è di Galois se e solo se $\text{Aut}(E/K) \triangleleft \text{Aut}(E/F)$. In tale caso $\text{Aut}(E/F)/\text{Aut}(E/K) \cong \text{Aut}(K/F)$.*

Dimostrazione. (\implies) Sia $F \subseteq K$ estensione di Galois. Consideriamo

$$\begin{array}{ccc} \Phi: \text{Aut}(E/F) & \longrightarrow & \text{Aut}(K/F) \\ \psi & \longmapsto & \psi|_K. \end{array}$$

La mappa Φ è ben definita in quanto $\psi|_K$ è in effetti un automorfismo di K (segue dal Corollario 4.1). Inoltre è immediato vedere che Φ è un omomorfismo di gruppi. Per definizione $\ker \Phi = \text{Aut}(E/K)$, in quanto sono gli automorfismi di E che ristretti a K danno l'identità. Questo mostra che $\text{Aut}(E/K)$ è un sottogruppo normale.

Mostriamo che Φ è surgettivo. Sia $\tau : K \rightarrow K$ un automorfismo di $\text{Aut}(K/F)$. Dato che $K \subseteq E$ è un'estensione di Galois avremo che E è il campo di spezzamento di un polinomio separabile $g(x) \in K[x]$. Inoltre $\tilde{\tau}(g(x)) = g(x)$ e dunque sappiamo, per il Teorema 1.4, che si può estendere τ ad un automorfismo di E , il quale lascerà fisso F . Dunque Φ è surgettivo e per il primo teorema di omomorfismo si conclude che

$$\text{Aut}(E/F)/\text{Aut}(E/K) \cong \text{Aut}(K/F).$$

(\impliedby) Sia $\text{Aut}(E/K)$ sottogruppo normale in $\text{Aut}(E/F)$. Visto che $K \subseteq E$ è un'estensione di Galois si ha

$$K = \{a \in E \mid \sigma(a) = a \forall \sigma \in \text{Aut}(E/K)\},$$

e per la normalità del sottogruppo possiamo anche scrivere, fissato $\psi \in \text{Aut}(E/F)$

$$K = \{a \in E \mid \psi^{-1}\sigma\psi(a) = a \forall \sigma \in \text{Aut}(E/K)\}.$$

Osserviamo che se $\psi(a) \in E - K$ allora esiste un σ in $\text{Aut}(E/K)$ che non lo lascia fisso (corollario 3.2), e quindi la sua controimmagine mediante ψ non può essere a . Ma allora possiamo anche riscrivere

$$K = \{a \in E \mid \psi(a) \in K\} = \psi^{-1}(K),$$

e dunque $\psi(K) = K$: questo ci dice che restringendo ψ a K otteniamo un automorfismo di K , e precisamente $\psi|_K \in \text{Aut}(K/F)$. Adesso ci chiediamo chi è il campo fisso di $\text{Aut}(K/F)$: se è F abbiamo concluso. Sia ora $k \in K$ un elemento lasciato fisso da tutti gli elementi di $\text{Aut}(K/F)$, vediamo cosa succede se prendiamo però un automorfismo in $\text{Aut}(E/F)$. Sia $\psi \in \text{Aut}(E/F)$, allora $\psi|_K(k) = k$ poiché k è lasciato fisso da tutti gli automorfismi di $\text{Aut}(K/F)$ e come sappiamo $\psi|_K \in \text{Aut}(K/F)$. Quindi k è lasciato fisso anche da tutti gli elementi di $\text{Aut}(E/F)$. Essendo $F \subseteq E$ un'estensione di Galois, segue che $k \in F$. Questo mostra che il campo fisso di $\text{Aut}(K/F)$ è F stesso e che quindi $K \supseteq F$ è un'estensione di Galois. \square

Teorema 5.3 (terzo teorema di Galois). *Sia $F \subseteq E$ un'estensione di Galois. Se $F \subseteq K \subseteq E$ allora $|\text{Aut}(E/K)| = [E : K]$ e $[K : F] = i_{\text{Aut}(E/F)}(\text{Aut}(E/K))$.*

Dimostrazione. La prima parte è vera perché $K \subseteq E$ è un'estensione di Galois e quindi avevamo già mostrato questo fatto. Per l'altra parte, infine, basta osservare che

$$|\text{Aut}(E/F)| = [E : F] = [E : K][K : F] = |\text{Aut}(E/K)| \cdot [K : F],$$

e concludere dividendo. \square

6 Applicazione: teorema fondamentale dell'algebra (ARGOMENTO FACOLTATIVO, CONSIGLIATO !)

Teorema 6.1 (fondamentale dell'algebra). *Ogni polinomio non costante a coefficienti complessi ammette una radice complessa.*

Dimostrazione. Dimostrare il teorema equivale a dimostrare che $\mathbb{C} = \mathbb{R}(i)$ ammette estensioni finite solo di grado uno.

Cominciamo con l'osservare che ogni estensione finita di $\mathbb{R}(i)$ è contenuta in un'estensione più grande $E \supseteq \mathbb{R}(i)$ che è di Galois su \mathbb{R} . Sia infatti $\mathbb{R}(i) \subseteq L$ un'estensione finita, allora sarà

$$L = \mathbb{R}(i)(\alpha_1, \dots, \alpha_n)$$

per certi α_i . Ma, per il teorema dell'elemento primitivo, $L = \mathbb{R}(\delta)$ in quanto tutti gli elementi aggiunti sono separabili (siamo in caratteristica 0). Sia dunque $f(x) \in \mathbb{R}[x]$ il polinomio irriducibile di δ su \mathbb{R} , e sia E un campo di spezzamento di $f(x)$ che contiene $L = \mathbb{R}(\delta)$. L'estensione E è di Galois su \mathbb{R} perché è campo di spezzamento del polinomio separabile $f(x) \in \mathbb{R}[x]$. Inoltre E contiene $\mathbb{R}(i)$ (visto che $\mathbb{R}(i) \subseteq L$).

Bisogna dunque dimostrare che $E = \mathbb{R}(i)$ (così $L = \mathbb{R}(i)$ e abbiamo dimostrato che L ha grado uno). Sia $G = \text{Aut}(E/\mathbb{R})$, allora

$$|G| = [E : \mathbb{R}] = [E : \mathbb{R}(i)][\mathbb{R}(i) : \mathbb{R}] = 2[E : \mathbb{R}(i)],$$

e quindi G ha ordine pari. Allora consideriamo N_2 , un 2-Sylow di G , e, in base alla corrispondenza di Galois, consideriamo il campo fisso di N_2 , che abbiamo indicato con $j(N_2)$. Si ha $E \supseteq j(N_2) \supseteq \mathbb{R}$ e quindi per i teoremi di Galois si ha

$$[j(N_2) : \mathbb{R}] = i_{\text{Aut}(E/\mathbb{R})}(\text{Aut}(E/j(N_2))) = i_{\text{Aut}(E/\mathbb{R})}(N_2)$$

che è un numero dispari. Per il teorema dell'elemento primitivo $j(N_2) = \mathbb{R}(\alpha)$ e quindi α è radice di un polinomio irriducibile su \mathbb{R} di grado dispari: allora questo polinomio deve avere grado uno, in quanto non ci sono polinomi irriducibili in $\mathbb{R}[x]$ di grado dispari e maggiore di uno⁶. Ma allora $\alpha \in \mathbb{R}$, dunque $\mathbb{R}(\alpha) = \mathbb{R}$ e quindi $j(N_2) = \mathbb{R}$. Da questo segue $N_2 = \text{Aut}(E/\mathbb{R})$ (perchè dalla formula precedente si nota che N_2 ha indice 1 oppure potremmo applicare direttamente la Proposizione 5.1). Siamo arrivati a concludere che $\text{Aut}(E/\mathbb{R})$ è un 2-gruppo, diciamo di ordine 2^n .

Sia $G_1 = \text{Aut}(E/\mathbb{R}(i))$: essendo un sottogruppo di $\text{Aut}(E/\mathbb{R})$ sarà un 2-gruppo e ci sono due possibilità. Se $G_1 = \{id\}$ allora

$$[E : \mathbb{R}(i)] = |\text{Aut}(E/\mathbb{R}(i))| = 1$$

e abbiamo finito. Se invece $G_1 \neq \{e\}$, ricordiamo che, per il secondo teorema di Sylow, un 2-gruppo non banale ammette sempre un sottogruppo di indice 2. Prendiamo dunque $G_2 < G_1$ un sottogruppo di indice 2 e consideriamo il suo campo fisso $j(G_2)$. Ma

$$[j(G_2) : \mathbb{R}(i)] = 2$$

per il terzo teorema di Galois. Tale fatto è assurdo: infatti $j(G_2)$ sarebbe un'estensione di grado 2 di $\mathbb{R}(i)$, ma tali estensioni non esistono. Infatti implicherebbero l'esistenza di un polinomio a coefficienti complessi di grado 2 irriducibile, ossia senza radici complesse. La formula risolutiva per i polinomi di secondo grado ci garantisce invece che ci sono sempre radici complesse. \square

Esercizio 6.1 (di ripasso). Dimostrare, usando il Teorema di Cauchy ma senza usare il Teorema di Sylow, che, dato un numero primo p , se H è un p -gruppo non banale allora H ha un sottogruppo di indice p .

⁶Stiamo usando il fatto che un polinomio a coefficienti in \mathbb{R} di grado dispari ha sempre una radice reale. Assume infatti valori negativi per $x \ll 0$, positivi per $x \gg 0$ ed è una funzione continua...

7 Esercizi

Esercizio 7.1. Sia $\alpha = \sqrt{2 + i\sqrt{2}}$. Determinare il polinomio minimo di α e di $\alpha^2 + 1$ sul campo \mathbb{Q} .

Esercizio 7.2. Determinare il polinomio minimo di $\alpha = 1 + \sqrt{3}$ su \mathbb{Q} .

Esercizio 7.3. Determinare il polinomio minimo di ζ_5 su $\mathbb{Q}(i)$.

Esercizio 7.4. Sia $\alpha = \sqrt{2 + \sqrt{3}}$. Determinare il polinomio minimo di α e su \mathbb{Q} e il grado del suo campo di spezzamento.

Esercizio 7.5. Si consideri il polinomio $x^3 - 3x - 1$ in $\mathbb{Q}[x]$. Si dimostri che è irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Q}(i)[x]$.

Esercizio 7.6. Sia L/K una estensione di campi finita di grado n e sia $f(x) \in K[x]$ irriducibile di grado m . Dimostrare che se n e m sono primi fra loro allora $f(x)$ è irriducibile in $L[x]$.

Esercizio 7.7. I due campi $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono isomorfi?

Esercizio 7.8. È vero o falso che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Esercizio 7.9. Sia K il campo di spezzamento del polinomio $X^4 - 6X^2 + 25 \in \mathbb{Q}[X]$. Calcolare il gruppo di Galois $\text{Aut}(K/\mathbb{Q})$.

Esercizio 7.10. Dimostrare che il campo di spezzamento su \mathbb{Q} di $x^4 + 2x^3 - 8x^2 - 6x - 1$ è $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3} - \sqrt{2})$. Trovare il polinomio irriducibile di $\sqrt{3} - \sqrt{2}$ su $\mathbb{Q}(\sqrt{3})$.

Esercizio 7.11. Sia K il campo di spezzamento del polinomio $(X^4 - 2)(X^3 - 27) \in \mathbb{Q}[x]$ e sia G il suo gruppo di Galois su \mathbb{Q} . Calcolare $[K : \mathbb{Q}]$ e descrivere G .

Esercizio 7.12. Sia $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$. Dimostrare che $\mathbb{K} \supseteq \mathbb{Q}$ è di Galois e determinare $\text{Aut}(K/\mathbb{Q})$. Determinare inoltre tutti i campi F con $\mathbb{Q} \subseteq F \subseteq K$ tali che $[F : \mathbb{Q}] = 6$.

Esercizio 7.13. Studiare la struttura del campo di spezzamento E di $x^4 - 2$ su \mathbb{Q} e stabilire la corrispondenza tra sottogruppi del gruppo di Galois e sottocampi di E .

Esercizio 7.14. Determinare il gruppo di Galois di $x^6 - 2x^4 - 8x^2 + 16$ su \mathbb{Q} , su \mathbb{F}_3 e su \mathbb{F}_9 . In ciascuno dei tre casi elencare i campi intermedi fra il campo base e il campo di spezzamento.

Esercizio 7.15. Calcolare, al variare di $m \in \mathbb{Z}$, il gruppo di Galois del polinomio $(x^4 + 1)(x^2 - m)$ su \mathbb{Q} .

Esercizio 7.16. Sia K un campo finito di caratteristica p e sia $[K : \mathbb{Z}_p] = n$.

a) Dimostrare che K è il campo di spezzamento su \mathbb{Z}_p del polinomio $x^{p^n} - x$ e dunque l'estensione $\mathbb{Z}_p \subset K$ è di Galois.

b) Dimostrare che il gruppo di Galois $\text{Aut}(K/\mathbb{Z}_p)$ è isomorfo a \mathbb{Z}_n ed è generato dall'isomorfismo di Frobenius $F : K \rightarrow K$ definito da

$$F(a) = a^p \quad \forall a \in K.$$

Esercizio 7.17. Sia F un campo e consideriamo $g = \frac{x^3}{x+1} \in F(x)$.

a) Dimostrare che g non è algebrico su F (ossia è *trascendente*).

b) Dimostrare che $F(x)$ è una estensione algebrica semplice di $F(g)$. Trovare il polinomio minimo di x su $F(g)$.

Esercizio 7.18. Sia $q(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado p , con p numero primo. Supponiamo che $q(x)$ abbia esattamente due radici non reali in \mathbb{C} . Allora il gruppo di Galois (di un campo di spezzamento) di $q(x)$ su \mathbb{Q} è isomorfo a S_p .

Esercizio 7.19. Siano K_1 e K_2 estensioni di Galois del campo k , e sia L un campo che contiene sia K_1 sia K_2 . Dimostrare che l'estensione $k \subseteq K_1K_2$ è di Galois⁷. Dimostrare inoltre che l'omomorfismo

$$\Phi : \text{Aut}(K_1K_2/k) \rightarrow \text{Aut}(K_1/k) \times \text{Aut}(K_2/k)$$

dato dalla restrizione su ogni componente, è iniettivo, e infine dimostrare che se $K_1 \cap K_2 = k$ allora Φ è un isomorfismo.

Esercizio 7.20. Sia F una estensione di k , sia K una estensione di Galois di k , e sia L un campo che contiene sia K sia F . Dimostrare che le estensioni $F \subseteq KF$ e $(K \cap F) \subseteq K$ sono di Galois. Sia

$$\Phi : \text{Aut}(KF/F) \rightarrow \text{Aut}(K/k)$$

l'omomorfismo dato dalla restrizione. Dimostrare che Φ induce un isomorfismo fra $\text{Aut}(KF/F)$ e $\text{Aut}(K/(K \cap F))$.

Esercizio 7.21. Sia ω una radice primitiva n -esima dell'unità (n intero positivo). Dimostrare che $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ è una estensione di Galois e che il suo gruppo di Galois è isomorfo a \mathbb{Z}_n^* . [Svolto a lezione]

⁷Ricordiamo che abbiamo definito a lezione il *campo composto* K_1K_2 .

Esercizio 7.22. Dimostrare che se n e m sono due interi positivi primi fra loro, allora

$$(1) \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{mn}) \quad (2) \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q},$$

dove, per ogni intero positivo k , ζ_k indica una radice k -esima primitiva complessa dell'unità.

8 Appendice

8.1 Qualche informazione sulla chiusura algebrica di un campo.

Definizione 8.1. Un campo K si dice algebricamente chiuso se ogni polinomio $f(x) \in K[x]$ si fattorizza in $K[x]$ come prodotto di fattori lineari.

Esercizio 8.1. Dimostrare che un campo K è algebricamente chiuso se e solo se ogni polinomio $f(x) \in K[x]$ ammette una radice in K .

Esercizio 8.2. Dimostrare che un campo K è algebricamente chiuso se e solo se gli elementi irriducibili di $K[x]$ sono i polinomi $x - a$ con $a \in K$.

Esercizio 8.3. Dimostrare che un campo K è algebricamente chiuso se e solo se non ammette estensioni algebriche L con $K \subsetneq L$.

Una estensione del concetto di campo di spezzamento è data dal concetto di *chiusura algebrica* di un campo F .

Definizione 8.2. Una estensione \bar{F} di F si dice *chiusura algebrica* di F se verifica entrambe le seguenti condizioni:

1. \bar{F} è algebricamente chiuso;
2. \bar{F} è algebrico su F .

Per esempio, come abbiamo dimostrato nel Paragrafo 6, \mathbb{C} è una chiusura algebrica di \mathbb{R} .

Esercizio 8.4. Dimostrare che il campo \mathcal{A} dei numeri algebrici, ossia dei numeri complessi algebrici su \mathbb{Q} , è una chiusura algebrica di \mathbb{Q} .

Si possono dimostrare i seguenti risultati.

Teorema 8.1. *Ogni campo F ammette una chiusura algebrica. Date due chiusure algebriche E, E' di F , esiste un isomorfismo $\theta : E \rightarrow E'$ tale che $\theta|_F = id$.*

Teorema 8.2. *Sia F un campo e sia \bar{F} una sua chiusura algebrica. Allora, dato un polinomio $f(x) \in F[x]$ esiste un' unica estensione K di F che sia un sottocampo di \bar{F} (ossia $F \subseteq K \subseteq \bar{F}$) e che sia un campo di spezzamento per $f(x)$ su F .*

8.2 Complementi: sul teorema, visto già ad Aritmetica, dell'elemento primitivo di un sottogruppo moltiplicativo di un campo

Come avete visto nel corso di Aritmetica, il sottogruppo moltiplicativo di un campo finito è ciclico. Ecco un modo alternativo di esporre la dimostrazione, che utilizza alcuni risultati studiati nel corso di Algebra1.

Teorema 8.3. *Sia F un campo e G un sottogruppo finito del gruppo moltiplicativo di F . Allora G è ciclico.*

Dimostrazione. Essendo G sottogruppo finito di un campo abbiamo che G è un gruppo abeliano finito, dunque

$$G \cong \prod_{i=1}^k N_{p_i},$$

ossia G è il prodotto delle sue parti di p_i -torsione, che coincidono con i p_i sottogruppi di Sylow. Se dimostriamo che per ogni i si ha che N_{p_i} è ciclico abbiamo concluso. Intanto sappiamo dal teorema di struttura per i gruppi abeliani finiti che

$$N_{p_i} \cong \mathbb{Z}_{p_i^{a_1}} \times \mathbb{Z}_{p_i^{a_2}} \times \cdots \times \mathbb{Z}_{p_i^{a_n}},$$

con $0 < a_1 \leq a_2 \leq \cdots \leq a_n$, e affermiamo che c'è una sola componente, la $\mathbb{Z}_{p_1^{a_1}}$. Se per assurdo ci fosse anche la componente $\mathbb{Z}_{p_i^{a_2}}$ troveremmo in G un sottogruppo isomorfo a $\mathbb{Z}_{p_i} \times \mathbb{Z}_{p_i}$. Dunque avremmo almeno p_i^2 radici del polinomio $x^{p_i} - 1$, e questo contraddirebbe il fatto che un polinomio di grado n a coefficienti in un campo ha al più n radici nel campo. \square