

Poiché per il Lemma 2.3.4, si ha $|E_1 : F| = |E_1 : F(\alpha)||F(\alpha) : F|$ e $|F(\alpha) : F| = d$ allora

$$\begin{aligned} |\{\sigma : E_1 \rightarrow E_2 \mid \sigma(a) = \bar{a} \forall a \in F\}| &= |A_1| + \dots + |A_d| \\ &= |E_1 : F[\alpha]| + \dots + |E_1 : F[\alpha]| \\ &= d|E_1 : F[\alpha]| \\ &= |E_1 : F|. \end{aligned}$$

□

Corollario 2.4.11 *Sia F un campo e sia f un polinomio in $F[x]$. Sia $E \supset F$ un campo di spezzamento di f su F . Supponiamo che ogni fattore irriducibile di f abbia radici distinte in E . Allora esistono esattamente $|E : F|$ automorfismi $\sigma : E \rightarrow E$ tali che $\sigma(a) = a$ per ogni $a \in F$.*

Esempio 2.4.12 Sia $F = \mathbb{F}_2(t)$ il campo delle funzioni razionali su \mathbb{F}_2 in t e sia $f = x^2 + t \in F[x]$. Il polinomio f è irriducibile in $F[x]$ (Esercizio 3.5.2). Sia α una radice di f nel campo di spezzamento $E = F(\sqrt{t})$. Avremo che

$$(x + \alpha)^2 = x^2 + 2\alpha x + \alpha^2 = x^2 + t,$$

dato che $2\alpha x$ è zero in un campo di caratteristica 2. Segue che f ha due radici uguali in E . Infatti esiste un solo automorfismo $E \rightarrow E$ che è l'identità su F , e questo coincide con la mappa identica.

2.5 Esercizi

Esercizio 2.5.1 Sia F/\mathbb{Q} un'estensione di campi e sia $\sigma : F \rightarrow F$ un automorfismo.

1. Provare che $\sigma(1) = 1$.
2. Provare che $\sigma(a) = a$ per ogni $a \in \mathbb{Q}$.
3. Posto $F = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, provare che $\sigma : F \rightarrow F$, definito da $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, è un automorfismo di F . Provare che, fatta eccezione per l'identità, σ è l'unico automorfismo di F .

Esercizio 2.5.2 Sia $\alpha = 2 - \sqrt{3}$. Calcolare il polinomio minimo di α su \mathbb{Q} e il grado $|\mathbb{Q}(\alpha) : \mathbb{Q}|$. Analogo esercizio per $\alpha = \sqrt{3 + \sqrt{2}}$.

Esercizio 2.5.3 Provare che $\mathbb{Q}(\sqrt{2})(\sqrt{7}) = \mathbb{Q}(\sqrt{2} + \sqrt{7})$ e calcolare il polinomio minimo di $\sqrt{2} + \sqrt{7}$ su \mathbb{Q} e $|\mathbb{Q}(\sqrt{2} + \sqrt{7}) : \mathbb{Q}|$.

Esercizio 2.5.4 Provare che non esistono $a, b \in \mathbb{Q}$ con $(a + b\sqrt{2})^2 = 3$ e che $x^2 - 3$ è irriducibile in $\mathbb{Q}(\sqrt{2})[x]$. Provare che $|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 4$.

Esercizio 2.5.5 Provare che $\mathbb{Q}(\sqrt[4]{2}, i)$ è un campo di spezzamento di $x^4 - 2$ su \mathbb{Q} . A cosa è uguale $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}|$?

Esercizio 2.5.6 Sia $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Sia $\zeta \in \mathbb{C}$ uno zero di f . Provare che $\zeta^5 = 1$ e che $\zeta^2, \zeta^3, \zeta^4$ sono gli ancora radici di f in \mathbb{C} . Provare che $\mathbb{Q}(\zeta)$ è un campo di spezzamento di f su \mathbb{Q} . A cosa è uguale $|\mathbb{Q}(\zeta) : \mathbb{Q}|$?

Esercizio 2.5.7 Provare che $x^n - 2 \in \mathbb{Q}[x]$ è irriducibile e concludere che $|\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}| = n$. Provare che $|\mathbb{R} : \mathbb{Q}| = \infty$.

Esercizio 2.5.8 Si consideri l'Esempio 2.4.5. Provare che $\alpha, \frac{1}{2}(\beta - \alpha), -\frac{1}{2}(\beta + \alpha)$ sono radici distinte di f . Provare che $\mathbb{Q}(\alpha, \beta)$ è un campo di spezzamento di f .

Esercizio 2.5.9 Sia f un polinomio di grado n in $F[x]$. Sia E un campo di spezzamento di f su F . Si mostri che $|E : F|$ divide $n!$.

Si può procedere nel seguente modo:

1. Se f è irriducibile, esiste un campo $F(\alpha)$ dove α è una radice di f . In $F(\alpha)[x]$ si può scrivere $f = (x - \alpha)h$. Adesso $E/F(\alpha)$ è il campo di spezzamento di h su $F(\alpha)$. Usando la formula dei gradi si conclude per induzione.
2. Se f è riducibile, allora $f = gh$ dove i gradi di g, h sono rispettivamente k, l con $k + l = n$. Sia K/F un campo di spezzamento di h su F , con $K \subset E$. Allora E/K è un campo di spezzamento di g su K . Si conclude ancora usando la formula dei gradi.

che è isomorfo al 4-gruppo di Klein.

Esempio 3.4.4 Sia $f = x^3 - x - 1$ in $\mathbb{Q}[x]$ e sia $\mathbb{Q}(\alpha, \beta) \supset \mathbb{Q}$ il suo campo di spezzamento (vedere Esempio 2.4.5). In questo caso il gruppo di Galois dell'estensione $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ è isomorfo a un sottogruppo di S_3 . Poiché il grado dell'estensione è 6, segue che il gruppo di Galois è isomorfo a S_3 e ogni permutazione delle radici del polinomio f induce un automorfismo del campo.

Sia per esempio τ il 3-ciclo tale che

$$\begin{aligned}\tau(\alpha) &= -\frac{1}{2}(\alpha + \beta) \\ \tau(-\frac{1}{2}(\alpha + \beta)) &= \frac{1}{2}(\beta - \alpha) \\ \tau(\frac{1}{2}(\beta - \alpha)) &= \alpha.\end{aligned}$$

Allora

$$\frac{1}{2}(\beta - \alpha) = \tau(-\frac{1}{2}(\alpha + \beta)) = \frac{1}{4}(\alpha + \beta) - \frac{1}{2}\tau(\beta),$$

e da questo segue che $\tau(\beta) = -\frac{1}{2}\beta + \frac{3}{2}\alpha$.

3.5 Esercizi

Esercizio 3.5.1 Sia E/F un'estensione di campi con grado $|E : F| = 2$ e supponiamo che la caratteristica di F sia diversa da 2. Provare che E/F è un'estensione di Galois.

Esercizio 3.5.2 Sia $F = \mathbb{F}_2(t)$ il campo delle funzioni razionali nell'indeterminata t .

1. Provare che $x^2 - t$ è irriducibile in $F[x]$.
2. Sia $E = F[x]/(x^2 - t)$. Provare che E è un campo, e calcolare il gruppo $\text{Gal}(E/F)$ (in caratteristica 2 risulta $(u + v)^2 = u^2 + v^2$).
3. L'estensione E/F è un'estensione di Galois?

Esercizio 3.5.3 Sia E/F un'estensione di Galois tale che $|E : F|$ sia finito. Poniamo $G = \text{Gal}(E/F)$. Per $\alpha \in E$ consideriamo

$$\text{Tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$$

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

detti rispettivamente *traccia* e *norma* di α .

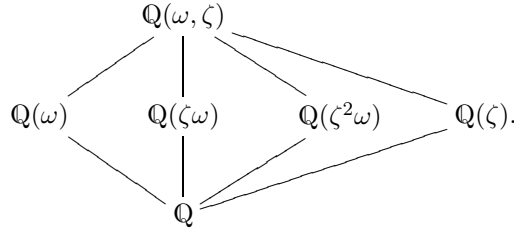
1. Provare che $\text{Tr}(\alpha), N(\alpha)$ sono elementi di F .
2. Sia $H = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$ lo *stabilizzatore* di α . Supponiamo che $f = x^m + a_{m-1}x^{m-1} + \dots + a_0$ sia il polinomio minimo di α su F . Provare che m è uguale all'indice di H in G (che per definizione è $|G|/|H|$).
3. Provare che $N(\alpha) = (-1)^{|G|} a_0^{|H|}$.
4. Provare che $\text{Tr}(\alpha) = -|H|a_{m-1}$.

Esercizio 3.5.4 Sia $\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid a \text{ è algebrico su } \mathbb{Q}\}$.

1. Provare che $\overline{\mathbb{Q}}$ è un campo.
2. Provare che $|\overline{\mathbb{Q}} : \mathbb{Q}| = \infty$ (suggerimento: si possono considerare i sottocampi $\mathbb{Q}(\sqrt[n]{2})$).
3. Provare che $\overline{\mathbb{Q}}/\mathbb{Q}$ è un'estensione di Galois (il gruppo $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ si chiama *gruppo di Galois assoluto* di \mathbb{Q}).

Esercizio 3.5.5 Sia F un campo di caratteristica $p > 0$. Sia E/F un'estensione algebrica con la proprietà che, se gli elementi $\alpha_1, \dots, \alpha_n \in E$ sono linearmente indipendenti su F , allora anche gli elementi $\alpha_1^p, \dots, \alpha_n^p$ sono linearmente indipendenti su F . Si dimostri che E/F è un'estensione separabile.

è un campo di spezzamento del polinomio $x^3 - 2$ e i campi intermedi possono essere così rappresentati



Esiste un automorfismo σ nel gruppo $\text{Gal}(\mathbb{Q}(\omega, \zeta)/\mathbb{Q})$ con $\omega \mapsto \zeta^2\omega$ e $\zeta \mapsto \zeta$. Abbiamo $\sigma(\mathbb{Q}(\omega)) = \mathbb{Q}(\zeta^2\omega)$ e $\sigma(\mathbb{Q}(\zeta^2\omega)) = \mathbb{Q}(\zeta\omega)$. Quindi $\mathbb{Q}(\omega)$, $\mathbb{Q}(\zeta\omega)$ e $\mathbb{Q}(\zeta^2\omega)$ non sono campi stabili e quindi le estensioni $\mathbb{Q}(\omega)/\mathbb{Q}$, $\mathbb{Q}(\zeta\omega)/\mathbb{Q}$ e $\mathbb{Q}(\zeta^2\omega)/\mathbb{Q}$ non sono estensioni di Galois.

Invece $\mathbb{Q}(\zeta)$ è un campo stabile e abbiamo $\mathbb{Q}(\zeta) = E^H$ dove H è un sottogruppo normale di ordine 3 di $\text{Gal}(\mathbb{Q}(\omega, \zeta)/\mathbb{Q})$.

Si ha che $\mathbb{Q}(\zeta)/\mathbb{Q}$ è il campo di spezzamento del polinomio $x^2 + x + 1$ quindi $\mathbb{Q}(\zeta)/\mathbb{Q}$ è un'estensione di Galois. Inoltre, per $\tau(\zeta) = \zeta^2$ abbiamo

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{1, \tau\} \cong \text{Gal}(\mathbb{Q}(\omega, \zeta)/\mathbb{Q})/H.$$

4.3 Esercizi

Esercizio 4.3.1 Sia $f = x^4 - x^2 + 1$ e sia $E = \mathbb{Q}(\alpha)$ il campo di spezzamento di f come nell'Esempio 4.1.1. Sia $\beta = \alpha - \frac{1}{2}\alpha^3$. Provare che il polinomio minimo di β su \mathbb{Q} ha grado 2 e calcolarlo.

Esercizio 4.3.2 Determinare il campo di spezzamento del polinomio $x^5 - 1$ su \mathbb{Q} e una tavola di moltiplicazione del relativo gruppo di Galois. Trovare i sottogruppi e i campi intermedi. Ripetere l'esercizio per $x^8 - 1$.

Esercizio 4.3.3 Determinare il campo di spezzamento per $x^3 - 2$ su \mathbb{Q} e una tavola di moltiplicazione del relativo gruppo di Galois. Provare che questo è isomorfo a S_3 . Trovare i sottogruppi e i campi intermedi.

Esercizio 4.3.4 Sia E/F un'estensione di Galois di grado finito. Sia $G = \text{Gal}(E/F)$. Siano H_1, H_2 due sottogruppi di G . Sappiamo che anche $H_1 \cap H_2$ è un sottogruppo di G . Sia K il più piccolo sottocampo di E che contiene $\alpha(H_1)$ e $\alpha(H_2)$ (quindi, se $K' \subset E$ è un campo che li contiene entrambi, allora $K \subset K'$).

1. Provare che $K \subset \alpha(H_1 \cap H_2)$.
2. Provare che $\beta(K) \subset H_1 \cap H_2$.
3. Provare che $K = \alpha(H_1 \cap H_2)$.

Esercizio 4.3.5 Sia E/F un'estensione di Galois di grado finito. Sia $G = \text{Gal}(E/F)$. Siano H_1, H_2 due sottogruppi di G . Sia H il più piccolo sottogruppo di G che contiene H_1, H_2 (in altre parole, H è il sottogruppo di G generato da H_1, H_2).

1. Provare che $E^H \subset E^{H_1} \cap E^{H_2}$.
2. Per un campo intermedio $F \subset K \subset E$ scriviamo $\beta(K) = \text{Gal}(E/K)$. Provare che $H_i \subset \beta(E^{H_1} \cap E^{H_2})$ per $i = 1, 2$.
3. Provare che $\beta(E^H) \subset \beta(E^{H_1} \cap E^{H_2})$.
4. Provare che $E^{H_1} \cap E^{H_2} = E^H$.

Esercizio 4.3.6 Consideriamo il polinomio $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. È dato che f è irriducibile. Sia

$$E = F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Q}, \alpha^3 = 3\alpha - 1\}.$$

Allora $F(\alpha)$ è isomorfo a $\mathbb{Q}[x]/(f)$ e quindi è un campo. Siano $\alpha_1 = \alpha$, $\alpha_2 = \alpha^2 - 2$, $\alpha_3 = -\alpha^2 - \alpha + 2$.

1. Provare che $\alpha_1, \alpha_2, \alpha_3$ sono le radici di f in E .
2. Provare che E è un campo di spezzamento di f su \mathbb{Q} .
3. Costruire il gruppo di Galois di E/\mathbb{Q} . Quanti sono i campi K tali che $F \subset K \subset E$?

Poiché $x^6 + x^3 + 1 = \Phi_9$ segue che $E = \mathbb{F}_5(\zeta)$ dove ζ è una radice primitiva nona dell'unità per la Proposizione 5.1.2. Sia $\alpha \in E^*$ un elemento primitivo. Abbiamo $|E^*| = 5^6 - 1 = 2^3 \cdot 3^2 \cdot 7 \cdot 31$. In particolare 9 divide l'ordine di α . Sia $s = (5^6 - 1)/9 = 1736$.

Allora $\zeta = \alpha^s$ è una radice primitiva nona dell'unità.

5.4 Esercizi

Esercizio 5.4.1 Calcolare Φ_9 e Φ_{12} .

Esercizio 5.4.2 Sia E il campo di spezzamento di $x^9 - 1$ su \mathbb{Q} . Determinare la tavola di moltiplicazione del gruppo $\text{Gal}(E/\mathbb{Q})$. Trovare i sottogruppi e i campi intermedi.

Esercizio 5.4.3 Sia E il campo di spezzamento di $x^{12} - 1$ su \mathbb{Q} . Provare che $\text{Gal}(E/\mathbb{Q})$ è isomorfo al 4-gruppo di Klein (vedere l'Esercizio 5.4.1 e l'Esempio 3.1.5).

Esercizio 5.4.4 Trovare un polinomio primitivo di grado 3 su \mathbb{F}_3 . Costruire una tavola dei logaritmi per \mathbb{F}_{27} .

Esercizio 5.4.5 Trovare un polinomio primitivo di grado 5 su \mathbb{F}_2 . Costruire una tavola dei logaritmi per \mathbb{F}_{32} .

Esercizio 5.4.6 Sia F un campo di caratteristica $p > 0$.

1. Provare che $(a + b)^p = a^p + b^p$ per ogni $a, b \in F$.
2. Sia $\varphi_p : F \rightarrow F$ definita da $\varphi_p(a) = a^p$. Questa viene detta *mappa di Frobenius*. Provare che φ_p è un omomorfismo iniettivo di campi (suggerimento: per dimostrare l'injectività si tenga conto del fatto che in $F[x]$ si ha $(x - 1)^p = x^p - 1$).
3. Provare che φ_p è un automorfismo se F è finito.

Possiamo concludere che K_{j+1}/K_j è un'estensione di Galois. Ma $K_{j+1} = K_j(\varepsilon)$ con $\varepsilon^3 = a$, quindi K_{j+1} contiene una radice del polinomio $x^3 - a$. Poiché K_{j+1}/K_j è un'estensione di Galois allora contiene tutte le radici, cioè $\varepsilon, \varepsilon\omega, \varepsilon\omega^2$ dove $\omega \in \mathbb{C}$ è una radice primitiva terza dell'unità.

Ma $\varepsilon\omega$ e $\varepsilon\omega^2$ non appartengono a \mathbb{R} quindi K non può essere reale. Abbiamo quindi una contraddizione. \square

Dal Teorema 6.5.2, appena dimostrato, segue che per esprimere le radici di f (che sono elementi di \mathbb{R}) in termini di radicali, abbiamo sempre bisogno di elementi di $\mathbb{C} \setminus \mathbb{R}$.

6.6 Esercizi

Esercizio 6.6.1 Lo scopo di questo esercizio è di risolvere per radicali un'equazione che ha un gruppo di Galois risolubile.

Sia $f = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$. È dato che f è irriducibile. Sia $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$ (quindi $\alpha^4 = \alpha^3 - \alpha^2 + \alpha - 1$).

1. Dimostrare che $\alpha, -\alpha^2, \alpha^3, -\alpha^3 + \alpha^2 - \alpha + 1$ sono le radici di f in $\mathbb{Q}(\alpha)$ (per l'ultimo si può osservare che se $\alpha_1, \dots, \alpha_n$ sono le radici di $x^n + ax^{n-1} + \dots$ allora $-\alpha_1 - \dots - \alpha_n = a$).
2. Calcolare il gruppo di Galois G di $\mathbb{Q}(\alpha)/\mathbb{Q}$ e provare che questo è ciclico (e quindi risolubile).
3. Trovare un sottogruppo normale $H \subset G$ di indice 2.
4. Sia $\gamma = -\alpha^3 + \alpha^2 + 1$. Provare che $\mathbb{Q}(\alpha)^H = \mathbb{Q}(\gamma)$. Trovare il polinomio minimo di γ e il gruppo $\text{Gal}(\mathbb{Q}(\gamma)/\mathbb{Q})$.
5. Sia $M = \mathbb{Q}(\gamma)$. Vogliamo scrivere M come estensione radicale di \mathbb{Q} . Poniamo $\text{Gal}(M/\mathbb{Q}) = \{1, \tau\}$. Sia $\delta \in M$ tale che $\tau(\delta) = -\delta$. Provare che $\delta^2 \in \mathbb{Q}$ e trovare un tale δ .
6. Adesso $\mathbb{Q}(\alpha) = M(\alpha)$ sia un'estensione di M di grado 2. Provare che $\text{Gal}(\mathbb{Q}(\alpha)/M) = H$. Poniamo $H = \{1, \pi\}$.
7. Provare che $\pi(\alpha) = -\alpha + \gamma$.

8. Adesso vogliamo vedere $M(\alpha)$ come estensione radicale di M . Sia $\epsilon \in M(\alpha)$ tale che $\pi(\epsilon) = -\epsilon$. Provare che $\epsilon^2 \in M$ e trovare un tale ϵ .
9. Concludere che $\mathbb{Q} \subset M \subset \mathbb{Q}(\alpha)$ è un'estensione radicale. Trovare un'espressione per α come elemento di \mathbb{C} (tramite le radici).

Esercizio 6.6.2 Lo scopo di questo esercizio è di provare il casus irreducibilis in un caso particolare.

Sia $y \in \mathbb{C}$ con $y^3 = \frac{1}{2}(-1 + \sqrt{-3})$ e $\zeta \in \mathbb{C}$ uno zero di $\zeta^2 + \zeta + 1 = 0$.

1. Provare che $\mathbb{Q}(y, \zeta)/\mathbb{Q}$ è un'estensione radicale.
2. Consideriamo il polinomio $f = x^3 - 3x + 1$. Sia $z = \frac{1}{y}$. Provare che $y+z$, $\zeta y + \zeta^2 z$ e $\zeta^2 y + \zeta z$ sono le radici di f in $\mathbb{Q}(y, \zeta)$ (non è difficile provare che sono distinte, ma non viene richiesto). Concludere che f è risolubile per radicali.
3. Provare che ognuno degli intervalli $[-2, 0]$, $[0, 1]$, $[1, 2]$ contiene una radice di f . Il campo di spezzamento di f è uguale a $\mathbb{Q}(y, \zeta)$?
4. Calcolare il gruppo di Galois di E/\mathbb{Q} , dove E è un campo di spezzamento di f su \mathbb{Q} (suggerimento: controllare tra gli esercizi precedenti). Il gruppo è risolubile?
5. Provare che E/\mathbb{Q} non è un'estensione radicale (suggerimento: basta provare che non esiste $\omega \in E$ con $\omega^m \in \mathbb{Q}$ per un certo m (perché?). Supponiamo che esista un tale ω . Scriviamo $\omega^m = \alpha$ e sia $f = x^m - \alpha$. Provare che f ha tutte le radici in E , e dedurre una contraddizione con il fatto che E è reale).