

Capitolo 1

Teoria dei campi

Definizione 1.1. Un campo $\mathbb{K}$ è un anello commutativo con identità tale che $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Siamo interessati allo studio delle soluzioni di equazioni algebriche $f(x) = 0$; in particolare, vogliamo studiare il comportamento di esse al variare del campo considerato. Siamo portati allora a trattare le estensioni di campi, cioè un contenimento $\mathbb{K} \subseteq \mathbb{L}$. Indicheremo un'estensione di campi con $\mathbb{L}/\mathbb{K}$.

Definizione 1.2. Siano $\mathbb{K}, \mathbb{L}$ tali che $\mathbb{K} \subseteq \mathbb{L}$. $\alpha \in \mathbb{L}$ si dice algebrico su $\mathbb{K}$ se esiste un polinomio non nullo $f \in \mathbb{K}[x]$ tale che $f(\alpha) = 0$. Se α non è algebrico, si dice trascendente.

Consideriamo allora l'omomorfismo di anelli

$$\begin{array}{ccc} \varphi_\alpha: & \mathbb{K}[x] & \longrightarrow \mathbb{K}[\alpha] \subseteq \mathbb{L} \\ & x & \longmapsto \alpha \end{array}$$

Notiamo che $\mathbb{K}[\alpha]$ è un dominio di integrità, perchè sottoanello di un campo. Di conseguenza, $\text{Ker}(\varphi_\alpha)$ è un ideale primo di $\mathbb{K}[x]$, che invece è un dominio a ideali principali. Vi sono allora due casi:

- Se $\text{Ker}(\varphi_\alpha) = (0)$, si ha che α è trascendente per definizione
- Se $\text{Ker}(\varphi_\alpha) \neq (0)$, allora per la caratterizzazione degli ideali di un PID, si ha che $\text{Ker}(\varphi_\alpha)$ è un ideale massimale e dunque $\mathbb{K}[\alpha]$ è un campo e α è algebrico.

Possiamo però ottenere anche di più. Per il primo teorema di omomorfismo, si ha che $\mathbb{K}[\alpha] \simeq \mathbb{K}[x]_{/\text{Ker}(\varphi_\alpha)}$. Poichè $\mathbb{K}[x]$ è a ideali principali, esiste un unico polinomio f_α monico tale che $\text{Ker}(\varphi_\alpha) = (f_\alpha)$.

Definizione 1.3. Sia $\alpha \in \mathbb{L}$ algebrico su $\mathbb{K}$. Chiamiamo f_α il polinomio minimo di α su $\mathbb{K}$.

Il polinomio minimo di α fornisce diverse informazioni rispetto all'estensione. Infatti, rappresenta la relazione di grado minimo a coefficienti in $\mathbb{K}$ che lega le potenze di α ; in particolare ci permette di trovare una base di $\mathbb{K}[\alpha]$ come $\mathbb{K}$ -spazio vettoriale. Detto $n = \deg(f_\alpha)$, l'insieme $\{1, \alpha, \dots, \alpha^{n-1}\}$ è una base di $\mathbb{K}[\alpha]$; se infatti non fossero linearmente indipendenti si negherebbe il fatto che f_α sia il polinomio minimo. D'altra parte, generano, perchè la relazione data da f_α permette di abbassare il grado di ogni relazione data fino a $n - 1$. Fino ad ora abbiamo però considerato un caso "semplice" di estensioni generate da un solo elemento. Questo tipo di estensione può essere però generalizzato:

Definizione 1.4. $\mathbb{L}/\mathbb{K}$ è un'estensione finita se $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}$ è finita; è invece algebrica se ogni $\alpha \in \mathbb{L}$ è algebrico su $\mathbb{K}$.

Esempio. $\mathbb{C}$ è algebrico su $\mathbb{R}$, ma non su $\mathbb{Q}$.

Per scoprire il grado di un'estensione, è essenziale il seguente teorema:

Teorema 1.5 (di estensione). *Consideriamo le estensioni di campi $L \supseteq E \supseteq K$. Allora $[L : K] = [L : E][E : K]$.*

Il problema è ora capire le relazioni tra le due estensioni che stiamo considerando.

Teorema 1.6. *Ogni estensione finita $\mathbb{L}/\mathbb{K}$ è algebrica.*

Dimostrazione. Mostriamo che ogni elemento di $\mathbb{L}$ è algebrico su $\mathbb{K}$. Sia $\alpha \in \mathbb{L}$. Poichè $[\mathbb{L} : \mathbb{K}] = n$, gli elementi $1, \alpha, \dots, \alpha^n$ sono linearmente dipendenti su $\mathbb{K}$. Di conseguenza, esistono $a_i \in \mathbb{K}$ tali che $\sum_{i=0}^n a_i \alpha^i = 0$. Di conseguenza, α annulla il polinomio $f = \sum_{i=0}^n a_i x^i$, da cui la tesi. $\square$

Notiamo che il viceversa è falso. Per mostrarlo ci serve prima un lemma:

Lemma 1.7. *Consideriamo un'estensione L/K e definiamo l'insieme $A = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$. Allora A è un campo.*

Dimostrazione. Siano $\alpha, \beta \in A$. Mostriamo che $\alpha + \beta$ e α^{-1} e $\alpha\beta$ sono elementi di A . Consideriamo l'estensione di K $K(\alpha, \beta)$. Tale estensione è algebrica e finitamente generata, di conseguenza finita per il teorema di estensione. Gli elementi cercati si trovano allora in $K(\alpha, \beta) \subseteq L$, da cui la tesi. $\square$

Mostriamo ora con un controesempio che non tutte le estensioni algebriche sono finite. Consideriamo il campo $\mathbb{Q}$ e definiamo

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$$

Per quanto detto, $\overline{\mathbb{Q}}$ è un'estensione algebrica di $\mathbb{Q}$ ma non è finita, poichè contiene tutti gli elementi del tipo $\sqrt[n]{2}$ che hanno grado n su $\mathbb{Q}$.

Proposizione 1.8. L/K è algebrica e finitamente generata $\iff$ è finita.

Proposizione 1.9. Consideriamo le estensioni L/E e E/K . Allora vale

$$L/K \text{ è algebrica } \iff L/E, E/K \text{ sono algebriche}$$

Dimostrazione.

($\Rightarrow$) L'implicazione è banale, se $\alpha \in L$ è algebrico su K , allora utilizzando lo stesso polinomio otteniamo la sua algebricità su E . Se $\alpha \in E$ allora in particolare $\alpha \in L$ e dunque è algebrico su K .

($\Leftarrow$) Sia $\alpha \in L$. Sappiamo allora che α è algebrico su E , di conseguenza esiste $p = \sum a_i x^i \in E[x]$ tale che $p(\alpha) = 0$. Notiamo che i coefficienti di p sono algebrici su K . Consideriamo allora il campo $E_0 = K(a_0, \dots, a_n)$; l'estensione E_0/K è finita perchè algebrica e finitamente generata. Abbiamo allora la seguente catena di implicazioni:

$$E_0(\alpha)/E_0 \text{ finita} \Rightarrow E_0(\alpha)/K \text{ finita} \Rightarrow E_0(\alpha)/K \text{ algebrica}$$

Conseguentemente, α è algebrico su K .

□

Tra le estensioni più ambite, ci sono le chiusure algebriche:

Definizione 1.10. Un campo K si dice algebricamente chiuso se ogni polinomio $f \in K[x]$ ammette una radice in K . Data un'estensione L/K , L si dice la chiusura algebrica di K se

- L è algebricamente chiuso
- L è algebrico su K

Indicheremo nel seguito la chiusura algebrica di un campo con $\overline{K}$.

Esempio. $\mathbb{C}$ è un campo algebricamente chiuso ed è la chiusura algebrica di $\mathbb{R}$, ma non di $\mathbb{Q}$.

Mostriamo ora che dato un campo K , esiste sempre una sua chiusura algebrica. Abbiamo prima bisogno di un lemma:

Lemma 1.11. Sia K un campo e sia $p \in K[x]$ un polinomio non nullo di grado positivo. Allora esiste un campo K' algebrico su K tale che p abbia una radice in K' .

Dimostrazione. Per le ipotesi scelte, p è un elemento non invertibile di $K[x]$; di conseguenza, esiste un ideale massimale $\mathfrak{M}$ che contiene p . Consideriamo allora il campo $K' = K[x]/\mathfrak{M}$. Chiaramente $K' \supseteq K$ tramite l'omomorfismo

$$K \xrightarrow{i} K[x] \xrightarrow{\pi} K[x]/\mathfrak{M}$$

che è iniettivo in quanto non banale. Sia $\alpha = \pi(x)$. Allora (notando che K viene fissato)

$$p(\alpha) = p(\pi(x)) = \pi(p(x)) = 0$$

come voluto. Ci manca da mostrare l'algebricità di K' su K . Poichè $K[x]$ è un PID, $\mathfrak{M} = (q)$. Di conseguenza, l'estensione è di grado finito su K e dunque algebrica. $\square$

Teorema 1.12 (di esistenza della chiusura algebrica). *Sia K un campo. Allora esiste un campo $\overline{K}$ chiusura algebrica di K .*

Dimostrazione. Sia Λ un insieme che indicizza i polinomi di $K[x]$ di grado positivo. Consideriamo l'insieme di indeterminate $X = \{x_\lambda \mid \lambda \in \Lambda\}$; abbiamo allora l'anello di polinomi $K[X]$ che ha come indeterminate gli x_λ . In tale anello, consideriamo l'ideale $I = (\{p_\lambda(x_\lambda) \mid \lambda \in \Lambda\})$. I è un ideale proprio di $K[X]$. Supponiamo infatti per assurdo che $1 \in I$. se così fosse, esisterebbero $a_1, \dots, a_n \in K[X]$ e $\lambda_1, \dots, \lambda_n$ tali che

$$\sum_{i=1}^n a_i(X) p_{\lambda_i}(x_{\lambda_i}) = 1$$

Per il lemma, esiste K' un campo nel quale $p_{\lambda_1}, \dots, p_{\lambda_n}$ ammettono una radice; siano $\alpha_1, \dots, \alpha_n$ tali radici. Consideriamo allora l'omomorfismo di anelli

$$\begin{aligned} \varphi: K[X] &\longrightarrow K' \\ x_{\lambda_i} &\longmapsto \alpha_i \\ x_\mu &\longmapsto 0 \quad \text{se } \mu \neq \lambda_i \end{aligned}$$

Poichè è un omomorfismo di anelli, $\varphi(1) = 1$; notiamo allora che

$$0 = \varphi\left(\sum_{i=1}^n a_i(X) p_{\lambda_i}(x_{\lambda_i})\right) = \varphi(1) = 1$$

da cui un assurdo. Esiste allora un ideale massimale $\mathfrak{M}$ che contiene I . Consideriamo allora $E_1 = K[X]/\mathfrak{M}$. Notiamo che $E_1 \supseteq K$. Inoltre, $\forall \lambda \in \Lambda$ $p_\lambda(x)$ ha una radice in E_1 , perchè $p_\lambda(x_\lambda) \in I \subseteq \mathfrak{M}$ e dunque $p_\lambda(\bar{x}_\lambda) = 0$. Possiamo iterare la costruzione e ottenere una catena di campo l'uno contenuto nel

successivo:

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \dots$$

nei quali ogni polinomio di $E_i[x]$ abbia almeno una radice in E_{i+1} . Consideriamo allora $E = \bigcup_{n \in \mathbb{N}} E_n$. E è un campo perchè unione di una catena ascendente di campi. Inoltre, E è algebricamente chiuso. Sia infatti $p \in E[x]$. Allora, esiste un naturale n tale che $p \in E_n[x]$. Di conseguenza, p ammette una radice in E_{n+1} . Non abbiamo però informazioni sul fatto che E sia algebrico su K . Ovviamente allora a questo problema: consideriamo cioè $\overline{K} = \{\alpha \in E \mid \alpha \text{ è algebrico su } K\}$. Sicuramente $\overline{K}$ è algebrico su K . Mostriamo che è algebricamente chiuso. Sia $p \in \overline{K}[x]$ e sia $\alpha \in E$ una sua radice. Allora α è algebrico su $\overline{K}$, che a sua volta è algebrico su K . Di conseguenza, α è algebrico su K e dunque $\alpha \in \overline{K}$, come voluto. $\square$

Per mostrare l'unicità, abbiamo bisogno di studiare gli omomorfismi tra campi e la loro estensione.

1.1 Estensioni e omomorfismi

Una domanda interessante è come si comportano gli omomorfismi rispetto alle estensioni di campo. Supponiamo cioè di avere un omomorfismo di campi $\varphi : K \rightarrow F$, con $K \subseteq F \subseteq \overline{K}$. Dato $\alpha \in \overline{K}$ ha senso chiedersi sotto quali condizioni φ si può estendere a $K(\alpha)$, cioè quando esiste un omomorfismo $\tilde{\varphi} : K(\alpha) \rightarrow F$ tale che $\tilde{\varphi}|_K = \varphi$.

Proposizione 1.13. *Sia K un campo e sia $K' = K(\alpha)$ un'estensione algebrica semplice di K . Sia $\sigma : K \rightarrow L$ un omomorfismo di campi e sia $f_\alpha = \sum a_i x^i$ il polinomio minimo di α .*

- Se $\sigma' : K' \rightarrow L$ è un omomorfismo di campi che prolunga σ , allora $\sigma'(\alpha)$ è una radice di $\sigma f_\alpha = \sum \sigma(a_i) x^i$.
- Per ogni radice $\beta \in L$ di $\sigma f_\alpha \in L[x]$ esiste un omomorfismo $\sigma' : K' \rightarrow L$ di σ tale che $\sigma'(\alpha) = \beta$.

Dimostrazione. Sia σ' un prolungamento di σ . Se $f(\alpha) = 0$, allora si ha $0 = \sigma'(f(\alpha)) = \sigma f(\sigma'(\alpha))$ e dunque il primo punto. Mostriamo ora il secondo. Consideriamo gli omomorfismi

$$\begin{array}{ccc} \varphi : & K[x] & \longrightarrow & K[\alpha] \\ & g & \longmapsto & g(\alpha) \end{array}$$

$$\begin{array}{ccc} \psi : & K[x] & \longrightarrow & L \\ & g & \longmapsto & \sigma g(\beta) \end{array}$$

Sappiamo che $\text{Ker}(\varphi) = (f_\alpha)$; poichè per ipotesi $\sigma f_\alpha(\beta) = 0$, si ha $(f_\alpha) \subseteq \text{Ker}(\psi)$. Passando al quoziente, si ottiene allora il diagramma:

$$\begin{array}{ccccc} & & K[x] & & \\ & \swarrow \varphi & \downarrow \pi & \searrow \psi & \\ K[\alpha] & \xleftarrow{\tilde{\varphi}} & K[x]/(f) & \xrightarrow{\tilde{\psi}} & L \end{array}$$

D'altronde $\tilde{\varphi}$ è un isomorfismo, dunque è ben definito l'omomorfismo $\sigma' = \tilde{\psi} \circ \tilde{\varphi}^{-1}$. L'omomorfismo è tale che $\sigma'(\alpha) = \beta$; infatti

$$\tilde{\psi} \circ \tilde{\varphi}^{-1}(\alpha) = \tilde{\psi}([x]) = \beta$$

dunque la tesi. $\square$

Possiamo riformulare quanto fatto in maniera più precisa:

Corollario 1.14. *Il numero di prolungamenti di un omomorfismo $\sigma': K(\alpha) \rightarrow L$ è uguale al numero delle radici distinte di σf_α in L .*

Il lemma di Zorn ci permette di estendere quanto fatto fino ad ora:

Teorema 1.15 (di estensione). *Sia F/K un'estensione algebrica e sia $\varphi: K \rightarrow \overline{K}$ un'immersione. Allora φ si estende a $\tilde{\varphi}: F \rightarrow \overline{K}$.*

Dimostrazione. Sia $X = \{(E, \psi) \mid K \subseteq E \subseteq F, \psi: E \rightarrow \overline{K}, \psi|_K = \varphi\}$ ordinato parzialmente:

$$(E, \psi) \leq (E', \psi') \iff E \subseteq E' \text{ e } \psi'|_E = \psi$$

Notiamo che $X \neq \emptyset$; mostriamo allora che possiamo applicare il lemma di Zorn. Sia $\{(E_i, \psi_i) \mid i \in I\}$ una catena. Allora $E = \cup E_i$ è un campo perchè unione ascendente di campi. Definiamo

$$\begin{array}{ccc} \psi: & E & \longrightarrow \overline{K} \\ & \alpha & \longmapsto \psi_i(\alpha) \quad \text{se } \alpha \in E_i \end{array}$$

ψ è ben definita perchè le funzioni considerate sono coerenti. Allora (E, ψ) è un maggiorante della catena. Per Zorn esiste allora (F_0, ψ_0) massimale per X . Mostriamo che $F_0 = F$. Se per assurdo $F_0 \subsetneq F$, sia $\alpha \in F \setminus F_0$. Allora possiamo considerare l'estensione semplice $F_0(\alpha)$; per quanto visto su tali estensioni, esiste $\tilde{\psi}_0$ che estende ψ_0 , da cui un assurdo. Di conseguenza $F = F_0$ e quindi la tesi. $\square$

Possiamo ora dimostrare l'unicità della chiusura algebrica:

Teorema 1.16 (Unicità della chiusura algebrica). *Sia K un campo e siano $\overline{K}_1$ e $\overline{K}_2$ due chiusure algebriche. Allora $\overline{K}_1 \simeq \overline{K}_2$.*

Dimostrazione. Sia $\iota: K \rightarrow \overline{K}_1$ l'inclusione e sia ψ un omomorfismo che estende ι a $\overline{K}_2$. Chiaramente ψ è iniettivo perchè è un omomorfismo di campi non nullo. Mostriamo che è surgettivo. Abbiamo

$$K \subseteq \psi(\overline{K}_2) \subseteq \overline{K}_1$$

L'estensione $\psi(\overline{K}_2) \subseteq \overline{K}_1$ è quindi algebrica poichè la è $K \subseteq \overline{K}_1$. Inoltre, poichè $\overline{K}_2$ è algebricamente chiuso, lo è anche $\psi(\overline{K}_2)$. Ma ogni estensione algebrica di un campo algebricamente chiuso è banale, da cui $\psi(\overline{K}_2) = \overline{K}_1$ e dunque la surgettività. Abbiamo allora trovato un isomorfismo tra le due chiusure algebriche. $\square$

Ora che abbiamo dimostrato l'esistenza della chiusura algebrica, continuiamo lo studio degli omomorfismi e delle loro estensioni. Abbiamo visto il caso di una radice semplice; in realtà possiamo ampliare quanto fatto a un'estensione finita qualunque:

Proposizione 1.17. *Sia E/K un'estensione finita di grado n e sia $\varphi: K \rightarrow \overline{K}$. Allora esistono $\varphi_1, \dots, \varphi_n$ omomorfismi tali che $\varphi_i: E \rightarrow \overline{K}$ e $\varphi_i|_K = \varphi$.*

Dimostrazione. Dimostriamo l'enunciato per induzione sul grado dell'estensione. Se $n = 1$, allora $E = K$ e dunque l'enunciato è ovvio.

Mostriamo che $n - 1 \Rightarrow n$. Sia $\alpha \in E \setminus K$. Otteniamo allora le sottoestensioni

$$[K(\alpha) : K] = d \qquad [E : K(\alpha)] = m \qquad n = d \cdot m$$

Per la proposizione dimostrata per le estensioni semplici, esistono $\varphi_1, \dots, \varphi_d$ che estendono φ . Per l'ipotesi induttiva applicata a ogni φ_i , esistono ψ_{i_j} che estendono φ_i . Abbiamo allora che le ψ_{i_j} sono n ed estendono φ . Ci manca da mostrare che sono tutte distinte e che sono tutte le possibili estensioni.

- Se $\psi_{i_j} = \psi_{l_k}$, allora $\psi_{i_j|_{K(\alpha)}} = \psi_{l_k|_{K(\alpha)}}$, di conseguenza $\varphi_i = \varphi_l$ e dunque $i = l$ perchè le φ_i sono tutte distinte. D'altronde, anche le applicazioni fornite dall'ipotesi induttiva sono distinte e quindi anche $j = k$.
- Sia η un'altra applicazione che estende φ ad E . Per la proposizione sulle estensioni semplici, necessariamente esiste un indice i tale che $\eta|_{K(\alpha)} = \varphi_i$; per ipotesi induttiva, esiste allora j tale che $\eta = \psi_{i_j}$.

$\square$

Definizione 1.18. Sia F/K un'estensione algebrica, $F \subseteq \overline{K}$. F è normale su K se $\forall \varphi: F \rightarrow \overline{K}$ tale che $\varphi|_K = id$ allora $\varphi(F) = F$.

In altre parole, F è un'estensione normale se ogni sua immersione in una sua chiusura algebrica che fissa K si può restringe a un automorfismo di F . Questa proprietà, che può sembrare misteriosa e poco rilevante, è in realtà cruciale:

Proposizione 1.19. Sia F/K un'estensione normale e sia $f \in K[x]$ un polinomio irriducibile che ammette una radice in F . Allora f si spezza in fattori lineari in $F[x]$.

Dimostrazione. Sia $\alpha \in F$ una radice di f e sia $\varphi: K \rightarrow \overline{K}$. Per quanto visto, esistono allora $\varphi_1, \dots, \varphi_n$ che estendono φ a $K(\alpha)$. Siano $\{\alpha_1, \dots, \alpha_n\}$ le radici di f in $\overline{K}$. Allora, a meno di riordinare le applicazioni, $\varphi_i(\alpha) = \alpha_i$. Per il teorema di estensione, possiamo estendere ogni φ_i a delle ψ_i definite su F , ottenendo allora la tesi per la normalità dell'estensione. Infatti $\psi_i(\alpha) = \alpha_i \in F$ e ogni α_i è una radice di f . $\square$

Proposizione 1.20. Sia F/K un'estensione finita. Sono equivalenti:

- F/K è un'estensione normale
- F è il campo di spezzamento di $f_1, \dots, f_n \in K[x]$

Dimostrazione. Supponiamo F/K normale. Poichè per ipotesi l'estensione è finita, esistono $\alpha_1, \dots, \alpha_k$ tali che $F = K(\alpha_1, \dots, \alpha_k)$. Siano allora $f_{\alpha_1}, \dots, f_{\alpha_k}$ i polinomi minimi di questi elementi. Per normalità dell'estensione, per la proposizione precedente, abbiamo che F contiene il campo di spezzamento di $f_{\alpha_1}, \dots, f_{\alpha_k}$. D'altronde, il campo di spezzamento di questi polinomi contiene $\alpha_1, \dots, \alpha_k$ e dunque contiene F . Per doppio contenimento, abbiamo allora mostrato un'implicazione.

Supponiamo ora che F sia il campo di spezzamento di $f_1, \dots, f_n$. Possiamo supporre, senza perdita di generalità, che questi polinomi siano irriducibili. Sia $\{\alpha_{i,j}\}$ l'insieme delle radici degli f_i . Allora per definizione di campo di spezzamento, $F = K(\{\alpha_{i,j}\})$. Mostriamo allora la normalità: consideriamo $\varphi: F \rightarrow \overline{K}$ tale che $\varphi|_K = id$. Sappiamo allora che $\varphi(\alpha_{i,j}) = \varphi(\alpha_{i,k})$ e dunque $\varphi(F) \subseteq F$. Notiamo però che

$$[F : K] = [\varphi(F) : \varphi(K)] = [\varphi(F) : K]$$

Di conseguenza, per motivi di dimensione come spazi vettoriali su K , si ha $\varphi(F) = F$ e dunque la tesi. $\square$

Definizione 1.21. Sia F/K un'estensione normale separabile finita. Definiamo

$$\text{Gal}(F/K) = \{\varphi: F \rightarrow F \mid \varphi|_K = \text{id}\}$$

Lemma 1.22. $\text{Gal}(F/K)$ è un gruppo rispetto alla composizione; la cardinalità di $\text{Gal}(F/K)$ è uguale al grado dell'estensione.

Dimostrazione. Chiaramente, l'elemento neutro è l'identità $\text{id}: F \rightarrow F$. Mostriamo l'esistenza dell'inversa. Sia $\varphi: F \rightarrow F$; allora $\text{Im}(\varphi) \subseteq F$. Per motivi di dimensione come K -spazi vettoriali, si ha allora la surgettività; φ è quindi un isomorfismo di campi e dunque ammette inversa. Per le proposizioni precedenti, abbiamo poi che se $[F:K] = n$, esistono esattamente n omomorfismi $\varphi_i: F \rightarrow \overline{K}$ che estendono l'identità. Per normalità di F , questi si restringono a omomorfismi $\varphi_i: F \rightarrow F$, e sono tutti e soli gli automorfismi di $\text{Gal}(F/K)$. $\square$

L'idea è ora quella di applicare la teoria dei gruppi allo studio delle estensioni. Consideriamo per esempio $f \in K[x]$ un polinomio irriducibile di grado n . f si spezza allora nella chiusura algebrica

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

Il campo di spezzamento è allora $F = K(\alpha_1, \dots, \alpha_n)$; sappiamo anche che gli automorfismi possono solo mischiare le radici. Infatti:

Teorema 1.23. $\text{Gal}(F/K)$ si immerge in S_n .

Dimostrazione. Interpretiamo $S_n = S\{\alpha_1, \dots, \alpha_n\}$. Consideriamo la mappa

$$\begin{aligned} \Phi: \quad \text{Gal}(F/K) &\longrightarrow S_n \\ \varphi &\longmapsto \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \end{aligned}$$

Tale applicazione è ben definita perchè l'immagine di una radice di f è ancora una radice di f e inoltre una applicazione tra campi è iniettiva e dunque la restrizione è una bigezione. Mostriamo che è un omomorfismo.

$$\Phi(\varphi \circ \rho) = \varphi \circ \rho|_{\{\alpha_1, \dots, \alpha_n\}} = \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \circ \rho|_{\{\alpha_1, \dots, \alpha_n\}} = \Phi(\varphi) \circ \Phi(\rho)$$

Inoltre Φ è iniettivo. Infatti, $\text{Ker}(\Phi) = \{\varphi \in \text{Gal}(F/K) \mid \varphi|_{\{\alpha_1, \dots, \alpha_n\}} = \text{id}\}$, cioè $\varphi(\alpha_i) = \alpha_i$. Poichè gli α_i e i loro prodotti generano F come K -spazio vettoriale, se un omomorfismo fissa questi, allora fissa tutto F ; di conseguenza $\text{Ker}(\varphi) = \{\text{id}\}$. $\square$

Corollario 1.24. $[F:K] \mid n!$

Dimostrazione. Per il teorema di Lagrange, la cardinalità di un sottogruppo deve dividere la cardinalità del gruppo; la cardinalità di S^n è $n!$. $\square$

Esempio. Tutte le estensioni di grado 2 sono normali. Supponiamo infatti $[F : K] = 2$ e sia $\alpha \in F \setminus K$. Abbiamo allora $F = K(\alpha)$ e $f_\alpha = x^2 + ax + b$ è il suo polinomio minimo. Di conseguenza, su F , il polinomio si spezza completamente e dunque F è il campo di spezzamento di f_α .

Radici dell'unità Delle estensioni normali particolarmente semplici sono i campi di spezzamento dei polinomi ciclotomici, cioè le estensioni per le radici dell'unità del campo. Sia ζ_n una radice n -esima primitiva dell'unità. Sappiamo allora che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(f_{\zeta_n})$. Poiché $g(x) = x^n - 1$ è un polinomio di $\mathbb{Q}[x]$ che si annulla in ζ_n , abbiamo che $f_{\zeta_n} \mid g$ e dunque $g = f_{\zeta_n} \cdot h$. Per separabilità di $\mathbb{Q}$, inoltre, si ha $(f_{\zeta_n}, h) = 1$. Fissato $i \in \{1, \dots, n\}$, consideriamo l'omomorfismo

$$\begin{array}{ccc} \varphi_i: & \mathbb{Q}(\zeta_n) & \longrightarrow \mathbb{Q}(\zeta_n) \\ & \zeta_n & \longmapsto \zeta_n^i \end{array}$$

Per essere un automorfismo, condizione necessaria è che $\text{ord}(\zeta_n) = \text{ord}(\zeta_n^i)$. Questo accade se e solo se $(i, n) = 1$ e dunque il numero di automorfismi è $\leq \phi(n)$, dove ϕ è la funzione di Eulero. Notiamo che altri automorfismi non possono esistere perché l'immagine di ζ_n deve essere una radice di g e le radici di g sono ζ_n^i al variare di i .

Mostriamo ora che se $(i, n) = 1$, allora $f_{\zeta_n}(\zeta_n^i) = 0$. Sia ora $p \in \mathbb{N}$ un primo, $(p, n) = 1$ e sia γ tale che $f_{\zeta_n}(\gamma) = 0$. Mostriamo che $f_{\zeta_n}(\gamma^p) = 0$. Sicuramente $0 = g(\gamma^p) = f_{\zeta_n}(\gamma^p)h(\gamma^p)$. Se per assurdo $h(\gamma^p) = 0$, allora $h(x^p)$ si annulla in γ e di conseguenza $f_{\zeta_n} \mid h(x^p)$ (perché f_{ζ_n} è irriducibile). Riducendo la relazione modulo p , si ottiene

$$\bar{f}_{\zeta_n} \mid \overline{h(x^p)} = \overline{h(x)}^p$$

e dunque $(\bar{f}_{\zeta_n}, \bar{h}) \neq 1$. Di conseguenza, dalla relazione $\bar{f} = \bar{f}_{\zeta_n} \bar{h}$ si ottiene che $\bar{f}$ ha radici multiple. D'altro canto, $\bar{f}' = nx^{n-1}$ e $p \nmid n$. Di conseguenza $(\bar{f}, \bar{f}') = 1$, da cui un assurdo per il criterio della derivata. Abbiamo così dimostrato che tutti e soli gli automorfismi di $\mathbb{Q}(\zeta_n)$ che fissano il campo $\mathbb{Q}$ sono i φ_i . Di conseguenza il gruppo di Galois dell'estensione è

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

e il grado è $\phi(n)$.

Il teorema dell'Elemento Primitivo Abbiamo visto che non tutte le estensioni algebriche sono finite; questo accade solo quando l'estensione è finitamente

generata. In tal caso, in ipotesi di separabilità, possiamo in realtà trovare un generatore dell'estensione:

Teorema 1.25 (dell'elemento primitivo). *Sia K un campo e sia E/K un'estensione finita e separabile. Allora esiste un elemento $\alpha \in E$ tale che $E = K(\alpha)$.*

Dimostrazione. Se $|K| < \infty$, poichè ogni sottogruppo moltiplicativo finito di un campo è ciclico, si ha che $E^* = \langle \alpha \rangle$ e dunque $E = K(\alpha)$. Supponiamo allora che K sia infinito. Poichè l'estensione è finita, è in particolare finitamente generata, e dunque $E = K(\alpha_1, \dots, \alpha_n)$. Mostriamo l'enunciato per induzione sul numero di generatori. Supponiamo cioè $E = K(\alpha, \beta)$ e $[E : K] = n$. Mostriamo che esiste $t \in K$ per il quale $E = K(\alpha + t\beta)$, cioè che $\alpha + t\beta$ ammette, per un'opportuna scelta di t , n coniugati distinti. Siano $\varphi_1, \dots, \varphi_n$ le estensioni a E dell'identità

$$\varphi_i: E \longrightarrow \bar{K} \qquad \varphi_i|_K = id$$

Definiamo allora il polinomio

$$F(x) = \prod_{i < j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)) \in \bar{K}[x]$$

Notiamo che F non è il polinomio nullo; infatti:

$$\begin{aligned} F = 0 &\iff \exists i < j \text{ tali che } \varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta) \\ &\iff (\varphi_i(\alpha) = \varphi_j(\alpha)) \wedge (\varphi_i(\beta) = \varphi_j(\beta)) \\ &\iff i = j \end{aligned}$$

Per il teorema di Ruffini, F ha allora al più $\deg(F)$ radici in K ; poichè il campo è infinito, esiste allora $t \in K$ per il quale $F(t) \neq 0$. Di conseguenza,

$$\varphi_i(\alpha + t\beta) \neq \varphi_j(\alpha + t\beta)$$

e dunque $\alpha + t\beta$ ha n coniugati distinti. Per induzione, la tesi. $\square$

1.2 Corrispondenza di Galois

Vogliamo ora studiare in che modo gli automorfismi del gruppo di Galois siano legato alle sottoestensioni dell'estensione data. Per definizione, ogni automorfismo del gruppo $Gal\left(\frac{L}{K}\right)$ fissa almeno il campo K . Chiaramente, potrebbe anche fissare altri elementi:

Definizione 1.26. Sia H un sottogruppo di $\text{Gal}\left(\frac{L}{K}\right)$. Definiamo

$$\text{Fix}(H) = L^H := \{\gamma \in L \mid \sigma(\gamma) = \gamma \ \forall \sigma \in H\}$$

Chiaramente L^H è un sottocampo di L .

Proposizione 1.27. Sia H un sottogruppo di $\text{Gal}\left(\frac{L}{K}\right)$. Allora

$$L^H = K \iff H = \text{Gal}\left(\frac{L}{K}\right)$$

Dimostrazione. ($\Rightarrow$) Supponiamo $L^H = K$ e sia $|G| = [L : K]$. Per il teorema dell'elemento primitivo 1.25, $L = K(\alpha)$. Consideriamo allora

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

Sicuramente, per normalità dell'estensione, $f \in L[x]$. In realtà, si può dire di più. Sia infatti $\rho \in H$. Allora, notando che la moltiplicazione per un elemento di un gruppo induce una permutazione del gruppo stesso,

$$\rho \circ f(x) = \rho\left(\prod_{\sigma \in H} (x - \sigma(\alpha))\right) = \prod_{\sigma \in H} (x - \rho \circ \sigma(\alpha)) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = f(x)$$

Dunque, $f \in L^H[x] = K[x]$. Poichè $\deg(f) = |H| \leq |\text{Gal}\left(\frac{L}{K}\right)|$ e $f(\alpha) = 0$, ne segue che f è il polinomio minimo di α che però genera l'estensione. Quindi

$$|H| = [K(\alpha) : K] = \left| \text{Gal}\left(\frac{L}{K}\right) \right|$$

da cui l'uguaglianza cercata.

($\Leftarrow$) Mostriamo che $L^H = K$. Per definizione $L^H \supseteq K$. Supponiamo per assurdo che $L^H \supsetneq K$ e sia $\alpha \in L^H \setminus K$. Sia $d = [K(\alpha) : K]$. Per il teorema 1.17, esistono $\varphi_1, \dots, \varphi_d$ immersioni $\varphi_i: K(\alpha) \rightarrow \bar{K}$; in particolare uno di questi omomorfismi non fissa α e possiamo chiamarlo φ . Possiamo ora estendere φ a $\tilde{\varphi}: E \rightarrow \bar{K}$. Dunque $\tilde{\varphi} \in \text{Gal}\left(\frac{L}{K}\right)$ ma $\tilde{\varphi}(\alpha) \neq \alpha$, mentre $\alpha \in L^H$, da cui un assurdo.

□

Mostriamo ora che esiste una corrispondenza tra i sottocampi di L e i sottogruppi del gruppo di Galois.

Definizione 1.28. Sia L/K un'estensione di Galois. Definiamo

$$\mathcal{E}_{L/K} := \{F \mid K \subseteq F \subseteq L\} \quad \mathcal{G}_{L/K} := \{H < \text{Gal}(L/K)\}$$

Teorema 1.29 (Primo Teorema di Corrispondenza). *Sia E/K un'estensione normale finita. Allora esiste una corrispondenza biunivoca tra $\mathcal{E}_{E/K}$ e $\mathcal{G}_{E/K}$ data da*

$$\begin{aligned} \mathcal{E}_{E/K} &\longleftrightarrow \mathcal{G}_{E/K} \\ F &\xrightarrow{\alpha} \text{Gal}(E/F) \\ \text{Gal}(E/F) &\xleftarrow{\beta} E^{\text{Gal}(E/F)} \end{aligned}$$

Dimostrazione. Mostriamo che le applicazioni indicate sono l'una l'inversa dell'altra, cioè

$$\alpha \circ \beta(H) = H \quad \beta \circ \alpha(F) = F$$

Mostriamo che $\alpha \circ \beta = id$. Sia H un sottogruppo di $\text{Gal}(E/F)$. Poiché $\beta(H) = \text{Gal}(E/E^H)$, dobbiamo mostrare che questo è $\text{Gal}(E/E^H) = H$.

$\supseteq$ Quest'inclusione è ovvia, poichè H fissa E^H per definizione.

$\subseteq$ Discende dalla precedente proposizione; detto infatti $L = E^H$, si ha che $H = \text{Gal}(E/L)$, come voluto.

Mostriamo ora che $\beta \circ \alpha = id$. Sia F un sottocampo di E che contiene K . Bisogna mostrare che $F = E^{\text{Gal}(E/F)}$.

$\subseteq$ Dalla definizione di $\text{Gal}(E/F)$, si ha che ogni $\varphi \in \text{Gal}(E/F)$ fissa F .

$\supseteq$ Discende dalla precedente proposizione; l'unico sottogruppo che fissa solo F è infatti $\text{Gal}(E/F)$.

□

Teorema 1.30 (Secondo teorema di corrispondenza). *Sia E/K un'estensione di Galois e sia F una sottoestensione. Allora*

$$F/K \text{ è di Galois} \iff F = E^H \text{ dove } H \trianglelefteq \text{Gal}(E/K)$$

In tal caso, vale l'isomorfismo

$$\text{Gal}(F/K) \simeq \text{Gal}(E/K) / \text{Gal}(E/F)$$