

RIASSUNTI DI ALGEBRA

MANUEL DEODATO

INDICE

1	Teoria dei gruppi	2
1.1	Automorfismi e azioni	2
1.2	I p-gruppi	3
1.3	Teoremi di Cauchy e Cayley	3
1.4	Commutatore e gruppo derivato	3
1.5	Il gruppo diedrale	4
1.6	Il gruppo simmetrico	5
1.7	I quaternioni	7
1.8	Prodotti diretti	8
1.9	Prodotti semi-diretti	8
1.10	Teorema di struttura per gruppi abeliani finiti	9
1.11	Teoremi di Sylow	9
1.12	Risultati sulle classificazioni	10
1.13	Risultati vari sui gruppi	10
2	Esercizi	11
2.1	Esercizi su gruppi 1	11
2.2	Esercizi su campi e anelli 1	11
2.3	Esercizi su gruppi 2	21
2.4	Esercizi su anelli 2	22
A	Nozioni fondamentali	23
A.1	Applicazioni	23
A.2	Relazioni	23

1 | TEORIA DEI GRUPPI

§1.1 Automorfismi e azioni

Proposizione 1.1. Dato un gruppo G , si ha che $\text{Int } G \triangleleft \text{Aut } G$ e $\text{Int } G \cong G/Z(G)$.

Definizione 1.1 (Azione). Un'azione di G gruppo su X insieme è un omomorfismo

$$\gamma : \begin{array}{ll} G & \longrightarrow S(X) = \{f : X \rightarrow X \mid f \text{ biettiva}\} \\ g & \longmapsto \psi_g : \psi_g(x) = g \cdot x \end{array}$$

Cioè un'azione di G permette di identificare un modo in cui un elemento del gruppo può agire (tramite una permutazione) sull'insieme X .

Un'azione di gruppo è ben definita se:

- (a). $e \cdot x = x$, $\forall x \in X$, con $e \in G$ identità;
- (b). $h \cdot (g \cdot x) = (hg) \cdot x$, per $g, h \in G$ e $x \in X$.

Relativamente ad un'azione $\gamma : G \rightarrow S(X)$, si definiscono:

- **orbita:** dato $x \in X$, la sua orbita è l'insieme $\text{Orb } x = \{g \cdot x \mid g \in G\}$;
- **stabilizzatore:** dato $x \in X$, il suo stabilizzatore è l'insieme

$$\text{Stab } x = \{g \in G \mid g \cdot x = x\} < G$$

Le orbite partizionano X , visto che $x \sim_\gamma y \iff \text{Orb } x = \text{Orb } y$, quindi:

$$|X| = \sum_{x \in \mathcal{R}} |\text{Orb } x|$$

Lemma 1.0.1 (Orbita-stabilizzatore). Esiste una biezione $\text{Orb } x \rightarrow G/\text{Stab } x$ definita da $g \cdot x \mapsto g \text{Stab } x$.

Per $X = G$ e $\gamma : G \rightarrow \text{Int } G \subset S(G)$ si ha l'azione per coniugio. Le orbite sono le **classi di coniugio** $\text{Cl}(x)$ e gli stabilizzatori sono detti **centralizzatori** $Z(x)$. Per il lemma orbita-stabilizzatore, si ha $|G| = |\text{Cl}(x)||Z(x)|$.

Si può far agire G su $X = \{H \leq G\}$ con $g \cdot H = gHg^{-1}$. In questo caso, le orbite non hanno un nome particolare, ma gli stabilizzatori si dicono **normalizzatori** $N_G(H)$. In questo senso, $H \triangleleft G \iff N_G(H) = G$. Questo significa che $N_G(H)$ contiene tutti i generatori g_1, \dots, g_n di G , quindi $g_i H g_i^{-1} = H, \forall i$.

Dall'azione per coniugio, si ottiene la **formula delle classi di coniugio**:

$$|G| = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z(x)|}$$

§1.2 I p-gruppi

Definizione 1.2. Un p -gruppo è un gruppo G di ordine p^n per qualche $n \in \mathbb{N}$.

Proposizione 1.2. Il centro di un p -gruppo è non-banale.

Proposizione 1.3. Un gruppo di ordine p^2 è abeliano.

Teorema 1.1. Ogni p -gruppo G di ordine p^n ha sottogruppi G_k di ordine p^k , $k = 0, \dots, n$ tali che

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

§1.3 Teoremi di Cauchy e Cayley

Teorema 1.2 (Cauchy). Sia p un primo e G un gruppo finito; se $p \mid |G|$, allora G ha un elemento di ordine p .

Teorema 1.3 (Cayley). Ogni gruppo G è isomorfo a un sottogruppo di $S(G)$. Se $|G| = n$, allora $G \hookrightarrow S_n$.

§1.4 Commutatore e gruppo derivato

Definizione 1.3 (Derivato). Dato G gruppo, si definisce il derivato come

$$G' = [G : G] := \langle [g, h] \mid g, h \in G \rangle$$

cioè è il più piccolo sottogruppo di G contenente tutti i commutatori.

Le sue proprietà sono le seguenti:

- $G' = \{e\} \iff G$ abeliano;
- $G' \triangleleft G$;
- G' caratteristico in G ;
- se $H \triangleleft G$ è tale che G/H è abeliano, allora $G' \subset H$.

Proposizione 1.4. Sia G un gruppo e G' il suo derivato. Allora $G_{\text{ab}} = G/G'$ è abeliano ed è il più grande quoziente abeliano di G .

§1.5 Il gruppo diedrale

Proposizione 1.5. Tutti gli elementi di D_n si scrivono come $\sigma\rho^i$, oppure come ρ^i , per $i = 0, \dots, n-1$.

Proposizione 1.6. In D_n , il numero di elementi di ordine k è dato da:

$$\begin{cases} n+1 & , \text{ se } k=2, n \text{ pari} \\ n & , \text{ se } k=2, n \text{ dispari} \\ \phi(k) & , \text{ se } k \mid n \\ 0 & , \text{ altrimenti} \end{cases}$$

Di seguito, si riportano tutte le caratteristiche riguardanti la struttura di D_n .

- **Sottogruppi.** Un sottogruppo di D_n può essere composto da sole rotazioni, caso in cui coincide con un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$, oppure ha, in egual numero, rotazioni e riflessioni, caso in cui è isomorfo a D_m , per qualche m .
- **Sottogruppi normali.** Visto che $[D_n : C_n] = 2$, allora $C_n \triangleleft D_n$. Ogni sottogruppo di C_n è caratteristico in C_n perché unico, quindi è automaticamente normale in D_n . Se n è pari, si può definire $H = \langle \rho^2 \rangle \sqcup \tau \langle \rho^2 \rangle$, per cui $[D_n : H] = 2 \Rightarrow H \triangleleft D_n$. In questo caso, sottogruppi di questa forma sono $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$. Se n è dispari, invece, un sottogruppo normale contenente una riflessione, le deve contenere tutte, quindi coincide con D_n .
- **Sottogruppi caratteristici.** Per $n \geq 3$, C_n e i suoi sottogruppi di ordine $d > 2$, $d \mid n$ sono gli unici ad essere sempre caratteristici. Per gli n pari, $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$ non sono caratteristici perché $\tau : D_n \rightarrow D_n$ con $\tau(\rho) = \rho$ e $\tau(\sigma) = \sigma\rho$ è un automorfismo ben definito che scambia i due sottogruppi.

- **Centro.** Se n è dispari, $Z(D_n) = \{e\}$, mentre, se n è pari, $Z(D_n) = \{e, \rho^{n/2}\} \cong \mathbb{Z}/2\mathbb{Z}$.
- **Quozienti.** Questi sono in corrispondenza biunivoca con i sottogruppi normali. In generale, si ha $D_n/\langle \rho^m \rangle \cong D_m$. Per n pari, invece, i quozienti relativi a $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$ hanno indice due, quindi sono isomorfi a $\mathbb{Z}/2\mathbb{Z}$.
- **Automorfismi.** Un automorfismo di D_n è della forma

$$\gamma : \begin{array}{ccc} D_n & \longrightarrow & D_n \\ \rho & \longmapsto & \rho^i \\ \sigma & \longmapsto & \sigma\rho^j \end{array}, \quad \gcd(i, n) = 1$$

Allora $|\text{Aut}(D_n)| = n\phi(n)$.

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$

§1.6 Il gruppo simmetrico

Proposizione 1.7. Ogni k -ciclo ha k scritte equivalenti.

Proposizione 1.8. I cicli di una permutazione di S_n sono le orbite degli elementi di $X = \{1, \dots, n\}$ formate dall'azione indotta da tale permutazione.

Corollario 1.3.1. S_n è generato dai cicli.

Proposizione 1.9. Ogni permutazione si scrive come composizione di trasposizioni.

L'applicazione **segno** è definita da

$$\text{sgn} : \begin{array}{ccc} S_n & \longrightarrow & \{\pm 1\} \\ \sigma & \longmapsto & \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{array}$$

ed è un omomorfismo di gruppi. Vale -1 sulle trasposizioni; infatti, restituisce la parità del numero di trasposizioni presenti nella decomposizione di una permutazione. Il suo nucleo coincide con $A_n \triangleleft S_n$.

Teorema 1.4. Due permutazioni in S_n sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli disgiunti.

Di seguito, la caratterizzazione di S_n e dei suoi elementi.

- **Numero di un certo tipo di permutazioni con precisa decomposizione.** In S_n , il numero complessivo di k -cicli è ottenuto tramite

$$\binom{n}{k}(k-1)!$$

Volendo cercare quante permutazioni con una precisa decomposizione in cicli disgiunti ci sono, si procede come da esempio. In S_{12} , il numero di permutazioni date dalla composizione di due 3-cicli e tre 2-cicli è

$$\binom{12}{3} \frac{3!}{3} \binom{9}{3} \frac{3!}{3} \binom{6}{3} \frac{2!}{2} \binom{4}{2} \frac{2!}{2} \binom{2}{2} \frac{2!}{2} \frac{1}{3!2!}$$

Questo si generalizza nella seguente formula:

$$\frac{n!}{\prod_{k \geq 1} [k^{m_k}(m_k!)]}$$

con m_k numero di k -cicli.

- **Ordine di una permutazione.** Un k -ciclo ha ordine k ; se una permutazione è composta da ℓ cicli disgiunti σ_i , allora il suo ordine è

$$\text{lcm}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_\ell))$$

- **Centralizzatore di una permutazione.** Sapendo che due permutazioni sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli disgiunti, si sa calcolare $|\text{Cl}(\sigma)|$ tramite la formula al primo punto. Per orbita-stabilizzatore, si ha $|Z(\sigma)||\text{Cl}(\sigma)| = n!$, quindi si può calcolare $|Z(\sigma)|$.

Proposizione 1.10. Per la formula delle classi, $|Z_{S_n}(\sigma)||\text{Cl}_{S_n}(\sigma)| = n!$ e $|Z_{A_n}(\sigma)||\text{Cl}_{A_n}(\sigma)| = n!/2$, con:

$$Z_{A_n}(\sigma) = Z_{S_n}(\sigma) \cap A_n$$

Per la stessa formula, nel passare da $\text{Cl}_{S_n}(\sigma)$ a $\text{Cl}_{A_n}(\sigma)$ e da $Z_{S_n}(\sigma)$ a $Z_{A_n}(\sigma)$, uno dei due dimezza di ordine, mentre l'altro rimane invariato.

Proposizione 1.11. Dato $H < S_n$, allora o $H \subset A_n$, quindi $|H \cap A_n| = |H|$, oppure $|H \cap A_n| = |H|/2$.

Proposizione 1.12. I 3-cicli sono tutti coniugati in A_n , per $n \geq 5$.

- | **Proposizione 1.13.** I 5-cicli in A_5 NON sono tutti coniugati.
- | **Proposizione 1.14.** A_4 non ha sottogruppi di ordine 6.
- | **Teorema 1.5.** A_n è semplice $\forall n \geq 5$.

$$S_n \cong A_n \rtimes \langle \tau \rangle, \text{ con } \tau \text{ trasposizione}$$

§1.7 I quaternioni

Il gruppo è definito come $Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = j^3i \rangle$. $i^4 = 1$ e $i^2 = j^2$, allora $j^4 = 1$, quindi $\text{ord}(j) \mid 4$. Poi $\text{ord}(j^2) = \text{ord}(i^2) = 2$, quindi $\text{ord}(j) = 4$. Allora Q_8 ha due gruppi ciclici di ordine 4: $\langle i \rangle$ e $\langle j \rangle$, con $\langle i \rangle \cap \langle j \rangle = \{1, i^2 = j^2\}$. Visto che $\langle i \rangle, \langle j \rangle < Q_8$ e $|\langle i \rangle \langle j \rangle| = 8$, allora

$$Q_8 = \langle i \rangle \langle j \rangle = \{1, i, i^2, i^3, j, j^3, ij, i^3j\}$$

visto che $\langle i \rangle, \langle j \rangle < Q_8$ (hanno indice 2).

- | **Osservazione 1.1.** Q_8 non è abeliano: $ij = j^3i = j^{-1}i \neq ji$.

Di seguito, la caratterizzazione strutturale del gruppo.

- **Sottogruppi.** $\langle i \rangle, \langle j \rangle < Q_8$ perché hanno indice 2. Anche $\langle i^2 \rangle = \langle j^2 \rangle < Q_8$ perché i^2 (quindi j^2) commuta con i generatori.
- **Centro.** Si ha $\langle i^2 \rangle = Z(Q_8)$ perché $\langle i^2 \rangle$ ha ordine 2, quindi contenuto in $Z(Q_8)$; al contempo, $|Z(Q_8)| \in \{2, 4, 8\}$, ma, se non fosse 2, Q_8 sarebbe abeliano.
- **Elementi.** Prendendo $k = ij$ e $i^2 = -1$, si ha

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Si ha $i^2 = -1 \Rightarrow i^3 = -i \Rightarrow i^3j = -ij = -k$. Quindi: $ij = k$, $jk = i$, $ki = j$ e $ji = -k$, $ik = -j$ e $kj = -i$. Infine, $k^2 = (ij)^2 = ijij = i^2$, quindi $\text{ord}(k) = 4$. In questi termini, $\langle -1 \rangle = Z(Q_8)$.

- **Sottogruppi normali e caratteristici.** Per quanto detto, $\langle -1 \rangle = Z(Q_8)$ quindi è caratteristico e, in particolare, normale. Invece $\langle i \rangle, \langle j \rangle, \langle k \rangle < Q_8$, ma non sono caratteristici. Allora ogni sottogruppo di Q_8 è normale.

- **Prodotto semi-diretto.** Si nota che Q_8 non si può ottenere come prodotto semi-diretto perché ogni coppia di sottogruppi non si interseca mai solo in 1, ma anche -1 .

§1.8 Prodotti diretti

Teorema 1.6 (Decomposizione diretta). Sia G un gruppo e siano $H, K \triangleleft G$; se $HK = G$ e $H \cap K = \{e\}$, allora $G \cong H \times K$.

Corollario 1.6.1. In un prodotto diretto, i fattori commutano fra loro.

Corollario 1.6.2. Se $G = H \times K$, allora $Z(H \times K) \cong Z(H) \times Z(K)$, visto che $Z(H) \times \{e_K\}$ e $\{e_H\} \times Z_K$ sono sottogruppi normali di $Z(H \times K)$. Questo implica che

$$\text{Int}(H \times K) \cong \frac{H \times K}{Z(H \times K)} \cong H/Z(H) \times K/Z(K) \cong \text{Int}(H) \times \text{Int}(K)$$

Teorema 1.7. Si ha $\text{Aut}(H \times K) \cong \text{Aut}(H) \times \text{Aut}(K)$ se e soltanto se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$. Altrimenti $\text{Aut}(H) \times \text{Aut}(K) \hookrightarrow \text{Aut}(H \times K)$.

Corollario 1.7.1. Sia $G = H \times K$, con $|H| = n$ e $|K| = m$; se $\gcd(n, m) = 1$, allora $H \times \{e_K\}$, $\{e_H\} \times K$ sono caratteristici in G .

§1.9 Prodotti semi-diretti

Definizione 1.4 (Prodotto semi-diretto). Siano H, K due gruppi e $\gamma : K \rightarrow \text{Aut}(H)$ un omomorfismo tale che $\gamma(k) = \gamma_k \in \text{Aut}(H)$. Allora si definisce $H \rtimes_\gamma K$ il gruppo $H \times K$ la cui operazione di gruppo è definita da

$$(h, k) * (h', k') = (h\gamma_k(h'), kk')$$

Il prodotto diretto è dato da $\gamma(K) = \text{Id}_H$.

Proposizione 1.15. Si considera $H \rtimes_\gamma K$ e si definiscono $\overline{H} = H \times \{e_K\}$ e $\overline{K} = \{e_H\} \times K$. Per costruzione, $\overline{K}, \overline{H} \triangleleft H \times K$, mentre:

- $\overline{H} \triangleleft H \rtimes_\gamma K$ sempre;
- $\overline{K} \triangleleft H \rtimes_\gamma K \iff$ il prodotto è diretto.

Teorema 1.8 (Decomposizione semi-diretta). Sia G un gruppo e siano $H \triangleleft G$ e $K < G$. Se $HK = G$ e $H \cap K = \{e\}$, allora $G \cong H \rtimes_{\gamma} K$, con $\gamma : K \rightarrow \text{Aut}(H)$ e $\gamma(k) = khk^{-1}$.

§1.10 Teorema di struttura per gruppi abeliani finiti

Definizione 1.5 (p -torsione). Dato un gruppo abeliano finito G , se ne definisce la p -componente

$$G(p) := \{g \in G \mid \text{ord}(g) = p^k, k \in \mathbb{N}\}$$

Proposizione 1.16. La p -torsione $G(p)$ di un gruppo G abeliano finito è un sottogruppo caratteristico.

Teorema 1.9. Se G è un gruppo abeliano di ordine $|G| = n = p_1^{e_1} \cdots p_s^{e_s}$, con p_i primi diversi fra loro, allora

$$G \cong G(p_1) \times \cdots \times G(p_s)$$

Lemma 1.9.1. Sia G un p -gruppo e $x_1 \in G$ elemento di ordine massimo. Dato anche $\bar{x} \in G/\langle x_1 \rangle$, $\exists y \in \pi_{\langle x_1 \rangle}^{-1}(\bar{x})$ tale che $\text{ord}_G(y) = \text{ord}_{G/\langle x_1 \rangle}(\bar{x})$.

Teorema 1.10. Se G è un p -gruppo abeliano, allora esistono unici $r_1, \dots, r_t \in \mathbb{N}$ tali che

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

con $r_1 \geq r_2 \geq \cdots \geq r_t$.

Teorema 1.11 (Teorema di struttura). Sia G un gruppo abeliano finito; allora G si decompone univocamente come

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

dove $n_{i+1} \mid n_i, \forall i = 1, \dots, s-1$.

§1.11 Teoremi di Sylow

Per i seguenti teoremi, si considera un gruppo finito G di ordine $|G| = p^n m$, con p primo e $\gcd(m, p) = 1$.

Teorema 1.12 (I teorema). Dato $\alpha \in \mathbb{N}$, con $0 \leq \alpha \leq n$, allora $\exists H < G$ di ordine $|H| = p^\alpha$.

Teorema 1.13 (II teorema). Ogni p -gruppo di G è contenuto in un p -Sylow. Inoltre, due qualunque p -Sylow di G sono coniugati.

Teorema 1.14 (III teorema). Dato n_p il numero di p -Sylow di G , si ha che $n_p \mid |G|$ e $n_p \equiv 1 \pmod{p}$. In particolare, si avrà $n_p \mid m$.

§1.12 Risultati sulle classificazioni

- Classificazione dei gruppi di ordine 6.
- Classificazione dei gruppi di ordine pq .
- Classificazione dei gruppi di ordine 1000.
- Classificazione dei gruppi di ordine 12.
- Classificazione dei gruppi di ordine 8.
- Classificazione dei gruppi di ordine 30.

§1.13 Risultati vari sui gruppi

Proposizione 1.17. $G/Z(G)$ ciclico $\iff G$ abeliano.

Proposizione 1.18. Se $H, K < G$, allora $HK < G \iff HK = KH$; in questo caso, $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proposizione 1.19. Se $H, K \triangleleft G$, con $H \cap K = \{e\}$, allora $hk = kh, \forall h \in H, \forall k \in K$.

Proposizione 1.20. Sia $H < G$ con $[G : H] = 2$; allora $H \triangleleft G$.

Proposizione 1.21. Siano $H \triangleleft G$ e K sottogruppo caratteristico di H ; allora $K \triangleleft G$.

Proposizione 1.22. Sia $H < G$, con $|H| = 2$; allora H è normale se e solo se $H < Z(G)$.

2 | ESERCIZI

§2.1 Esercizi su gruppi 1

Esercizio 2.1. Sia $G = \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$; determinare il numero degli omomorfismi $f : G \rightarrow G$. Inoltre, dati $n \in \mathbb{N}$ e $f_n : G \rightarrow G$ l'omomorfismo dato da $f_n(x) = nx$, determinare:

- (a). per quali valori di n , $\text{Ker } f_n$ è ciclico;
- (b). per quali valori di n , $\text{Im } f_n$ è ciclico.

§2.2 Esercizi su campi e anelli 1

Esercizio 2.2. Sia $f(x) = x^4 + x^3 - 3 \in \mathbb{F}_7[x]$. Determinare il numero di divisori dello zero e l'inverso di $\overline{x+1}$ in $\mathbb{F}_7[x]/\langle f(x) \rangle$.

Svolgimento. Si scompone $f(x)$ in $\mathbb{F}_7[x]$; per farlo, si vede se ha radici, calcolando $f(a)$, per $a = 0, 1, \dots, 6$. Provando, si vede che:

$$f(0) = -3 \equiv 4 \pmod{7}$$

$$f(1) = -1 \equiv 6 \pmod{7}$$

$$f(2) = 16 + 8 - 3 = 21 \equiv 0 \pmod{7}$$

$$f(3) = 81 + 27 - 3 = 105 \equiv 0 \pmod{7}$$

$$f(4) = 256 + 64 - 3 = 317 = 280 + 37 \equiv 2 \pmod{7}$$

$$f(5) = 625 + 125 - 3 = 747 = 735 + 12 \equiv 5 \pmod{7}$$

$$f(6) = 1296 + 216 - 3 = 1509 = 1498 + 11 \equiv 4 \pmod{7}$$

Per effettuare la fattorizzazione di $f(x)$, si usa Ruffini. Iniziando con $(x - 2)$, visto che $f(x) = x^4 + x^3 - 3 \equiv x^4 + x^3 + 4 \pmod{7}$, si ottiene:

$$\begin{array}{r|rrrrr} 2 & 1 & 1 & 0 & 0 & 4 \\ & & 2 & 6 & 5 & 3 \\ \hline & 1 & 3 & 6 & 5 & 0 \end{array}$$

$$f(x) = (x - 2)(x^3 + 3x^2 + 6x + 5) = (x - 2)g(x)$$

Evidentemente, $g(3) = 0 \implies (x - 3) \mid g(x)$; usando ancora Ruffini, si ha:

$$\begin{array}{r|rrrr} 3 & 1 & 3 & 6 & 5 \\ & & 3 & 4 & 2 \\ \hline & 1 & 6 & 3 & 0 \end{array}$$

$$f(x) = (x - 2)g(x) = (x - 2)(x - 3)(x^2 + 6x + 3)$$

dove si nota che $x^2 + 6x + 3$ non si annulla né per $x = 2$, né per $x = 3$, quindi è irriducibile in $\mathbb{F}_7[x]$ (altrimenti $f(x)$ avrebbe una radice diversa da $x = 2, 3$, che è assurdo per i calcoli svolti sopra). In questo modo, si può studiare nel dettaglio $\mathbb{F}_7[x]/\langle f(x) \rangle$. Intanto, visto che $f(x)$ è un polinomio di grado 4 in $\mathbb{F}_7[x]$, tale quoziente sarà composto da tutti i polinomi della forma

$$ax^3 + bx^2 + cx + d, \quad a, b, c, d \in \mathbb{F}_7$$

pertanto avrà un totale di 7^4 elementi. Le unità di $\mathbb{F}_7[x]/\langle f(x) \rangle$ sono tutte quelle classi $\overline{h(x)}$ tali che $(f(x), h(x)) = 1$; per studiare meglio questo fatto, si usa il teorema cinese del resto per anelli a partire dall'osservazione che $x - 2$, $x - 3$ e $x^2 + 6x + 3$ sono coprimi tra loro:

$$\frac{\mathbb{F}_7[x]}{\langle (x - 2)(x - 3)(x^2 + 6x + 3) \rangle} \cong \mathbb{F}_7[x]/\langle x - 2 \rangle \times \mathbb{F}_7[x]/\langle x - 3 \rangle \times \mathbb{F}_7[x]/\langle x^2 + 6x + 3 \rangle$$

Per studiare il numero delle unità complessive di $\mathbb{F}_7[x]/\langle f(x) \rangle$, si studia singolarmente ciascun fattore:

- $\mathbb{F}_7[x]/\langle x - 2 \rangle \cong \mathbb{F}_7$, quindi ha 7 elementi, per un totale di 6 unità;
- $\mathbb{F}_7[x]/\langle x - 3 \rangle \cong \mathbb{F}_7$, quindi ha 6 unità;
- $\mathbb{F}_7[x]/\langle x^2 + 6x + 3 \rangle$ è un campo perché $x^2 + 6x + 3$ è irriducibile in $\mathbb{F}_7[x]$ e ha un totale di $7^2 = 49$ elementi, quindi è isomorfo a \mathbb{F}_{49} , con un totale di 48 unità.

Da questo si conclude che il numero totale di unità in $\mathbb{F}_7[x]/\langle f(x) \rangle$ è $6 \cdot 6 \cdot 48 = 1728$ unità. Essendo interessati ai divisori dello zero, sapendo che divisori dello zero e unità partizionano l'anello (a parte lo zero), si ha che, in totale, sono $7^4 - 1728 = 2401 - 1728 = 673$ incluso lo zero.

Per finire, si calcola l'inverso di $\overline{x + 1}$ in $\mathbb{F}_7[x]/\langle f(x) \rangle$. Intanto si nota che $x + 1$ è coprimo con $f(x)$ perché si annulla in $-1 \equiv 6 \pmod{7}$, quindi l'inverso in $\mathbb{F}_7[x]/\langle f(x) \rangle$

esiste. Si cerca un polinomio $a(x) \in \mathbb{F}_7[x]$ che soddisfa

$$a(x)(x+1) + b(x)f(x) = 1$$

cosicché, in $\mathbb{F}_7[x]/\langle f(x) \rangle$, $\overline{a(x)}\overline{(x+1)} = 1$. Per iniziare, si divide $f(x)$ per $x+1$ (usando $-1 \equiv 6 \pmod{7}$):

$$\begin{array}{r|rrrrr} 6 & 1 & 1 & 0 & 0 & 4 \\ & & 6 & 0 & 0 & 0 \\ \hline & 1 & 0 & 0 & 0 & 4 \end{array}$$

$$f(x) = (x+1)x^3 + 4$$

In $\mathbb{F}_7[x]$, $4^{-1} \equiv 2 \pmod{7}$, quindi, moltiplicando tutto per 2 in $\mathbb{F}_7[x]/\langle f(x) \rangle$, si ha:

$$1 = 2f(x) - 2(x+1)x^3 \implies \overline{1} = \overline{-2(x+1)x^3}$$

da cui l'inverso di $\overline{x+1}$ è proprio $\overline{-2x^3} \equiv \overline{5x^3}$, visto che $-2 \equiv 5 \pmod{7}$. ■

Esercizio 2.3. Sia m un numero intero e sia

$$f_m(x) = (x^2 - m)(x^4 - 25)$$

Determinare, per ogni valore intero di m , il grado del campo di spezzamento di $f_m(x)$ su \mathbb{Q} .

Svolgimento. Il campo di spezzamento per $f_m(x)$ si ottiene aggiungendo a \mathbb{Q} le radici dei due fattori $x^2 - m$ e $x^4 - 25$. Si può notare che

$$x^4 - 25 = (x^2 + 5)(x^2 - 5)$$

Da qui, si ottiene che le radici di $x^4 - 25$ sono $\pm\sqrt{5}$ e $\pm i\sqrt{5}$, quindi il suo campo di spezzamento corrisponde con $K = \mathbb{Q}(\sqrt{5}, i)$. Per finire, si osserva che $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, per cui $[K : \mathbb{Q}] = 4$, dato che $i \notin \mathbb{Q}(\sqrt{5})$. Visto che K è indipendente da m , rimarrà fisso per il resto dell'esercizio.

Quanto al fattore $x^2 - m$, le sue radici sono $\pm\sqrt{m}$, ma qui il campo di spezzamento dipende dalla scelta dell'intero m .

- Se $m = 0$, le radici di $x^2 - m$ sono già contenute in \mathbb{Q} poiché è proprio lo zero.
- Se m è un quadrato perfetto positivo, allora $\sqrt{m} \in \mathbb{Q}$ e, anche in questo caso, \mathbb{Q} contiene già le radici.

- Se $m < 0$, invece, le radici sono date da $\pm i\sqrt{|m|}$; in questo caso, se $m = -n^2$, per qualche intero n , allora il suo campo di spezzamento coincide con $\mathbb{Q}(i)$, visto che $\sqrt{|m|} \in \mathbb{Q}$. Altrimenti, il suo campo di spezzamento sarà dato da $\mathbb{Q}(i\sqrt{|m|})$.
- Infine, se $m > 0$ non è un quadrato perfetto, il campo di spezzamento è ottenuto aggiungendo \sqrt{m} , quindi coincide con $\mathbb{Q}(\sqrt{m})$.

Allora, il campo di spezzamento per questo fattore, al variare di $m \in \mathbb{Z}$, è dato da:

$$L = \begin{cases} \mathbb{Q} \\ \mathbb{Q}(i\sqrt{m}) \\ \mathbb{Q}(\sqrt{m}) \end{cases}$$

Visto che i è già stato aggiunto per la radice del secondo fattore, ci si può concentrare sul trattare i casi in cui $L = \mathbb{Q}(\sqrt{m})$ o $L = \mathbb{Q}$.

Per concludere, quindi, il campo di spezzamento del polinomio $f_m(x)$ su \mathbb{Q} è dato da $E = KL$, con le varie possibilità per L al variare di $m \in \mathbb{Z}$:

- se $m = 0$, m (positivo o negativo) quadrato perfetto, oppure $m = \pm 5$, allora $E = \mathbb{Q}(\sqrt{5}, i)$;
- se m (positivo o negativo) NON è un quadrato perfetto e $|m| \neq 5$, allora $E = \mathbb{Q}(\sqrt{5}, \sqrt{|m|}, i)$.

Nel primo caso, il grado dell'estensione rimane quello di K , ossia $[E : \mathbb{Q}] = 4$, mentre, nel secondo caso, $[E : \mathbb{Q}] = 2^3 = 8$. ■

Esercizio 2.4. Siano $f(x) = x^3 + 3x - 1$ e $g(x) = x^2 - 2$.

- Se α è una radice complessa di $f(x)$, determinare il polinomio minimo di $1/(\alpha + 2)$ su \mathbb{Q} .
- Determinare l'insieme dei numeri primi p tali che $f(x)$ e $g(x)$, considerati a coefficienti in \mathbb{F}_p , hanno una radice comune.

Svolgimento. Si divide lo svolgimento nei due punti.

- Sia α una radice complessa di $f(x)$. Si cerca il polinomio minimo di

$$\beta = \frac{1}{\alpha + 2} \implies \alpha\beta + 2\beta = 1 \implies \alpha = \frac{1}{\beta} - 2$$

Visto che $f(\alpha) = 0$, allora:

$$\left(\frac{1}{\beta} - 2\right)^3 + 3\left(\frac{1}{\beta} - 2\right) - 1 = 0$$

Espandendo e riordinando si ottiene un polinomio in β :

$$\begin{aligned} \frac{1}{\beta^3} - 8 - \frac{6}{\beta^2} + \frac{12}{\beta} + \frac{3}{\beta} - 6 - 15 &= 0 \implies \frac{1}{\beta^3} - \frac{6}{\beta^2} + \frac{15}{\beta} = 15 \\ \implies 15\beta^3 &= 1 - 6\beta + 15\beta^2 \implies 15\beta^3 - 15\beta^2 + 6\beta - 1 = 0 \end{aligned}$$

In questo modo, si ricava il polinomio $p(x) = 15x^3 - 15x^2 + 6x - 1$, che è a coefficienti razionali, ha β come radice ed è di grado 3. Usando Eisenstein con $p = 3$ su $f(x)$, si conclude che è irriducibile su \mathbb{Q} , quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Infine, visto che $\beta \in \mathbb{Q}(\alpha)$ e, viceversa, $\alpha \in \mathbb{Q}(\beta)$, si conclude che $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, pertanto $p(x)$ coincide proprio con il polinomio minimo di β .

- (b). Si cercano i primi p tali per cui $\exists a \in \mathbb{F}_p$ con $f(a) = g(a) = 0$. Si nota che $g(a) = 0 \implies a^2 = 2$ in \mathbb{F}_p . Passando alla condizione $f(a) = 0$, si ha $a^3 + 3a - 1 = 0$; moltiplicando tutto per a , si ottiene $a^4 + 3a^2 - 1 = 0$. Sostituendo la condizione trovata prima, cioè $a^2 = 2$, si ottiene $4 + 6 - a = 0$, quindi $a = 10$ in \mathbb{F}_p .

In questo modo, si ricava che a deve soddisfare due condizioni in \mathbb{F}_p : $a \equiv 10 \pmod{p}$ e $a^2 \equiv 2 \pmod{p}$, cioè

$$100 \equiv 2 \pmod{p} \implies p \mid 98 = 2 \cdot 7^2$$

Allora le possibilità sono $p = 2$, oppure $p = 7$. Si nota che, per $p = 2$, $g(x) = x^2$ e $f(x) = x^3 + x + 1$, che non hanno radici comuni. Perciò, ci si convince facilmente che l'unico p che soddisfa la richiesta è $p = 7$.

■

Esercizio 2.5. Sia $f(x) = x^6 + 4x^3 + 2$.

- (a). Detta α una radice complessa di $f(x)$, determinare il polinomio minimo di $1/\alpha^2$ su \mathbb{Q} .
- (b). Determinare il campo di spezzamento di $f(x)$ su \mathbb{F}_7 .

Svolgimento. Si divide lo svolgimento nei due punti.

- (a). Si nota preliminarmente che $f(x)$ è irriducibile per il criterio di Eisenstein con $p = 2$. Inoltre, $f(\alpha) = 0$, quindi $\alpha^6 + 2 = -4\alpha^3$; elevando al quadrato, si ottiene che:

$$\alpha^{12} + 4 + 4\alpha^6 = 16\alpha^6 \implies \alpha^{12} - 12\alpha^6 + 4 = 0$$

In questo modo, sostituendo $y = \alpha^2$, si trova $y^6 - 12y^3 + 4 = 0$, quindi $y = \alpha^2$ soddisfa $p(y) = 0$, con $p(x) = x^6 - 12x^3 + 4$. Ora si deve mostrare che $p(x)$ è irriducibile per far vedere che è il polinomio minimo per α^2 . Visto che $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$, allora $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \leq 2$, quindi $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 3, 6$; si vuole escludere il caso in cui il grado sia 3. In questo caso, è facile convincersi che $p(x)$ dovrebbe scomporsi in due fattori cubici; riducendolo modulo 2, poi, si vede che $\overline{p(x)} = \overline{x^6}$, pertanto i polinomi di grado 3, $A(x)$ e $B(x)$, in cui si scompone $p(x)$ devono avere coefficienti pari, ad eccezione del primo. Svolgendo il prodotto, si vede anche che i termini noti dei due polinomi devono essere $c = c' = \pm 2$, quindi

$$A(x) = x^3 + ux^2 + vx \pm 2 \quad B(x) = x^3 + u'x^2 + v'x \pm 2$$

con $u, v, u', v' \equiv 0 \pmod{2}$. Svolgendo il prodotto, si ottengono le condizioni $u' = -u$, $v' = -v$ per i termini di grado 1 e 5, mentre si ottiene $u^2 = v^2 = 0$ per quelli di grado 4 e 2, da cui l'assurdo. Pertanto, $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$ e, visto che $\mathbb{Q}(1/\alpha^2) = \mathbb{Q}(\alpha^2)$, si conclude che il polinomio minimo di $\beta = 1/\alpha^2$ ha grado 6. Riprendendo l'espressione $\alpha^{12} - 12\alpha^6 + 4 = 0$ trovata prima e sostituendo $\alpha^2 = 1/\beta$, si trova:

$$\frac{1}{\beta^6} - \frac{12}{\beta^3} + 4 = 0 \implies 4\beta^6 - 12\beta^3 + 1 = 0 \implies \beta^6 - 3\beta^3 + \frac{1}{4} = 0$$

da cui $P(x) = x^6 - 3x^3 + 1/4$ è il polinomio minimo di β perché soddisfa $P(\beta) = 0$ e ha stesso grado dell'estensione $\mathbb{Q}(\beta)$.

- (b). Bisogna capire se $f(x)$ è irriducibile in \mathbb{F}_7 . Si osserva che, ponendo $t = x^3$, si ottiene $t^2 + 4t + 2 = 0$, con $\Delta = 16 - 8 = 8 \equiv 1 \pmod{7}$, che è un quadrato in \mathbb{F}_7 , pertanto $f(x)$ non è irriducibile. Si nota, poi, che $-3 \equiv 4 \pmod{7}$ e $-5 \equiv 2 \pmod{7}$, per cui le radici di $t^2 + 4t + 2 = 0$ sono $t = 1, 2$. Tale polinomio, quindi, si scompone in

$$t^2 + 4t + 2 = (t - 1)(t - 2) \implies f(x) = x^6 + 4x^3 + 2 = (x^3 - 1)(x^3 - 2)$$

Si osserva, ora, che gli elementi di \mathbb{F}_7^\times soddisfano $x^6 = 1$; tramite la mappa $\varphi : \mathbb{F}_7^\times \rightarrow \mathbb{F}_7^\times$ tale che $x \mapsto x^3$, si ottiene che $x^2 = 1$. In questo modo, si possono capire quali sono i cubi di \mathbb{F}_7 ; da tale relazione, si trova che questi sono $x = \pm 1$,

cioè 1, 6. Questo significa che 1 è un cubo e, pertanto, $x^3 - 1$ è riducibile, mentre $x^3 - 2$ no. Le radici di $x^3 = 1$ sono gli elementi di \mathbb{F}_7^\times che hanno ordine 3; visto che $3 \mid 6$, ci sono sicuramente elementi del genere e sono dati da 1, 2, 4, quindi

$$f(x) = (x - 1)(x - 2)(x - 4)(x^3 - 2)$$

è la scomposizione in irriducibili di $f(x)$. Visto che le radici dei fattori di primo grado sono già in \mathbb{F}_7 , $\text{Spl}_{\mathbb{F}_7} f(x) = \text{Spl}_{\mathbb{F}_7} x^3 - 2$. Essendo $x^3 - 2$ irriducibile di grado 3, allora, se ξ è una radice di $x^3 - 2$, si ha $\mathbb{F}_7(\xi) \cong \mathbb{F}_{7^3}$. Questo permette di concludere che $\text{Spl}_{\mathbb{F}_7} f(x) = \mathbb{F}_{7^3}$. ■

Esercizio 2.6. Determinare il campo di spezzamento di $x^6 - 4$ su \mathbb{Q} e su \mathbb{F}_{11} .

Svolgimento. Si inizia col determinarlo su \mathbb{Q} . Per farlo, è necessario capire se $x^6 - 4$ è irriducibile; si nota, però, che $x^6 - 4 = (x^3 - 2)(x^3 + 2)$. Questi due fattori, poi, sono irriducibili per Eisenstein con $p = 2$, quindi il campo di spezzamento di $x^6 - 4$ è determinato dai campi di spezzamento di questi due polinomi di grado 3 su \mathbb{Q} . Visto che sono irriducibili, la loro estensione avrà grado 3:

- per $\text{Spl}_{\mathbb{Q}} x^3 - 2$, si ha $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, con $\zeta_3 = e^{2\pi i/3}$ radice cubica dell'unità;
- per $\text{Spl}_{\mathbb{Q}} x^3 + 2$, si ha lo stesso campo di spezzamento $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, visto che $(-\sqrt[3]{2})^3 = -2$.

Se ne conclude che il campo di spezzamento di $x^6 - 4$ su \mathbb{Q} è dato da $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ed è un'estensione di grado 6 perché prodotto di un'estensione di grado 2, $\mathbb{Q}(\zeta_3)$, e di un'estensione di grado 3, $\mathbb{Q}(\sqrt[3]{2})$.

Quanto al caso su \mathbb{F}_{11} , il procedimento è analogo: si cerca di capire se $x^6 - 4$ ha qualche radice, o se è irriducibile. Si deve capire se $\exists x \in \mathbb{F}_{11}^\times$ tale che $x^6 = 4$, sapendo che gli elementi di tale campo soddisfano $x^{10} = 1$. Pertanto $x^6 = 4$ è soddisfatta se e solo se $4^{10/\text{gcd}(10,6)} = 1$ in \mathbb{F}_{11} ; visto che $\text{gcd}(10, 6) = 2$, si verifica che $4^5 = 1024 \equiv 1 \pmod{11}$. Si nota che:

$$\begin{aligned} 4^2 &= 16 \equiv 5 \pmod{11} & 4^4 &\equiv 5^2 = 25 \equiv 3 \pmod{11} \\ 4^5 &\equiv 3 \cdot 4 = 12 \equiv 1 \pmod{11} \end{aligned}$$

Quindi $x^6 - 4$ si scompone in \mathbb{F}_{11} . Per trovare le radici di questo polinomio ci sono due vie: partendo dal fatto che ci sono due elementi che soddisfano $x^6 - 4 = 0$ in \mathbb{F}_{11} ,

essendo $\gcd(10, 6) = 2$, si procede a trovarle manualmente e si usa che, se a è una radice, allora anche $-a$ lo è, oppure si usa che 2 è un generatore di \mathbb{F}_{11}^\times , quindi

$$x^6 = 4 \iff (2^k)^6 = 2^2 \iff 6k \equiv 2 \pmod{10}$$

che si riduce, dividendo per 2, a $3k \equiv 1 \pmod{5}$. Usando che l'inverso di 3 modulo 5 è 2, si ha la congruenza $k \equiv 2 \pmod{5}$, che, modulo 10, si traduce in $k = 2, 7$. In questo modo, gli elementi che soddisfano $x^6 - 4 = 0$ sono $2^2 = 4$ e $2^7 = 128 \equiv 7 \pmod{11}$. Se ne conclude che $x^6 - 4 = (x - 4)(x - 7)p(x)$, dove la divisione per $x - 2$ restituisce (usando che $-4 \equiv 7 \pmod{11}$):

$$\begin{array}{r|rrrrrrr} 4 & 1 & 0 & 0 & 0 & 0 & 0 & 7 \\ & & 4 & 5 & 9 & 3 & 1 & 4 \\ \hline & 1 & 4 & 5 & 9 & 3 & 1 & 0 \end{array}$$

$$x^6 - 4 = (x - 4)(x^5 + 4x^4 + 5x^3 + 9x^2 + 3x + 1)$$

Applicando nuovamente Ruffini, si ottiene:

$$\begin{array}{r|rrrrrr} 7 & 1 & 4 & 5 & 9 & 3 & 1 \\ & & 7 & 0 & 2 & 0 & 10 \\ \hline & 1 & 0 & 5 & 0 & 3 & 0 \end{array}$$

$$x^6 - 4 = (x - 4)(x - 7)(x^4 + 5x^2 + 3)$$

Allora il campo di spezzamento su \mathbb{F}_{11} di $x^6 - 4$ coincide con quello di $x^4 + 5x^2 + 3$. Per trovare il campo di spezzamento di questo polinomio, si prende $t = x^2$, per cui si ottiene $t^2 + 5t + 3 = 0$, da cui

$$t_{1,2} = \frac{-5 \pm \sqrt{25 - 12}}{2} \equiv \frac{6 \pm \sqrt{2}}{2} = 3 \pm \frac{1}{\sqrt{2}} \in \mathbb{F}_{11}(\sqrt{2}) \cong \mathbb{F}_{11^2}$$

Ne segue che il campo di spezzamento di $x^6 - 4$ è proprio \mathbb{F}_{11^2} , in quanto, contenendo t_1 e t_2 , contiene anche le rispettive radici quadrate $\pm\sqrt{t_1}$ e $\pm\sqrt{t_2}$. ■

Esercizio 2.7. Calcolare i gradi delle estensioni $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ e $\mathbb{Q}(\sqrt{3} - \sqrt{5})/\mathbb{Q}$. Poi, trovare i polinomi minimi di $\sqrt{3} - \sqrt{5}$ e di $\sqrt{\sqrt{3} - \sqrt{5}} - 1$ su \mathbb{Q} .

Svolgimento. Per calcolare $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}]$, si nota che una possibile base è data da $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$. Questo significa che tale estensione ha grado 4. Si nota che quella

esposta è effettivamente una base perché $\sqrt{3}$ e $\sqrt{5}$ sono indipendenti. Per calcolare il grado della seconda estensione, si tiene a mente quanto appena visto; si farà vedere che $\sqrt{3}, \sqrt{5} \in \mathbb{Q}(\sqrt{3} - \sqrt{5})$. Per farlo, è sufficiente osservare che $1/(\sqrt{3} - \sqrt{5}), (3 - 5) \in \mathbb{Q}(\sqrt{3} - \sqrt{5})$, per cui:

$$\frac{3 - 5}{\sqrt{3} - \sqrt{5}} = \frac{(\sqrt{3} - \sqrt{5})(\sqrt{3} + \sqrt{5})}{\sqrt{3} - \sqrt{5}} = \sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3} - \sqrt{5})$$

Ma allora

$$\sqrt{3} = \frac{(\sqrt{3} - \sqrt{5}) + (\sqrt{3} + \sqrt{5})}{2} \quad \sqrt{5} = \frac{(\sqrt{3} + \sqrt{5}) - (\sqrt{3} - \sqrt{5})}{2}$$

quindi $\sqrt{3}, \sqrt{5} \in \mathbb{Q}(\sqrt{3} - \sqrt{5})$. Visto che $\sqrt{3} - \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$, si conclude facilmente che $\mathbb{Q}(\sqrt{3} - \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, da cui $[\mathbb{Q}(\sqrt{3} - \sqrt{5}) : \mathbb{Q}] = 4$.

Per trovare il polinomio minimo di $\sqrt{3} - \sqrt{5}$, si prende $x = \sqrt{3} - \sqrt{5}$; allora si nota che:

$$\begin{aligned} x^2 &= 3 + 5 - 2\sqrt{15} \Rightarrow \sqrt{15} = \frac{x^2 - 8}{2} \\ \Rightarrow 15 &= \frac{1}{4} [x^4 + 64 - 16x^2] \Rightarrow x^4 - 16x^2 + 4 = 0 \end{aligned}$$

In questo modo, il candidato polinomio minimo di $\sqrt{3} - \sqrt{5}$ è proprio $p(y) = y^4 - 16y^2 + 4$ perché è stato costruito in modo tale che $p(x) = 0$, $x = \sqrt{3} - \sqrt{5}$. Visto che l'estensione $\mathbb{Q}(\sqrt{3} - \sqrt{5})/\mathbb{Q}$ ha grado 4 e che $p(y)$ è un polinomio di grado 4 a coefficienti razionali che ha $\sqrt{3} - \sqrt{5}$ come radice, allora è automaticamente il polinomio minimo.

Per $\sqrt{\sqrt{3} - \sqrt{5}} - 1$, si procede in maniera analoga, ponendo $\beta = \sqrt{\sqrt{3} - \sqrt{5}} - 1 \Rightarrow \beta + 1 = \sqrt{\sqrt{3} - \sqrt{5}}$; in questo modo, si ha:

$$\begin{aligned} (\beta + 1)^2 &= \sqrt{3} - \sqrt{5} \Rightarrow (\beta + 1)^4 = 3 + 5 - 2\sqrt{15} \\ \Rightarrow \sqrt{15} &= \frac{8 - (\beta + 1)^4}{2} \Rightarrow 15 = \frac{1}{4} [64 + (\beta + 1)^8 - 16(\beta + 1)^4] \\ \Rightarrow (\beta + 1)^8 &- 16(\beta + 1)^4 + 4 = 0 \end{aligned}$$

Questo permette di ottenere un polinomio monico di grado 8 a coefficienti razionali e con β come radice; per concludere che è il polinomio minimo, è sufficiente mostrare che il grado dell'estensione è 8. Si osserva che, per $\alpha = \sqrt{3} - \sqrt{5}$, si ha $\beta + 1 = \sqrt{\alpha}$,

quindi $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{\alpha})$. Perciò

$$[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}(\alpha)]$$

con $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}(\alpha)] \leq 2$ perché ottenuta aggiungendo una radice quadrata. Si può mostrare che questa estensione ha grado esattamente 2; infatti, se α fosse un quadrato, avrebbe tutti coniugati positivi, visto che $\mathbb{Q}(\alpha)$ è un campo totalmente reale, però un possibile coniugato è $-\sqrt{3} - \sqrt{5} < 0$, quindi α non può essere un quadrato. Allora $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = 8$ e, dunque, quello trovato è proprio il polinomio minimo di β . ■

Esercizio 2.8. Determinare il grado del campo di spezzamento di $f(x) = x^4 - 2$ su \mathbb{Q} , su \mathbb{F}_3 e su \mathbb{F}_{17} .

Svolgimento. Per $\text{Spl}_{\mathbb{Q}} x^4 - 2$, si nota che ha radici date da $\sqrt[4]{2}, \sqrt[4]{2}\zeta_4, \sqrt[4]{2}\zeta_4^2, \sqrt[4]{2}\zeta_4^3$, con $\zeta_4 = i$ radice quartica dell'unità. Evidentemente, il suo campo di spezzamento è dato da $\mathbb{Q}(\sqrt[4]{2}, \zeta_4)$, dove $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ e $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$; essendo queste estensioni indipendenti, il grado complessivo dell'estensione è 8.

Per $\text{Spl}_{\mathbb{F}_3} x^4 - 2$, si nota che tale polinomio è irriducibile: $-2 \not\equiv 0 \pmod{3}$, $-1 \not\equiv 0 \pmod{3}$ e $2^4 - 2 = 14 \equiv 2 \not\equiv 0 \pmod{3}$. Inoltre, $x^4 - 2$ non si scompone neanche in fattori quadratici in \mathbb{F}_3 perché, altrimenti, 2 dovrebbe essere un quadrato, ma $2^2 = 1$ e $1^2 = 1$. Allora $x^4 - 2$ è irriducibile di grado 4 su \mathbb{F}_3 , il che vuol dire che si decompone completamente in \mathbb{F}_{3^4} .

Per $\text{Spl}_{\mathbb{F}_{17}} x^4 - 2$, infine, si usa il fatto che un elemento di \mathbb{F}_{17}^\times soddisfa $x^{16} = 1$, per cui vale $x^4 = 2$ se e soltanto se è verificata la relazione $2^4 \equiv 1 \pmod{17}$, ma questa non è verificata perché $2^4 = 16$. Inoltre, $x^4 - 2$ non si può scomporre in fattori quadratici; se così fosse, infatti, dovrebbe essere soddisfatta la relazione $x^2 = 2 \iff 2^8 \equiv 1 \pmod{17}$, ma $2^8 = 4^4 = 256 \equiv 8 \pmod{17}$. Quindi $x^4 - 2$ è irriducibile di grado 4 anche in \mathbb{F}_{17} , per cui il suo campo di spezzamento sarà \mathbb{F}_{17^4} .

Nota: si può dimostrare che $x^4 - a$ è riducibile in un certo campo K se e soltanto se a è una potenza quarta in tale campo, oppure è un quadrato. Questo permette di giustificare i passaggi nell'esercizio e la dimostrazione si basa sul proseguire per conto diretto, assumendo una generica decomposizione in fattori quadratici. ■

§2.3 Esercizi su gruppi 2

Esercizio 2.9. Sia $G = \mathbb{Z}/4\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/4\mathbb{Z}$ definito da $\phi(1) = -1 \in (\mathbb{Z}/4\mathbb{Z})^* \cong \text{Aut}(\mathbb{Z}/4\mathbb{Z})$.

- (a). Per ogni intero n , contare gli elementi di ordine n in G .
- (b). Dimostrare che $Z(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- (c). Calcolare G' e la classe di isomorfismo di $G_{\text{ab}} := G/G'$.

Svolgimento. Si divide lo svolgimento nei vari punti.

- (a). I possibili n sono 1, 2, 4, 8, 16.

Per $n = 1$, si ha evidentemente l'identità $(0, 0)$.

Per $n = 2$, si osserva che:

$$(a, b)^2 = (0, 0) \iff (a + (-1)^b a, 2b) = (0, 0)$$

Conviene dividere i casi in cui b è pari o dispari. Se b pari (cioè $b = 0, 2$), allora il quadrato è pari a $(2a, 2b)$ e questo coincide con $(0, 0)$ se e soltanto se $a, b \in \{0, 2\}$. Escludendo l'identità stessa, ci sono tre possibilità: $(2, 0)$, $(2, 2)$, $(0, 2)$. Se b è dispari, invece, il quadrato è pari a $(0, 2b)$; questo risulterebbe pari a $(0, 0)$ se $b \equiv 0 \pmod{2}$, ma questo è impossibile perché si è assunto b dispari.

Per $n = 4$, invece, si impone $(a, b)^4 = (0, 0)$, cioè:

$$(a + (-1)^b a, 2b)(a + (-1)^b a, 2b) = \begin{cases} (0, 4b) \equiv (0, 0) \pmod{4} & , b \text{ dispari} \\ (4a, 4b) \equiv (0, 0) \pmod{4} & , b \text{ pari} \end{cases}$$

Questo conteggio permette di concludere che tutti gli elementi di G che non sono di ordine 1 o 2 sono di ordine 4. Visto che l'identità e gli elementi di ordine 2 sono quattro in totale, si conclude che quelli di ordine 4 sono 12.

- (b). Per il lemma orbita-stabilizzatore, $|Z(G)| \mid |G|$, quindi le possibili cardinalità sono 1, 2, 4, 8, 16. G è un p -gruppo, quindi 1 non è ammissibile; inoltre, 8 e 16 non sono possibili in quanto G risulterebbe abeliano, che è assurdo. Allora $|Z(G)| \in \{2, 4\}$. Tuttavia, neanche $|Z(G)| = 2$ è possibile perché $Z(G)$ contiene tutti gli elementi

di ordine 2; infatti, dato $(a, b) \in G$ con $a, b \equiv 0 \pmod{2}$, si ha:

$$\begin{aligned}(c, d)(a, b) &= (c + (-1)^d a, d + b) \\ (a, b)(c, d) &= (a + (-1)^b c, b + d) = (a + c, b + d)\end{aligned}$$

Questi coincidono per ogni elemento $(c, d) \in G$ se e solo se $a + c = c - a$; però si è assunto $a \equiv 0 \pmod{2}$, quindi verifica $a \equiv -a \pmod{4}$ e, allora, $(c, d)(a, b) = (a, b)(c, d)$, $\forall (c, d) \in G$. Se ne conclude che $|Z(G)| = 4$, dove tre elementi sono di ordine 2 e l'ultimo è l'identità. Essendo un gruppo di ordine 4 per forza abeliano, il teorema di struttura assicura che $Z(G) \cong \mathbb{Z}/4\mathbb{Z}$, oppure $Z(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; per quanto appena detto sugli ordini degli elementi di $Z(G)$, l'unica possibilità è proprio quella richiesta: $Z(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c). Per costruire G' , si nota che i quozienti

$$G/Z(G) \cong \frac{G}{\mathbb{Z}/4\mathbb{Z} \times \{0\}}$$

sono abeliani (visto che il quoziente ha cardinalità 4), quindi

$$G' \subseteq Z(G) \cap (\mathbb{Z}/4\mathbb{Z} \times \{0\}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cap (\mathbb{Z}/4\mathbb{Z} \times \{0\}) = \{(0, 0), (1, 0)\}$$

Quindi $|G'| = \{1, 2\}$; visto che G non è abeliano, $|G'| = 2$ e, quindi, $G' = \{(0, 0), (2, 0)\}$, dato che $Z(G)$ contiene gli elementi di G di ordine 2. In questo modo, G_{ab} ha cardinalità 8 ed è abeliano, quindi le classi di isomorfismo possibili, per il teorema di struttura, sono le seguenti:

$$(\mathbb{Z}/2\mathbb{Z})^3 \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \mathbb{Z}/8\mathbb{Z}$$

Però G_{ab} ha elementi di ordine 4 e non ha elementi di ordine 8, quindi l'unica possibilità rimanente è $G_{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. ■

§2.4 Esercizi su anelli 2

Esercizio 2.10. Siano $I = (4, 3x + 1)$ e $J = (3, x^2 + 1)$, ideali dell'anello $\mathbb{Z}[x]$. Contare gli ideali massimali di $\mathbb{Z}[x]/IJ$.

A | NOZIONI FONDAMENTALI

§A.1 Applicazioni

Proposizione A.1. Sia $f : X \rightarrow Y$; valgono le seguenti proprietà:

$$\begin{aligned} f^{-1}(A \cup B) &= f^{-1}(A) \cup f^{-1}(B) & f^{-1}(A \cap B) &= f^{-1}(A) \cap f^{-1}(B) \\ f(A \cup B) &= f(A) \cup f(B) & f(A \cap B) &\subseteq f(A) \cap f(B) \end{aligned}$$

Un diagramma è detto **commutativo** se e soltanto se ogni cammino con stessa partenza e stesso arrivo danno lo stesso risultato per composizione. Nel caso del diagramma

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ g \downarrow & & \downarrow h \\ A & \xleftarrow{i} & B \end{array}$$

questo è commutativo se e solo se $(h \circ f)(x) = (i \circ g)(x)$.

§A.2 Relazioni

Sia X un insieme e $R \subseteq X \times X$. Si dice che ad R è associata una **relazione** \sim_R (o più semplicemente \sim quando non vi è ambiguità) su X se $x \sim_R y \iff (x, y) \in R$.

Un esempio, sono le relazioni di equivalenza, cioè relazioni che soddisfano le proprietà *riflessiva* ($x \sim x$), *simmetrica* ($x \sim y \iff y \sim x$) e *transitiva* ($x \sim y, y \sim z \implies x \sim z$).

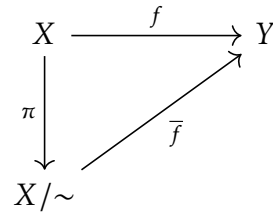
Teorema A.1. Se \sim è una relazione di equivalenza su X , allora la famiglia delle sue classi di equivalenza è una partizione di X . Viceversa, se \mathcal{P} è una partizione di X , allora induce, su X , una relazione di equivalenza data da

$$x \sim y \iff \exists C \in \mathcal{P} : x, y \in C$$

che ha, per classi, gli insiemi C della partizione \mathcal{P} .

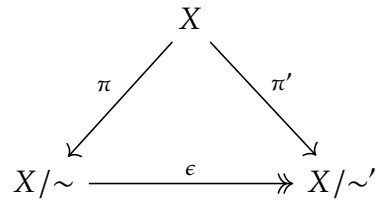
Definizione A.1. $f : X \rightarrow Y$ è *compatibile* con \sim su X se $x \sim y \implies f(x) = f(y)$.

Data $X \xrightarrow{f} Y$ compatibile con \sim su X e $\pi : X \rightarrow X/\sim$ proiezione al quoziente, allora esiste un'unica applicazione $\bar{f} = \bar{f} \circ \pi$ che rende



commutativo.

Se \sim e \sim' sono due relazioni su X , con $x \sim y \Rightarrow x \sim' y$, allora la partizione \mathcal{P} indotta da \sim è più fine di \mathcal{P}' , cioè quella indotta da \sim' . Questo significa che per ogni classe $C \in \mathcal{P}$, $\exists C' \in \mathcal{P}'$ tale che $C \subseteq C'$; in questo senso, la corrispondenza $C \mapsto C'$ è un'applicazione suriettiva ϵ che rende commutativo il seguente diagramma:



Definizione A.2 (Insieme di rappresentanti). Dato X un insieme e \sim relazione di equivalenza su X , un insieme $\mathcal{R} \subseteq X$ è un *insieme di rappresentanti* se

$$\pi|_{\mathcal{R}} : \mathcal{R} \subseteq X \rightarrow X/\sim$$

è biettiva.

Questo vuol dire che, per ogni classe di equivalenza, si è scelto un singolo elemento di X ad essa associato tramite la proiezione al quoziente π .