

# RIASSUNTI DI ALGEBRA

## INDICE

<b>1</b>	<b>Teoria dei gruppi</b>	<b>3</b>
1.1	Automorfismi e azioni	3
1.2	I p-gruppi	4
1.3	Teoremi di Cauchy e Cayley	4
1.4	Commutatore e gruppo derivato	4
1.5	Il gruppo diedrale	5
1.6	Il gruppo simmetrico	6
1.7	I quaternioni	8
1.8	Prodotti diretti	9
1.9	Prodotti semi-diretti	9
1.10	Teorema di struttura per gruppi abeliani finiti	10
1.11	Teoremi di Sylow	10
1.12	Risultati sulle classificazioni	11
1.13	Risultati vari sui gruppi	12
<b>2</b>	<b>Teoria degli anelli</b>	<b>14</b>
2.1	Proprietà di base	14
2.2	Omomorfismi e quoziente	15
2.3	Ideali primi e ideali massimali	16
2.4	Anello delle frazioni	17
2.5	Divisibilità nei domini	18
2.6	ED, PID e UFD	19
2.6.1	ED	19
2.6.2	PID	19
2.6.3	UFD	20
2.7	Anelli di polinomi	20
2.8	Risultati vari sugli anelli	21
<b>3</b>	<b>Teoria dei campi</b>	<b>22</b>
3.1	Estensioni di campi	22
3.2	Chiusura algebrica	23

3.3	Estensioni normali	24
3.4	Teoria di Galois	25
3.4.1	Gruppo di Galois di $\mathbb{F}_{q^d}/\mathbb{F}_q$	25
3.4.2	Teorema di corrispondenza di Galois	26
3.5	Risultati vari sui campi	26
<b>4</b>	<b>Esercizi</b>	<b>28</b>
4.1	Esercizi su gruppi 2	28
4.2	Esercizi su anelli 2	30

# 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  $\rho^i$ , 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  $\ell$  cicli disgiunti  $\sigma_i$ , 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.

Si ha  $|G| = 2 \cdot 3$ , quindi sono presenti, per Cauchy, un sottogruppo  $P_2$  di ordine 2 e un sottogruppo  $P_3$  di ordine 3. Visto che  $P_3$  ha indice 2 è normale in  $G$ . Inoltre,  $P_3 \cap P_2 = \{e\}$  perché gli altri elementi di un gruppo hanno ordine coprimo con l'ordine dell'altro gruppo. Questo implica che  $P_2 P_3 = G$ , quindi  $G \cong P_3 \rtimes_{\phi} P_2$ , con

$$\phi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \text{Aut } \mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$$

Ne segue che ci sono due possibili omomorfismi:  $\phi(1) = 0$ , che corrisponde al prodotto diretto  $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$ , oppure  $\phi(1) = 2 \in (\mathbb{Z}/3\mathbb{Z})^*$ . Riguardo l'ultimo caso, notando che  $2 \equiv -1 \pmod{3}$ , si conclude che l'ultimo omomorfismo consiste nel prodotto per  $-1$ . Pertanto, dati  $(a, b), (c, d) \in \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/2\mathbb{Z}$ , il prodotto è definito da:

$$(a, b) * (c, d) = (a + (-1)^b c, b + d)$$

Per finire, si nota che, per  $a \in (\mathbb{Z}/3\mathbb{Z})^*$ :

$$(0, 1)(a, 0)(0, 1)^{-1} = (0, 1)(a, 0)(0, 1) = (-2a, 0) = (a, 0)^{-1}$$

Quindi,  $G$  soddisfa la presentazione di  $S_3$ , per cui  $G \cong S_3$ . Si conclude che se  $G$  è un gruppo di ordine 6, le possibilità sono:

$$\mathbb{Z}/6\mathbb{Z} \quad S_3$$

rispettivamente nel caso abeliano e non-abeliano.

- **Classificazione dei gruppi di ordine  $pq$ .** Se  $p = q$ ,  $G$  è abeliano e  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  oppure  $G \cong \mathbb{Z}/p^2\mathbb{Z}$ .

Se  $q > p$  e  $p \nmid q - 1$ , allora si può avere solo  $G \cong \mathbb{Z}/pq\mathbb{Z}$ ; altrimenti si ha un prodotto semi-diretto non-banale, unico a meno di isomorfismo.

- **Classificazione dei gruppi di ordine 12.**

$$\mathbb{Z}/12\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad A_4 \quad \mathbb{Z}/3\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z} \quad D_6$$

- **Classificazione dei gruppi di ordine 8.**

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (\mathbb{Z}/2\mathbb{Z})^3 \quad D_4 \quad Q_8$$

- **Classificazione dei gruppi di ordine 30.**

$$\mathbb{Z}/30\mathbb{Z} \quad D_{15} \quad D_5 \times \mathbb{Z}/3\mathbb{Z} \quad D_3 \times \mathbb{Z}/5\mathbb{Z}$$

### §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  $H < Z(G)$ .

**Teorema 1.15.** Se  $H < G$  abeliano, allora  $\text{Hom}(G, H) \longleftrightarrow \text{Hom}(G/G', H)$ .

**Teorema 1.16.**  $S'_n = A_n$ .

**Teorema 1.17.**  $Z(S_n) = \{e\}$ , per  $n > 2$ .

**Lemma 1.17.1 (Normalizzatore-Centralizzatore).** Dato  $H < G$ , si ha:

(a).  $Z_G(H) \triangleleft N_G(H)$ ;

(b).  $N_G(H)/Z_G(H) \hookrightarrow \text{Aut}(H)$ .

**Teorema 1.18 (Isomorfismo di prodotti semi-diretti).** Siano  $N, H$  due gruppi e  $\varphi : H \rightarrow \text{Aut}(N)$ . Se  $f \in \text{Aut}(H)$ , allora:

$$N \rtimes_{\varphi} H \cong N \rtimes_{\varphi \circ f} H$$

## 2 | TEORIA DEGLI ANELLI

### §2.1 Proprietà di base

**Proposizione 2.1.** Sia  $A$  un anello commutativo con identità; allora:

- (a).  $(A^*, \cdot)$  è un gruppo abeliano;
- (b).  $A^* \cap D(A) = \emptyset$ ;
- (c). se  $A$  è finito, allora  $A = D(A) \cup A^*$ .

*Dimostrazione (c).*  $A^*, D(A) \subseteq A$ , quindi  $A^* \cup D(A) \subseteq A$ . Viceversa, per vedere che  $A \subseteq A^* \cup D(A)$ , si nota che se  $x \in D(A)$ , la tesi è vera, mentre se  $x \in A \setminus D(A)$ , allora si può definire

$$\varphi_x : \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & xa \end{array}$$

con  $\text{Ker } \varphi_x = \{a \in A \mid xa = 0\}$ . Però  $x \notin D(A)$ , quindi  $\text{Ker } \varphi_x = \{0\}$ ; usando che  $A$  è finito,  $\varphi_x$  è iniettiva e, quindi, anche suriettiva, per cui  $1 \in \text{Im } \varphi_x$ . Questo significa che  $\exists \bar{a} \in A$  per cui  $x\bar{a} = 1$ , quindi  $x \in A^*$ .  $\square$

**Definizione 2.1 (Ideale).** Dato  $A$  anello,  $I \subseteq A$  è un *ideale* se

- (a).  $(I, +) < (A, +)$ ;
- (b). per ogni  $a \in A$ , si ha  $aI \subset I$  e  $Ia \subset I$ .

**Definizione 2.2 (Ideale generato).** Dato  $A$  anello e  $S = \{s_1, \dots, s_n\} \subset A$ , l'ideale generato da  $S$  è:

$$\langle S \rangle := \left\{ \sum_{i=1}^n a_i s_i \mid a_i \in A \right\}$$

**Proposizione 2.2.** Dato  $A$  anello e  $I, J \subseteq A$  due suoi ideali, le seguenti operazioni producono altri ideali:

- (a).  $I \cap J$ ;
- (b).  $I + J := \langle I, J \rangle = \{i + j \mid i \in I, j \in J\}$ ;
- (c).  $IJ = \{\sum_{k=1}^n i_k j_k \mid n \geq 1, i_k \in I, j_k \in J\}$ ;
- (d).  $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$ ;

(e).  $(I : J) = \{x \in A \mid xJ \subseteq I\}$ .

**Proposizione 2.3.**  $A$  anello e  $I, J$  ideali; in generale,  $IJ \subseteq I \cap J$ , mentre  $IJ = I \cap J$  se e solo se  $I + J = A$ .

**Proposizione 2.4.**  $I \subset A$  è un ideale proprio se e solo se  $I \cap A^* = \emptyset$ .

**Corollario 2.0.1.**  $A$  è un campo se e solo se i suoi unici ideali sono  $\{0\}$  e  $A$ .

## §2.2 Omomorfismi e quoziente

**Proposizione 2.5.** Gli ideali di un anello  $A$  sono tutti e soli i nuclei degli omomorfismi da  $A$ .

**Teorema 2.1 (I teorema di omomorfismo).** Sia  $f : A \rightarrow B$  un omomorfismo; allora esiste un unico omomorfismo iniettivo  $\varphi : A/\text{Ker}(f) \rightarrow B$  tale che  $f = \varphi \circ \pi$ , ossia con  $\text{Im } f = \text{Im } \varphi$ .

**Teorema 2.2 (II teorema di omomorfismo).** Dati  $I, J \subset A$  due ideali, con  $I \subset J$ , allora  $J/I$  è un ideale di  $A/I$  e

$$\frac{A/I}{J/I} \cong A/J$$

**Teorema 2.3 (III teorema di omomorfismo).** Sia  $I \subset A$  ideale e  $B \subset A$  sottoanello; allora:

$$\frac{B+I}{I} \cong \frac{B}{B \cap I}$$

**Lemma 2.3.1.** Sia  $f : A \rightarrow B$  un omomorfismo; allora:

(a).  $\forall J$  ideale di  $B$ , si ha che  $f^{-1}(J)$  è un ideale di  $A$ ;

(b). se  $f$  è suriettiva, allora  $\forall I$  ideale di  $A$ , si ha che  $f(I)$  è un ideale di  $B$ .

**Teorema 2.4 (Teorema di corrispondenza).** Sia  $I$  un ideale di  $A$  e  $\pi$  la proiezione al quoziente  $A/I$ . Tale proiezione induce una corrispondenza biunivoca tra gli ideali di  $A/I$  e gli ideali di  $A$  che contengono  $I$ .

**Teorema 2.5 (Teorema cinese del resto).** Sia  $A$  un anello commutativo con unità e  $I, J$  due suoi ideali; allora

$$f : \begin{array}{ccc} A & \longrightarrow & A/I \times A/J \\ a & \longmapsto & (a+I, a+J) \end{array}$$

è un omomorfismo, con  $\text{Ker } f = I \cap J$ . Inoltre, vale  $I + J = A \iff f$  è suriettiva;

in questo caso:

$$A/IJ \cong A/I \times A/J$$

## §2.3 Ideali primi e ideali massimali

**Definizione 2.3 (Maggiorante).** Dato  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato e  $X \subset \mathcal{F}$  un sottoinsieme, si dice che  $M \in \mathcal{F}$  è un maggiorante per  $X$  se,  $\forall A \in X$ ,  $A \leq M$ .

**Definizione 2.4 (Elemento massimale).** Dato  $(\mathcal{F}, \leq)$ , si ha  $A \in \mathcal{F}$  elemento massimale per  $\mathcal{F}$  se,  $\forall B \in \mathcal{F} : A \leq B$ , si ha  $A = B$ .

**Definizione 2.5 (Massimo).**  $A \in \mathcal{F}$  è detto *massimo* per  $\mathcal{F}$  se,  $\forall B \in \mathcal{F}$ , si ha  $B \leq A$ .

**Definizione 2.6 (Catena).** Una catena di  $\mathcal{F}$  è un suo sottoinsieme totalmente ordinato.

**Definizione 2.7 (Insieme induttivo).** Si dice che  $\mathcal{F}$  è induttivo se ogni sua catena ammette un maggiorante al suo interno.

**Lemma 2.5.1 (Lemma di Zorn).** Se  $(\mathcal{F}, \leq)$  è un insieme parzialmente ordinato e induttivo, allora contiene elementi massimali.

**Definizione 2.8 (Ideale primo).** Un  $I$  ideale proprio di  $A$  anello, si dice *primo* se

$$xy \in I \implies x \in I \text{ oppure } y \in I, \forall x, y \in A$$

**Definizione 2.9 (Ideale massimale).**  $I \subsetneq A$  è detto *massimale* se è un elemento massimale della famiglia  $\mathcal{F}$  di tutti gli ideali propri di  $A$ , cioè se e solo se  $\forall J \subsetneq A : I \subseteq J \implies I = J$ .

**Proposizione 2.6.** Ogni anello unitario ammette ideali massimali.

**Proposizione 2.7 (Proprietà degli ideali massimali).** Dato  $A$  anello, si ha che

- (a). ogni ideale proprio di  $A$  è contenuto in un ideale massimale;
- (b). ogni elemento non-invertibile di  $A$  è contenuto in un ideale massimale.

**Proposizione 2.8 (Caratterizzazione degli ideali primi e massimali).** Sia  $A$  un anello e  $I \subsetneq A$  un suo ideale proprio; allora:

- (a).  $I$  è primo se e solo se  $A/I$  è un dominio;
- (b).  $I$  è massimale se e solo se  $A/I$  è un campo;
- (c).  $A$  è un dominio se e solo se  $(0)$  è un ideale primo;



(d).  $A$  è un campo se e solo se  $(0)$  è un ideale massimale;

(e).  $I$  massimale  $\implies I$  primo.

**Proposizione 2.9.** La biezione tra ideali data da  $\pi : A \rightarrow A/I$  preserva ideali primi e massimali (contenenti  $I$ ).

## §2.4 Anello delle frazioni

**Definizione 2.10 (Parte moltiplicativa).** Dati  $A$  dominio (commutativo e con identità) e  $S \subset A$ , si dice che  $S$  è una *parte moltiplicativa* di  $A$  se:

(a).  $0 \notin S$ ;

(b).  $1 \in S$ ;

(c).  $S$  è chiuso sotto moltiplicazione, cioè, dati  $x, y \in S$ , allora  $xy \in S$ .

**Definizione 2.11 (Insieme delle frazioni).** Dato un dominio  $A$  e data  $S$  una sua parte moltiplicativa, si definisce l'*insieme delle frazioni* come

$$S^{-1}A = \left\{ \frac{a}{s} \mid a \in A, s \in S \right\} / \sim$$

dove  $a/s \sim b/t \iff at = bs$ .

**Proposizione 2.10.** L'applicazione

$$f : \begin{array}{ccc} A & \longrightarrow & S^{-1}A \\ a & \longmapsto & a/1 \end{array}$$

è un omomorfismo iniettivo, quindi  $S^{-1}A$  è un'estensione di  $A$ .

**Proposizione 2.11.** Sia  $A$  un dominio e  $S = A \setminus \{0\}$  una sua parte moltiplicativa; allora l'anello delle frazioni  $S^{-1}A$  è il più piccolo campo contenente  $A$ .

**Definizione 2.12 (Localizzato).** Dato un dominio  $A$  e  $P \subset A$  un suo ideale primo, considerando  $S = A \setminus P$ , si definisce  $S^{-1}A = A_P$  come il localizzato di  $A$  a  $P$ .

**Osservazione 2.1.**  $A_P$  è un anello locale, ossia ha un unico ideale massimale.

Di seguito, alcune caratteristiche di  $S^{-1}A$ .

- **Invertibili.** Sono tutti gli  $a/s \in S^{-1}A$  tali che  $s/a \in S^{-1}A$ , ossia quelli tali che  $\exists b \in A : ab \in S$ .
- **Ideali.** Dato  $I \subset A$ , si costruisce l'insieme  $S^{-1}I = \{x/s \in S^{-1}A \mid x \in I, s \in S\}$ . Per questo, vale la seguente proposizione.

**Proposizione 2.12.** Sia  $I \subset A$  e  $S^{-1}A$  l'anello delle frazioni di  $A$ . Allora:

- (a).  $S^{-1}I$  è un ideale di  $S^{-1}A$ ;
- (b). per ogni ideale  $J \subset S^{-1}A$ , si trova un ideale  $I \subset A$  tale che  $J = S^{-1}I$ ;
- (c).  $S^{-1}I$  è proprio se e solo se  $I \cap S = \emptyset$ ;
- (d). dato  $P$  ideale primo, allora  $S^{-1}P$  è un ideale primo di  $S^{-1}A$ .

## §2.5 Divisibilità nei domini

**Definizione 2.13 (Divisibilità).** Siano  $a, b \in A$  dominio, con  $a \neq 0$ ; allora  $a \mid b \iff \exists c \in A : b = ac$ .

**Osservazione 2.2.**  $a \mid b \iff \langle b \rangle \subseteq \langle a \rangle$ ; infatti,  $ca = b \Rightarrow b \in \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle$ .

**Definizione 2.14 (Elemento associato).** Dati  $a, a' \in A$  dominio, si dicono *associati* se vale una delle seguenti, equivalenti, condizioni:

- (a).  $a \mid a'$  e  $a' \mid a$ ;
- (b).  $\exists u \in A^*$  tale che  $a = ua'$ ;
- (c).  $\langle a \rangle = \langle a' \rangle$ .

**Definizione 2.15 (MCD).** Per  $a, b \in A$  dominio non entrambi nulli,  $d$  è un MCD se valgono entrambe le seguenti condizioni:

- (a).  $d \mid a$  e  $d \mid b$ ;
- (b).  $\forall x \in A$  tale che  $x \mid a$  e  $x \mid b$ , si ha  $x \mid d$ .

**Proposizione 2.13.** Dati  $a, b \in A$ , si dice che  $d$  e  $d'$  sono loro MCD se e solo se  $d \sim d'$ .

**Definizione 2.16 (Elemento primo).**  $x \in A \setminus (A^* \cup \{0\})$  è primo se,  $\forall a, b \in A$ , si ha  $x \mid ab \implies x \mid a$  oppure  $x \mid b$ .

**Definizione 2.17 (Elemento irriducibile).**  $x \in A \setminus (A^* \cup \{0\})$  è irriducibile se,  $\forall a, b \in A$ , vale  $x = ab \implies a \in A^*$  oppure  $b \in A^*$ .

**Proposizione 2.14.** Se  $x \in A$  dominio è primo, allora è irriducibile.

**Proposizione 2.15 (Caratterizzazione elementi primi e irriducibili).** Sia  $x \in A$  dominio. Allora:

- (a).  $x$  è primo  $\iff \langle x \rangle$  è un ideale primo non-nullo;
- (b).  $x$  è irriducibile  $\iff \langle x \rangle$  è un ideale massimale nell'insieme degli ideali principali.

## §2.6 ED, PID e UFD

### §2.6.1 ED

**Definizione 2.18 (ED).**  $A$  dominio è *euclideo* se si può definire una mappa  $d : A \setminus \{0\} \rightarrow \mathbb{N}$  tale che:

- (a).  $d(x) \leq d(xy)$ ,  $\forall x, y \in A \setminus \{0\}$ ;
- (b).  $\forall x \in A$ ,  $\forall y \in A \setminus \{0\}$ , si trovano  $q, r \in A$  tali che  $x = yq + r$ , con  $d(r) < d(y)$  oppure  $r = 0$ .

**Proposizione 2.16 (Algoritmo di Euclide).** In  $A$  dominio euclideo, per ogni coppia  $a, b \in A$ , esiste un MCD ottenuto tramite algoritmo di Euclide.

**Proposizione 2.17.** Gli elementi di grado minimo di  $A$  dominio euclideo coincidono con gli elementi di  $A^*$ .

**Proposizione 2.18.** Tutti gli ideali di  $A$  dominio euclideo sono principali e generati da un elemento di grado minimo nell'ideale in questione.

### §2.6.2 PID

**Definizione 2.19 (PID).** Un dominio  $A$  è a *ideali principali* se ogni suo ideale è principale.

**Proposizione 2.19.** Se  $A$  è un PID, i suoi unici ideali primi sono  $\langle 0 \rangle$  e quelli massimali.

**Proposizione 2.20 (MCD nei PID).** Dati  $x, y \in A$  PID non entrambi nulli, si ha  $\langle x, y \rangle = \langle d \rangle$ , con  $d = (x, y)$ .

### §2.6.3 UFD

**Definizione 2.20 (UFD).**  $A$  dominio è a *fattorizzazione unica* se ogni elemento  $x \in A \setminus (A^* \cup \{0\})$  si decompone univocamente in irriducibili, a meno di prodotto per un'unità.

**Proposizione 2.21.** Dati  $a, b \in A$  UFD non entrambi nulli, esiste sempre un loro MCD.

**Teorema 2.6 (Caratterizzazione degli UFD).**  $A$  dominio è un UFD se e solo se sono soddisfatte entrambe le seguenti condizioni:

- (a). ogni irriducibile è primo;
- (b). ogni catena discendente di divisibilità è stazionaria, cioè data  $\{a_i\}_{i \geq 0} \subset A$ , con  $a_{i+1} \mid a_i$ , allora  $\exists n_0 \in \mathbb{N}$  tale che  $a_i \sim a_{n_0}, \forall i \geq n_0$ .

**Corollario 2.6.1.** Se  $A$  è un PID, allora è un UFD.

$$\text{ED} \implies \text{PID} \implies \text{UFD}$$

### §2.7 Anelli di polinomi

**Definizione 2.21 (Contenuto).** Dato  $f(x) \in A[x]$ , con  $A$  UFD e  $f(x) = \sum_{i=0}^n a_i x^i$ , si definisce il *contenuto* di  $f(x)$  come l'MCD dei suoi coefficienti:

$$c(f(x)) = \gcd(a_0, \dots, a_n)$$

**Definizione 2.22 (Elemento primitivo).**  $f(x) \in A[x]$ , con  $A$  UFD, è *primitivo* se  $c(f(x)) \sim 1$ .

**Lemma 2.6.1 (Lemma di Gauss).** Dati  $f(x), g(x) \in A[x]$ , allora:

$$c(f(x)g(x)) = c(f(x))c(g(x))$$

**Corollario 2.6.2.** Dati  $f(x), g(x) \in A[x]$ , con  $c(f(x)) = 1$  e  $f(x) \mid g(x)$  in  $K[x]$ , con  $K$  campo dei quozienti di  $A$ , allora  $f(x) \mid g(x)$  in  $A[x]$ .

**Corollario 2.6.3.** Dato  $f(x) \in A[x]$ , con  $f(x) = g(x)h(x)$  in  $K[x]$  (con  $K$  campo dei quozienti di  $A$ ) e  $\deg g(x), \deg h(x) \geq 1$  (quindi  $f$  riducibile in  $K[x]$ ), allora  $\exists \delta \in K^*$  tale che  $g_1(x) = \delta g(x) \in A[x]$  e  $h_1(x) = \delta^{-1} h(x) \in A[x]$ , per cui  $f(x) = g_1(x)h_1(x)$  in  $A[x]$ .

**Teorema 2.7.** Gli irriducibili di  $A[x]$ , con  $A$  UFD, soddisfano una tra le seguenti condizioni:

- (a).  $f(x) \in A$  e irriducibile in  $A$ ;
- (b).  $f(x) \in A[x]$ , con  $\deg f(x) \geq 1$ ,  $c(f(x)) = 1$  e  $f(x)$  irriducibile in  $K[x]$ .

**Teorema 2.8.** Se  $A$  è un UFD, allora  $A[x]$  è un anello a fattorizzazione unica.

**Corollario 2.8.1.** Se  $A$  è un UFD, allora  $A[x_1, \dots, x_n]$  è un anello a fattorizzazione unica.

**Proposizione 2.22 (Eisenstein).** Sia  $A$  un UFD e  $f(x) \in A[x]$  primitivo, con  $f(x) = \sum_{i=0}^n a_i x^i$ . Dato  $p \in A$  un primo tale che

- (a).  $p \nmid a_n$ ,
- (b).  $p \mid a_i, \forall i = 0, \dots, n-1$ ,
- (c).  $p^2 \nmid a_0$ ;

allora  $f(x)$  è irriducibile in  $A[x]$  e in  $K[x]$ .

## §2.8 Risultati vari sugli anelli

**Teorema 2.9.** Dato  $A$  un anello qualsiasi e dati  $I, J$  due suoi ideali, allora

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

**Proposizione 2.23.** Sia  $M$  un ideale massimale di  $\mathbb{Z}[x]$  tale che  $M \cap \mathbb{Z}$  contiene un primo  $p$ ; allora  $M = (p, f(x))$ , con  $f(x) \bmod p$  irriducibile in  $\mathbb{F}_p[x]$ .

## 3 | TEORIA DEI CAMPI

### §3.1 Estensioni di campi

**Definizione 3.1 (Elementi algebrici e trascendenti).** Dato  $K$  campo e  $L$  una sua estensione,  $\alpha \in L$  è algebrico su  $K$  se  $\exists f(x) \in K[x] \setminus \{0\}$  tale che  $f(\alpha) = 0$ . Altrimenti,  $\alpha$  è detto trascendente su  $K$ .

**Definizione 3.2 (Grado di un'estensione).** Data  $L/K$  estensione, il suo grado si indica con  $[L : K] = \dim_K L$  ed è la dimensione di  $L$  come spazio vettoriale su  $K$ .

**Proposizione 3.1.** Sia  $L/K$  un'estensione, con  $\alpha \in L$ ; allora:

$$[K(\alpha) : K] = \begin{cases} +\infty & , \alpha \text{ trascendente} \\ \deg \mu_\alpha(x) & , \alpha \text{ algebrico} \end{cases}$$

con  $\mu_\alpha(x)$  polinomio minimo di  $\alpha$  in  $K[x]$ .

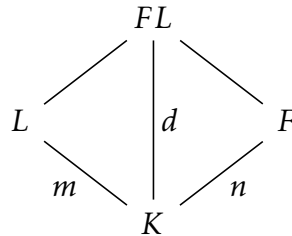
**Proposizione 3.2 (Formula della torre).** Sia data la torre di estensioni  $K \subset F \subset L$ ; allora  $L/K$  è finita se e solo se  $L/F$  e  $F/K$  sono finite e vale

$$[L : K] = [L : F][F : K]$$

**Definizione 3.3 (Estensione composta).** Sia  $\Omega$  un campo e  $L, M \subset \Omega$ ; allora  $LM = L(M) = M(L)$  è il più piccolo sottocampo di  $\Omega$  contenente  $L$  e  $M$ . Se  $M, L$  sono estensioni finitamente generate, cioè  $L = K(\alpha_1, \dots, \alpha_n)$  e  $M = K(\beta_1, \dots, \beta_m)$ , vale

$$LM = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$$

**Proposizione 3.3.** Si considerano le due torri  $K \subset L \subset FL$  e  $K \subset F \subset FL$ , con  $[L : K] = m$  e  $[F : K] = n$ ; allora  $[FL : K] = d < +\infty$  e  $[m, n] \mid d$ .



**Definizione 3.4 (Estensione algebrica).**  $L/K$  è algebrica se  $\forall \alpha \in L$ ,  $\alpha$  è algebrico su  $K$ .

**Proposizione 3.4.** Ogni estensione finita è algebrica.

**Proposizione 3.5.** Data estensione  $L/K$ , allora  $A = \{\alpha \in L \mid \alpha \text{ algebrico su } K\}$  è un campo e un'estensione algebrica di  $K$ .

**Proposizione 3.6.**  $L/K$  è un'estensione finitamente generata da algebrici, cioè  $L = K(\alpha_1, \dots, \alpha_n)$ , se e solo se  $L/K$  è finita.

**Teorema 3.1 (Caratterizzazione delle estensioni algebriche).** Valgono i due seguenti punti.

- (a). Data la torre  $K \subset L \subset F$ ,  $F/K$  è algebrica se e solo se  $F/L$  e  $L/K$  sono algebriche.
- (b). Date due estensioni  $L/K$  e  $M/K$ , queste sono algebriche se e solo se  $LM/K$  è algebrica.

### §3.2 Chiusura algebrica

**Definizione 3.5 (Campo algebricamente chiuso).**  $\Omega$  è detto algebricamente chiuso se ogni  $f(x) \in \Omega[x]$  non costante ha almeno una radice in  $\Omega$ .

**Definizione 3.6 (Chiusura algebrica).**  $\Omega/K$  è una chiusura algebrica di  $K$  se valgono i due seguenti punti:

- (a).  $\Omega$  è algebricamente chiuso;
- (b).  $\Omega/K$  è un'estensione algebrica.

**Teorema 3.2 (Esistenza e unicità della chiusura).** Dato  $K$  campo, allora esiste sempre una sua chiusura algebrica, che è unica a meno di isomorfismo.

**Definizione 3.7 (Campo di spezzamento).** Dato  $f(x) \in K[x]$ , con  $\deg f(x) \geq 1$ , e date  $\alpha_1, \dots, \alpha_n \in \bar{K}$  e sue radici, se ne definisce il campo di spezzamento su  $K$  come il sotto campo di  $\bar{K}$  dato da  $K(\alpha_1, \dots, \alpha_n)$ .

**Proposizione 3.7.** Sia  $K$  un campo e  $\alpha \in \bar{K}$ . Se  $k$  è il numero di radici distinte di  $\mu_\alpha(x)$  in  $\bar{K}$ , allora

$$\exists \varphi_1, \dots, \varphi_k : K(\alpha) \hookrightarrow \bar{K}$$

estensioni dell'immersione  $K \hookrightarrow \bar{K}$  data dall'identità, con  $\varphi_i|_K = \text{Id}_K$ .

**Teorema 3.3 (Criterio della derivata).** Sia  $f(x) \in K[x]$ ; allora  $f(x)$  ha radici multiple in  $\bar{K}$  se e solo se  $\gcd(f(x), f'(x)) \neq 1$ . Se  $f$  è irriducibile in  $K[x]$ , allora  $f$  ha radici multiple se e solo se  $f'(x) = 0$ .

**Definizione 3.8 (Campo perfetto).**  $K$  è perfetto se ogni irriducibile di  $K[x]$  ha derivata non-nulla.

**Proposizione 3.8.** Sia  $\alpha \in \bar{K}$ , con  $[K(\alpha) : K] = n$ . Allora, per ogni  $\varphi : K \hookrightarrow \bar{K}$

$$\exists \varphi_1, \dots, \varphi_n : K(\alpha) \hookrightarrow \bar{K}$$

con  $\varphi_i|_K = \varphi$ ,  $\forall i$ .

**Corollario 3.3.1.**  $E/K$  estensione di grado  $n$ ; allora  $\forall \varphi : K \hookrightarrow \bar{K}$ , si trovano esattamente  $n$  immersioni  $\varphi_1, \dots, \varphi_n : E \hookrightarrow \bar{K}$ , con  $\varphi_i|_K = \varphi$ .

**Definizione 3.9 (Elementi coniugati).** Per  $\alpha \in \bar{K}$ , i suoi coniugati su  $K$  sono le radici del suo polinomio minimo su  $K$ .

**Definizione 3.10 (Estensione separabile).**  $K \subset L$  estensione algebrica è separabile se il polinomio minimo di ogni suo elemento è separabile, cioè se ha tutte radici distinte in un campo di spezzamento.

**Teorema 3.4 (Teorema dell'elemento primitivo).** Sia  $K$  un campo e  $E/K$  un'estensione finita e separabile; allora  $E/K$  è semplice, cioè  $\exists \gamma \in E : E = K(\gamma)$ .

### §3.3 Estensioni normali

**Definizione 3.11 (Estensione normale).**  $F/K$  estensione algebrica è normale se  $\forall \varphi : F \hookrightarrow \bar{K}$ , con  $\varphi|_K = \text{Id}_K$ , si ha  $\varphi(F) = F$ .

**Proposizione 3.9.** Sia  $F/K$  algebrica e finita. Allora le seguenti affermazioni sono equivalenti:

- (a).  $F/K$  è normale;
- (b). ogni irriducibile  $f(x) \in K[x]$  che ha una radice in  $F$ , le ha tutte in  $F$ ;
- (c).  $F$  è il campo di spezzamento su  $K$  di una famiglia di polinomi di  $K[x]$ .

**Proposizione 3.10.** Ogni estensione di grado 2 è normale in caratteristica diversa da 2.

**Proposizione 3.11.** Siano  $F/K$  e  $L/K$  due estensioni normali di  $K$  nella chiusura  $\bar{K}$ ; allora anche  $FL/K$  e  $(F \cap L)/K$  sono normali.



**Proposizione 3.12.** Data la torre  $K \subset F \subset L$  nella chiusura  $\overline{K}$ , se  $L/K$  è normale, allora  $L/F$  è normale.

### §3.4 Teoria di Galois

**Definizione 3.12 (Estensione di Galois).** Un'estensione  $E/K$  è di Galois se e solo se è normale e separabile.

**Definizione 3.13 (Gruppo di Galois).** Dato

$$\text{Aut}_K E = \{\varphi : E \xrightarrow{\sim} E \mid \varphi|_K = \text{Id}_K\}$$

l'insieme delle immersioni  $\{\varphi : E \hookrightarrow \overline{K} \mid \varphi|_K = \text{Id}_K\}$  che fissano  $E$  (perché  $E/K$  è normale) con immagine in  $E$ , si definisce

$$\text{Gal}(E/K) := (\text{Aut}_K E, \circ)$$

**Osservazione 3.1.** Visto che il numero di immersioni  $E \hookrightarrow \overline{K}$  coincide con il grado dell'estensione, si ha:

$$|\text{Gal } E/K| = [E : K]$$

**Proposizione 3.13.** Sia  $f(x) \in K[x]$  irriducibile di grado  $n$ ; se  $F$  è il suo campo di spezzamento su  $K$ , allora  $n \mid [F : K] \mid n!$  e  $\text{Gal } F/K \hookrightarrow S_n$ .

**Osservazione 3.2.** L'azione di  $\text{Gal } F/K$  sull'insieme delle radici di  $f(x)$  è fedele e transitiva.

#### §3.4.1 Gruppo di Galois di $\mathbb{F}_{q^d}/\mathbb{F}_q$

**Proposizione 3.14.** L'estensione  $\mathbb{F}_{q^d}/\mathbb{F}_q$ , con  $q = p^r$  e  $p$  primo, è normale.

**Corollario 3.4.1.** Tutte le estensioni di campi finiti sono normali.

**Definizione 3.14 (Automorfismo di Frobenius).** Si definisce come

$$\phi : \begin{array}{ccc} \mathbb{F}_{q^d} & \xrightarrow{\sim} & \mathbb{F}_{q^d} \\ x & \mapsto & x^q \end{array}$$

**Teorema 3.5.** Il gruppo di Galois di  $\mathbb{F}_{q^d}/\mathbb{F}_q$  è generato dall'automorfismo di Frobenius.

### §3.4.2 Teorema di corrispondenza di Galois

**Definizione 3.15.** Sia  $L/K$  un'estensione di Galois finita e  $H < \text{Gal } L/K$ ; allora si definisce

$$L^H := \text{Fix}(H) = \{\alpha \in L \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\} \subseteq L$$

**Proposizione 3.15.**  $L^H$  è un sottocampo.

**Lemma 3.5.1.** Sia  $L/M$  di Galois e  $H \leq \text{Gal } L/M$ ; allora

$$M = L^H \iff H = \text{Gal } L/M$$

**Lemma 3.5.2.** Sia  $L/K$  di Galois e  $H < \text{Gal } L/K$ . Per  $\sigma \in \text{Gal } L/K$ , si ha  $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ .

**Teorema 3.6 (Teorema di corrispondenza di Galois).** Data  $L/K$  di Galois, l'insieme delle sottoestensioni di  $L/K$  e l'insieme dei sottogruppi di  $\text{Gal } L/K$  sono in corrispondenza biunivoca; inoltre,  $H < \text{Gal } L/K \iff L^H/K$  è normale e, in tal caso:

$$\text{Gal } L^H/K \cong \frac{\text{Gal } L/K}{\text{Gal } L/L^H}$$

**Proposizione 3.16 (Proprietà della corrispondenza).** Siano  $H, S \leq \text{Gal } L/K$ . Allora valgono i seguenti punti:

- (a).  $H \leq S \iff L^H \supseteq L^S$ ;
- (b).  $L^{H \cap S} = L^H L^S$  (composto dei due campi);
- (c).  $L^{\langle S, H \rangle} = L^H \cap L^S$ .

### §3.5 Risultati vari sui campi

**Teorema 3.7 (Campo di spezzamento di  $x^n - 1$  su  $\mathbb{F}_p$ ).** Dato  $n = p^k m$ , con  $(m, p) = 1$ , il campo di spezzamento di  $x^n - 1$  su  $\mathbb{F}_p$  è  $\mathbb{F}_{p^d}$ , con  $d$  ordine moltiplicativo di  $p$  modulo  $n$ , cioè è il minimo valore positivo che soddisfa

$$p^x \equiv 1 \pmod{m}$$

**Proposizione 3.17.**  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ .

**Proposizione 3.18.** Date le torri  $F \subset K \subset KL$  e  $F \subset L \subset KL$ , se  $K/F$  di Galois, allora:

- $KL/L$  è di Galois;
- $\text{Gal}(KL/L) \cong \text{Gal}(K/L \cap K)$ .

**Corollario 3.7.1.** Siano date le torri  $F \subset K \subset KL$  e  $F \subset L \subset KL$ , con  $K/F$  di Galois e  $K \cap L = F$ ; allora:

$$[KL : F] = [K : F][L : F]$$

**Teorema 3.8 (Biquadratiche).** Dato  $p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$  irriducibile e dato  $K$  il suo campo di spezzamento su  $\mathbb{Q}$ , allora:

- (a).  $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  se  $b$  è un quadrato su  $\mathbb{Q}$ ;
- (b).  $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$  se  $b\Delta = b(a^2 - 4b)$  è un quadrato su  $\mathbb{Q}$ ;
- (c).  $\text{Gal}(K/\mathbb{Q}) \cong D_4$  altrimenti.

## 4 | ESERCIZI

### §4.1 Esercizi su gruppi 2

**Esercizio 4.1.** 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,  $G_{\text{ab}}$  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  $G_{\text{ab}}$  ha elementi di ordine 4 e non ha elementi di ordine 8, quindi l'unica possibilità rimanente è  $G_{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ . ■

**Esercizio 4.2.** Determinare il più piccolo  $m$  tale che esiste un sottogruppo di  $S_m$  isomorfo a  $A_5 \times \mathbb{Z}/6\mathbb{Z}$ .

*Svolgimento.* Si deve trovare un  $m$  compatibile con il fatto che gli elementi di  $A_5$  e quelli di  $\mathbb{Z}/6$  devono commutare. Gli elementi di  $A_5$  sono tutte le permutazioni pari che agiscono fedelmente su 5 elementi; pertanto,  $A_5$  contiene elementi di ordine 5,

mentre  $\mathbb{Z}/6$  contiene elementi di ordine 6. Mentre un elemento di ordine 5 in  $S_m$  è per forza un 5-ciclo, un elemento di ordine 6 si può costruire componendo un 2-ciclo con un 3-ciclo, quindi deve avere a disposizione almeno 5 elementi su cui agire. Per fare in modo che elementi di ordine 5 e 6 commutino, si deve far in modo che agiscano su elementi distinti; per quanto appena detto, quindi, il più piccolo  $m$  che permette ciò è  $m = 10$ . Per dimostrarlo, si fa prima vedere che  $S_9$  non sarebbe sufficiente e poi si dà un esempio concreto in  $S_{10}$ .

Sia, allora,  $\varphi : A_5 \times \mathbb{Z}/6\mathbb{Z} \rightarrow S_9$ . Dato  $\sigma \in A_5$ ,  $\varphi(\sigma, 0)$  deve avere ordine 5 perché  $\varphi$  sia un isomorfismo, quindi deve essere necessariamente un 5-ciclo; inoltre,  $\varphi(e, 1)$  deve avere ordine 6 e commutare con  $\varphi(\sigma, 0)$ . A questo punto, si osserva che

$$|\text{Cl}_{S_9}(\varphi(\sigma, 0))| = \binom{9}{5} 4! = \frac{9!}{4!5!} = \frac{9!}{5!} \implies |Z_{S_9}(\varphi(\sigma, 0))| = \frac{9!}{9!/5!} = 5!$$

Data  $\varphi(\sigma, 0) = (1\ 2\ 3\ 4\ 5)$ , prendendo

$$H := \langle (1\ 2\ 3\ 4\ 5) \rangle \quad K := \{\text{permutazioni di } S_9 \text{ che fissano } \{1\ 2\ 3\ 4\ 5\}\} \cong S_4$$

questi sono sottogruppi di  $Z_{S_9}(\varphi(\sigma, 0))$ , commutano, si intersecano nell'identità e sono tali che  $|HK| = 5!$ , quindi, per il teorema di decomposizione diretta, si può scrivere che

$$Z_{S_9}(1\ 2\ 3\ 4\ 5) \cong \mathbb{Z}/5 \times S_4$$

Ma a questo punto sorge un assurdo: non può esistere alcun elemento di ordine 6 nel centralizzatore, quindi questo isomorfismo non va bene.

Ora si mostra che è possibile costruire un isomorfismo in  $S_{10}$ . Siano  $H$  il sottogruppo di  $S_{10}$  delle permutazioni pari agiscono su  $\{1\ 2\ 3\ 4\ 5\}$  e  $\tau = (6\ 7)(8\ 9\ 10) \in S_{10}$ , quindi  $H \cong A_5$  e  $K = \langle \tau \rangle \cong \mathbb{Z}/6$ . Si nota che  $H$  e  $K$  commutano e hanno intersezione banale perché agiscono su elementi differenti, quindi, per il teorema di decomposizione diretta, esiste un sottogruppo di  $S_{10}$  isomorfo a  $H \times K \cong A_5 \times \mathbb{Z}/6$ . ■

## §4.2 Esercizi su anelli 2

**Esercizio 4.3.** Siano  $I = (4, 3x + 1)$  e  $J = (3, x^2 + 1)$ , ideali dell'anello  $\mathbb{Z}[x]$ . Contare gli ideali massimali di  $\mathbb{Z}[x]/IJ$ .

*Svolgimento.* Si vuole utilizzare il teorema cinese del resto per scrivere  $\mathbb{Z}[x]/IJ \cong \mathbb{Z}[x]/I \times \mathbb{Z}[x]/J$ . Per farlo, si osserva che  $1 \in I + J$  perché  $4 \in I$  e  $3 \in J$ , quindi

$1 = 4 - 3 \in I + J$ , da cui  $I + J = \mathbb{Z}[x]$ . Questo assicura l'isomorfismo voluto. Ora si nota che

$$\mathbb{Z}[x]/(4, 3x + 1) \cong \mathbb{Z}_4[x]/(3x + 1)$$

dove  $(3x + 1)$  nell'espressione finale è l'ideale in  $\mathbb{Z}_4[x]$ ; per questo motivo, visto che 3 è un'unità in  $\mathbb{Z}_4$ , si ha che  $(3x + 1) = (x + 3) \subset \mathbb{Z}_4[x]$ . Ne segue che  $\mathbb{Z}[x]/(4, 3x + 1) \cong \mathbb{Z}_4[x]/(x + 3) \cong \mathbb{Z}_4$ . Per l'altro fattore, si ha:

$$\mathbb{Z}[x]/(3, x^2 + 1) \cong \mathbb{F}_3[x]/(x^2 + 1) \cong \mathbb{F}_9$$

perché  $x^2 + 1$  è irriducibile in  $\mathbb{F}_3$  e il campo risultante è quello con 9 elementi. Se ne conclude che  $\mathbb{Z}[x]/IJ \cong \mathbb{Z}_4 \times \mathbb{F}_9$ . Ora,  $\mathbb{F}_9$  ha, come unico ideale proprio, quello banale, mentre  $\mathbb{Z}_4$  ha solo (2) come ideale massimale. Questo significa che gli ideali massimali di  $\mathbb{Z}[x]/IJ$  sono due e sono dati da  $(2) \times \mathbb{F}_9$  e  $\mathbb{Z}_4 \times \{0\}$ . ■

**Esercizio 4.4.** Sia  $A = \mathbb{Z}[x, y]/(y^2 + 1)$ .

- (a). Contare il numero di omomorfismi da  $A$  in  $\mathbb{F}_7$  e  $\mathbb{F}_{49}$ .
- (b). Contare gli ideali di  $A$  che contengono  $(7, x^2 + 1)$ .

*Svolgimento.* Per il punto (a), si contano quanti omomorfismi da  $\mathbb{Z}[x, y]/(y^2 + 1)$  in  $\mathbb{F}_7$  e  $\mathbb{F}_{49}$  sono possibili, perché la scelta di dove mappare  $x$  è totalmente arbitraria, visto che non ci sono vincoli. Per  $y$ , invece, è necessario che un omomorfismo  $\varphi : \mathbb{Z}[x, y]/(y^2 + 1) \rightarrow \mathbb{F}_7, \mathbb{F}_{49}$  rispetti la condizione

$$\varphi(y)^2 + 1 = 0 \implies \varphi(y)^2 = -1$$

Questo si analizza studiando se, nel rispettivo campo di arrivo, è possibile che  $-1$  sia un quadrato.

- (i). Caso per  $\mathbb{F}_7$ .

In questo campo,  $-1 \equiv 6 \pmod{7}$ , quindi è necessario risolvere  $a^2 \equiv 6 \pmod{7}$ ,  $a \neq 0$ . Visto che  $a^6 \equiv 1 \pmod{7}$ , allora deve risultare

$$(a^2)^3 \equiv 1 \pmod{7} \implies 6^3 \equiv 1 \pmod{7}$$

Ma  $6^3 = 216 = 210 + 6 \equiv 6 \pmod{7}$ , quindi non c'è alcun omomorfismo in  $\mathbb{F}_7$  che possa soddisfare tale relazione.

- (ii). Caso per  $\mathbb{F}_{49}$ .

Questa volta, la relazione da soddisfare è  $a^{48} \equiv 1 \pmod{49}$ , ossia  $(-1)^{24} \equiv 1 \pmod{49}$ , che è verificato perché  $24 \equiv 0 \pmod{2}$ . Ora, visto che  $-1$  è un quadrato in  $\mathbb{F}_{49}$ , ci saranno due elementi di  $\mathbb{F}_{49}$  che soddisfano  $t^2 = -1$ , quindi ci sono due scelte per  $\varphi(y)$ . Al contempo, ci sono 49 possibili scelte per  $\varphi(x)$ , per un totale di 98 omomorfismi.

Per il punto (b), invece, contare gli ideali di  $A$  che contengono  $(7, x^2 + 1)$  è equivalente a contare gli ideali di  $A/(7, x^2 + 1)$ . Allora:

$$A/(7, x^2 + 1) \cong \frac{\mathbb{Z}[x, y]/(y^2 + 1)}{(7, x^2 + 1)}$$

Usando il secondo teorema di omomorfismo, si ha  $A/J \cong \frac{A/I}{J/I}$ , quindi:

$$\frac{\mathbb{Z}[x, y]/(y^2 + 1)}{(7, x^2 + 1)} \cong \frac{\mathbb{Z}[x, y]/(y^2 + 1)}{(7, x^2 + 1, y^2 + 1)/(y^2 + 1)} \cong \mathbb{Z}[x, y]/(7, x^2 + 1, y^2 + 1) \cong \frac{\mathbb{F}_7[x, y]}{(x^2 + 1, y^2 + 1)}$$

Ora, usando il fatto che  $x^2 + 1$  è irriducibile in  $\mathbb{F}_7[x]$  e che, detta  $\alpha$  una sua radice, si ha  $\mathbb{F}_7[x]/(x^2 + 1) \cong \mathbb{F}_7[\alpha] \cong \mathbb{F}_{49}$

$$\frac{\mathbb{F}_7[x, y]}{(x^2 + 1, y^2 + 1)} \cong \frac{(\mathbb{F}_7[x]/(x^2 + 1))[y]}{(y^2 + 1)} \cong \frac{\mathbb{F}_{49}[y]}{(y^2 + 1)}$$

In  $\mathbb{F}_{49}[y]$ , il polinomio  $y^2 + 1 = (y - \alpha)(y + \alpha)$ , con  $(y + \alpha) - (y - \alpha) = 2\alpha \in \mathbb{F}_{49}^\times$ , quindi  $\langle y - \alpha \rangle + \langle y + \alpha \rangle = \mathbb{F}_{49}[y]$  e si può applicare il teorema cinese del resto:

$$\frac{\mathbb{F}_{49}[y]}{(y^2 + 1)} \cong \frac{\mathbb{F}_{49}[y]}{(y + \alpha)} \times \frac{\mathbb{F}_{49}[y]}{(y - \alpha)} \cong \mathbb{F}_{49} \times \mathbb{F}_{49}$$

I suoi ideali, allora, sono dati da  $\{0\} \times \{0\}$ ,  $\{0\} \times \mathbb{F}_{49}$ ,  $\mathbb{F}_{49} \times \{0\}$  e  $\mathbb{F}_{49} \times \mathbb{F}_{49}$ , pertanto ci sono 4 ideali in  $\mathbb{Z}[x, y]/(y^2 + 1)$  che contengono  $(7, x^2 + 1)$ . ■

**Esercizio 4.5.** Sia  $A = \mathbb{Z}[i]$  e siano  $I = (x - 2 - i)$ ,  $J = (x - 2 + i)$  due ideali di  $A[x]$ .

- (a). Dimostrare che  $I \cap J$  è principale.
- (b). Dimostrare che esiste un unico ideale massimale  $M$  in  $A[x]$  che contiene  $I + J$ .
- (c). Dimostrare che  $I + J$  non è principale.

*Svolgimento.* Per il punto (a), visto che i polinomi  $x - 2 - i$  e  $x - 2 + i$  hanno radici distinte e si è in un UFD, un elemento  $f \in I \cap J$  deve essere diviso sia da  $x - 2 - i$ , che da  $x - 2 + i$ , quindi deve essere diviso dal prodotto. Se ne conclude immediatamente



che ogni elemento di  $I \cap J$  è diviso da  $(x - 2 - i)(x - 2 + 1)$  perché un elemento di  $A[x]$  diviso sia da  $x - 2 + i$  che da  $x - 2 - i$ , per quanto appena detto, deve essere diviso dal prodotto. Quindi  $I \cap J = ((x - 2 + i)(x - 2 - i)) = (x^2 - 4x + 5)$ .

Per il punto (b)

