

# **Appunti Algebra 1**

APPUNTI DEL CORSO DI ALGEBRA 1 TENUTO  
DALLA PROF. DEL CORSO E DAL PROF. LOMBARDO

DIEGO MONACO  
d.monaco2@studenti.unipi.it

Anno Accademico 2022-23

## Indice

<b>1</b>	<b>Gruppi</b>	<b>4</b>
1.1	Automorfismi	4
1.2	Automorfismi interni	4
1.3	Azione di un gruppo su un insieme	9
1.4	Azione di coniugio	13
1.5	Applicazioni ai $p$ -gruppi	14
1.6	Teorema di Cauchy	15
1.7	Azione di coniugio su un sottogruppo	16
1.8	Teorema di Cayley	17
1.9	Permutazioni	20
1.10	Classi di coniugio in $S_n$	26
1.11	Prodotto diretto	28
1.12	Prodotto semidiretto	30
1.13	Teorema di struttura per i gruppi abeliani finiti	36
1.14	Teorema di Sylow	43
1.15	Gruppo dei Quaternioni	51
<b>2</b>	<b>Anelli</b>	<b>57</b>
2.1	Riepilogo sugli anelli	57
2.2	Operazioni tra ideali	61
2.3	Anelli quoziente e omomorfismi di anelli	65
2.4	Prodotto diretto di anelli	69
2.5	Ideali primi e massimali	71
2.6	Anello delle frazioni di un dominio	75
2.7	Divisibilità nei domini	81
2.8	Domini euclidei (ED)	84
2.9	Domini a ideali principali (PID)	88
2.10	Domini a fattorizzazione unica (UFD)	89
2.11	Terne pitagoriche	99
<b>3</b>	<b>Campi</b>	<b>102</b>
3.1	Riepilogo sulle estensioni di campi	102
3.2	Chiusura algebrica di un campo	109
3.3	Estensioni normali	114
3.4	Gruppo di Galois	120
3.5	Gruppo di Galois di $\mathbb{F}_{q^d}/\mathbb{F}_q$	124
3.6	Teorema dell'elemento primitivo	128
3.7	Teorema di corrispondenza di Galois	130

## Ringraziamenti

**Davide Ranieri**, Federico Allegri, Pietro Crovetto, **Francesco Sorce**, Leonardo Migliorini, Matteo Gori, Daniele Lapadula, Alessandro Fenu, **Leonardo Alfani**, Clementina Salamina, Giorgia Capecchi, Gianni Bellu, Carlo Rotolo, Lorenzo Picinelli, Alessandro Moretti, Lorenzo Bonetti, Vittorio Monti.

Quest'opera è stata rilasciata con licenza Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale. Per leggere una copia della licenza visita il sito web <https://creativecommons.org/licenses/by-nc/4.0/deed.it>.



## §1 Gruppi

### §1.1 Automorfismi

Dato un gruppo  $G$  possiamo definire l'insieme degli automorfismi di  $G$  come segue:

$$\text{Aut}(G) = \{\varphi : G \longrightarrow G \mid \varphi \text{ isomorfismo}\}$$

si verifica facilmente che  $(\text{Aut}(G), \circ)$  è un gruppo, e in particolare  $\text{Aut}(G) \leq S(G)$ , ovvero il gruppo delle permutazioni di  $G$ . Si osserva che  $id \in \text{Aut}(G)$ ,  $\varphi \in \text{Aut}(G) \implies \varphi^{-1} \in \text{Aut}(G)$  e  $\varphi, \psi \in \text{Aut}(G) \implies \varphi \circ \psi \in \text{Aut}(G)$ .

#### Esempio 1.1 (Esempi di automorfismi)

Esempi di insiemi di automorfismi:

- $\text{Aut}(\mathbb{Z}) = \{\pm id\}$ .
- $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$ .
- $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$ .
- $\text{Aut}(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{n \text{ volte}}) \cong GL_n(\mathbb{F}_p)$

### §1.2 Automorfismi interni

**Definizione 1.2.** Dato un gruppo  $G$  possiamo definire l'omomorfismo di **coniugio**:

$$\varphi_g : G \longrightarrow G : x \longmapsto gxg^{-1}$$

dove l'elemento  $gxg^{-1}$  si dice **coniugato** di  $g$ .

#### Proposizione 1.3

Valgono i seguenti fatti:

- (1)  $\varphi_g \in \text{Aut}(G)$ ,  $\forall g \in G$ .
- (2)  $\{\varphi_g \mid g \in G\} = \text{Inn}(G) \trianglelefteq \text{Aut}(G)$ .<sup>a</sup>

<sup>a</sup> $\text{Inn}(G)$  si definisce **gruppo degli automorfismi interni**.

*Dimostrazione.* Proviamo le due affermazioni:

- (1) Per verificare che  $\varphi_g$  è un automorfismo bisogna verificare che  $\varphi_g$  è ben definita, ma ciò segue dalla chiusura di  $G$  per l'operazione. Verifichiamo che sia un omomorfismo:

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y) \quad \forall x, y \in G$$

ci resta da verificare che sia una bigezione. Partiamo dalla surgettività, vogliamo verificare che  $\forall y \in G, \exists x \in G$  :

$$\varphi_g(x) = y$$

in tal caso basta prendere  $x = g^{-1}yg \in G$ . Per l'iniettività si osserva:

$$\ker \varphi_g = \{x \in G \mid \varphi_g(x) = e\} = \{x \in G \mid gxg^{-1} = e \iff x = e\} = \{e\}$$

pertanto  $\varphi_g$  è iniettivo.

- (2) Verifichiamo che  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ ; mostriamo prima che  $\text{Inn}(G)$  è un sottogruppo di  $\text{Aut}(G)$ , infatti:  $id = \varphi_e \in \text{Inn}(G)$ ,  $\forall g_1, g_2 \in G$  vale che  $\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2} \in \text{Inn}(G)$ , infatti:

$$\varphi_{g_1} \circ \varphi_{g_2}(x) = \varphi_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = \varphi_{g_1 g_2}(x)$$

infine,  $(\varphi_g)^{-1} = \varphi_{g^{-1}} \in \text{Inn}(G)$ :

$$(\varphi_g)^{-1} \circ \varphi_g(x) = (\varphi_g)^{-1}(g x g^{-1}) = x \iff (\varphi_g)^{-1} = \varphi_{g^{-1}}$$

e analogamente per l'inversa a destra. Per verificare la normalità bisogna mostrare che:

$$f \circ \text{Inn}(G) \circ f^{-1} \subseteq \text{Inn}(G) \quad \forall f \in \text{Aut}(G)$$

ovvero:

$$f \circ \varphi_g \circ f^{-1} \in \text{Inn}(G) \quad \forall f \in \text{Aut}(G), \forall \varphi_g \in \text{Inn}(G)$$

si osserva che  $f \circ \varphi_g \circ f^{-1} = \varphi_{f(g)} \in \text{Inn}(G)$ , infatti:

$$\begin{aligned} f \circ \varphi_g \circ f^{-1}(x) &= f(\varphi_g(f^{-1}(x))) = f(g(f^{-1}(x))g^{-1}) = \\ &= f(g)f(f^{-1}(x))f(g^{-1}) = f(g)x(f(g))^{-1} = \varphi_{f(g)}(x) \end{aligned}$$

□

**Osservazione 1.4** — Se  $G$  è abeliano, allora  $\text{Inn}(G) = \{id\}$ , infatti:

$$g x g^{-1} = g g^{-1} x = x \quad \forall x \in G, \forall g \in G$$

### Proposizione 1.5

Dato un gruppo  $G$  si ha:

$$\text{Inn}(G) \cong G/Z(G)$$

*Dimostrazione.* Per dimostrare il teorema ci basta trovare un omomorfismo surgettivo da  $G$  in  $\text{Inn}(G)$  e poi sfruttare il Primo Teorema di Omomorfismo. Sia:

$$\phi : G \longrightarrow \text{Inn}(G) : g \longmapsto \varphi_g$$

tale applicazione è chiaramente ben definita, ed è surgettiva per come abbiamo definito  $\text{Inn}(G)$ . Verifichiamo che è un omomorfismo:

$$\phi(g_1 g_2) = \varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2} = \phi(g_1) \circ \phi(g_2) \quad \forall g \in G$$

dove la penultima uguaglianza è vera per quanto visto nella dimostrazione del (2) della proposizione precedente. A questo punto, per il primo teorema di omomorfismo si ha che:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \text{Inn}(G) \\ \pi_{\ker \phi} \downarrow & \nearrow & \\ G/\ker \phi & & \end{array}$$

dunque:

$$\frac{G}{\ker \phi} \cong \text{Inn}(G)$$

non ci resta che osservare:

$$\begin{aligned} \ker \phi &= \{g \in G \mid \phi(g) = \varphi_g = id\} = \{g \in G \mid gxg^{-1} = x, \forall x \in G\} = \\ &= \{g \in G \mid gx = xg, \forall x \in G\} = Z(G) \end{aligned}$$

□

**Osservazione 1.6** — L'isomorfismo trovato è del tipo  $gZ(G) \mapsto \varphi_g$ , ricordiamo che è ben definito per il Primo Teorema di Omomorfismo.

**Osservazione 1.7** — Si ricorda che se  $G/Z(G)$  è ciclico, allora  $G$  è abeliano (e quindi  $G/Z(G)$  è banale), infatti, sia:

$$G/Z(G) = \langle gZ(G) \rangle$$

Presi  $g_1, g_2 \in G$ , si ha che  $g_1Z(G) = g^{k_1}Z(G)$  e  $g_2Z(G) = g^{k_2}Z(G)$ , da cui:

$$g^{-k_1}g_1Z(G) = Z(G) \iff g^{-k_1}g_1 \in Z(G)$$

ovvero  $\exists z_1 \in Z(G) : g_1 = g^{k_1}z_1$  e analogamente  $g_2 = g^{k_2}z_2$ , da cui:

$$g_1g_2 = g^{k_1}z_1g^{k_2}z_2 = g^{k_1}g^{k_2}z_1z_2 = g^{k_1+k_2}z_1z_2$$

e contemporaneamente:

$$g_2g_1 = g^{k_2}z_2g^{k_1}z_1 = g^{k_2}g^{k_1}z_2z_1 = g^{k_2+k_1}z_2z_1 = g^{k_1+k_2}z_1z_2$$

dove nell'ultimo passaggio si è sfruttato il fatto che  $k_1, k_2 \in \mathbb{Z}$  e  $z_1, z_2 \in Z(G)$ . Da ciò segue che  $G$  è abeliano.

**Osservazione 1.8** — Dunque  $\text{Inn}(G)$  ciclico  $\implies G/Z(G)$  ciclico  $\implies G$  abeliano da cui:

$$\text{Inn}(G) \cong G/Z(G) \cong \{e\}$$

**Osservazione 1.9** —  $N \trianglelefteq G \iff \forall \varphi_g \in \text{Inn}(G)$  si ha  $\varphi_g(N) = N$  (o anche  $\varphi_g(N) \subseteq N$ ). Equivalentemente, i sottogruppi normali di  $G$  sono i sottogruppi **invarianti** per automorfismi interni (ovvero sono tali che  $gNg^{-1} = N, \forall g \in G$ ). Se  $N \trianglelefteq G$ , si può considerare:

$$\text{Inn}(G) \longrightarrow \text{Aut}(N) : \varphi_g \longmapsto \varphi_{g|N}$$

con  $\varphi_{g|N} : N \longrightarrow N$  che è un automorfismo, infatti rimane iniettivo, la surgettività segue dal fatto che  $\varphi_g(N) = N$ , e infine, essendo  $\varphi_g$  un omomorfismo su tutti gli elementi di  $G$ , lo sarà in particolare anche su tutti gli elementi di  $N$ . Dunque

quando si ha un sottogruppo normale, ogni automorfismo interno si restringe a un automorfismo di  $N$ .

Abbiamo visto che i sottogruppi normali sono invarianti per automorfismi interni, possiamo generalizzare quest'idea e considerare i sottogruppi invarianti per automorfismi:

**Definizione 1.10.** Dato un sottogruppo  $H \leq G$ , esso si dice **caratteristico** se è invariante per automorfismi:

$$f(H) = H \quad \forall f \in \text{Aut}(G)$$

Anche in questo caso basta verificare che  $f(H) \subseteq H$ ,  $\forall f \in \text{Aut}(G)$ , perché si ha anche che:

$$f^{-1}(H) \subseteq H$$

da cui si ottiene:

$$f(f^{-1}(H)) \subseteq f(H)$$

**Osservazione 1.11** — Si osserva che se  $H$  è caratteristico in  $G$ , allora è invariante per tutti gli automorfismi di  $G$  (e quindi in particolare quelli interni), dunque se  $H$  è caratteristico in  $G$ , allora è anche normale. Il viceversa è falso.

**Osservazione 1.12** — Se  $H$  è caratteristico in  $G$  (dunque normale), si può scrivere un'applicazione:

$$\text{Aut}(G) \longrightarrow \text{Aut}(H) : f \longmapsto f|_H$$

dove  $f|_H$  è un automorfismo di  $H$ .

**Osservazione 1.13** — Si osserva che se  $H$  è l'unico sottogruppo di  $G$  di un certo ordine, allora  $H$  è caratteristico in  $G$  (segue immediatamente dal fatto che gli automorfismi preservano gli ordini degli elementi). In modo analogo, se  $H$  è caratterizzato da una proprietà invariante per automorfismo, allora è caratteristico.

**Esercizio 1.14.** Il centro di un gruppo  $Z(G)$  è un sottogruppo caratteristico.

*Soluzione.* Per dimostrare che  $Z(G)$  è caratteristico è sufficiente far vedere che:

$$f(Z(G)) \subseteq Z(G) \quad \forall f \in \text{Aut}(G)$$

ovvero:

$$f(z) \in Z(G) \quad \forall f \in \text{Aut}(G), \forall z \in Z(G)$$

dunque bisogna verificare che:

$$gf(z) = f(z)g \quad \forall g \in G$$

poiché  $f$  è un automorfismo, allora  $\exists h \in G : f(h) = g$ , dunque:

$$gf(z) = f(h)f(z) = f(hz) = f(zh) = f(z)f(h) = f(z)g \quad \forall g \in G$$

□

**Esempio 1.15**

Sia  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}$ ,  $G$  ha ordine 4 ed ha tre sottogruppi ciclici di ordine 2:

$$H_1 = \langle (\bar{1}, \bar{0}) \rangle \quad H_2 = \langle (\bar{0}, \bar{1}) \rangle \quad H_3 = \langle (\bar{1}, \bar{1}) \rangle$$

ed essendo  $G$  abeliano si ha  $H_1, H_2, H_3 \trianglelefteq G$  (e quindi i sottogruppi sono invarianti per automorfismi interni). Tuttavia nessuno dei sottogruppi è caratteristico, infatti possiamo prendere un automorfismo non banale (e quindi non uno interno) e vedere come i sottogruppi di questo tipo non siano invarianti:

$$f = \begin{cases} (\bar{1}, \bar{0}) \mapsto (\bar{1}, \bar{1}) \\ (\bar{0}, \bar{1}) \mapsto (\bar{0}, \bar{1}) \end{cases}$$

la definizione della mappa data tuttavia non è completa, perché abbiamo stabilito solo dove vengono mandati i generatori, dobbiamo definire cosa faccia un elemento generico:

$$f((\bar{a}, \bar{b})) = af((\bar{1}, \bar{0})) + bf((\bar{0}, \bar{1})) = (\bar{a}, \bar{a}) + (\bar{0}, \bar{b}) = (\bar{a}, \bar{a} + \bar{b})$$

a questo punto abbiamo definito completamente l'applicazione (rimarrebbe da verificare che  $f$  sia un omomorfismo), e si verifica facilmente che  $f(H_1) = H_3$  quindi  $H_1 \trianglelefteq G$ , ma non caratteristico.

A questo punto è facile verificare che:

$$\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

infatti, ogni automorfismo del gruppo si ottiene fissando l'elemento neutro  $(\bar{0}, \bar{0}) \mapsto (\bar{0}, \bar{0})$ , quindi il numero possibile di bigezioni è al più 3!, occorre verificare che tutte e 6 le funzioni sono omomorfismi. Dimostriamo invece che:

$$\boxed{\text{Aut}(S_3) \cong S_3}$$

Per farlo, poiché  $S_3$  non è abeliano, possiamo osservare che:

$$\text{Inn}(S_3) \cong S_3 / Z(S_3) \cong S_3$$

in quanto l'unico elemento che commuta con tutti gli altri in  $S_3$  è l'identità, quindi  $Z(S_3) = \{id\} \cong \{e\}$ . Per quanto detto si ha  $\text{Inn}(S_3) \trianglelefteq \text{Aut}(S_3)$  e quindi  $\text{Aut}(S_3)$  contiene una copia isomorfa di  $S_3$  come sottogruppo normale, pertanto, se verifichiamo che  $|\text{Aut}(S_3)| \leq 6$  abbiamo concluso. Sia  $f \in \text{Aut}(S_3)$ ,  $f$  può al più scambiare i 3 elementi di ordine 2, d'altra parte, fissate le immagini di  $\tau_1, \tau_2, \tau_3$ <sup>1</sup>, i due 3-cicli<sup>2</sup> sono completamente determinati, ciò significa che si hanno al più 3! automorfismi, dunque:

$$\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3 \implies \text{Aut}(S_3) \cong S_3$$

<sup>1</sup>Con  $\tau_i$  si intendono le trasposizioni che lasciano fisso l'elemento  $i$ .

<sup>2</sup>Come si vedrà  $S_3 = \langle \tau_1, \tau_2, \tau_3 \rangle$



### §1.3 Azione di un gruppo su un insieme

**Definizione 1.16.** Sia  $G$  un gruppo e  $X$  un insieme, un'azione di  $G$  su  $X$  è un omomorfismo:

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g$$

dove  $\varphi_g : X \longrightarrow X : x \longmapsto \varphi_g(x)$ <sup>3</sup>, con  $\varphi_g$  bigettiva,  $\forall g \in G$ . Si può definire un'azione anche come:

$$\varphi : G \times X \longrightarrow X : (g, x) \longmapsto \varphi_g(x)$$

Un'azione di  $G$  su  $X$  si indica con  $G \curvearrowright X$ .

#### Esempio 1.17

Sia  $X = G$ , quindi  $\varphi : G \longrightarrow S(G) : g \longmapsto \varphi_g$ , con  $\varphi_g$  coniugio,  $\varphi$  è un'azione. Come si è visto nell'(1) della [Proposizione 1.3](#)  $\varphi_g$  è un automorfismo di  $G$  (e quindi una bigezione), e  $\varphi$  è un omomorfismo. In questo caso si ha che:

$$\varphi_g(x) = gxg^{-1}$$

#### Esempio 1.18

Sia  $V$  un  $K$ -spazio vettoriale, sia:

$$\varphi : K^* \longrightarrow S(V) : \lambda \longmapsto \varphi_\lambda$$

con  $\varphi_\lambda : V \longrightarrow V : v \longmapsto \lambda v$ ,  $\varphi$  è un'azione di  $K^*$  su  $V$ .

Sia  $\varphi : G \longrightarrow S(X)$  un'azione,  $\varphi$  definisce una relazione di equivalenza su  $X$ :

$$x \sim y \iff \exists g \in G : \varphi_g(x) = y$$

ovvero due elementi sono in relazione se esiste un'applicazione  $\varphi_g \in S(X)$ , per cui un elemento è l'immagine dell'altro mediante tale applicazione. La relazione è appunto di equivalenza, infatti:  $x \sim x$ , per  $g = e$  si ha (essendo  $\varphi$  un omomorfismo)  $\varphi_e(x) = id(x) = x$ ,  $x \sim y \implies y \sim x$ :

$$\varphi_g(x) = y \implies x = (\varphi_g(y))^{-1} = \varphi_{g^{-1}}(y)$$

infine  $x \sim y, y \sim z \implies x \sim z$ , infatti si avrebbe:  $\varphi_g(x) = y, \varphi_h(y) = z$  da cui:

$$z = \varphi_h(\varphi_g(x)) = \varphi_{hg}(x) \implies x \sim z$$

**Definizione 1.19.** Data la relazione di equivalenza  $\sim$  si definiscono **orbite** le classi di equivalenza di  $X$  rispetto alla relazione  $\sim$ :

$$\text{Orb}(x) = \{\varphi_g(x) | g \in G\} (\subseteq X)$$

Da cui:

$$X = \bigcup_{x \in \mathcal{R}} \text{Orb}(x)$$

Con  $\mathcal{R}$  insieme di rappresentanti. Un'orbita è quindi l'insieme di tutte le immagini di un elemento in un insieme, mediante tutte le possibili applicazioni (permutazioni) dell'insieme  $\varphi(G)$ .

<sup>3</sup>Alternativamente si può indicare l'immagine con  $\varphi_g : x \longmapsto g * x$  dove il simbolo  $*$  indica l'azione di  $g$  su  $x$ .

**Definizione 1.20.** Per ogni  $x \in X$  si dice **stabilizzatore** di  $x$ :

$$\text{St}(x) = \{g \in G \mid \varphi_g(x) = x\}$$

Cioè lo stabilizzatore è l'insieme degli elementi di  $G$ , che danno origine mediante  $\varphi$  alle applicazioni  $\varphi_g \in S(X)$ , che lasciano fisso un determinato elemento.

### Esempio 1.21

Se  $X = \mathbb{R}^2$  e  $G$  è il gruppo di traslazioni di vettore  $\underline{v} = (0, l)$ , allora:

$$\varphi : G \longrightarrow S(X) : \tau_{(0,l)} \longmapsto \tau_{(0,l)}^a$$

con:

$$\text{Orb}(x, y) = \{(x, y + l) \mid l \in \mathbb{R}\} \quad \text{e} \quad \text{St}(x, y) = \{\tau_{(0,l)} \mid (x, y + l) = (x, y)\} = \{id\}$$

<sup>a</sup>Si osserva che il primo  $\tau_{(0,l)}$  è un elemento del gruppo  $G$ , mentre il secondo è un'applicazione bigettiva di  $X$ .

### Esempio 1.22

Se  $X = \mathbb{R}^2$  e  $G$  è il gruppo delle rotazioni di centro  $O$ , allora:

$$\varphi : G \longrightarrow S(\mathbb{R}^2) : r_\theta \longmapsto r_\theta$$

con:

$$\text{St}(x, y) = \begin{cases} \{id\} & \text{se } (x, y) \neq (0, 0) \\ G & \text{se } (x, y) = (0, 0) \end{cases}$$

e, detta  $\omega$  la circonferenza di centro  $O$  e raggio  $\sqrt{x^2 + y^2}$ :

$$\text{Orb}(x, y) = \{(x', y') \in \mathbb{R}^2 \mid (x', y') \in \omega\}$$

### Proposizione 1.23 ( $\text{St}(x) \leq G$ )

Dato un gruppo  $G$  e un'azione  $\varphi : G \longrightarrow S(X)$ , si ha che  $\text{St}(x) \leq G$ .<sup>a</sup>

<sup>a</sup>In generale lo stabilizzatore non è un sottogruppo normale.

*Dimostrazione.* Si osserva che  $e \in \text{St}(x)$ , in quanto  $\varphi_e(x) = id(x) = x$ , inoltre, presi  $g, h \in \text{St}(x)$ , ovvero  $\varphi_g(x) = \varphi_h(x) = x$ , allora:

$$\varphi(gh)(x) = \varphi_{gh}(x) = \varphi_g \circ \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g(x) = x \implies gh \in \text{St}(x)$$

dove si ha che  $\varphi_{gh}(x) = \varphi_g \circ \varphi_h(x)$  in quanto  $\varphi$  è un omomorfismo. Infine, preso  $g \in \text{St}(x)$ , si ha  $g^{-1} \in \text{St}(x)$ , infatti  $\varphi_g$  è bigettiva e quindi ammette inversa:

$$(\varphi_g)^{-1} \circ \varphi_g(x) = x \implies (\varphi_g)^{-1}(\varphi_g(x)) = x \implies (\varphi_g)^{-1}(x) = x$$

con  $(\varphi_g)^{-1}(x) = (\varphi(g))^{-1}(x) = (\varphi(g^{-1}))(x) = \varphi_{g^{-1}}(x)$  e per quanto detto:

$$\varphi_{g^{-1}}(x) = x \implies g^{-1} \in \text{St}(x)$$

□

**Osservazione 1.24** ( $\text{Orb}(x) \longleftrightarrow [G : \text{St}(x)]$ ) — Sia  $x \in X$  e  $g, h \in G$ , allora:

$$\varphi_g(x) = \varphi_h(x) \iff \varphi_{h^{-1}g}(x) = x$$

e per le proprietà di omomorfismo dell'azione  $\varphi$ , si ha:

$$\varphi_{h^{-1}g}(x) = x \iff \varphi_{h^{-1}g}(x) = x \iff h^{-1}g \in \text{St}(x)$$

ovvero  $g \text{St}(x) = h \text{St}(x)$ , in quanto  $\text{St}(x) \leq G$  e la condizione ottenuta è esattamente quella dell'equivalenza modulo  $\text{St}(x)$ , quindi:

$$\text{Orb}(x) \longleftrightarrow \text{classi laterali di } \text{St}(x) \text{ in } G = [G : \text{St}(x)]$$

cioè due elementi danno la stessa immagine (di un fissato elemento  $x \in X$ ) se e solo se stanno nella stessa classe laterale modulo  $\text{St}(x)$ , e la corrispondenza biunivoca tra orbita e classi laterali è data da:

$$g \text{St}(x) \mapsto \varphi_g(x) \quad \text{e} \quad h \text{St}(x) \mapsto \varphi_h(x)$$

che è ben definita e per quanto detto all'inizio è iniettiva:

$$\varphi_g(x) = \varphi_h(x) \iff g \text{St}(x) = h \text{St}(x)$$

(quindi due elementi di un'orbita sono uguali se e solo se lo sono le classi laterali dei rispettivi elementi che generano le applicazioni sono uguali modulo  $\text{St}(x)$ , dunque per ogni elemento dell'orbita c'è una e una sola classe laterale modulo  $\text{St}(x)$ ) e surgettiva:

$$\forall y \in \text{Orb}(x), y = \varphi_g(x) \implies g \text{St}(x) \mapsto y$$

e quindi concludiamo che il numero di classi laterali di  $\text{St}(x)$  in  $G$  è lo stesso della cardinalità di  $\text{Orb}(x)$ .

Per quanto detto si ha:

$$|G| = |\text{St}(x)|[G : \text{St}(x)]$$

ma  $[G : \text{St}(x)]$  è il numero di classi laterali di  $\text{St}(x)$  in  $G$ , che è proprio uguale a  $|\text{Orb}(x)|$  pertanto vale la seguente:

**Proposizione 1.25** (Lemma orbita-stabilizzatore)

Sia  $G$  un gruppo finito e  $X$  un insieme, allora:

$$|G| = |\text{Orb}(x)| |\text{St}(x)| \quad \forall x \in X$$

**Osservazione 1.26** — Si osserva che essendo  $\text{St}(x) \leq G$ , allora è ovvio (per Lagrange) che  $|\text{St}(x)| \mid |G|$ , tuttavia, per la proposizione precedente, si ha che:  $|\text{Orb}(x)| \mid |G|$  con  $\text{Orb}(x) \subseteq X$ .

Ricordando che:

$$X = \bigcup_{x \in \mathcal{R}} \text{Orb}(x)$$

se  $|X| < +\infty$  si ha:

$$|X| = \sum_{x \in \mathcal{R}} |\text{Orb}(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|\text{St}(x)|}$$

## §1.4 Azione di coniugio

**Definizione 1.27.** Si parla di **azione di coniugio**, quando si ha un'azione di  $G$  su  $G$  stesso:

$$\varphi : G \longrightarrow \text{Inn}(G) (\trianglelefteq \text{Aut}(G)) : g \longrightarrow \varphi_g$$

Abbiamo già osservato che è un'azione (ovvero che  $\varphi$  è un omomorfismo). In questo caso:

$$\text{Orb}(x) = \{\varphi_g(x) | g \in G\} = \{gxg^{-1} | g \in G\} = \mathcal{C}\ell_G(x)$$

dove  $\mathcal{C}\ell_G(x)$  prende il nome di **classe di coniugio** di  $x$ <sup>4</sup>. Mentre:

$$\text{St}(x) = \{g \in G | \varphi_g(x) = gxg^{-1} = x\} = \{g \in G | gx = xg\} = Z_G(x)$$

dove  $Z_G(x)$  si dice **centralizzatore** di  $x$ . Per quanto detto in precedenza si ha:

$$|G| = |\mathcal{C}\ell_G(x)| |Z_G(x)|$$

In particolare  $|\mathcal{C}\ell_G(x)| \mid |G|$  e :

$$|G| = \sum_{x \in \mathcal{R}} |\mathcal{C}\ell_G(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|Z_G(x)|}$$

**Osservazione 1.28** —  $\mathcal{C}\ell_G(x)$  è un sottoinsieme, non un sottogruppo di  $G$ , poiché non c'è mai l'identità.

**Osservazione 1.29** — Osserviamo che  $Z_G(x) = G \iff x \in Z(G)$ , infatti per un elemento del centro si ha che  $\forall g \in G$  l'elemento commuta, e dunque il suo centralizzatore è tutto il gruppo.

**Osservazione 1.30** — Per un'azione di coniugio si ha che  $x \in Z(G)$  se e solo se  $\text{Orb}(x) = \{x\}$  e  $\text{St}(x) = G$  (ovvero  $\varphi_g(x) = x, \forall g \in G$ ).

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

ma, per quanto detto, se  $x \in Z(G)$ , allora  $\frac{|G|}{|Z_G(x)|} = |\mathcal{C}\ell_G(x)| = \{x\}$ , segue dunque la relazione:

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

che prende il nome di **formula delle classi** (di coniugio).

<sup>4</sup>Si può indicare anche con  $C_x$ .

## §1.5 Applicazioni ai $p$ -gruppi

**Definizione 1.31.** Si definisce  **$p$ -gruppo** un gruppo di ordine  $p^n$ , con  $p$  primo e  $n \geq 1$ .

Se  $G$  è un  $p$ -gruppo la formula delle classi diventa:

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

con  $|Z(G)| = p^z$ ,  $0 \leq z \leq n$ , facciamo due osservazioni fondamentali:

- (1) Il centro di un  $p$ -gruppo non è mai banale, infatti, se osserviamo la formula delle classi, si ha:

$$p^n = |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \implies |Z(G)| + \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \equiv 0 \pmod{p}$$

con  $\frac{|G|}{|Z_G(x)|} > 1$ , poiché  $Z_G(x) = G$  se e solo se  $x \in Z(G)$ , viceversa deve essere che  $\frac{|G|}{|Z_G(x)|} = p^{k_x}$ ,  $k > 0$ , poiché  $G$  è un  $p$ -gruppo (e quindi anche  $Z_G(x)$ ), dunque:

$$|Z(G)| \equiv 0 \pmod{p} \implies |Z(G)| \geq 2$$

e quindi il centro di un  $p$ -gruppo non è mai banale.

- (2) Un gruppo di ordine  $p^2$  è abeliano, infatti, si ha:

$$|G| = p^2 \implies |Z(G)| = \begin{cases} 1 & \text{non può accadere per (1)} \\ p & \text{no perché allora } G/Z(G) \text{ ciclico, ma } G \text{ non è abeliano} \\ p^2 & \end{cases}$$

dunque l'unica possibilità è che  $Z(G) = G \iff G$  abeliano.

## §1.6 Teorema di Cauchy

### Teorema 1.32 (Teorema di Cauchy)

Dato un gruppo  $G$  e un primo  $p$ , se  $p \mid |G|$ , allora  $\exists x \in G : \text{ord}_G(x) = p$ .<sup>a</sup>

<sup>a</sup>Si considera già noto il teorema per gruppi abeliani.

*Dimostrazione.* Sia  $|G| = pn$ , procediamo per induzione su  $n$ , nel caso  $n = 1$  il teorema è ovvio. Supponiamo vera la tesi per i gruppi di ordine  $pm$ , con  $1 \leq m < n$  e proviamola per  $n$ . Distinguiamo due casi:

- Se esiste  $H \leq G$  con  $p \mid |H|$ , ovvero  $|H| = pm \implies$  vale il teorema di Cauchy per ipotesi induttiva (essendo  $m < n$ ), quindi  $\exists x \in H : \text{ord}_H(x) = p$ , ma essendo  $H \subset G \implies x \in G$  e quindi la tesi è vera.
- Se  $\forall H \leq G$  si ha  $p \nmid |H|$ , allora si può applicare a  $G$  la formula delle classi rispetto all'azione di coniugio:

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

ricordando che il centralizzatore di  $x$  è uno stabilizzatore (e quindi un sottogruppo di  $G$ ), si ha  $p \nmid |Z_G(x)|$ , e quindi:

$$p \mid \sum_{x \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$$

da cui segue che  $p \mid |Z(G)| = \underbrace{|G|}_{=pn} - \sum pl_x$ <sup>5</sup>, per quanto premesso ( $\forall H \leq G$  si ha  $p \nmid |H|$ ), ed essendo  $Z(G) \leq G$ , l'unica possibilità è che  $Z(G) = G$  e vale il teorema poiché è già stato dimostrato per il caso in cui  $G$  è abeliano.

□

<sup>5</sup>Con  $pl_x$  indichiamo le varie cardinalità del rapporto tra  $|G|$  e  $|Z_G(x)|$  al variare di  $x$ .

### §1.7 Azione di coniugio su un sottogruppo

Sia  $X = \{H \leq G\}$  e  $\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g(X)$ , con  $\varphi_g : X \longrightarrow X : H \longmapsto gHg^{-1} = \{ghg^{-1} | h \in H\}$ . Si verifica facilmente che  $\varphi$  è un omomorfismo; mostriamo invece che  $\varphi_g$  è una permutazione (cioè bigettiva), per l'iniettività si osserva che:

$$\varphi_g(H) = \varphi_g(K) \iff gHg^{-1} = gKg^{-1} \iff H = K$$

mentre per la surgettività si ha che  $\forall H \in X, \exists L \in X$ :

$$\varphi_g(L) = H \iff gLg^{-1} = H \iff L = g^{-1}Hg$$

inoltre si ha anche:

$$\text{Orb}(H) = \{\varphi_g(H) | g \in G\} = \{gHg^{-1} | g \in G\} \quad \text{St}(H) = \{g \in G | \varphi_g(H) = H\} = N_G(H)$$

dove  $\text{Orb}(H)$  è l'insieme dei coniugati di  $H$ , mentre  $\text{St}(H) = N_G(H)$  prende il nome di **normalizzatore** di  $H$ .

**Osservazione 1.33** — Si osserva che  $H \trianglelefteq G$  se e solo se  $\text{Orb}(H) = \{H\} \iff N_G(H) = G$ , ovvero se  $H$  è sempre chiuso per coniugio in  $G$ .

Per quanto affermato nella [Proposizione 1.25](#) si ha:

$$|G| = |\text{Orb}(H)| |N_G(H)| \implies |\text{Orb}(H)| = \frac{|G|}{|N_G(H)|}$$

**Osservazione 1.34** — Quindi in generale, dato  $H \leq G$  si ha che  $\#\{gHg^{-1}\} = [G : H]$  e  $\#\{gHg^{-1}\} = [G : N_G(H)]$ .

**Osservazione 1.35** (Sulla definizione di sottogruppo normale) — I sottogruppi normali possono essere ridefiniti nella maniera seguente,  $H \trianglelefteq G$  se e solo se:

$$H = \bigcup_{h \in H} \mathcal{C}\ell_h$$

cioè un sottogruppo è normale se e solo se è l'unione delle classi di coniugio dei suoi elementi. Infatti:

$$H \trianglelefteq G \iff ghg^{-1} \in H \quad \forall h \in H, \forall g \in G$$

che equivale a:

$$\mathcal{C}\ell_h = \{ghg^{-1} | h \in H\} \subseteq H \quad \forall h \in H \implies \bigcup_{h \in H} \mathcal{C}\ell_h \subseteq H$$

d'altra parte se  $H$  è normale è chiuso per coniugio, ovvero il coniugio di ogni suo elemento è ancora in  $H$  ( $ghg^{-1} = h', \forall h \in H$ ) e in particolare ciò significa che:

$$H \subseteq \bigcup_{h \in H} \mathcal{C}\ell_h$$



## §1.8 Teorema di Cayley

### Teorema 1.36 (Teorema di Cayley)

Ogni gruppo è isomorfo ad un sottogruppo di un gruppo di permutazioni. In particolare, se  $|G| = n$ , allora  $G$  è isomorfo a un sottogruppo di  $S_n$ .

*Dimostrazione.* Definiamo la mappa:

$$\lambda : G \hookrightarrow S(G) : g \mapsto \varphi_g$$

con  $\varphi_g : G \rightarrow G : x \mapsto gx$ , l'applicazione  $\lambda$  prende il nome di **rappresentazione regolare a sinistra** di  $G$ , si vuole dimostrare che  $\lambda$  è un omomorfismo iniettivo. Osserviamo innanzitutto che  $\lambda$  è ben definita, cioè  $\varphi_g \in S(G)$ , infatti  $\varphi_g$  è iniettiva (segue dalle leggi di cancellazione) e surgettiva, perché  $\forall y \in G, \exists g^{-1}y \in G : \varphi_g(g^{-1}y) = y$ . Verifichiamo che  $\lambda$  è un omomorfismo:

$$\lambda(g_1g_2) = \varphi_{g_1g_2}$$

con  $\varphi_{g_1g_2}(x) = \varphi_{g_1} \circ \varphi_{g_2}(x)$ ,  $\forall x \in G$ , e quindi:

$$\lambda(g_1g_2) = \lambda(g_1)\lambda(g_2) \quad \forall g_1, g_2 \in G$$

infine, per l'injectività si ha che:

$$\ker \lambda = \{g \in G \mid \lambda(g) = \varphi_g = id = \varphi_e\} = \{e\}$$

da ciò segue che  $G \cong \lambda(G) \leq S(G)$ , e se  $|G| = n$  si ha che  $\text{Im}(\lambda) \leq S_n$ .  $\square$

**Osservazione 1.37** — In generale, dato  $G = \{g_1 = e, g_2, \dots, g_n\}$  e  $\lambda : G \hookrightarrow S(G) \cong S_n$ , si ha che:

$$g_1 = e \mapsto \lambda_{g_1} \quad \text{con} \quad \lambda_{g_1} : G \rightarrow G : g_i \mapsto g_i$$

$$g_2 \mapsto \lambda_{g_2} \quad \text{con} \quad \lambda_{g_2} : G \rightarrow G : x \mapsto g_2x \mapsto g_2^2x \mapsto \dots \mapsto g_2^{k-1}x$$

con  $k = \text{ord}_G(g_2)$ .  $\lambda_{g_2}$  può essere rappresentata mediante la notazione dei cicli:

$$(x, g_2x, \dots, g_2^{k-1}x)$$

preso poi  $y \notin \lambda_{g_2}(G)$ , si ha analogamente:

$$(y, g_2y, \dots, g_2^{k-1}y)$$

### Esempio 1.38

Nel caso in cui  $G = \mathbb{Z}/8\mathbb{Z}$  consideriamo l'azione:

$$\lambda : G \longrightarrow S(\mathbb{Z}/8\mathbb{Z}) \cong S_8^a : \bar{a} \longmapsto \lambda_a$$

che, per quanto visto genera ad esempio le applicazioni:<sup>b</sup>

$$\begin{aligned} 1 &\longmapsto \lambda_1 : X \longrightarrow X : a \longmapsto 1 + a \implies (0, 1, \dots, 7) \\ 2 &\longmapsto \lambda_2 : X \longrightarrow X : a \longmapsto 2 + a \implies (0, 2, 4, 6)(1, 3, 5, 7) \\ 4 &\longmapsto \lambda_4 : X \longrightarrow X : a \longmapsto 4 + a \implies (0, 4)(1, 5)(2, 6)(3, 7) \end{aligned}$$

che permutano gli elementi di  $X$  secondo i cicli trovati.

<sup>a</sup>Perché appunto  $S(\mathbb{Z}/8\mathbb{Z})$  è l'insieme di permutazioni di un insieme di 8 elementi.

<sup>b</sup>Per  $+$  si intende la somma modulo 8.

**Definizione 1.39.** Un'azione  $\lambda$  si dice **fedele** se è iniettiva.

Ad esempio l'azione di rappresentazione regolare a sinistra è fedele:

$$\ker \lambda = \{g \in G | \lambda(g) = id\} = \{g \in G | \lambda_g(e) = e\} = \{g \in G | ge = e\} = \{e\}$$

infatti  $\lambda(e) = \lambda_e = id$  e inoltre

$$\lambda(g) = \lambda_g = id \implies \lambda_g(e) = e \implies ge = e \implies g = e$$

da cui  $\lambda$  fedele.

**Osservazione 1.40** — Esiste anche un'applicazione  $\rho : G \longrightarrow S(G) (\cong S_n)$ , ( $n = |G|$ ), detta azione di **rappresentazione regolare a destra**, con:

$$g \longmapsto \rho_g : x \longmapsto xg^{-1}$$

### Lemma 1.41 (Lemma di Ranieri)

Sia  $G$  un gruppo abeliano di ordine  $n$ , allora  $\forall d \mid n, \exists H \leq G : |H| = d$ .<sup>ab</sup>

<sup>a</sup>Il nome ovviamente non è ufficiale, ma deriva da un curioso aneddoto in cui è coinvolto il buon Davide Ranieri, pertanto vi consiglio di citarlo con questo nome in contesti ufficiali, ma se volete farlo comunque è a vostro rischio e pericolo :)

<sup>b</sup>La dimostrazione non è stata fatta durante il corso, ma è stata comunque aggiunta per completezza.

*Dimostrazione.* Si consideri innanzitutto il caso  $d = p^k$ ,  $p$  primo, e mostriamolo per induzione: per  $k = 1$  la tesi è equivalente al **Teorema di Cauchy** (anche solo per i gruppi abeliani). Supponiamo la tesi per  $k - 1$ . Poiché in particolare  $p \mid |G|$  scegliamo un sottogruppo  $H$  di  $G$  di ordine  $p$ ; tale sottogruppo è normale poiché  $G$  è abeliano.  $p^{k-1} \mid |G/H| \implies$  per ipotesi induttiva  $\exists K \leq G/H : |K| = p^{k-1}$ .

Prendendo la controimmagine di  $K$  tramite la proiezione al quoziente troviamo il sottogruppo di  $G$  cercato.

A questo punto possiamo scrivere in generale  $d = p_1^{k_1} \dots p_s^{k_s}$ ; per ogni  $i$  troviamo sottogruppi  $H_i$  di ordini  $p_i^{k_i}$  (tutti normali), poiché considerando il generato dagli elementi di ordine potenza di  $p_i$ : questo è un  $p_i$ -gruppo ed è normale per abelianità, se non avesse

ordine  $p_i^{k_i}$  allora quozientando  $G$  per questo avremmo per Cauchy un elemento di ordine  $p_i$  e considerando la controimmagine della proiezione avremmo perso un elemento di ordine potenza di  $p_i$  (dato che avevamo quozientato per un  $p_i$ -gruppo). Si ha quindi che  $H_1 H_2 \leq G$  per normalità, inoltre  $|H_1 \cap H_2| = 1$  poiché l'ordine di un elemento in tale intersezione deve dividere  $(p_1^{k_1}, p_2^{k_2}) = 1$ . Pertanto  $|H_1 H_2| = p_1^{k_1} p_2^{k_2}$ . Ragionando per induzione otteniamo che il sottogruppo  $H_1 \dots H_k$  ha ordine  $d$  come voluto.  $\square$

**Esercizio 1.42.** Sia  $G$  un gruppo, se  $|G| = p^n$ , allora esiste:

$$\{e\} = H_n < H_{n-1} < \dots < H_1 < G$$

con  $H_i \leq G$  e  $|H_i| = p^{n-i}$ ,  $\forall i \in \{1, \dots, n\}$ .

*Soluzione.* Procediamo per induzione su  $n$ , per  $n = 1$  è ovvio, infatti si ha  $H_1 = \{e\} \leq G$ . Supponiamo la tesi vera  $\forall 1 \leq k \leq n - 1$ , osserviamo che  $G$  è un  $p$ -gruppo, pertanto il suo centro non è banale:

$$|Z(G)| = p^z \quad z \geq 1$$

sia  $\mathcal{G} = G/Z(G)$ , essendo  $|G/Z(G)| < p^n$  (perché deve essere  $|Z(G)| \geq p$ ), allora vale l'ipotesi induttiva, dunque  $|\mathcal{G}| = p^m$ , con  $m = n - z (< n)$ , allora esiste:

$$\mathcal{H}_m = \{e_{\mathcal{G}}\} < \mathcal{H}_{m-1} < \dots < \mathcal{H}_1 < \mathcal{G}$$

con  $|\mathcal{H}_i| = p^{m-i}$  e  $\mathcal{H}_i \leq \mathcal{G}$ . Data la proiezione al quoziente:

$$\pi_{Z(G)} : G \longrightarrow \mathcal{G}$$

per il Teorema di Corrispondenza dei sottogruppi, esiste una bigezione tra i sottogruppi di  $G/Z(G)$  e i sottogruppi di  $G$  che contengono  $Z(G)$ , la quale preserva normalità e indice del sottogruppo, pertanto preso  $\mathcal{H}_i \leq G/Z(G)$  è sufficiente applicare  $\pi_{Z(G)}^{-1}$  alla catena scritta sopra e troviamo:

$$Z(G) = \pi_{Z(G)}^{-1}(\mathcal{H}_m) < \dots < \pi_{Z(G)}^{-1}(\mathcal{H}_1) < \pi_{Z(G)}^{-1}(\mathcal{G}) (= G)$$

Segue per il teorema di corrispondenza che  $\pi_{Z(G)}^{-1}(\mathcal{H}_i) = H_i \leq G$ , ovvero si preserva la normalità dei sottogruppi, inoltre, segue sempre dal teorema che:

$$p^i = [\mathcal{G} : \mathcal{H}_i] = [G : H_i]$$

dunque la catena esiste e  $|H_i| = p^{n-i}$  per  $1 \leq i \leq m$ . Essendo  $Z(G)$  abeliano, i sottogruppi di ogni suo ordine (che esistono sempre per il [Lemma Di Ranieri](#)) sono normali in  $Z(G)$ , inoltre  $|Z(G)| = p^z$  (dunque si hanno sottogruppi normali di ordine  $p^l$  per  $l \geq z$ ), pertanto esiste la catena:

$$\{e\} = H_n < \dots < H_m = Z(G) \quad \text{con } |H_j| = p^{n-j}, \forall m \leq j \leq n$$

Bisogna infine verificare che  $H_j \leq G$ , dunque:

$$gH_jg^{-1} = H_j \quad \forall g \in G$$

ma  $H_j \subset Z(G)$  (quindi è invariante per coniugio rispetto a ogni  $g \in G$ ) dunque è sempre verificata l'ultima uguaglianza.  $\square$

## §1.9 Permutazioni

Ricordiamo brevemente che:

**Definizione 1.43.** Dato un insieme  $X$  si definisce **permutazione** un'applicazione bigettiva di  $X$  in se stesso.

Indichiamo con  $S(X)$  il gruppo delle permutazioni di  $X$  e con  $S_n$  il gruppo delle permutazioni di un insieme di cardinalità  $n$ , che per semplicità indichiamo con  $\{1, \dots, n\}$ . Le permutazioni si possono indicare in vari modi, ad esempio, preso  $\sigma \in S_{12}$  si può rappresentare mediante la matrice di permutazione:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 2 & 4 & 5 & 1 & 9 & 8 & 7 & 6 & 12 & 11 & 10 \end{pmatrix}$$

o anche con la notazione dei cicli:

$$\sigma = (1\ 3\ 4\ 5)(6\ 9)(7\ 8)(10\ 12)$$

ogni ciclo prende il nome di  **$k$ -ciclo** (dove  $k$  indica la sua lunghezza), come si osserva i cicli di lunghezza 1 sono stati omessi, in quanto lasciano fissi gli elementi, inoltre, i 2-cicli prendono il nome di **trasposizioni**.

Formalmente, sia  $\sigma \in S_n$  una permutazione di un insieme di  $n$  elementi, per descrivere tale permutazione possiamo considerare l'insieme  $X$ , con  $|X| = n$ , il gruppo  $G = \langle \sigma \rangle$  e definire l'azione:

$$\varphi : G = \langle \sigma \rangle \hookrightarrow S(X) \cong S_n : \sigma \mapsto \sigma$$

con  $\sigma \in S_n$  e  $\sigma : i \mapsto \sigma(i)$ , dunque abbiamo definito l'azione  $\langle \sigma \rangle \curvearrowright X$  data dall'inclusione, la quale ci permetterà di descrivere come  $\sigma$  agisce sull'insieme  $\{1, \dots, n\}$ . Osserviamo che:

$$\text{Orb}(x) = \{\sigma(x) | \sigma \in \langle \sigma \rangle\} = \{\sigma^l(x) | l \in \mathbb{N}\} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{m_x-1}(x)\}$$

con  $|\text{Orb}(x)| = m_x$ , con  $m_x = \min\{k > 0 | \sigma^k(x) = x\}$ , perché se  $\sigma^k(x) = x$ , allora  $\sigma^{k+1}(x) = \sigma(x)$ , pertanto, sia  $k \in \mathbb{N}$  tale che  $\sigma^k(x) \in \{x, \dots, \sigma^{k-1}(x)\}$ , allora  $\exists h$ :

$$\sigma^k(x) = \sigma^h(x) \quad \text{con } 0 \leq h \leq k-1$$

Dunque vale che  $\sigma^{k-h}(x) = x \in \{x, \dots, \sigma^{k-1}(x)\}$  e per la minimalità di  $k$  si ha che  $h = 0$ . L'azione di  $\langle \sigma \rangle$  su  $X$  divide  $X$  in orbite e su ogni orbita  $\sigma$  agisce ciclicamente (ovvero  $\sigma(\text{Orb}(x)) = \text{Orb}(x)$ ).

**Definizione 1.44.** Si dice **ciclo** di  $\sigma \in S_n$  l'orbita di un elemento  $x \in \{1, \dots, n\}$  vista come insieme ordinato:

$$(x, \sigma(x), \dots, \sigma^{m_x-1}(x))$$

**Osservazione 1.45** — Un ciclo di lunghezza  $k$  (un  $k$ -ciclo) ha  $k$  scritte distinte, in quanto possiamo scegliere arbitrariamente il primo elemento.

**Osservazione 1.46** — Data  $\sigma \in S_n$ , essa è determinata dalle immagini di  $\{1, \dots, n\}$ , dunque è determinata dai suoi cicli.

### Esempio 1.47

Presa ad esempio  $\sigma \in S_{10}$ :

$$\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9)$$

chiamiamo i suoi cicli:

$$\sigma_1 = (1\ 2\ 3) \quad \sigma_2 = (4\ 5) \quad \sigma_3 = (6\ 7\ 8\ 9)$$

dove appunto  $\sigma_1, \sigma_2, \sigma_3 \in S_{10}$  e:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$$

**Definizione 1.48.** Una permutazione si dice **ciclica** se ha un unico ciclo (orbita) non banale.<sup>6</sup>

**Osservazione 1.49** — Si osserva che:

- Cicli disgiunti commutano.
- L'ordine di una permutazione ciclica è la lunghezza del suo ciclo:

$$\sigma = (x_1, \dots, x_k) \implies \text{ord } \sigma = k$$

quindi  $\sigma^k = id$  e se  $d < k$ , allora  $\sigma^d(x_1) = x_{d+1} \neq x_1$ .

### Proposizione 1.50 (Struttura Delle Permutazioni)

Ogni permutazione si scrive in modo unico (a meno dell'ordine e della scrittura di cicli) come prodotto di cicli disgiunti, ovvero come composizione di permutazioni cicliche che agiscono su insiemi disgiunti.

*Dimostrazione.* I cicli della permutazione sono univocamente determinati in quanto orbite della permutazione, sappiamo che ogni permutazione si scrive come prodotto dei suoi cicli, e per concludere basta osservare che i cicli disgiunti commutano.  $\square$

**Osservazione 1.51** — Si osserva che l'unicità della scrittura di una permutazione vista nella [Proposizione 1.50](#) è effettivamente valida solo nel caso di cicli disgiunti, infatti, prendendo ad esempio:

$$\sigma = (1\ 2)(2\ 4) \in S_4 \quad \text{con} \quad \sigma_1 = (2\ 4) \quad \text{e} \quad \sigma_2 = (1\ 2)$$

non essendo  $\sigma_1, \sigma_2$  cicli disgiunti, si osserva che  $\sigma_2 \circ \sigma_1 = (2\ 4\ 1)$  e quindi  $\sigma$  era in realtà un 3-ciclo, e la sua fattorizzazione è unica come tale (mentre non era unica come prodotto di cicli non disgiunti).

<sup>6</sup>D'ora in avanti si utilizzeranno i termini "permutazione ciclica" e "ciclo" come sinonimi, in quanto una permutazione ciclica è appunto un singolo ciclo non banale.

### Corollario 1.52

$S_n$  è generato dalle permutazioni cicliche.

*Dimostrazione.* Segue immediatamente dal fatto che ogni permutazione si ottiene mediante composizione di permutazioni cicliche.  $\square$

### Esempio 1.53

Per esempio, preso  $S_4$ , le permutazioni possibili sono cicli del tipo:

$$id \quad (a \ b) \quad (a \ b \ c) \quad (a \ b \ c \ d) \quad (a \ b)(c \ d)$$

per contare il numero di 2-cicli, ci basta scegliere 2 elementi dell'insieme in  $\binom{4}{2}$  modi e poi considerare tutti i possibili riordinamenti ciclici (dove la scelta del primo elemento è arbitraria), e ciò può essere fatto in  $\frac{2!}{2}$  modi, per un totale di:

$$\binom{4}{2} \frac{2!}{2} = 6$$

e ragionando analogamente per i 3-cicli e i 4-cicli si ottiene:

$$\binom{4}{3} \frac{3!}{3} = 8 \quad \text{e} \quad \binom{4}{4} \frac{4!}{4} = 6$$

infine, per quanto riguarda le permutazioni ottenute dalla composizione di due 2-cicli, possiamo scegliere e permutare due coppie di elementi, come nei casi precedenti, tuttavia, essendo i cicli disgiunti, questi commutano (banalmente perché lasciano fissi gli altri elementi del dominio), quindi bisogna anche dividere per il numero di permutazioni dei cicli della stessa lunghezza, ovvero  $2!$  dunque:

$$\binom{4}{2} \frac{2!}{2} \binom{2}{2} \frac{2!}{2} \cdot \frac{1}{2!} = 3$$

e dal conteggio delle permutazioni di  $S_4$  divise per cicli di diversa lunghezza si ottiene:  $1 + 6 + 8 + 6 + 3 = 24 = |S_4|$ .

**Osservazione 1.54** — Quanto visto nell'esempio precedente può essere generalizzato ottenendo:

$$\#\{\sigma \in S_n \mid \sigma \text{ è un } k\text{-ciclo}\} = \binom{n}{k} \frac{k!}{k} = \binom{n}{k} (k-1)!$$

### Esempio 1.55

Per quanto detto risulta semplice ad esempio calcolare:

$$\#\{\sigma \in S_{20} \mid \sigma \text{ si fattorizza in cicli del tipo } 2 + 2 + 2 + 4 + 5 + 5\}$$

applicando quanto detto nell'osservazione precedente si trovano:

$$\frac{\binom{20}{2}\binom{18}{2}\binom{16}{2}1!1!1!}{3!} \cdot \binom{14}{4}3! \cdot \frac{\binom{10}{5}\binom{5}{5}4!4!}{2!}$$

### Proposizione 1.56 (Ordine di una permutazione)

Data  $\sigma \in S_n$  con  $\sigma = \sigma_1 \dots \sigma_k$ , con  $\sigma_i$  cicli disgiunti, allora:

$$\text{ord } \sigma = [\text{ord } \sigma_1, \dots, \text{ord } \sigma_k]$$

*Dimostrazione.* Sia  $\sigma_i$  un  $l_i$ -ciclo, ovvero  $\text{ord } \sigma_i = l_i$ , vogliamo dimostrare che:

$$\text{ord } \sigma = [l_1, \dots, l_k] = d$$

osserviamo che  $\sigma^d = (\sigma_1 \dots \sigma_k)^d = \sigma_1^d \dots \sigma_k^d$ , in quanto i cicli  $\sigma_i$  sono disgiunti (pertanto commutano), ed essendo  $d = [l_1, \dots, l_k]$  si ha che  $l_i \mid d, \forall i \in \{1, \dots, k\}$ , pertanto:

$$\sigma^d = \sigma_1^d \dots \sigma_k^d = id \implies \text{ord } \sigma = m \mid d$$

d'altra parte, si ha che:

$$\sigma^m = \sigma_1^m \dots \sigma_k^m = id \iff \sigma_i^m = id, \forall i \in \{1, \dots, k\}$$

dunque  $\text{ord } \sigma_i = l_i \mid m, \forall i \in \{1, \dots, k\}$ , ovvero  $[l_1, \dots, l_k] \mid m$  da cui si conclude che  $m = [l_1, \dots, l_k]$ .  $\square$

### Proposizione 1.57 ( $S_n$ è generato dalle trasposizioni)

Le trasposizioni generano  $S_n, \forall n \geq 2$ .

*Dimostrazione.* Per dimostrare l'affermazione bisogna mostrare che ogni permutazione è prodotto di trasposizioni (in generale non disgiunte). Poiché ogni permutazione, per quanto affermato nella [Proposizione 1.50](#), è il prodotto di cicli (permutazioni cicliche) disgiunti, è sufficiente mostrare che i cicli sono tutti prodotto di trasposizioni, infatti si può osservare che:

$$(1 \dots k) = (1 \ k)(1 \ k-1) \dots (1 \ 2)$$

dove l'uguaglianza è tra funzioni, quindi ci basta mostrare che danno la stessa immagine. Se  $i > k$ , allora entrambe le funzioni mandano  $i \mapsto i$ , se  $i \leq k$ , allora la funzione a sinistra manda  $i \mapsto i+1$  e  $k \mapsto 1$ , quella a destra lascia fisso  $i$  fino al ciclo  $(1 \ i)$  che manda  $i \mapsto 1$ , e il ciclo successivo (alla sinistra del precedente)  $(1 \ i+1)$  manda  $1 \mapsto i+1$ , infine i cicli successivi lasciano fisso  $i+1$  (quindi complessivamente abbiamo  $i \mapsto i+1$ ), mentre  $k$  viene lasciato fisso da tutti i cicli tranne  $(1 \ k)$ , quindi  $k \mapsto 1$ .  $\square$

**Osservazione 1.58** — La scrittura di una permutazione come prodotto di trasposizioni non è unica. Ad esempio in  $S_4$ :

$$\sigma = (1\ 2)(2\ 4) = (1\ 2)(3\ 4)(3\ 4)(2\ 4)$$

La seguente proposizione ci mostra invece che è fissata la parità della decomposizione in trasposizioni, cioè se  $\sigma$  si scompone come prodotto di  $m$  trasposizioni, ogni altra decomposizione come prodotto di trasposizioni ha un numero di trasposizioni con la stessa parità.

**Proposizione 1.59** (Segno di una permutazione)

L'applicazione:

$$\text{sgn} : S_n \longrightarrow \{\pm 1\} : \sigma \longmapsto \text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

è un omomorfismo di gruppi. Inoltre, se  $\sigma$  è una trasposizione, allora  $\text{sgn}(\sigma) = -1$ .

*Dimostrazione.* Osserviamo inizialmente che  $\text{sgn}$  è ben definita cioè:

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{\pm 1\}$$

al denominatore del prodotto vi sono tutte le possibili coppie  $i - j$  (in  $\{1, \dots, n\}$ , prese tutte ordinatamente con  $i < j$ ) e anche al numeratore poiché  $\sigma$  è bigettiva, l'unica cosa che può cambiare è l'ordine (ovvero potrebbe comparire  $i - j$  al numeratore e  $j - i$  al denominatore), quindi  $\text{sgn}(\sigma) \in \{\pm 1\}$ . Mostriamo che  $\text{sgn}$  è un omomorfismo:

$$\text{sgn}(\sigma \circ \tau) = \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} = \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \frac{\tau(i) - \tau(j)}{\tau(i) - \tau(j)}$$

da cui:

$$\prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j} = \underbrace{\prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}}_{\text{sgn}(\sigma)} \underbrace{\prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j}}_{\text{sgn}(\tau)} \quad \forall \sigma, \tau \in S_n$$

Ci resta da verificare che il segno di una trasposizione è  $-1$ . Sia  $\sigma = (a\ b)$ , analizzando il segno delle varie coppie, distinguiamo le seguenti possibilità per i vari fattori del prodotto:

- $\{i, j\} \cap \{a, b\} = \emptyset$ , in tal caso  $\sigma$  lascia fissi gli elementi,  $\sigma(i) = i, \sigma(j) = j \implies \frac{\sigma(i) - \sigma(j)}{i - j} = 1$ .
- $\{i, a\}$  con  $i \neq b$  (il caso  $\{i, b\}$  con  $i \neq a$  è analogo), in tal caso  $\frac{\sigma(i) - \sigma(a)}{i - a} = \frac{i - b}{i - a}$ , però vi è anche il fattore  $\frac{\sigma(i) - \sigma(b)}{i - b} = \frac{i - a}{i - b}$  e il loro prodotto dà 1.
- Infine, nel caso in cui  $\{i, j\} = \{a, b\}$  si ha:

$$\frac{\sigma(a) - \sigma(b)}{a - b} = \frac{b - a}{a - b} = -1$$

Dunque si conclude che  $\text{sgn}((a\ b)) = -1$ . □



**Osservazione 1.60** — La proposizione appena vista dimostra quanto detto sopra, ovvero:

$$\sigma = \tau_1 \dots \tau_m \quad \text{con } \tau_i \text{ trasposizione}$$

$$\text{allora } \operatorname{sgn}(\sigma) = \prod_{1 \leq i \leq m} \operatorname{sgn}(\tau_i) = (-1)^m.$$

**Definizione 1.61.** Una permutazione  $\sigma \in S_n$  si dice **pari** se  $\operatorname{sgn}(\sigma) = 1$ , **dispari** se  $\operatorname{sgn}(\sigma) = -1$ .

**Definizione 1.62.** Dato l'omomorfismo  $\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$ , si definisce **gruppo alterno**:

$$\mathcal{A}_n = \ker \operatorname{sgn} = \{\sigma \in S_n \mid \sigma \text{ è pari}\}$$

**Osservazione 1.63** — Si osserva che  $\mathcal{A}_n \trianglelefteq S_n$  e  $|\mathcal{A}_n| = \frac{n!}{2}$  poiché  $S_n/\mathcal{A}_n \cong \{\pm 1\}$ .

**Osservazione 1.64** — Per quanto detto nella [Proposizione 1.57](#), un  $k$ -ciclo si può scrivere nella forma:

$$(1 \dots k) = \underbrace{(1 \ k)(1 \ k-1) \dots (1 \ 2)}_{k-1 \text{ trasposizioni}}$$

dunque un  $k$ -ciclo è pari se  $k \equiv 1 \pmod{2}$ , dispari se  $k \equiv 0 \pmod{2}$ .

## §1.10 Classi di coniugio in $S_n$

### Teorema 1.65

Due permutazioni in  $S_n$  sono coniugate se e solo se hanno la stessa decomposizione in cicli disgiunti.

*Dimostrazione.* Mostriamo le due implicazioni:

- Presa  $\sigma = (a_1 \dots a_k)$  e  $\tau \in S_n$ , vogliamo dimostrare che  $\tau \circ \sigma \circ \tau^{-1}$  è ancora un  $k$ -ciclo. Sia  $\tau(a_i) = b_i$ , allora si ha che  $\tau \sigma \tau^{-1} = (b_1 \dots b_k)$ , con  $b_i \neq b_j$ ,  $\forall i \neq j$ , poiché  $\tau$  è bigettiva; verifichiamo l'uguaglianza mostrando che le due funzioni coincidono per tutti gli elementi. Si osserva che nel ciclo a destra accade semplicemente che  $b_i \mapsto b_{i+1}$ , a sinistra invece:

$$b_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} b_{i+1} \quad \forall i \in \{1, \dots, k\}$$

Se, invece,  $x \neq b_i, \forall i \in \{1, \dots, k\}$ , a sinistra si ha  $\tau^{-1}(x) \neq a_1, \dots, a_k$  (perché non si parte da alcun  $b_i$ ), quindi  $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$ , e quindi  $\tau \sigma \tau^{-1}(x) = \tau \tau^{-1}(x) = x$ ; a destra invece, essendo  $x \neq b_i \forall i$  viene lasciato fisso, ciò conclude che le due funzioni sono uguali e quindi  $\tau \sigma \tau^{-1}$  è un  $k$ -ciclo.

- Mostriamo ora che due permutazioni con la stessa fattorizzazione in cicli disgiunti sono coniugate. Siano:

$$\sigma = (a_1 \dots a_l)(b_1 \dots b_s) \dots (z_1 \dots z_t)$$

$$\rho = (a'_1 \dots a'_l)(b'_1 \dots b'_s) \dots (z'_1 \dots z'_t)$$

per dimostrare la tesi è sufficiente trovare  $\tau \in S_n$  tale che  $\tau \circ \sigma \circ \tau^{-1} = \rho$ . Scegliamo  $\tau$  definita da:

$$\tau(a_i) = a'_i, \tau(b_i) = b'_i, \dots, \tau(z_i) = z'_i$$

ed eventualmente si aggiungono altri elementi. Verifichiamo allora che  $\tau \circ \sigma \circ \tau^{-1} = \rho$ , consideriamo (WLOG) il primo ciclo:

$$a'_i \xrightarrow{\tau^{-1}} a_i \xrightarrow{\sigma} a_{i+1} \xrightarrow{\tau} a'_{i+1}$$

e quindi  $a'_i \mapsto a'_{i+1}$ , pertanto  $\tau \circ \sigma \circ \tau^{-1}$  e  $\rho$  coincidono sempre.

□

### Esempio 1.66

In  $S_5$  la classe di coniugio di  $\sigma = (1 \ 2)(3 \ 4)$  è  $C_\sigma = \{(a \ b)(c \ d) \in S_5\}$ , con:

$$\#C_\sigma = \frac{\binom{5}{2}\binom{3}{2}1!1!}{2!} = 15$$

e da ciò si ricava anche che:

$$\#Z_{S_5}(\sigma) = \frac{|S_5|}{|C_\sigma|} = \frac{5!}{15} = 8$$

**Esempio 1.67**

Sia  $\sigma = (3\ 5)(14) \in S_5$  e sia  $\rho = (1\ 2)(3\ 4)$ , cerchiamo  $\tau \in S_5$  tale che:

$$\tau \circ \sigma \circ \tau^{-1} = \rho$$

si può scegliere  $\tau = (1\ 3)(2\ 5)$ , da cui:

$$(1\ 3)(2\ 5) \circ (3\ 5)(14) \circ (1\ 3)(2\ 5) = (1\ 2)(3\ 4) = \rho$$

**Corollario 1.68**

Valgono i seguenti fatti:

- (1) Il numero di classi di coniugio in  $S_n$  è uguale al numero di partizioni di  $n$ .
- (2) Se  $H \leq S_n$ , allora  $H \trianglelefteq S_n$  se e solo se contiene tutte le permutazioni di un certo tipo o nessuna.

### §1.11 Prodotto diretto

Ricordiamo brevemente che se  $G_1$  e  $G_2$  sono gruppi, allora l'insieme  $G_1 \times G_2$  con l'operazione fatta componente per componente prende il nome di **prodotto diretto**.

#### Esempio 1.69

Presi ad esempio  $\mathbb{Z}/7\mathbb{Z}$  e  $S_4$ , si ha  $\mathbb{Z}/7\mathbb{Z} \times S_4$ , con  $\sigma = (\bar{1}, (1\ 2\ 3))$  e  $\rho = (\bar{4}, (1\ 4\ 2\ 4))$  in  $\mathbb{Z}/7\mathbb{Z} \times S_4$  e l'operazione:

$$\sigma \cdot \rho = (\bar{1} + \bar{4}, (1\ 2\ 3) \circ (1\ 4\ 2\ 3)) = (\bar{5}, (1\ 4\ 3\ 2))$$

**Osservazione 1.70** — Si ricordano i seguenti fatti:

- Se  $H, K \leq G$  in generale  $HK$  non è un sottogruppo, ma  $HK \leq G \iff HK = KH$ . Ovviamente se uno tra  $H$  e  $K$  è normale in  $G$ , allora questo è sempre vero.
- $H \times K \leq G \times G$ .

#### Lemma 1.71

Siano  $H, K \leq G$  e  $H \cap K = \{e\}$ , allora  $hk = kh$ ,  $\forall h \in H, \forall k \in K$ .

*Dimostrazione.* Preso  $hkh^{-1}k^{-1}$ , si ha:

$$hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})}_{\substack{=k' \\ \in K}} k^{-1} = h \underbrace{(kh^{-1}k^{-1})}_{\substack{=h' \\ \in H}}$$

dunque  $hkh^{-1}k^{-1} \in H \cap K \implies hkh^{-1}k^{-1} = e$ , da cui segue la tesi.  $\square$

#### Teorema 1.72 (Decomposizione in prodotto diretto)

Sia  $G$  un gruppo e siano  $H, K \leq G$  tali che:

- (1)  $HK = G$ .
- (2)  $H \cap K = \{e\}$ .

Allora  $G \cong H \times K$ .

*Dimostrazione.* Definiamo l'applicazione:

$$\varphi : H \times K \longrightarrow G : (h, k) \mapsto hk$$

Si verifica che è un omomorfismo:

$$\varphi((h_1, k_1)(h_2, k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$$

per il Lemma 1.71 si ha che  $h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi((h_1, k_1))\varphi((h_2, k_2))$ ,  $\forall h_1, h_2 \in H$ ,  $\forall k_1, k_2 \in K$ . Si osserva ora che  $\varphi$  è surgettiva, per l'ipotesi (1); infine, è iniettiva in quanto:

$$\ker \varphi = \{(h, k) \in H \times K | hk = e\} = \{(h, k) \in H \times K | h = k^{-1}\} = \{e\}$$

dove nell'ultima uguaglianza si è usato il fatto che  $H \cap K = \{e\}$ . □

**Osservazione 1.73** — Se abbiamo due sottogruppi  $G_1$  e  $G_2$  e costruiamo  $G = G_1 \times G_2$ , allora presi:

$$H = G_1 \times \{e_2\} \trianglelefteq G \quad \text{e} \quad K = \{e_1\} \times G_2 \trianglelefteq G$$

$H, K$  sono normali, hanno intersezione banale e sono tali che  $HK = G$ , quindi verifichiamo le ipotesi del teorema, pertanto  $G \cong H \times K$ .

### Esempio 1.74

Sia  $G$  un gruppo con  $|G| = p^2$ , dalla formula delle classi avevamo ottenuto che  $G$  è necessariamente abeliano, quindi  $G$  è isomorfo a  $\mathbb{Z}/p^2\mathbb{Z}$  o  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ . Se  $G$  è ciclico, allora  $G \cong \mathbb{Z}/p^2\mathbb{Z}$ . Mostriamo che se non lo è, allora  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  e in questo caso tutti gli elementi di  $G$  hanno ordine  $p$ .

Consideriamo  $(e \neq)x \in G$  e  $H = \langle x \rangle \trianglelefteq G$  (in quanto  $G$  abeliano); prendiamo  $y \in G \setminus \langle x \rangle$  e analogamente  $K = \langle y \rangle \trianglelefteq G$ , da ciò segue che  $H \cap K = \{e\}$ , infatti  $H$  e  $K$  sono sottogruppi ciclici di  $G$  aventi ordini due primi distinti e quindi hanno in comune solo l'elemento neutro. Osservando infine che per cardinalità  $HK = G$ , per cardinalità:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2$$

le ipotesi del [Teorema 1.72](#) sono verificate, dunque:

$$G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

## §1.12 Prodotto semidiretto

**Definizione 1.75.** Dati due gruppi  $H, K$  e l'azione:

$$\varphi : K \longrightarrow \text{Aut}(H)(\leq S(H)) : k \longmapsto \varphi_k$$

si dice **prodotto semidiretto** di  $H$  e  $K$  via  $\varphi$ :

$$H \rtimes_{\varphi} K$$

(o anche  $K_{\varphi} \ltimes H$ ) l'insieme ottenuto come prodotto cartesiano  $H \times K$  con l'operazione definita da:

$$(h, k)(h', k') = (h \cdot_H \varphi_k(h'), k \cdot_K k')$$

### Proposizione 1.76 (Il Prodotto Semidiretto è un gruppo)

Dati due gruppi  $H, K$ , allora  $H \rtimes_{\varphi} K$  è un gruppo.

*Dimostrazione.* Come si verifica facilmente l'operazione indotta dal prodotto semidiretto è associativa, verifichiamo che  $(e_H, e_K)$  è l'elemento neutro:

$$(h, k)(e_H, e_K) = (h \cdot \varphi_k(e_H), ke_K) = (he_H, k) = (h, k)$$

dove  $\varphi_k(e_H) = e_H$  poiché  $\varphi_k$  è un automorfismo (e quindi in particolare un omomorfismo), a sinistra, invece, si ha:

$$(e_H, e_K)(h, k) = (e_H \cdot \varphi_{e_K}(h), e_K k) = (e_H \cdot id(h), k) = (e_H h, k) = (h, k)$$

Per l'inverso si osserva:

$$(h, k)^{-1} = ((\varphi_k)^{-1}(h^{-1}), k^{-1}) = (\varphi_{k^{-1}}(h^{-1}), k^{-1})^7$$

dunque si verifica a destra:

$$\begin{aligned} (h, k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) &= (h \cdot \varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = \\ &= (h \cdot id(h^{-1}), e_K) = (hh^{-1}, e_K) = (e_H, e_K) \end{aligned}$$

e analogamente a sinistra:

$$\begin{aligned} (\varphi_{k^{-1}}(h^{-1}), k^{-1})(h, k) &= (\varphi_{k^{-1}}(h^{-1}) \cdot \varphi_{k^{-1}}(h), k^{-1}k) = \\ &= (\varphi_{k^{-1}}(h^{-1}h), e_K) = (\varphi_{k^{-1}}(e_H), e_K) = (e_H, e_K) \end{aligned}$$

□

<sup>7</sup>L'uguaglianza  $(\varphi_k)^{-1} = \varphi_{k^{-1}}$  segue dal fatto che  $\varphi$  è un omomorfismo e quindi manda inversi in inversi.

**Osservazione 1.77** — Si osserva che  $H \rtimes_{\varphi} K$  è il prodotto diretto se e solo se  $\varphi_k = id_H, \forall k \in K$ . Infatti:

$$(h, k)(h', k') = (h \cdot \varphi_k(h'), kk') = (hh', kk') \iff \varphi_k(h') = h' \quad \forall k \in K$$

e dunque  $\varphi_k = id_H$ .

**Teorema 1.78** (Decomposizione in prodotto semidiretto)

Sia  $G$  un gruppo e siano  $H, K \leq G$ , con  $H \trianglelefteq G$ , tali che:

- (1)  $HK = G$ .
- (2)  $H \cap K = \{e\}$ .

Allora  $G \cong H \rtimes_{\varphi} K$ , dove  $\varphi : K \longrightarrow \text{Aut}(H) : k \longmapsto \varphi_k$ , con  $\varphi_k : H \xrightarrow{\sim} H : h \longmapsto khk^{-1}$ .

*Dimostrazione.* Costruiamo esplicitamente un isomorfismo tra i due gruppi:

$$\mathcal{F} : H \rtimes_{\varphi} K \longrightarrow G : (h, k) \longmapsto hk$$

Verifichiamo che è un omomorfismo:

$$\mathcal{F}((h, k)(h', k')) = \mathcal{F}(h \cdot \varphi_k(h'), kk') = \mathcal{F}(\underbrace{hkh'k^{-1}}_{=\varphi_k(h')}, kk') = hkh'k^{-1}kk' = \underbrace{hk}_{=\mathcal{F}(h, k)} \underbrace{h'k'}_{=\mathcal{F}(h', k')}$$

Si vede inoltre che  $\mathcal{F}$  è surgettiva per l'ipotesi (1) e iniettiva per la (2), infatti:

$$\ker \mathcal{F} = \{(h, k) \in H \rtimes_{\varphi} K \mid \mathcal{F}(h, k) = hk = e\} = \{e\}$$

□

**Osservazione 1.79** — Si osserva che  $\varphi_k$  è la restrizione al sottogruppo  $H$  dell'automorfismo interno  $g \longmapsto kgk^{-1}$ , poiché  $H \trianglelefteq G$ , allora la restrizione a  $H$  di ogni elemento di  $\text{Inn}(G)$  è un automorfismo di  $H$ .

**Osservazione 1.80** — Sapendo che  $G \cong H \rtimes_{\varphi} K$  e seguendo i passaggi della verifica di omomorfismo al contrario, si ricava che necessariamente  $\varphi$  è esattamente l'azione di coniugio su  $H$ .

**Osservazione 1.81** — Siano  $\overline{H} = H \times \{e_K\}$  e  $\overline{K} = \{e_H\} \times K$ , si osserva che  $\overline{H}, \overline{K} \leq G = H \rtimes_{\varphi} K$ , infatti sono chiusi per prodotto (ristretto):

$$(h, e_K)(h', e_K) = (h \cdot \varphi_{e_K}(h'), e_K) = (h \cdot id(h'), e_K) = (hh', e_K)$$

$$(e_H, k)(e_H, k') = (e_H \cdot \varphi_k(e_H), kk') = (e_H, kk')$$

e si verifica facilmente anche per inverso. Si osserva che  $\overline{H} \trianglelefteq G^a$ , in quanto  $\overline{H} = \ker \pi$ , con:

$$\pi : H \rtimes_{\varphi} K \longrightarrow K : (h, k) \longmapsto k$$

con  $\pi$  omomorfismo come si vede:

$$\pi((h, k)(h', k')) = \pi(h \cdot \varphi_k(h'), kk') = kk' = \pi((h, k))\pi((h', k'))$$

Per come li abbiamo presi si nota subito che  $\overline{H}\overline{K} = G$  e  $\overline{H} \cap \overline{K} = \{e\}$ , quindi valgono le ipotesi del [Teorema 1.78](#), pertanto:

$$G \cong H \rtimes_{\varphi} K \cong \overline{H} \rtimes_{\varphi} \overline{K}$$

---

<sup>a</sup> $\overline{K}$  in generale non è normale, lo è solo se il prodotto è diretto, infatti in quel caso vale il [Teorema 1.72](#).

### Esempio 1.82 ( $S_n \cong \mathcal{A}_n \rtimes_{\varphi} \langle(1\ 2)\rangle$ )

Verifichiamo che  $S_n$  è prodotto semidiretto di  $H = \mathcal{A}_n$  e  $K = \langle(1\ 2)\rangle$  <sup>a</sup> usando il [Teorema 1.78](#), per quanto detto nel (1) del [Corollario 1.68](#) sappiamo che  $\mathcal{A}_n \triangleleft S_n$ , inoltre, sempre per il punto (1), essendo  $|\mathcal{A}_n| = \frac{n!}{2}$ , segue per cardinalità che  $HK = S_n$ . Essendo  $\mathcal{A}_n = \ker \text{sgn}$  e  $\langle(1\ 2)\rangle$  una trasposizione  $H \cap K = \{e\}$  (in quanto il nucleo dell'omomorfismo segno contiene solo permutazioni pari), pertanto segue la tesi:

$$S_n \cong \mathcal{A}_n \rtimes_{\varphi} \langle(1\ 2)\rangle$$

Osserviamo inoltre che:

$$\varphi : \langle(1\ 2)\rangle \longrightarrow \text{Aut}(\mathcal{A}_n) : (1\ 2) \longmapsto \varphi_{(1\ 2)}, id \longmapsto id$$

con  $\varphi_{(1\ 2)} : \mathcal{A}_n \longrightarrow \mathcal{A}_n : \rho \longmapsto (1\ 2)\rho(1\ 2)^{-1}$ .

---

<sup>a</sup>In generale va bene qualsiasi trasposizione (che esiste sempre in  $S_n$  per  $n \geq 2$ ).



**Esempio 1.83** ( $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ )

Ricordando che  $D_n = \langle r, s | r^n = s^2 = id, sr s^{-1} = r^{-1} \rangle$ , possiamo osservare ancora una volta che le ipotesi del [Teorema 1.78](#) sono soddisfatte. Poiché  $\text{ord } r = n$ , allora  $|\langle r \rangle| = n$ , e in particolare  $[D_n : \langle r \rangle] = 2 \implies \langle r \rangle \triangleleft D_n$ ; inoltre,  $\langle r \rangle \cap \langle s \rangle = \{id\}$  perché  $\det(r_i) = 1$ , mentre  $\det(sr_i) = -1, \forall i \in \{1, \dots, n\}$ . Infine, essendo  $\text{ord } s = 2$ , allora il prodotto di sottogruppi avrà cardinalità:

$$|\langle r \rangle \langle s \rangle| = \frac{|\langle r \rangle| |\langle s \rangle|}{|\langle r \rangle \cap \langle s \rangle|} = \frac{2n}{1} = 2n$$

dunque  $\langle r \rangle \langle s \rangle = D_n$ . Pertanto  $D_n \cong \langle r \rangle \rtimes_{\varphi} \langle s \rangle$ , dove  $\langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$  e  $\langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$ , quindi:

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

con:

$$\varphi : \langle s \rangle \longrightarrow \text{Aut}(\langle r \rangle) : s \longmapsto \varphi_s$$

dove  $\varphi_s : \langle r \rangle \longrightarrow \langle r \rangle : r \longmapsto sr s^{-1} (= r^{-1})$ . Si osserva che deve essere  $\text{ord } \varphi_s | \text{ord } s = 2$ , quindi ci sono soltanto due possibilità:

$$\varphi_s = \begin{cases} id \\ r \longmapsto r^{-1} \end{cases}$$

nel caso in cui  $\varphi_s = id$  si ottiene il prodotto diretto, nell'altro caso si ottiene il prodotto semidiretto che definisce  $D_n$ . Se in  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  ci sono altri elementi di ordine due (ad esempio se  $\text{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ) si possono definire anche altri prodotti semidiretti:

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

Rimane il problema di verificare se danno o meno due gruppi isomorfi.

**Esempio 1.84** (Gruppi di ordine  $pq$ )

Sia  $|G| = pq$ , per il [Teorema Di Cauchy](#) esistono  $x, y \in G$  tali che  $\text{ord } x = q$ ,  $\text{ord } y = p$ , assumiamo (WLOG)  $q > p$ , allora si ha che:

$$H = \langle x \rangle \triangleleft G$$

poiché  $[G : H] = p$ , con  $p$  più piccolo primo che divide  $|G|$ . Alternativamente si può vedere che  $H$  è caratteristico in  $G$  poiché è l'unico sottogruppo di quell'ordine; se  $H' < G$  e  $|H'| = q$ , se fosse  $H \neq H'$ , allora  $H \cap H' = \{e\}$  e quindi:

$$|HH'| = \frac{|H||H'|}{|H \cap H'|} = \frac{q \cdot q}{1} = q^2 > pq$$

quindi  $H'$  non può essere un sottogruppo di  $G$ . Si verifica che, detto  $K = \langle y \rangle$ , le ipotesi del [Teorema 1.78](#) sono soddisfatte:

$$HK = G \quad H \cap K = \{e\} \quad H \triangleleft G$$

da ciò segue che ogni gruppo di ordine  $pq$  è prodotto semidiretto:  $G \cong H \rtimes_{\varphi} K$ .

Per classificare tutti i gruppi di ordine  $pq$  bisogna classificare tutti i possibili prodotti semidiretti  $\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z}$  a meno di isomorfismo. Osserviamo che un prodotto semidiretto deve avere un'operazione definita da:

$$\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

Essendo  $\mathbb{Z}/p\mathbb{Z} = \langle y \rangle$  e  $\mathbb{Z}/q\mathbb{Z} = \langle x \rangle$  possiamo scrivere:

$$\varphi : \langle y \rangle \longrightarrow \text{Aut}(\langle x \rangle) (\cong \mathbb{Z}/q\mathbb{Z}^* \cong \mathbb{Z}/(q-1)\mathbb{Z}) : y \longmapsto \varphi_y$$

dove  $\varphi_y : \langle x \rangle \longrightarrow \langle x \rangle : x \longmapsto x^l$  (poiché gli automorfismi di un gruppo ciclico mandano un elemento in una sua potenza, o prodotto se la notazione è additiva). Per definire  $\varphi$  su  $\langle y \rangle$  (un dominio ciclico) basta assegnare  $\varphi_y$  con la condizione  $\text{ord } \varphi_y \mid \text{ord } y = p$ , inoltre,  $\varphi_y \in \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z} \implies \text{ord } \varphi_y \mid q-1$ , quindi  $\text{ord } \varphi_y \mid (p, q-1)$ . Distinguiamo due casi:

- Se  $p \nmid q-1$ , si ha che  $\text{ord } \varphi_y \mid 1 \implies \varphi_y = id$ , dunque l'unico automorfismo possibile di  $\mathbb{Z}/q\mathbb{Z}$  è l'identità, pertanto si ha un prodotto diretto tra  $\mathbb{Z}/p\mathbb{Z}$  e  $\mathbb{Z}/q\mathbb{Z}$  e quindi esiste ed è unico il gruppo di ordine  $pq$ :  $\mathbb{Z}/pq\mathbb{Z}$ .
- Se  $p \mid q-1$ , allora o  $\text{ord } \varphi_y = 1$  e quindi ancora  $\varphi_y = id$ ; oppure  $\text{ord } \varphi_y = p$ , e poiché ci sono  $p-1$  elementi di ordine  $p$  in  $\mathbb{Z}/(q-1)\mathbb{Z}$ , abbiamo  $p-1$  scelte per  $\varphi_y$  che danno un prodotto semidiretto.

Si osserva che  $\text{ord}_{\text{Aut}(\langle x \rangle)} \varphi_y = \text{ord}_{\mathbb{Z}/q\mathbb{Z}^*}(\bar{l})$ , in quanto:

$$\varphi_y(x) = x^l \implies (\varphi_y(x))^{k8} = x^{l^k}$$

quindi  $\text{ord } \varphi_y = p \iff l^p \equiv 1 \pmod{q} \iff \text{ord}(\bar{l}) = p$ .

Possiamo verificare che le  $p-1$  scelte per  $\varphi_y$  danno tutti gruppi isomorfi, quindi se  $p \mid q-1$  ci sono esattamente due gruppi di ordine  $pq$  a meno di isomorfismo. Detti:

$$G_1 \cong \langle x \rangle \rtimes_{\varphi} \langle y \rangle \quad \text{e} \quad G_2 \cong \langle x \rangle \rtimes_{\psi} \langle y \rangle$$

con  $\varphi_y(x) = x^l$ ,  $\psi_y(x) = x^{\lambda}$  e  $\text{ord}_{\mathbb{Z}/q\mathbb{Z}^*}(\bar{\lambda}) = \text{ord}_{\mathbb{Z}/q\mathbb{Z}^*}(\bar{l}) = p$  (necessariamente, per quanto detto sopra è l'unico altro ordine possibile, oltre ad 1), abbiamo  $\langle l \rangle = \langle \lambda \rangle$  se e solo se  $l = \lambda^r$ , con  $0 < r < p$ . Consideriamo l'applicazione:

$$\mathcal{F} : G_1 \longrightarrow G_2 : x \longmapsto x, y \longmapsto y^r$$

essa definisce un isomorfismo tra i due gruppi  $G_1$  e  $G_2$ . Per verificare che la mappa sia effettivamente un isomorfismo, consideriamo le presentazioni dei due gruppi:

$$G_1 = \langle x, y \mid x^q = y^p = e_1, yxy^{-1} = x^l \rangle \quad \text{e} \quad G_2 = \langle x, y \mid x^q = y^p = e_2, yxy^{-1} = x^{\lambda} \rangle$$

affinché  $\mathcal{F}$  sia un isomorfismo, deve rispettare gli ordini dei generatori e verificare che sia preservata la relazione di commutazione su di essi definita; osserviamo che:

$$\mathcal{F}(x^q) = (\mathcal{F}(x))^q = x^q = e_2 \quad \text{in quanto } x^q = e_2 \text{ in } G_2$$

e anche:

$$\mathcal{F}(y^p) = (\mathcal{F}(y))^p = (y^r)^p = (y^p)^r = e_2 \quad \text{in quanto } y^p = e_2 \text{ in } G_2$$

---

<sup>8</sup>In questo caso si intende  $\underbrace{\varphi_y \circ \dots \circ \varphi_y}_{k\text{-volte}}(x)$ , da cui l'esponente  $l^k$  di  $x$ .

ed infine:

$$\mathcal{F}(yxy^{-1}) = \mathcal{F}(x^l)$$

in quanto:

$$\mathcal{F}(yxy^{-1}) = \mathcal{F}(y)\mathcal{F}(x)\mathcal{F}(y^{-1}) = \underbrace{y^r xy^{-r}}_{\in G_2} = (\varphi_y(x))^{r^9} = x^{\lambda^r} = {}^{10}x^l = \mathcal{F}(x^l)$$

ciò garantisce che  $\mathcal{F}$ , ottenuto estendendo l'assegnamento  $x \mapsto x, y \mapsto y^r$  a tutto il gruppo, è un omomorfismo; si verifica inoltre che è anche una bigezione e quindi è un isomorfismo.

---

<sup>9</sup>Anche in questo caso si intende la composizione  $r$  volte.

<sup>10</sup>Qui stiamo usando l'ipotesi per cui  $l = \lambda^r$ .

### §1.13 Teorema di struttura per i gruppi abeliani finiti

#### Teorema 1.85 (Teorema Di Struttura Dei Gruppi Abeliani Finiti)

Sia  $G$  un gruppo abeliano finito, allora  $G$  è prodotto diretto di gruppi ciclici, cioè:

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

Inoltre tale scrittura è unica se  $n_{i+1} \mid n_i, \forall i \in \{1, \dots, s-1\}$ .

#### Osservazione 1.86 (Schema della dimostrazione) — Sia:

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

$G(p)$  prende il nome di  **$p$ -componente** o componente di  **$p$ -torsione**. Si osserva che:

- $G(p)$  è un sottogruppo di  $G$  perché  $G$  è abeliano, dunque:

$$\text{ord}(xy) \mid [\text{ord}(x), \text{ord}(y)] \quad \forall x, y \in G$$

quindi se  $x$  ed  $y$  hanno per ordine una potenza di  $p$ , anche il prodotto ha per ordine una potenza di  $p$ , quindi  $xy \in G(p)$ , ed essendo  $G$  finito allora  $G(p)$  è un sottogruppo. <sup>a</sup>

- $G(p)$  è un sottogruppo caratteristico di  $G$  (ciò segue dal fatto che gli automorfismi conservano l'ordine degli elementi, e quindi  $G(p)$  viene mandato in  $G(p)$ ).

<sup>a</sup>Si osserva che le  $p$ -componenti sono  $p$ -gruppi.

#### Teorema 1.87 (I gruppi abeliani sono prodotto delle loro $p$ -componenti)

Sia  $G$  un gruppo abeliano, con  $|G| = n = p_1^{e_1} \dots p_s^{e_s}$ , con i primi  $p_i \neq p_j, \forall i \neq j$ , allora:

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

Inoltre la decomposizione di  $G$  come prodotto di  $p$ -gruppi di ordine tra loro coprimi è unica.

#### Teorema 1.88 (I $p$ -gruppi si spezzano come prodotto di $p$ -gruppi ciclici)

Sia  $G$  un  $p$ -gruppo abeliano. Esistono e sono univocamente determinati  $r_1, \dots, r_s$  tali che  $r_1 \geq r_2 \geq \dots \geq r_t$  <sup>a</sup>, per i quali:

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

<sup>a</sup>L'ordine degli esponenti assicura l'unicità della fattorizzazione.

Segue la dimostrazione del [Teorema Di Struttura Dei Gruppi Abeliani Finiti](#):

*Dimostrazione.* **Esistenza:** Dato il gruppo  $G$ , abeliano e finito, per il [Teorema 1.87](#) si ha:

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

possiamo applicare il [Teorema 1.88](#) ad ognuno dei fattori  $G(p_i)$  ed ottenere:

$$\begin{aligned} G &\cong G(p_1) \times \dots \times G(p_s) \cong \\ &\cong (\mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}) \end{aligned}$$

con  $r_{i1} \geq \dots \geq r_{it_i}$ . Per il Teorema Cinese del Resto possiamo rimettere assieme i termini formati da primi distinti in modo da mantenere la relazione di divisibilità (e quindi unicità) richiesta dal teorema:

$$\underbrace{\mathbb{Z}/(p_1^{r_{11}} \dots p_s^{r_{s1}})\mathbb{Z}}_{n_1} \times \dots \times \underbrace{\mathbb{Z}/(p_1^{r_{1t}} \dots p_s^{r_{st}})\mathbb{Z}}_{n_t}$$

dove  $t = \max\{t_1, \dots, t_s\}$  e poniamo  $r_{ih} = 0$  se  $h > t_i$ . Si osserva che, per come abbiamo riscritto la fattorizzazione si ha:  $n_t \mid n_{t-1} \mid \dots \mid n_1$ .

**Unicità:** Segue dall'unicità del [Teorema 1.87](#) e del [Teorema 1.88](#), infatti se ci fossero due decomposizioni di  $G$  diverse con ordini che si dividono in catena, ripercorrendo gli isomorfismi, avremmo all'inizio due diverse decomposizioni per  $G(p)$  (o per  $G$  come prodotto di  $p$ -componenti).  $\square$

### Esempio 1.89

Sia  $G \cong \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ , e raggruppando in base all'ordine degli elementi otteniamo i  $p$ -sottogruppi:

$$G \cong \underbrace{(\mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})}_{G(2)} \times \underbrace{(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})}_{G(3)} \times \underbrace{(\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})}_{G(5)}$$

e per il [Teorema Di Struttura](#) possiamo riscrivere il prodotto in ordine decrescente (rimettendo assieme  $p$ -gruppi ciclici di ordine massimo):

$$G \cong \mathbb{Z}/(2^3 \cdot 3 \cdot 5^2)\mathbb{Z} \times \mathbb{Z}/(2^2 \cdot 3 \cdot 5)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

**Esempio 1.90**

Classificare i gruppi abeliani di ordine 1000. Per fare ciò osserviamo che  $1000 = 2^3 \cdot 5^3$ , allora:

$$G = G(2) \times G(5)$$

con  $|G(2)| = 2^3$ , e  $|G(5)| = 5^3$  pertanto le  $p$ -componenti possono essere scritti come prodotto di gruppi ciclici nei seguenti modi:

$$G(2) \cong \begin{cases} \mathbb{Z}/2^3\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \quad \text{e} \quad G(5) \cong \begin{cases} \mathbb{Z}/5^3\mathbb{Z} \\ \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases}$$

Dunque i gruppi abeliani di ordine 1000 (a meno di isomorfismo) sono  $3 \cdot 3 = 9$ , in quanto per il [Teorema di Struttura](#) abbiamo una fattorizzazione unica come prodotto di gruppi cicli finiti, e per tale fattorizzazione abbiamo 3 scelte per la 2-componente e 3 scelte per la 5-componente.

Dimostriamo ora il [Teorema 1.87](#)

*Dimostrazione. Esistenza:* Sia  $|G| = n$ , con  $n = p_1^{e_1} \dots p_s^{e_s}$ , procediamo per induzione su  $s$ . Nel caso in cui  $s = 1$ , si ha  $|G| = p_1^{e_1} \implies G = G(p_1)$ . Supponiamo la tesi vera  $\forall m : 2 \leq m < n$ , possiamo scrivere  $n = mm'$  con  $(m, m') = 1$  e  $m, m' < n$ , allora (in notazione additiva) vogliamo verificare che:

$$G \cong mG \times m'G$$

È facile verificare che  $mG, m'G < G$  (basta vedere la chiusura per l'operazione), ed essendo  $G$  abeliano si ha anche  $mG, nG \triangleleft G$ ; si osserva inoltre che, essendo  $(m, m') = 1$ , allora  $\exists h, k \in \mathbb{Z}$ :

$$mh + m'k = 1 \implies m(gh) + m'(gk) = g \quad \forall g \in G \implies G \subseteq mG + m'G$$

il contrario è ovvio (per chiusura di  $G$  rispetto all'operazione), dunque:

$$mG + m'G = G$$

Inoltre, sia  $x \in mG \cap m'G$ , ovvero  $x = mg = m'g'$ , allora si osserva che  $m'x = m'mg = ng = 0$  e  $mx = mm'g' = m'g' = 0$ , dunque:

$$\text{ord}(x) \mid m \quad \text{e} \quad \text{ord}(x) \mid m' \implies \text{ord}(x) \mid (m, m') = 1 \implies x = 0$$

Quindi  $mG \cap m'G = \{e\}$ , pertanto sono verificate ipotesi del [Teorema 1.72](#), dunque è vero che  $G \cong mG \times m'G$ . Osserviamo che:

$$mG = G_{m'} = \{g \in G \mid m'g = 0\} \quad \text{e} \quad m'G = G_m = \{g \in G \mid mg = 0\}$$

Verifichiamo (WLOG)  $m'G = G_m$  (ovvero l'insieme dei multipli di  $m'$  è uguale a quello degli elementi di  $G$  il cui ordine divide  $m$ ) mostrando la doppia inclusione tra insiemi. Per verificare che  $m'G \subseteq G_m$ , consideriamo  $m'x \in m'G$ , poiché  $mm'x = nx = 0$ , allora  $\text{ord}(x) \mid m$  (stiamo escludendo  $m'$  perché per ipotesi stiamo considerando un elemento  $m'x$  diverso da 0) dunque  $m'x \in G_m$ ; viceversa, preso  $x \in G_m$ , ovvero  $mx = 0$ , per quanto visto sopra abbiamo che:

$$\underbrace{mx}_{=0}h + m'kx = x \implies x = m'(kx) \implies x \in m'G$$

quindi  $G_m \subseteq m'G \implies m'G = G_m$ . Pertanto possiamo scrivere:

$$G \cong G_m \times G_{m'}$$

A questo punto siamo sicuri che  $|G_m|, |G_{m'}| < |G|$ , perché  $G_m$  contiene tutti e soli gli elementi di  $G$  di ordine che divide  $m$ , e  $G_m \neq \{0\}$  (per [Cauchy](#), dato che  $1 < m < n$ ), pertanto  $G_{m'} \leq G$  e  $G_m \leq G$ .<sup>11</sup> Ora che sappiamo che i due sottogruppi sono propri possiamo applicare l'ipotesi induttiva e scrivere:

$$G_m = \prod_{i \in I} G(p_i) \quad \text{e} \quad G_{m'} = \prod_{j \in J} G(p_j)$$

con  $I \cup J = \{1, \dots, s\}$  e  $I \cap J = \emptyset$  (poiché  $(m, m') = 1$ ).

**Unicità:** La scrittura come prodotto di  $p$ -componenti è unica, perché se  $G$  fosse anche isomorfo ad altri  $p$ -gruppi:

$$G \cong H_1 \times \dots \times H_n \quad \text{con } H_i \text{ } p_i\text{-gruppo e } H_i < G$$

allora  $H_i \subseteq G(p_i)$  (in quanto  $G(p_i)$  contiene tutti gli elementi di ordine potenze di  $p_i$ ), ma:

$$|G| = |H_1| \dots |H_s| = |G(p_1)| \dots |G(p_s)| \implies |H_i| = |G(p_i)| \quad \forall i \in \{1, \dots, s\}$$

quindi segue che  $H_i = G(p_i)$ ,  $\forall i \in \{1, \dots, s\}$ .  $\square$

### Lemma 1.91

Sia  $G$  un  $p$ -gruppo abeliano e sia  $x_1$  un elemento di ordine massimo in  $G$ , preso  $\bar{x} \in G/\langle x_1 \rangle$  esiste  $y \in \pi_{\langle x_1 \rangle}^{-1}(\bar{x})$  :  $\text{ord}_G(y) = \text{ord}_{G/\langle x_1 \rangle}(\bar{x})$ , ovvero preso un elemento nel quoziente, esiste sempre un elemento nella sua fibra con lo stesso ordine.

*Dimostrazione.* Nelle ipotesi in cui siamo, sia  $\pi_{\langle x_1 \rangle}^{-1}(\bar{x}) = \pi_{\langle x_1 \rangle}^{-1}(x + \langle x_1 \rangle)$ , dunque l'elemento  $y \in \pi_{\langle x_1 \rangle}^{-1}(\bar{x})$  che cerchiamo è della forma:

$$y = x + ax_1$$

Sappiamo che  $\pi_{\langle x_1 \rangle}(y) = \pi_{\langle x_1 \rangle}(x) = \bar{x}$  (stiamo considerando due elementi nella stessa classe laterale); dato che il quoziente è ancora un  $p$ -gruppo, sia  $p^r = \text{ord}_{\langle x_1 \rangle}(\pi_{\langle x_1 \rangle}(y)) = \text{ord}_{\langle x_1 \rangle}(\bar{x}) \mid \text{ord}_G(y)$  (per le proprietà di omomorfismo), possiamo scegliere  $y$  (scegliendo  $a$ <sup>13</sup>) in modo che il suo ordine sia esattamente  $p^r$  (dalla divisibilità precedente sappiamo che  $p^r$  divide il suo ordine):

$$(p^r y =) p^r x + p^r ax_1 = 0 \iff p^r x = -p^r ax_1$$

dove essendo  $\text{ord}_{\langle x_1 \rangle}(\bar{x}) = p^r$  allora  $p^r x \in \langle x_1 \rangle$  (ovvero la sua proiezione modulo  $\langle x_1 \rangle$ , sta nella classe laterale banale) dunque  $p^r x = bx_1$ . Per ipotesi avevamo assunto che  $x_1$  ha ordine massimo, chiamiamolo  $p^{r_1}$ , deve essere che  $r \leq r_1$ , ma:

$$0 = p^{r_1} x \iff p^{r_1-r} p^r x = 0 \iff p^{r_1-r} bx_1 = 0$$

<sup>11</sup>Il problema dell'avere sottogruppi propri con le cardinalità giuste per poter applicare l'ipotesi induttiva poteva essere risolto anche in altri modi anziché passare ai gruppi  $G_m$  e  $G_{m'}$  come abbiamo fatto, ad esempio fissando inizialmente  $m = p_1^{e_1}$  e  $m' = p_2^{e_2} \dots p_s^{e_s}$ .

<sup>12</sup>Ciò deriva dal fatto che per coprimarietà tra gli altri fattori  $|G(p_i)|$  divide  $|H_i|$ , dunque vale anche la divisibilità inversa tra gli ordini.

<sup>13</sup>Infatti  $x_1$  è fissato per ipotesi, mentre  $x$  è fissato perché determinato da  $\bar{x}$ , sempre per ipotesi.

<sup>14</sup>Abbiamo moltiplicato e diviso per  $p^r$ .

e l'ultima uguaglianza è vera se e solo se  $p^{r_1} \mid p^{r_1-r}b$  (essendo  $\text{ord}_G(x_1) = p^{r_1}$ ), dunque se e solo se  $p^r \mid b \implies b = p^r b_1$ . Infine, scegliendo  $a = -b_1$  e sostituendo nell'espressione iniziale, si ha:

$$p^r y = p^r x - p^r b_1 x_1 = b x_1 - \underbrace{p^r b_1}_{=b} x_1 = 0$$

pertanto  $y = x - b_1 x_1 \in G$  realizza la proprietà richiesta.  $\square$

Dimostriamo ora il [Teorema 1.88](#):

*Dimostrazione.* **Esistenza:** Sia  $G$  un  $p$ -gruppo,  $|G| = p^n$ , proviamo la tesi per induzione su  $n$ . Per  $n = 1$  si ha che  $|G| = p \implies G \cong \mathbb{Z}/p\mathbb{Z}$ , e quindi la tesi è verificata. Supponiamo la tesi vera per  $1 \leq m < n$  e proviamola per  $n$ ; sia  $x_1 \in G$  un elemento di ordine massimo,  $\text{ord}(x_1) = p^{r_1}$ :

- Se  $r_1 = n$ , allora  $G$  è ciclico  $\implies G \cong \mathbb{Z}/p^n\mathbb{Z}$ .
- Se  $r_1 < n$ , poiché  $G$  è abeliano si ha  $\langle x_1 \rangle \triangleleft G$ , quindi possiamo considerare  $G/\langle x_1 \rangle$  che ha ordine  $p^{n-r_1} < p^n$ , dunque vale l'ipotesi induttiva ed il gruppo quoziente può essere fattorizzato come prodotto di gruppi ciclici:

$$G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle^{15}$$

sia  $\text{ord}(\overline{x_i}) = p^{r_i}$ , e supponiamo di aver scritto il prodotto diretto in modo ordinato, con  $r_2 \geq \dots \geq r_t$ . Consideriamo la proiezione al quoziente:

$$\pi : G \longrightarrow G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle^{16}$$

per il [Lemma 1.91](#) esistono  $x_2, \dots, x_t \in G$  tali che  $\text{ord}_G(x_i) = \text{ord}_{G/\langle x_1 \rangle}(\overline{x_i}) = p^{r_i}$ . Vogliamo mostrare allora che:

$$H = \langle x_2, \dots, x_t \rangle \cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$$

ovvero che il sottogruppo di  $G$  finitamente generato da  $x_2, \dots, x_t$  è isomorfo al prodotto diretto dei singoli sottogruppi ciclici generati dai medesimi elementi.<sup>17</sup> Consideriamo di nuovo la proiezione al quoziente modulo  $\langle x_1 \rangle$ , ma ristretta ad  $H$ :

$$\pi|_H : H \longrightarrow G/\langle x_1 \rangle \cong \langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle : a_2 x_2 + \dots + a_t x_t \longmapsto (a_2 \overline{x_2}, \dots, a_t \overline{x_t})$$

è un isomorfismo, infatti  $\pi$  è un omomorfismo, è surgettivo (in quanto si possono mandare tutti i generatori  $x_i$  di  $H$  nelle  $t$ -uple di generatori di  $G/\langle x_1 \rangle$ ); per l'iniettività si osserva che gli elementi del nucleo sono del tipo:

$$\pi(a_2 x_2 + \dots + a_t x_t) = (a_2 \overline{x_2}, \dots, a_t \overline{x_t}) = (0, \dots, 0) \iff a_i \overline{x_i} = 0 \quad \forall i \in \{2, \dots, t\}$$

cioè se e solo se  $\text{ord}_{G/\langle x_1 \rangle}(\overline{x_i}) = p^{r_i} \mid a_i$ , ma essendo anche che  $\text{ord}(x_i) = p^{r_i}$ , allora la divisibilità precedente è equivalente al chiedere  $a_i x_i = 0$ ,  $\forall i \in \{2, \dots, t\}$ . Segue che  $\pi|_H$  è un isomorfismo e si ha:

$$H \cong \langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle \cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle$$

<sup>15</sup>Dunque si ha  $|\langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle| = p^{n-r_1}$ .

<sup>16</sup>L'isomorfismo tra i due gruppi è quello che manda  $(G/\langle x_1 \rangle \ni) \bar{g} = a_2 \overline{x_2} + \dots + a_t \overline{x_t}$  (poiché  $G/\langle x_1 \rangle$  è finito è anche finitamente generato) in  $(a_2 \overline{x_2}, \dots, a_t \overline{x_t}) \in (\langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle)$ .

<sup>17</sup>Per fare questo mostriamo prima l'isomorfismo tra il gruppo finitamente generato e il prodotto  $\langle \overline{x_2} \rangle \times \dots \times \langle \overline{x_t} \rangle$ , e da ciò successivamente seguirà l'isomorfismo voluto.

<sup>18</sup>Qui stiamo usando ancora il [Lemma 1.91](#)



Dove l'ultimo isomorfismo deriva dal fatto che abbiamo scelto elementi di ordini uguali, che quindi generano gli stessi gruppi ciclici a meno di isomorfismo. Mostriamo che  $G \cong \langle x_1 \rangle \times H (\cong \langle x_2 \rangle \times \dots \times \langle x_t \rangle)$  e per farlo verifichiamo che le ipotesi del [Teorema 1.72](#) siano soddisfatte.

Per mostrare che l'intersezione è banale, consideriamo un elemento in quest'ultima, ovvero un elemento che può essere scritto come:

$$a_1 x_1 = a_2 x_2 + \dots + a_t x_t$$

con  $a_1$  e  $a_2, \dots, a_t$  fissati; applicando  $\pi_{\langle x_1 \rangle}$  alle due scritture si ha:

$$\bar{0} = a_2 \bar{x}_2 + \dots + a_t \bar{x}_t \iff (a_2 \bar{x}_2, \dots, a_t \bar{x}_t) = (\bar{0}, \dots, \bar{0})$$

in quanto  $G/\langle x_1 \rangle \cong \prod_{i=2}^t \langle \bar{x}_i \rangle$ , dunque l'unica possibilità di annullare la somma scritta è che  $a_i \equiv 0 \pmod{p^{r_i}}$  (ovvero  $a_i$  è multiplo dell'ordine di  $\bar{x}_i$ ),  $\forall i \in \{2, \dots, t\}$ , da ciò segue che nel gruppo di partenza  $x_i = 0$  (perché come prima  $p^{r_i}$  è ordine anche di  $x_i$ , pertanto se  $a_i$  è sempre un suo multiplo, allora tutti i fattori  $a_i x_i$  sono nulli),  $\forall i \in \{2, \dots, t\}$ , e quindi  $a_1 x_1 = 0$ , pertanto  $\langle x_1 \rangle \cap H = \{0\}$ . Per mostrare che  $\langle x_1 \rangle + H = G$ , osserviamo che  $\langle x_1 \rangle + H \subseteq G$  e che la sua cardinalità è:

$$|\langle x_1 \rangle + H| = \frac{|\langle x_1 \rangle| |H|}{|\langle x_1 \rangle \cap H|} = \frac{p^{r_1} \cdot p^{n-r_1}}{1} = p^n$$

Le ipotesi sono soddisfatte e quindi  $G \cong \langle x_1 \rangle \times H \cong \langle x_1 \rangle \times \dots \times \langle x_t \rangle$ .

**Unicità:** Sia  $|G| = p^n$  e procediamo ancora per induzione su  $n$ . Per  $n = 1$  segue sempre  $G \cong \mathbb{Z}/p\mathbb{Z}$  e quindi la tesi è verificata. Supponiamo la tesi vera per  $m < n$  e proviamola per  $n$ ; sia:

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{k_s}\mathbb{Z}$$

dove supponiamo  $r_1 \geq \dots \geq r_t$  e  $k_1 \geq \dots \geq k_s$ . Deve essere necessariamente che  $t = s$ , perché, considerando:

$$G_p = \{g \in G \mid pg = 0\}^{19}$$

con  $G_p$  gruppo caratteristico (poiché gli isomorfismi conservano gli ordini degli elementi) e quindi gli elementi di  $G$  di ordine che divide  $p$  stanno tutti in  $G_p$ , pertanto  $G_p$  è isomorfo ad un sottogruppo del tipo  $(\mathbb{Z}/p\mathbb{Z})^l$  (che è esattamente quello che contiene tutti e soli gli elementi con ordine che divide  $p$ ), con  $l$  numero dei fattori  $\mathbb{Z}/p^h\mathbb{Z}$  distinti, di entrambe le fattorizzazioni:

$$G_p \cong (\mathbb{Z}/p\mathbb{Z})^t \cong (\mathbb{Z}/p\mathbb{Z})^s \iff t = s$$

Quindi le lunghezze delle fattorizzazioni sono uguali, per concludere dobbiamo mostrare che anche le singole potenze di tutti i fattori sono a due a due uguali; possiamo applicare l'ipotesi induttiva al gruppo  $pG$  (con  $|pG| = p^{n-t}$ ):

$$\begin{aligned} pG &\cong \frac{p\mathbb{Z}}{p^{r_1}\mathbb{Z}} \times \dots \times \frac{p\mathbb{Z}}{p^{r_t}\mathbb{Z}} \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_t-1}\mathbb{Z} \cong \\ &\cong \mathbb{Z}/p^{k_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{k_t-1}\mathbb{Z} \cong \frac{p\mathbb{Z}}{p^{k_1}\mathbb{Z}} \times \dots \times \frac{p\mathbb{Z}}{p^{k_t}\mathbb{Z}} \end{aligned}$$

dove la sequenza di isomorfismi è valida perché stiamo assumendo ci siano due fattorizzazioni per  $G$  (e quindi anche per  $pG$ ), ma  $pG$  ha decomposizione unica (per ipotesi induttiva). dunque segue che:

$$r_1 - 1 = k_1 - 1, \dots, r_t - 1 = k_t - 1 \iff r_1 = k_1, \dots, r_t = k_t$$

e quindi i singoli fattori sono esattamente gli stessi. □

<sup>19</sup>Il sottogruppo degli elementi di  $G$  il cui ordine divide  $p$ .

**Osservazione 1.92** — Il [Lemma 1.91](#) non vale in generale per quozienti qualsiasi, ad esempio:

$$\mathbb{Z}/p^2\mathbb{Z}/\langle p \rangle \cong \frac{\mathbb{Z}/p^2\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z}$$

e con la proiezione:

$$\pi : \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \frac{\mathbb{Z}/p^2\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z} : 1 \longmapsto \bar{1}$$

con  $\bar{1}$  che ha ordine  $p$  nel gruppo di arrivo, mentre:

$$\pi^{-1}(\bar{1}) = \{1 + kp\}_{k=1, \dots, p-1}$$

con  $1 + kp$  che ha ordine  $p^2$ ,  $\forall k : 1 \leq k \leq p$ , dunque stiamo quozientando per un elemento che non ha ordine massimo; nelle condizioni del lemma, invece, stiamo quozientando per un elemento di ordine massimo.

## §1.14 Teorema di Sylow

**Osservazione 1.93** — Dato un gruppo  $G$  finito cosa possiamo dire dell'esistenza di elementi e sottogruppi di un certo ordine? Riepiloghiamo di seguito i principali risultati visti:

- $H \leq G \implies |H| \mid |G|$  (Teorema Di Lagrange).
- $\forall p$  primo tale che  $p \mid |G|$ ,  $\exists x \in G : \text{ord}_G(x) = p$  (Teorema Di Cauchy).
- Se  $G$  è ciclico,  $\forall d \mid |G|$ ,  $\exists x \in G : \text{ord}_G(x) = d$  (dalla definizione di gruppo ciclico).
- $G$  è ciclico se e solo se  $d = |G|$  (esiste  $x \in G$  tale che  $d = \text{ord}_G(x)$ ).
- Se  $G$  è abeliano  $\forall d \mid |G|$ ,  $\exists H \leq G$  tale che  $|H| = d$  (Lemma Di Ranieri).

L'ultimo fatto può essere ricavato (alternativamente) dal Teorema di Struttura, infatti:

$$G = G_{p_1} \times \dots \times G_{p_r}$$

con  $|G| = p_1^{e_1} \dots p_r^{e_r}$ , se  $d = p_1^{a_1} \dots p_r^{a_r}$ , bisogna verificare che per ogni  $i$  esiste  $H_{p_i} \leq G_{p_i}$  tale che  $|H_{p_i}| = p^{a_i}$ . Poiché:

$$G = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_s}\mathbb{Z} \quad \text{con } \sum n_i = e$$

possiamo costruire sottogruppi di ogni ordine<sup>20</sup>; inoltre, dato che  $G$  è abeliano il prodotto di sottogruppi è un sottogruppo:

$$H_{p_1} \dots H_{p_r} < H$$

e inoltre:

$$H_{p_1} \dots H_{p_r} \cong H_{p_1} \times \dots \times H_{p_r}$$

poiché  $H_{p_i} \cap H_{p_j} = \{e\}$ , dunque:

$$|H_{p_1} \dots H_{p_r}| = \prod |H_{p_i}| = \prod p_i^{a_i} = d$$

e quindi otteniamo il sottogruppo di ordine  $d$  voluto.

**Osservazione 1.94** — Se  $G$  non è abeliano e  $d \mid |G|$  non è detto che  $G$  abbia sottogruppi di ordine  $d$ .

<sup>20</sup>Ad esempio  $|H_p| = p^{72}$ , preso  $G_p = \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z}$ , può essere ottenuto come  $H_p = \mathbb{Z}/p^{30}\mathbb{Z} \times \mathbb{Z}/p^{30}\mathbb{Z} \times p^{18}\mathbb{Z}/p^{30}\mathbb{Z}$ .

**Esempio 1.95** ( $\mathcal{A}_4$  non contiene sottogruppi di ordine 6)

Sappiamo che  $|\mathcal{A}_4| = 4!/2 = 12$ , se  $\exists H < \mathcal{A}_4$  di ordine 6, allora  $H \triangleleft \mathcal{A}_4$ ; per [Cauchy](#)  $\exists x \in H : \text{ord}(x) = 2$ , con  $x = (a\ b)(c\ d)$ , deve essere quindi che:

$$\mathcal{C}\ell_{\mathcal{A}_4}(x) \subset H$$

poiché  $H \triangleleft \mathcal{A}_4$  e per definizione è unione di classi di coniugio in  $\mathcal{A}_4$ . Sappiamo che:

$$\mathcal{C}\ell_{\mathcal{A}_4}(x) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Visto che  $|\mathcal{C}\ell_{\mathcal{A}_4}((a\ b)(c\ d))| = 3$ , allora  $\mathcal{C}\ell_{\mathcal{A}_4}((a\ b)(c\ d)) = \mathcal{C}\ell_{S_4}((a\ b)(c\ d))$ , dunque se  $H \triangleleft \mathcal{A}_4 \implies H \supset \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = V$ <sup>a</sup>, allora  $V < H$ , ma  $4 \nmid 6 \implies$  assurdo.

<sup>a</sup> $V$  prende il nome di [gruppo di Klein](#) o [Klein 4-group](#).

**Lemma 1.96**

Sia  $G$  un  $p$ -gruppo e  $H \leq G$ , allora  $H \leq N_G(H)$ .

*Dimostrazione.* Essendo  $G$  un  $p$ -gruppo abbiamo che  $|G| = p^n$ . Procediamo per induzione su  $n$ . Se  $n = 0$  non c'è niente da dimostrare. Se  $n > 0$  consideriamo due casi:

- Se  $Z(G) \not\subseteq H$ , dato che  $H \cup Z(G) \subseteq N_G(H)$ , abbiamo che  $\emptyset \neq Z(G) \setminus H \subseteq N_G(H) \setminus H$  da cui la tesi.
- Se  $Z(G) \subseteq H$  osserviamo che  $Z(G)$  è normale in  $G$  e che  $Z(G)$  non è banale perché  $G$  è un  $p$ -gruppo, dunque possiamo considerare  $G/Z(G)$  di ordine strettamente minore all'ordine di  $G$ . Sia  $\pi : G \longrightarrow G/Z(G)$  la mappa di proiezione al quoziente. Per ipotesi induttiva  $N_{G/Z(G)}(H/Z(G))$  contiene strettamente  $H/Z(G)$ , quindi per il teorema di corrispondenza si ha che anche le loro controimmagini tramite  $\pi$  rispettano un contenimento stretto (perché si preservano gli indici). Sempre per corrispondenza  $\pi^{-1}(N_{G/Z(G)}(H/Z(G))) = H$ , quindi basta mostrare che  $\pi^{-1}(N_{G/Z(G)}(H/Z(G))) \subseteq N_G(H)$ , e questo deriva dal fatto che se  $g \in \pi^{-1}(N_{G/Z(G)}(H/Z(G)))$  allora  $gHg^{-1} \subseteq HZ(G) = H$ .<sup>21</sup>

□

**Definizione 1.97.** Dato  $G$  un gruppo finito e  $p$  un primo, tali che  $|G| = p^n m$ , con  $p^n \parallel |G|$ <sup>22</sup> e  $n \geq 1$  e  $(m, p) = 1$ , allora un sottogruppo di  $G$  di ordine  $p^n$  prende il nome di [p-sottogruppo di Sylow](#) ([p-Sylow](#)).<sup>23</sup>

<sup>21</sup>Dimostrazione proposta da Francesco Sorce.

<sup>22</sup>Il simbolo  $\parallel$  indica la divisibilità esatta, ovvero  $p^n$  è la massima potenza di  $p$  che divide  $|G|$ .

<sup>23</sup>I  $p$ -sottogruppi di Sylow possono anche essere pensati come  $p$ -sottogruppi di ordine massimale.

**Teorema 1.98 (Teorema Di Sylow)**

Sia  $G$  un gruppo finito, con  $|G| = p^n m$ , con  $p$  primo,  $n \geq 1$  e  $(m, p) = 1$ <sup>a</sup>, allora:

- (1)  $\forall \alpha : 0 \leq \alpha \leq n, \exists H \leq G : |H| = p^\alpha$ . (Esistenza)
- (2)  $\forall \alpha : 0 \leq \alpha \leq n - 1$ , ogni sottogruppo di ordine  $p^\alpha$  è contenuto in un sottogruppo di ordine  $p^{\alpha+1}$ . In particolare, ogni  $p$ -sottogruppo è contenuto in un  $p$ -sottogruppo di Sylow. (Inclusione)
- (3) Due qualunque  $p$ -sottogruppi di Sylow di  $G$  sono coniugati (quindi tutti i  $p$ -sottogruppi di ordine massimale sono isomorfi). (Coniugio)
- (4) Sia  $n_p$  il numero di  $p$ -sottogruppi di Sylow di  $G$ , allora: (Numero)

$$n_p \mid |G| \quad \text{e} \quad n_p \equiv 1 \pmod{p} \quad \text{e} \quad n_p = [G : N_G(S)]^b$$

<sup>a</sup>Ovvero  $p^n \parallel |G|$ , o anche  $\nu_p(|G|) = n$  (dove con  $\nu_p$  intendiamo la **valutazione  $p$ -adica**).

<sup>b</sup>Con  $S$  ci si riferisce a un qualsiasi  $p$ -Sylow, per un  $p$  fissato.

*Dimostrazione.* Dimostriamo tutte le affermazioni del teorema:

- (1) Dimostriamo che  $\forall \alpha : 0 \leq \alpha \leq n$  esiste almeno un sottogruppo di ordine  $p^\alpha$ ; sia  $\mathcal{M} = \{X \subset G \mid |X| = p^\alpha\}$ , allora:

$$|\mathcal{M}| = \binom{|G|}{p^\alpha} = \binom{p^n m}{p^\alpha} = \frac{p^n m (p^n m - 1) \dots (p^n m - p^\alpha + 1)}{p^\alpha (p^\alpha - 1) \dots (p^\alpha - p^\alpha + 1)}^{24}$$

Possiamo riscrivere il prodotto dei termini nel modo seguente:

$$\prod_{i=0}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i}$$

dove nell'ultimo passaggio abbiamo raccolto il primo termine,  $p^{n-\alpha} m$ , e lo abbiamo portato fuori dalla produttoria.

Osserviamo a questo punto che  $p^{n-\alpha}$  è la più grande potenza di  $p$  che divide  $|\mathcal{M}|$ <sup>25</sup>, infatti, si osserva che  $p \nmid \prod_{i=1}^{p^\alpha-1} \frac{p^n m - i}{p^\alpha - i}$ , cioè  $\forall i \in \{1, \dots, p^\alpha - 1\}$  si ha che  $p \nmid \frac{p^n m - i}{p^\alpha - i}$ , come si osserva infatti:

$$\nu_p(p^n m - i) = \nu_p(p^\alpha - i) = \nu_p(i)$$

dunque, se  $p \nmid i \implies p^n m - i$  e  $p^\alpha - i$  non sono divisibili per  $p$ ; se fosse  $i = p^k j$ , con  $(j, p) = 1$ , allora  $p^\alpha - i = p^\alpha - p^k j = p^k \underbrace{(p^{\alpha-k} - j)}_{\text{non divisibile per } p}$ , con  $k < \alpha$ , (analogamente

per  $p^n m - i$ ), per quanto abbiamo detto deve essere necessariamente che:

$$p^{n-\alpha} \parallel |\mathcal{M}|$$

ovvero  $p^{n-\alpha}$  è l'esatta potenza di  $p$  che divide  $|\mathcal{M}|$ . Consideriamo  $M \in \mathcal{M}$ , allora  $gM \in \mathcal{M}, \forall g \in G$ , dunque possiamo considerare l'azione:

$$\phi : G \longrightarrow S(\mathcal{M}) : g \longmapsto \varphi_g$$

<sup>24</sup>Si osserva che abbiamo semplificato al numeratore e al denominatore il termine  $(p^n m - p^\alpha)!$ .

<sup>25</sup>O anche  $p^{n-\alpha} \parallel |\mathcal{M}|$ , o ancora  $\nu_p(|\mathcal{M}|) = n - \alpha$ .

dove  $\varphi_g : \mathcal{M} \longrightarrow \mathcal{M} : M \longmapsto gM$  è una bigezione. Data l'azione  $\phi$  sappiamo che:

$$\mathcal{M} = \bigcup_{i=1}^s \text{Orb}(M_i) \implies |\mathcal{M}| = \sum_{i=1}^s |\text{Orb}(M_i)| = \sum_{i=1}^s \frac{|G|}{|\text{St}(M_i)|}$$

unendo ciò a quanto detto si ha che  $p^{n-\alpha} \parallel \sum_{i=1}^s \frac{|G|}{|\text{St}(M_i)|}$ , quindi non tutte le orbite possono essere divisibili per una potenza maggiore di  $p^{n-\alpha}$ , ovvero esiste almeno un  $i$  tale per cui  $p^{n-\alpha+1} \nmid |\text{Orb}(M_i)|$  (ovvero non può essere diviso per una potenza più grande di quanto detto), da ciò segue:  $p^{n-\alpha+1} \nmid |\text{Orb}(M_i)| = \frac{|G|}{|\text{St}(M_i)|} = \frac{p^n m}{|\text{St}(M_i)|}$ , pertanto deve essere necessariamente che:

$$p^\alpha \mid |\text{St}(M_i)| = t$$

cioè, affinché il rapporto non sia divisibile per  $p^\alpha$ , al denominatore deve esserci una potenza di  $p$  maggiore o uguale ad  $\alpha$ . D'altra parte, sia  $x \in M_i$ , la funzione:

$$\varphi_x : \text{St}(M_i) \longrightarrow M_i : y \longmapsto yx$$

è iniettiva<sup>26</sup>, dunque  $t = |\text{St}(M_i)| \leq |M_i| = p^\alpha$ , segue quindi  $t = p^\alpha$ , pertanto  $\text{St}(M_i)$  è il sottogruppo di ordine  $p^\alpha$  cercato.

- (2) Sia  $S$  un  $p$ -sottogruppo di Sylow di  $G$ , con  $|S| = p^n$ , e sia  $H \leq G$ , con  $|H| = p^\alpha$ ; consideriamo l'insieme  $G/S = X$  dato dalle classi laterali di  $S$  in  $G$ , allora:

$$|X| = [G : S] = \frac{p^n m}{p^n} = m$$

Consideriamo l'azione di  $H$  su  $X$  data da:

$$\varphi : H \longrightarrow S(X) : h \longmapsto \varphi_h$$

con  $\varphi_h : X \longrightarrow X : gS \longmapsto hgS$  bigezione; per la formula delle classi si ha:

$$m = |X| = \sum_{i=1}^r |\text{Orb}(g_i S)| = \sum_{i=1}^r \frac{|H|}{|\text{St}(g_i S)|} = \sum_{i=1}^r p^{a_i}$$

(essendo  $p$ -gruppi). Poiché per ipotesi  $p \nmid m$ , allora esiste  $i$  tale che  $a_i = 0$  (dunque c'è un 1 nella fattorizzazione che impedisce la divisibilità di  $m$  per  $p$ )  $\implies \text{Orb}(g_i S) = \{g_i S\} \implies \text{St}(g_i S) = H$  (ovvero per tale  $i$  si ha una classe laterale  $g_i S$  la cui orbita è solo se stessa, e quindi il suo stabilizzatore è tutto  $H$ ). Da ciò segue che  $\forall h \in H$ :

$$hg_i S = g_i S \iff hg_i \in g_i S \iff h \in g_i S g_i^{-1} \iff H \subset g_i S g_i^{-1}$$

dove  $|g_i S g_i^{-1}| = |S|$  dunque  $g_i S g_i^{-1}$  è un  $p$ -Sylow ed  $H$  di ordine  $p^\alpha$  è contenuto in un  $p$ -Sylow. Questo dimostra il punto (3), ovvero due  $p$ -Sylow di  $G$  sono coniugati, infatti la relazione trovata vale per ogni  $\alpha$  ed in particolare prendendo  $|H| = p^n \implies H \leq g_i S g_i^{-1}$  ma i due sottogruppi hanno lo stesso ordine, quindi  $H = g_i S g_i^{-1}$ ; pertanto, tutti i  $p$ -Sylow per ogni  $p$  sono coniugati tra loro in  $G$ .

Per completare la dimostrazione del punto (2) utilizziamo il risultato del [Lemma 1.95](#), considerando  $|H| = p^\alpha$ , con  $\alpha \leq n-1$  e  $H \leq S$  (stiamo supponendo che

<sup>26</sup>Si vede che  $\varphi_x(y) = \varphi_x(z) \iff yx = zx \iff y = z$ .

$H$  stia in  $S$ ), dunque  $H \leq N_S(H)$  <sup>27</sup>, sia ora  $\frac{N_S(H)}{H}$ , esso è un  $p$ -gruppo non banale e per il [Teorema di Cauchy](#) esiste una classe laterale  $\bar{x}(=xH)$  di ordine  $p$ , infine, per il Teorema di Corrispondenza <sup>28</sup>,  $\pi_H^{-1}(\langle \bar{x} \rangle)$  è un sottogruppo di  $N_S(H)$  che contiene  $H$  (sempre per il Teorema Di Corrispondenza) ed ha ordine  $p^{\alpha+1}$  (poiché stiamo considerando la controimmagine di un sottogruppo con  $p$  elementi, ciascuno dei quali fatto da classi laterali di  $p^\alpha$  elementi, dunque la cardinalità della controimmagine si ottiene moltiplicando la fibra di ciascun elemento, che appunto ha ordine  $p^\alpha$ , per il numero di elementi  $p$ ).

- (4) Sia  $n_p$  il numero dei  $p$ -sottogruppi di Sylow, per quanto detto al punto (3) i  $p$ -sottogruppi di Sylow sono tutti coniugati, dunque per ciò che abbiamo visto sul numero di coniugi rispetto all'azione di coniugio si ha  $n_p = |\mathcal{Cl}(S)| = [G : N_G(S)]$ , da cui:

$$n_p = \frac{|G|}{|N_G(S)|} \implies |G| = n_p |N_G(S)| \implies n_p \mid |G|$$

Sia  $X$  l'insieme dei  $p$ -Sylow di  $G$ , consideriamo l'azione di coniugio:

$$\phi : S \longrightarrow S(X) : s \longmapsto \varphi_s$$

con  $\varphi_s : X \longrightarrow X : H \longmapsto sHs^{-1}$  bigezione;  $\phi$  ha un'unica orbita banale, ovvero quella del gruppo  $S$ ,  $\text{Orb}(S) = \{S\}$ , infatti, per ogni altra orbita si ha:

$$\text{Orb}(H) = \{sHs^{-1} \mid s \in S\} = \{H\} \iff sHs^{-1} = H \quad \forall s \in S$$

ovvero:

$$S \subset N_G(H)$$

ma sappiamo anche che  $H \leq N_G(H)$ , pertanto si deve avere che:

$$HS < N_G(H)$$

(poiché  $S$  normalizza  $H$  il prodotto di sottogruppi da un sottogruppo), ma questo è assurdo se  $S \neq H$ , perché avremmo:

$$|SH| = \frac{|S||H|}{|S \cap H|} = \frac{p^n \cdot p^n}{p^k} \stackrel{29}{=} p^{2n-k} \nmid |G|$$

Quindi esiste un'unica orbita banale e applicando la formula delle classi otteniamo:

$$n_p = |X| = \sum_{i=1}^r \underbrace{|\text{Orb}(H_i)|}_{p^{a_i} \neq 1} + \underbrace{|\text{Orb}(S)|}_{=1} = pf + 1 \quad f \in \mathbb{Z}$$

o equivalentemente  $n_p \equiv 1 \pmod{p}$ .

□

<sup>27</sup>Si noti che abbiamo preso il normalizzatore di  $H$  in  $S$ .

<sup>28</sup>Tra i sottogruppi di  $\frac{N_S(H)}{H}$  ed i sottogruppi di  $N_S(H)$  che contengono  $H$ .

<sup>29</sup> $k < n$ .

**Corollario 1.99**

Sia  $G$  un gruppo abeliano finito,  $\forall p$  primo tale che  $p \mid |G|$ ,  $G(p)$  è l'unico  $p$ -Sylow di  $G$ . Inoltre  $G$  è il prodotto diretto dei suoi  $p$ -Sylow:

$$G \cong G(p_1) \times \dots \times G(p_r)$$

con  $|G| = \prod p_i^{e_i}$ .

*Dimostrazione.*

□

**Esempio 1.100** (Classificazione dei gruppi di ordine 12)

Poiché  $12 = 2^2 \cdot 3$ , per Sylow, sappiamo che  $\exists P_2, P_3$ , con  $P_2$  2-Sylow,  $P_3$  3-Sylow e  $|P_2| = 4$ ,  $|P_3| = 3$ ; abbiamo che  $P_2 \cap P_3 = \{e\}$  poiché  $p$ -gruppi distinti, dunque  $G = P_2 P_3$ , in quanto:

$$|P_2 P_3| = \frac{|P_2| |P_3|}{|P_2 \cap P_3|} = \frac{4 \cdot 3}{1} = 12$$

inoltre, almeno uno tra  $P_2$  e  $P_3$  è normale. Se  $P_3 \triangleleft G$  allora abbiamo un sottogruppo normale; se  $P_3 \not\triangleleft G$ , allora osserviamo che, per quanto detto al punto (4) del [Teorema Di Sylow](#), possiamo avere solo che  $n_3 = 1, 4$ , ma non essendo  $P_3$  normale  $n_3$  non può essere 1, dunque  $n_3 = 4$ ; da ciò segue che in  $G$  ci sono 8 elementi di ordine  $3^a$  e 4 elementi di ordine diverso da 3, che quindi formano l'unico 2-Sylow, equivalentemente  $n_2 = 1$ , e quindi  $P_2$  è normale. Osserviamo che supponendo invece  $P_2 \not\triangleleft G$ , si arriva simmetricamente a concludere che  $P_3 \triangleleft G$ , pertanto uno dei due sottogruppi di Sylow è necessariamente normale e in entrambi i casi sono soddisfatte le ipotesi del [Teorema 1.78](#), segue che  $G$  è un prodotto semidiretto tra  $P_2$  e  $P_3$ . Studiamo separatamente i due casi.

---

<sup>a</sup> $4 \cdot 3 - 4 = 8$ .



**Esempio 1.101** ( $G \cong P_2 \rtimes_{\varphi} P_3$ )

Se  $P_2 \triangleleft G$ , allora  $G \cong P_2 \rtimes_{\varphi} P_3$ .  $P_2$  ha ordine 4, dunque è  $\mathbb{Z}/4\mathbb{Z}$  o  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , mentre  $P_3$  è necessariamente  $\mathbb{Z}/3\mathbb{Z}$ ; nel primo caso abbiamo:

$$\mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} \quad \text{con} \quad \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

in questo caso l'unica possibilità è  $[1]_3 \mapsto id$ , dunque il prodotto semidiretto è in realtà sempre un prodotto diretto, dunque il primo gruppo trovato è:

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$$

nel secondo caso abbiamo:

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} \quad \text{con} \quad \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

a questo punto, possiamo o mandare  $[1]_3 \mapsto id$  ottenendo il prodotto diretto:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

oppure mandare  $[1]_3$  in un altro elemento il cui ordine divida 3 (in questo caso uno dei due 3-cicli), dunque abbiamo due scelte per  $\varphi([1]_3)$ ; entrambe le scelte danno origine a due prodotti semidiretti isomorfi<sup>a</sup>. Osserviamo che abbiamo:

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} = G \hookrightarrow S_4$$

infatti,  $G$  agisce per coniugio sull'insieme  $\{P_3, P'_3, P''_3, P'''_3\}$  dei quattro 3-Sylow di  $G$ , pertanto abbiamo l'azione transitiva  $\phi : G \longrightarrow S(X) \cong S_4$ , con  $\ker \phi = \{id\}$  (dunque è un'azione fedele). Si verifica facilmente che l'unica possibilità è che  $G$  sia isomorfo al gruppo alternante di 4 elementi, dunque abbiamo ottenuto il gruppo:

$$\mathcal{A}_4$$

<sup>a</sup>Come nel caso dei gruppi di ordine  $pq$ .

**Esempio 1.102** ( $G \cong P_3 \rtimes_{\varphi} P_2$ )

Se  $P_3 \triangleleft G$ , allora  $G \cong P_3 \rtimes_{\varphi} P_2$ . Analogamente a quanto visto prima  $P_2$  ha ordine 4, dunque è  $\mathbb{Z}/4\mathbb{Z}$  o  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , e  $P_3$  è  $\mathbb{Z}/3\mathbb{Z}$ . Il primo prodotto che abbiamo è:

$$\mathbb{Z}/3\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z} \quad \text{con} \quad \varphi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

dunque  $[1]_4 \mapsto id, -id$ , nel primo caso riotteniamo il prodotto diretto e  $\mathbb{Z}/12\mathbb{Z}$ , nel secondo caso invece otteniamo un prodotto semidiretto che ci dà il gruppo:

$$\mathbb{Z}/3\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z}$$

L'ultimo prodotto possibile è:

$$\mathbb{Z}/3\mathbb{Z} \rtimes_{\varphi} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \quad \text{con} \quad \varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

se mandassimo tutti gli elementi nell'identità otterremmo un prodotto diretto, alternativamente, riscrivendo  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  come  $\langle x \rangle \times \langle y \rangle$  (i cui elementi saranno  $\{e, x, y, xy\}$ ), abbiamo due elementi di ordine 2 che vanno in  $-id$  e l'elemento neutro e un altro elemento di ordine 2 che vanno in  $id$ . Possiamo dunque costruire tre prodotti semidiretti che danno origine a gruppi isomorfi, supponiamo (WLOG) che:

$$\varphi_x = id \quad \varphi_y = -id \quad \varphi_{xy} = -id$$

dunque abbiamo:

$$\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{e} \quad \langle z \rangle \cong \mathbb{Z}/3\mathbb{Z}$$

possiamo osservare che:

$$\varphi_x(z) = xzx^{-1} = id(z) = z \implies x \text{ commuta con } z$$

similmente:

$$\varphi_y(z) = yzy^{-1} = -id(z) = -z$$

dunque il sottogruppo generato da  $y$  e  $z$  è:

$$\langle y, z | y^2 = 1, z^3 = 1, yzy^{-1} = z^{-1} \rangle \cong D_3$$

quindi il gruppo che si ottiene con i tre prodotti semidiretti è  $\mathbb{Z}/2\mathbb{Z} \times D_3$  (il prodotto diretto deriva dal fatto che  $x$  commuta sia con  $y$  che con  $z$ ), ovvero:

$$D_6$$

Abbiamo quindi classificato tutti i gruppi di ordine 12:

$$\mathbb{Z}/12\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad \mathcal{A}_4 \quad \mathbb{Z}/3\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z} \quad D_6$$

## §1.15 Gruppo dei Quaternioni

**Definizione 1.103.** Si definisce gruppo dei **quaternioni** il gruppo con la seguente presentazione:

$$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = j^3i \rangle$$

**Osservazione 1.104 (Ordini di  $i$  e  $j$ )** — Osserviamo che  $\text{ord}(i) = 4$ , per la definizione che ne abbiamo dato, da ciò si ricava che, essendo  $j^2 = i^2$ , allora  $j^4 = 1 \implies \text{ord}(j) \mid 4$ , ciò unito al fatto che:

$$\text{ord}(j^2) = \frac{\text{ord}(j)}{(2, \text{ord}(j))} = \text{ord}(i^2) = 2$$

implica che  $\text{ord}(j) = 4$ . Dunque abbiamo due gruppi ciclici di ordine 4,  $\langle i \rangle$  e  $\langle j \rangle$ , con  $\langle i \rangle \cap \langle j \rangle = \{1, i^2 = j^2\}$ .

Dalla presentazione del gruppo, sappiamo che  $Q_8 = \langle i \rangle \langle j \rangle$  dunque possiamo stabilire l'ordine:

$$|Q_8| = |\langle i \rangle \langle j \rangle| = \frac{|\langle i \rangle| |\langle j \rangle|}{|\langle i \rangle \cap \langle j \rangle|} = \frac{4 \cdot 4}{2} = 8$$

quindi il gruppo dei quaternioni ha 8 elementi, dati da:

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

**Osservazione 1.105** —  $Q_8$  non è abeliano perché:

$$ij = j^3i = j^{-1}i \neq ji$$

**Osservazione 1.106** — Osserviamo che  $\langle i \rangle, \langle j \rangle \triangleleft Q_8$  perché hanno indice 2, inoltre  $\langle i^2 \rangle, \langle j^2 \rangle \triangleleft Q_8$  (per verifica diretta).

Ricordando che un sottogruppo di ordine 2 è normale se e solo se è un sottogruppo di  $Z(G)$  <sup>30</sup>, possiamo osservare che:

**Osservazione 1.107** —  $\langle i^2 \rangle = Z(Q_8)$ , infatti, per quanto detto si deve avere che  $\langle i^2 \rangle \leq Z(Q_8)$ , inoltre  $Q_8$  è un  $p$ -gruppo non abeliano, ed essendo  $|Q_8| = p^3$  segue che:

$$|Z(Q_8)| = \begin{cases} 1 & \text{assurdo per quanto detto sui } p\text{-gruppi} \\ p & \\ p^2 & \text{ma allora } Q_8/Z(Q_8) \text{ ciclico} \implies Q_8 \text{ abeliano} \\ p^3 & \implies Z(Q_8) = Q_8, \text{ assurdo} \end{cases}$$

ovvero  $|Z(Q_8)| = 2$  e quindi è proprio  $\langle i^2 \rangle$ .

Posto convenzionalmente  $ij = k$ , gli elementi si possono riscrivere anche come:

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

con  $i^2 = -1, i^3 = -i, j^2 = -1, j^3 = -j, k^2 = -1, k^3 = -k$ .

<sup>30</sup>Infatti, preso  $H = \{e, h\} \leq G$ , allora  $ghg^{-1} = H, \forall g \in G$ , ovvero  $ghg^{-1} \in H \iff ghg^{-1} = h \iff gh = hg, \forall g \in G$ , dunque  $h \in Z(G)$  (nel caso in cui  $ghg^{-1} = e$ , allora  $h = e$ , e ovviamente appartiene al centro), pertanto  $H \leq Z(G)$ .

**Osservazione 1.108 (Prodotto in  $Q_8$ )** — I prodotti tra gli elementi di  $Q_8$  seguono il 3-ciclo:



che percorso in senso orario ci dà i prodotti:

$$ij = k \quad jk = i \quad ki = j$$

ed in senso antiorario:

$$ji = -k \quad ik = -j \quad kj = -i$$

Le operazioni fatte in questo modo sono equivalenti a quelle che si ottengono con le regole di commutazione della presentazione, ad esempio:

$$k^2 = (ij)^2 = ijij = ijj^3i = i^2$$

**Osservazione 1.109 (Ordine degli elementi)** — Dunque in  $Q_8$  1 ha ordine 1,  $-1$  ha ordine 2, mentre  $i, -i, j, -j, k, -k$  hanno ordine 4.

Abbiamo visto che  $Q_8$  è un gruppo di ordine 8 non è abeliano, e per quanto detto  $Q_8 \not\cong D_4$ , poiché  $Q_8$  ha sei elementi di ordine 4, mentre  $D_4$  ne ha soltanto uno.

**Osservazione 1.110 (Sottogruppi di  $Q_8$ )** — Per quanto riguarda i sottogruppi di  $Q_8$  osserviamo in primis che  $\langle -1 \rangle = Z(Q_8)$  ed è caratteristico (perché è il centro oppure perché è l'unico sottogruppo di ordine 2);  $\langle i \rangle, \langle j \rangle, \langle k \rangle$  sono sottogruppi di ordine 4, dunque sono normali. Abbiamo quindi dimostrato che tutti i sottogruppi (incluso ovviamente quelli banali) di  $Q_8$  sono normali.

Concludiamo la discussione su  $Q_8$  osservando che non può essere prodotto semidiretto di due suoi sottogruppi, infatti  $\forall H_1, H_2 \leq Q_8$  si ha  $H_1 \cap H_2 \neq \{1\}$ , infatti, l'intersezione contiene sempre il sottogruppo  $\{1, -1\}$ .

**Esercizio 1.111.** Dimostrare che  $Q_8 \hookrightarrow GL_2(\mathbb{C})$ .

*Soluzione.*

□

A questo punto siamo pronti per classificare tutti i gruppi di ordine 8:

**Esempio 1.112 (Classificazione dei gruppi di ordine 8)**

Distinguiamo innanzitutto i gruppi in base all'abelianità:

- Se  $G$  è abeliano, allora per il nel [Teorema di Struttura](#) abbiamo che  $G \cong G(2)$  e per la 2-componente abbiamo le seguenti possibilità:

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

- Se  $G$  non è abeliano, allora ha almeno un elemento di ordine 4 (se avesse tutti elementi di ordine 2 sarebbe isomorfo a  $(\mathbb{Z}/2\mathbb{Z})^3$ ), sia  $a \in G$  tale che  $\text{ord}(a) = 4$ , allora  $\langle a \rangle \triangleleft G$  e:

$$G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\} \quad b \in G \setminus \langle a \rangle$$

dove deve essere  $b^2\langle a \rangle = \langle a \rangle$ , infatti se fosse  $b^2\langle a \rangle = b\langle a \rangle \implies b\langle a \rangle = \langle a \rangle \implies b \in \langle a \rangle$ , che è assurdo, dunque:

$$b^2\langle a \rangle = \langle a \rangle \implies b^2 \in \{e, a, a^2, a^3\}$$

ma non può essere che  $b^2 = a, a^3$ , altrimenti  $b$  avrebbe ordine 8, dunque rimangono soltanto i casi  $b^2 = 1$  e  $b^2 = a^2$ .

- (1) Se  $a^4 = 1$  e  $b^2 = 1$ , allora  $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$  da cui (si verificano facilmente le ipotesi del [Teorema 1.78](#)) segue:

$$G \cong \langle a \rangle \rtimes_{\varphi} \langle b \rangle \cong D_4$$

dove  $\varphi : \langle b \rangle \longrightarrow \text{Aut}(\langle a \rangle) \cong \mathbb{Z}/2\mathbb{Z} : b \longmapsto \varphi_b$  e  $\varphi_b : \langle a \rangle \longmapsto \langle a \rangle : a \longmapsto a^{-1}$  (ovvero  $\varphi_b = -id$ , se avessimo scelto l'identità avremmo ottenuto uno dei prodotti diretti già visti sopra).

- (2) Se  $a^4 = 1$  e  $b^2 = a^2$ , osserviamo che  $bab^{-1} \in \langle a \rangle$  (essendo il generato da  $a$  normale in  $G$ ), inoltre non può essere che  $bab^{-1} = 1$  (altrimenti  $a = 1$ ) o  $bab^{-1} = a^2$  (poiché il coniugio conserva l'ordine degli elementi) e non può nemmeno essere che  $bab^{-1} = a$  (poiché abbiamo supposto che  $G$  non sia commutativo). Pertanto abbiamo necessariamente  $bab^{-1} = a^3 \iff ba = a^3b$ , da cui segue:

$$G \cong Q_8$$

dove l'isomorfismo manda  $a \longmapsto i$  e  $b \longmapsto j$ .

Dunque i gruppi di ordine 8 sono:

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad D_4 \quad Q_8$$

**Esercizio 1.113.** Determinare il minimo  $n$  tale che  $Q_8 \hookrightarrow S_n$ .

*Soluzione.* Osserviamo inizialmente che per il [Teorema di Cayley](#)  $n \leq 8$  e che per quello di Lagrange l'ordine dell'immagine di  $Q_8$  deve dividere quello di  $S_n$ , pertanto  $n \geq 4$ , dunque abbiamo un numero finito di possibilità:

$$S_4, S_5, S_6, S_7, S_8$$

Se  $Q_8$  si immergesse in  $S_4$ , con  $|S_4| = 2^3 \cdot 3$ , sarebbe un suo 2-Sylow; poiché  $D_n$  si immerge sempre in  $S_n$  <sup>31</sup>, sappiamo che  $D_4 \hookrightarrow S_4$ , ed in particolare  $D_4$  è un 2-Sylow di  $S_4$ , ma ciò significa che  $Q_8$  non è in  $S_4$ , poiché non è un coniugato di  $D_4$ .

Si ragiona in maniera analoga per  $S_5$ , infatti  $|S_5| = 2^3 \cdot 3 \cdot 5$  e  $D_4 \subset S_4 \subset S_5$ , dunque i due 2-Sylow di  $S_4$  sono isomorfi a quelli di  $S_5$ , ed ancora una volta ciò significa che  $Q_8$  non si immerge nel gruppo.

Sia  $|S_6| = 2^4 \cdot 3^2 \cdot 5$ , detto  $P_2$  un 2-Sylow di  $S_6$ , osserviamo che se fosse  $Q_8 \hookrightarrow S_6$ , dovremmo avere:

$$i \mapsto \sigma \quad j \mapsto \rho \quad k \mapsto \sigma\rho = \eta$$

con  $\text{ord}(\sigma) = \text{ord}(\rho) = 4$  e  $\sigma^2 = \rho^2 = \eta^2$ , dove  $\text{ord}(\sigma^2) = \text{ord}(\rho^2) = \text{ord}(\eta^2) = 2$ . Osserviamo che le permutazioni di ordine 4 in  $S_6$  possono essere soltanto 4-cicli o 4-cicli uniti a 2-cicli, mentre le permutazioni di ordine 2 sono prodotto di trasposizioni (al più tre, essendo in  $S_6$ ).

**Osservazione 1.114** — Osserviamo che una permutazione è un quadrato se e solo se i cicli di lunghezza pari compaiono a coppie. Infatti:

- Se  $\eta$  è un  $k$ -ciclo, con  $k$  dispari,  $\eta$  è un quadrato di un  $k$ -ciclo, ovvero:

$$\eta = \eta^{k+1} = \left( \eta^{\frac{k+1}{2}} \right)^2$$

Se  $\eta$  è un  $k$ -ciclo, con  $k$  pari, allora si verifica che:

$$(a_1 \dots a_k)(b_1 \dots b_k) = (a_1 b_1 \dots a_k b_k)^2$$

- Se  $x^2 = (\eta_1 \dots \eta_2)^2 = \eta_1^2 \dots \eta_s^2$ , allora otteniamo cicli di lunghezza dispari e coppie di cicli.

Ad esempio, in  $S_6$ , una coppia di 3-cicli può essere sia un quadrato di un ciclo di lunghezza pari, sia il quadrato di altri due 3-cicli:

$$(1 \ 2 \ 3)(4 \ 5 \ 6) = (1 \ 4 \ 2 \ 5 \ 3 \ 6)^2 = ((1 \ 2 \ 3)(4 \ 5 \ 6))^2$$

mentre in  $S_4$  una coppia di cicli di lunghezza pari può essere soltanto il quadrato di un 4-ciclo:

$$(1 \ 2)(3 \ 4) = ((1 \ 4 \ 2 \ 3))^2 = ((1 \ 3 \ 2 \ 4))^2$$

Dunque il fatto che  $\sigma^2 = \rho^2 = \eta^2$  hanno ordine 2 (quindi sono fatte da sole trasposizioni) e che sono quadrati (quindi i cicli di lunghezza pari compaiono a coppie), ci dice che le trasposizioni sono prodotti di un numero pari di trasposizioni, pertanto l'unica possibilità è che:

$$\sigma^2 = \rho^2 = \eta^2 = (a \ b)(c \ d)$$

<sup>31</sup>In tal caso infatti basta mandare  $x \in D_4$  nella corrispondente permutazione dei vertici.

Risolvendo  $x^2 = (1\ 2)(3\ 4)$ , otteniamo:

$$x_1 = (1\ 3\ 2\ 4) \quad x_2 = (1\ 4\ 2\ 3) \quad x_3 = (1\ 3\ 2\ 4)(5\ 6) \quad x_4 = (1\ 4\ 2\ 3)(5\ 6)$$

abbiamo quindi 4 soluzioni in  $S_6$ , mentre in  $Q_8$  ne avevamo 6, pertanto nemmeno  $S_6$  contiene una copia isomorfa di  $Q_8$ .

$Q_8$  non si immerge nemmeno in  $S_7$  perché i 2-Sylow di  $S_7$  sono isomorfi a quelli di  $S_6$ , e quindi siamo nello stesso caso di prima.

Dunque per esclusione deve essere necessariamente che:

$$Q_8 \hookrightarrow S_8 \implies n = 8$$

Per Cayley l'immersione è di  $Q_8$  in  $S(Q_8)$ , dunque la mappa che realizza ciò è data da:

$$i \mapsto \varphi_i \quad \text{con} \quad \varphi_i : Q_8 \rightarrow Q_8 : x \mapsto ix$$

in particolare con la notazione dei cicli abbiamo che l'immagine di  $\varphi_i$  di  $Q_8$  è data da:

$$(1\ i\ -1\ i)(j\ k\ -j\ -k)$$

analogamente per  $\varphi_j(Q_8)$ :

$$(1\ j\ -1\ -j)(i\ -k\ -i\ k)$$

e numerando in qualsiasi ordine gli elementi di  $Q_8$  possiamo scrivere le permutazioni corrispondenti in  $S_8$ :

$$i \mapsto (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \quad j \mapsto (1\ 5\ 2\ 6)(3\ 8\ 4\ 7)$$

□

**Esempio 1.115** (Classificazione dei gruppi di ordine 30)

Osserviamo che  $|G| = 2 \cdot 3 \cdot 5$  e distinguiamo due casi:

- Se  $G$  è abeliano, allora per il [Teorema di Struttura](#)  $G \cong G(2) \times G(3) \times G(5)$ , dunque l'unica possibilità è che il gruppo sia ciclico:

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}$$

- Se  $G$  non è abeliano, osserviamo che (in generale)  $30 = 2d$ , con  $d$  dispari, dunque  $G$  ha un sottogruppo di ordine 15, che è normale in quanto ha indice 2 ed è ciclico, in quanto è un gruppo di ordine  $pq$  con  $p \nmid q - 1$ , pertanto  $G$  contiene una copia isomorfa di  $\mathbb{Z}/15\mathbb{Z}$ . Per [Cauchy](#) esiste un elemento di ordine 2 e quindi anche una copia isomorfa a  $\mathbb{Z}/2\mathbb{Z}$  in  $G$  (in particolare potevamo prendere direttamente il 2-Sylow), dunque i due gruppi verificano le ipotesi del [Teorema 1.78](#), da cui: <sup>a</sup>

$$G \cong \mathbb{Z}/15\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$

con:

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong \mathbb{Z}/15\mathbb{Z}^* \cong \mathbb{Z}/3\mathbb{Z}^* \times \mathbb{Z}/5\mathbb{Z}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

dove abbiamo che  $[1]_2 \mapsto \varphi_y$ , e adottando la notazione moltiplicativa,  $\varphi_y : \mathbb{Z}/15\mathbb{Z} \mapsto \mathbb{Z}/15\mathbb{Z} : \bar{x} \mapsto \bar{x}^l$ , abbiamo  $\text{ord}(\varphi_y) \mid 2$ , dunque ci sono due possibilità, o  $\varphi_y = id$  (quindi  $l = 1$ ), o  $\varphi_y^2 = id \implies \varphi_y^2(x) = (x^l)^l = x^{l^2} = x$ , da cui segue (essendo  $x$  un generatore di  $\mathbb{Z}/15\mathbb{Z}$ ):

$$l^2 \equiv 1 \pmod{15} \implies x \equiv \pm 1, \pm 4 \pmod{15}$$

Dunque, per  $l = 1$  otteniamo il prodotto diretto già trovato sopra, per gli altri tre possibili  $l$  invece otteniamo 3 gruppi non isomorfi di ordine 30, infatti, per  $l = -1$ , abbiamo:

$$\varphi_y(x) = x^{-1} \iff yxy^{-1} = x^{-1} \implies \mathbb{Z}/15\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z} \cong D_{15}$$

Per  $l = 4$  invece si ottiene  $D_5 \times \mathbb{Z}/3\mathbb{Z}$  e per  $l = -4$  si ottiene  $D_3 \times \mathbb{Z}/5\mathbb{Z}$  <sup>b</sup>, i quali sono gruppi non isomorfi, ad esempio perché hanno centri diversi:

$$Z(D_{15}) = \langle id \rangle \quad Z(D_5 \times \mathbb{Z}/3\mathbb{Z}) = Z(D_5) \times Z(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$$

$$Z(D_3 \times \mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$$

<sup>a</sup>La direzione del prodotto semidiretto è data dal fatto che  $\mathbb{Z}/15\mathbb{Z}$  è l'unico normale tra i due sottogruppi.

<sup>b</sup>Andrebbe aggiunto il perché ma non è chiarissimo dalle note della Del Corso.

I gruppi di ordine 30 sono quindi:

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



## §2 Anelli

### §2.1 Riepilogo sugli anelli

**Definizione 2.1.** Un **anello** è un insieme non vuoto munito di due operazioni  $(A, +, \cdot)$  tali che:

- $(A, +)$  è un gruppo abeliano.
- $\cdot$  è associativa.
- Valgono le leggi distributive a destra e sinistra:

$$a(b + c) = ab + ac \quad \text{e} \quad (a + b)c = ac + bc \quad \forall a, b, c \in A$$

#### Esempio 2.2 (Anelli)

Esempi di anelli:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ .
- Dato un anello  $A$ ,  $A[x]$ , l'insieme dei polinomi a coefficienti in  $A$  è un anello.
- $M_{m \times m}(K)$ .
- $\text{End}(G) = \text{Hom}(G, G)$ , con  $G$  gruppo abeliano e le operazioni di somma e composizione.

Riepiloghiamo brevemente <sup>32</sup> le definizioni che riguardano gli anelli: <sup>33</sup>

**Definizione 2.3.** Un anello  $A$  si dice **commutativo** se l'operazione  $\cdot$  è commutativa.

**Definizione 2.4.** Un anello  $A$  si dice **con identità** se esiste  $1 \in A$  elemento neutro per il prodotto.

**Definizione 2.5.** Un anello  $(A, +, \cdot)$  si dice **campo** se  $(A \setminus \{0\}, \cdot)$  è un gruppo abeliano.

**Definizione 2.6.** Un anello  $(A, +, \cdot)$  si dice **corpo** se  $(A \setminus \{0\}, \cdot)$  è un gruppo.

**Definizione 2.7.** Dato un anello  $A$ ,  $x \in A$  si dice **divisore di zero** se  $\exists y \in A, y \neq 0$  tale che  $xy = yx = 0$ .

**Definizione 2.8.** Dato un anello  $A$ ,  $x \in A$  si dice **nilpotente** se  $\exists n \in \mathbb{N}$  tale che  $x^n = 0$ .

**Definizione 2.9.** Dato un anello  $A$ ,  $x \in A$  si dice **invertibile** se  $\exists y \in A$  tale che  $xy = yx = 1$ .

**Definizione 2.10.** Un anello  $A$  si dice **dominio d'integrità** se:

$$D(A) = \{x \in A \mid x \text{ è un divisore di } 0\} = \{0\}$$

Definiamo inoltre l'insieme degli elementi invertibili di  $A$ :

$$A^* = \{x \in A \mid x \text{ è invertibile}\}$$

e dei nilpotenti:

$$\mathcal{N} = \{x \in A \mid x \text{ è nilpotente}\}$$

<sup>32</sup>In caso di dubbi sulle definizioni si può fare riferimento alle **dispense di Aritmetica** dove sono state trattate più ampiamente.

<sup>33</sup>Per convenzione adotteremo lo 0 per indicare l'elemento neutro rispetto all'operazione  $+$  e l'1 per indicare l'elemento neutro rispetto all'operazione  $\cdot$ .

**Esercizio 2.11.** Calcolare i divisori di zero, gli invertibili ed i nilpotenti di:

$$\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

*Soluzione.*

□

### Proposizione 2.12

Dato  $A$  un anello commutativo con identità:

- (1)  $(A^*, \cdot)$  è un gruppo abeliano.
- (2)  $A^* \cap D(A) = \emptyset$ .
- (3) Se  $A$  è un anello finito, allora  $A = D(A) \cup A^*$ . In particolare, un dominio d'integrità finito è un campo.

*Dimostrazione.* Proviamo le affermazioni:

- (1) Per provare che  $(A^*, \cdot)$  è un gruppo abeliano, è sufficiente verificare le proprietà richieste dalla definizione:
  - (a) Chiusura: osserviamo che  $\forall x, y \in A^*$ , allora  $\exists x^{-1}y^{-1} \in A$ , pertanto  $xy \in A^*$ , poiché  $y^{-1}x^{-1} \in A^*$ .
  - (b) Associatività: poiché  $A^* \subseteq A$ , allora, essendo  $A$  associativo rispetto al  $\cdot$ , allora anche gli elementi di un suo qualsiasi sottoinsieme saranno associativi tra loro.
  - (c) Elemento Neutro:  $1 \in A$ , infatti, l'inverso di 1 è se stesso, quindi 1 è invertibile.
  - (d) Inverso: Segue per la stessa definizione di  $A^*$  che ogni suo elemento debba avere inverso moltiplicativo nel gruppo,  $\forall x \in A, \exists x^{-1} \in A$ :

$$x \cdot x^{-1} = x^{-1} \cdot x = 1 \quad \forall x \in A$$

- (e) L'abelianità segue immediatamente dall'abelianità di  $A$  (infatti  $A^* \subset A$ , dunque l'abelianità vale in particolare per gli elementi di  $A^*$ ).
- (2) Supponiamo per assurdo che  $D(A) \cap A^* \neq \emptyset$ , e consideriamo  $x \in D(A) \cap A^*$ , poiché  $x \in D(A)$ , allora  $\exists z \in A, z \neq 0$ , tale per cui:

$$xz = zx = 0$$

d'altra parte, poiché  $x \in A^*$ , allora  $\exists y$  per cui:

$$xy = yx = 1$$

da cui segue:

$$(zx)y = z(xy) \implies 0 \cdot y = z \implies z = 0$$

ma ciò è assurdo, pertanto  $D(A) \cap A^*$  è vuoto.

- (3) Il contenimento  $D(A) \cup A^* \subseteq A$  è ovvio in quanto i primi due sono sottoinsiemi del primo, ci resta da verificare quello opposto. Sia  $x \in A$ , se  $x \in D(A)$  abbiamo concluso, se  $x \in A \setminus D(A)$ , allora possiamo definire l'omomorfismo di gruppi:

$$\varphi_x : A \longrightarrow A : a \longmapsto xa$$

con:

$$\ker \varphi_x = \{y \in A \mid \varphi_x(y) = xy = 0\} = \{0\}$$

infatti, non essendo  $x$  un divisore di zero, l'unica possibilità, in base all'annullamento del prodotto è che  $y = 0 \implies xy = 0$ . Poiché  $|A| < +\infty$  l'omomorfismo è anche surgettivo, dunque è una bigezione, pertanto  $1 \in \text{Im} \varphi_x \implies \exists a \in A$  tale che  $\varphi_x(a) = xa = 1 \implies x \in A^*$ .

□

**Definizione 2.13.** Dato  $B \subset A$  non vuoto, si dice che  $B$  è un **sottoanello** di  $A$  se è chiuso rispetto alle operazioni  $+$  e  $\cdot$  ristrette a  $B$ .

**Definizione 2.14.** Dato  $I \subset A$ , con  $A$  anello commutativo, si dice che  $A$  è un **ideale** di  $A$  se:

- $(I, +) < (A, +)$ .
- Vale la **proprietà di assorbimento** a destra e sinistra:<sup>34</sup>

$$aI \subset I \quad \text{e} \quad Ia \subset I \quad \forall a \in A$$

**Osservazione 2.15** — Per verificare che un sottoinsieme di un anello commutativo con identità è un ideale ci basta verificare soltanto che  $(I, +)$  è chiuso per l'operazione  $+$  e che valga la proprietà di assorbimento, infatti, da ciò segue che  $(-1)a \in I$ , dove  $(-1)$  esiste in  $A$  è un gruppo rispetto al  $+$ .

Da questo momento in poi, anche se non specificato, assumiamo di star operando sempre in anelli commutativi con identità.

### Esempio 2.16 (Ideali)

Gli ideali vanno ricercati tra i sottogruppi di un anello, ad esempio:

- Considerando l'anello  $\mathbb{Z}$ , abbiamo gli ideali dati da  $\{n\mathbb{Z}\}_{n \in \mathbb{N}}$ , infatti:

$$xn\mathbb{Z} \subset n\mathbb{Z} \quad \forall x \in \mathbb{Z}$$

ed essendo  $\mathbb{Z}$  abeliano, abbiamo un ideale.

- I sottogruppi  $\{0\}$  (ideale **banale**) e  $A$  (ideale **improprio**) sono ideali dell'anello  $A$ .

**Esercizio 2.17.** Dato l'anello delle matrici  $A = M_{n \times n}(K)$  dimostrare che non ha ideali bilateri diversi da  $\{0\}$  e  $A$ .

*Soluzione.* Sia  $J \subseteq A$  un ideale non banale e  $M \in J$  non nulla. Osserviamo che l'Algoritmo di Gauss applicato ad  $M$  può essere espresso come moltiplicazione di  $M$  a sinistra e a destra per opportuni elementi di  $A$ . Dunque, se  $k = \text{rk } M > 0$ , la matrice

$$N = \left( \begin{array}{c|c} I_k & 0 \\ \hline 0 & 0 \end{array} \right)$$

<sup>34</sup>Se  $A$  non è un anello commutativo e  $(I, +) < (A, +)$ , possono valere separatamente le proprietà di assorbimento, nel caso in cui valga  $aI \subset I, \forall a \in A$ , si parla di **ideale sinistro**, mentre nel caso  $Ia \subset I, \forall a \in A$ , si parla invece di **ideale destro**.

appartiene a  $J$ . Allora anche

$$N' = N \left( \frac{1}{0} \middle| \frac{0}{0} \right) = \left( \frac{1}{0} \middle| \frac{0}{0} \right)$$

è elemento di  $J$ . Coniugando  $N'$  per matrici di permutazione di base troviamo nell'ideale matrici diagonali con diagonale nulla tranne per un 1 nella  $i$ -esima riga per ogni  $i$ , e sommando tutte queste matrici otteniamo  $I_n \in J$ , ovvero  $J = A$ .<sup>35</sup>  $\square$

**Definizione 2.18.** Dato un sottoinsieme non vuoto di un anello  $S \subset A$ , si definisce **ideale generato** da  $S$  in  $A$ :

$$(S) := \left\{ \sum_{i=1}^n a_i s_i \middle| a_i \in A, s_i \in S, n \in \mathbb{N} \right\}$$

Osserviamo che se  $S = \{x\}$  possiamo definire l'ideale generato da un elemento:

$$(x) = \{ax \mid a \in A\} = Ax$$

in tal caso l'ideale prende anche il nome di **ideale principale**.

### Proposizione 2.19

L'ideale generato da un sottoinsieme  $S$  di un anello  $A$  è un ideale.

*Dimostrazione.* Per verificare che un ideale generato sia effettivamente un ideale, bisogna verificare che sia un sottogruppo del gruppo abeliano  $(A, +)$  e che valga la proprietà di assorbimento (bilaterale in questo caso, poiché stiamo operando nel caso di anelli commutativi). Presi  $x, y \in S$ , ovvero della forma:

$$x = \sum_{i=1}^n a_i s_i \quad \text{e} \quad y = \sum_{j=1}^m \alpha_j \sigma_j \quad a_i, \alpha_j \in A \quad s_i, \sigma_j \in S$$

si osserva che:

$$x + y = \sum_{i=1}^n a_i s_i + \sum_{j=1}^m \alpha_j \sigma_j \in (S)$$

dunque  $I$  è chiuso per la somma. Infine, per ogni  $a \in A$  si ha:

$$ax = a \sum_{i=1}^n a_i s_i = \sum_{i=1}^n \underbrace{aa_i}_{\in A} s_i \in (S)$$

dunque  $(S)$  è un ideale.  $\square$

### Esempio 2.20 (Ideali generati)

Alcuni esempi di ideali generati possono essere:

- $n\mathbb{Z} = (n)$ , con  $n \in \mathbb{Z}$ .
- Dato  $K \subset F$  e  $\alpha \in F$  algebrico su  $K$ , sia  $\mu_\alpha(x) \in K[x]$  il polinomio minimo di  $\alpha$ , sappiamo che:

$$(\mu_\alpha(x)) = \{p(x) \in K[x] \mid p(\alpha) = 0\}$$

<sup>35</sup>Dimostrazione proposta da Davide Ranieri.

## §2.2 Operazioni tra ideali

### Proposizione 2.21 (Operazioni tra ideali)

Dato  $A$  un anello commutativo e  $I, J \subset A$  ideali, abbiamo che:

- $I \cap J$  è un ideale.
- $I + J = (I, J) = \{i + j | i \in I, j \in J\}$  è un ideale.
- $IJ = (\{xy | x \in I, y \in J\})$  è un ideale.
- $\sqrt{I} = \{x \in A | \exists n \in \mathbb{N} : x^n \in I\}$  è un ideale. In particolare  $\sqrt{0} = \mathcal{N}$  è un ideale.
- $(I : J) = \{x \in A | xJ \subseteq I\}$  è un ideale.

*Dimostrazione.* Verifichiamo tutte le affermazioni:

- $I \cap J$  è un sottogruppo di  $A$  e,  $\forall x \in I \cap J$  si ha:

$$ax \in I \quad \text{e} \quad ax \in J \quad \forall a \in A$$

dunque  $I \cap J$  assorbe e quindi è un ideale (bilatero in quanto abbiamo supposto l'anello commutativo).

- Dato  $I + J = \{i + j | i \in I, j \in J\}$ , presi  $x, y \in I + J$ , ovvero:

$$x = i_1 + j_1 \quad \text{e} \quad y = i_2 + j_2 \implies x + y = \underbrace{(i_1 + i_2)}_{\in I} + \underbrace{(j_1 + j_2)}_{\in J} \in I + J$$

inoltre,  $\forall a \in A$  si ha che:

$$ax = \underbrace{ai_1}_{\in I} + \underbrace{aj_1}_{\in J} \in I + J \quad \forall x \in I + J$$

dunque  $I + J$  è un ideale. Verifichiamo che  $I + J = (I, J)$ ; osserviamo che ovviamente:

$$\forall i + j \in I + J, i + j \in (I, J) \implies I + J \subseteq (I, J)$$

per verificare l'altro contenimento bisogna verificare che  $I, J \subset I + J$  e da queste inclusioni e dal fatto che  $I + J$  è un ideale segue che  $I + J$  contiene il più piccolo ideale di  $A$  che contiene sia  $I$  che  $J$  (e quindi contiene il loro generato). Osserviamo innanzitutto che in generale:

$$(S) = \bigcap_{\substack{S \subseteq X \subseteq A \\ X \text{ ideale}}} X$$

dove l'intersezione è appunto il più piccolo ideale di  $A$  che contiene  $S$ . Dobbiamo dimostrare ora quanto detto; osserviamo che  $(S)$  è contenuto nell'intersezione in quanto è uno dei termini di quest'ultima; il contenimento opposto segue dal fatto che  $\forall x \in S$  si ha  $x = \sum a_i s_i \in X$  (poiché  $X$  è un ideale che contiene  $S$ , per come l'abbiamo definito), d'altra parte, per vedere che un ideale generato  $(S)$  è contenuto a sua volta in un ideale  $\mathcal{I}$  di  $A$ , basta vedere che  $S \subset \mathcal{I}$  (ed è ciò che abbiamo appena fatto con  $S$ ). A questo punto, tornando all'inclusione iniziale, ci basta

verificare che, come abbiamo anticipato,  $I + J$  contenga sia  $I$  che  $J$ ; essendo  $0 \in J$  abbiamo:

$$I \subset I + J$$

infatti basta considerare sempre  $j = 0$  per ottenere tutti gli elementi di  $I$ ; in maniera simmetrica si dimostra la stessa cosa per  $J$ , dunque  $I, J \subset I + J \implies (I, J) \subset I + J \implies I + J = (I, J)$ .

- $IJ = (\{xy | x \in I, y \in J\})$  è un ideale per definizione.
- Verifichiamo che  $\sqrt{I} = \{x \in A | x^n \in I, n \in \mathbb{N}\}$  è un ideale, presi  $x, y \in \sqrt{I}$ , ovvero  $x^n, y^m \in I, n, m \in \mathbb{N}$ , vogliamo provare che  $x + y \in \sqrt{I}$  (ovvero che esiste  $d \in \mathbb{N}$  tale che  $(x + y)^d \in I$ ), osserviamo che:

$$(x + y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}$$

dove  $\forall i \in \{0, \dots, n+m\}$  si ha che  $i \geq n \implies x^i \in I$ , oppure che  $n + m - i \geq m \implies y^{n+m-i} \in I$ , dunque tutti i termini di  $(x + y)^{n+m}$  stanno in  $I$  e quindi  $x + y \in \sqrt{I}$ . Osserviamo che  $\forall a \in A$  si ha che:

$$(ax)^n = a^n \underbrace{x^n}_{\in I} \in I \implies ax \in \sqrt{I}$$

- Dato  $(I : J) = \{x \in A | xJ \subseteq I\}$  e presi  $x, y \in (I : J)$  si ha che:

$$(x + y)J = \underbrace{xJ}_{\subseteq I} + \underbrace{yJ}_{\subseteq I} \implies x + y \in (I : J)$$

inoltre,  $\forall a \in A$  abbiamo:

$$axJ = a(xJ) \subseteq aI \subseteq I \implies ax \in (I : J) \quad \forall x \in (I : J)$$

□

**Osservazione 2.22** ( $I \cup J$ ) —  $I \cup J$  in generale non è un ideale.

**Osservazione 2.23** ( $IJ \subset I \cap J$ ) — Osserviamo che  $IJ \subset I \cap J$ , infatti presi  $x \in I$  e  $y \in J$  si ha dalla proprietà di assorbimento che:

$$\underbrace{x}_{\in I} \underbrace{y}_{\in A} \in I \quad \text{e} \quad \underbrace{x}_{\in A} \underbrace{y}_{\in J} \in J \implies xy \in I \cap J$$

**Osservazione 2.24** ( $IJ = I \cap J$ ) — Se  $I + J = A$ , allora  $IJ = I \cap J$ . Dall'ipotesi possiamo dedurre che:

$$i + j = 1$$

vogliamo verificare che  $\forall x \in I \cap J$  si ha  $x \in IJ$  (dall'osservazione precedente sappiamo già che  $IJ \subset I \cap J$ , quindi stiamo verificando il contenimento opposto), possiamo scrivere:

$$x \cdot 1 = x(i + j) = \underbrace{xi}_{\in IJ} + \underbrace{xj}_{\in IJ} \in IJ$$

dove l'appartenenza segue dal fatto che stiamo considerando la somma di due elementi in  $IJ$  (che è un gruppo additivo).

### Esempio 2.25 (Operazioni tra ideali in $\mathbb{Z}$ )

Osserviamo che presi ad esempio gli elementi nell'intersezione degli ideali  $m\mathbb{Z}$  e  $n\mathbb{Z}$ , questi sono i multipli comuni sia ad  $m$  che ad  $n$  in  $\mathbb{Z}$ , ovvero:

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$$

Mentre, il prodotto tra i due ideali contiene gli interi multipli sia di  $m$  che di  $n$ :

$$m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$$

Osserviamo poi che la somma è data da tutti gli interi multipli del loro M.C.D.:

$$m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$$

infatti, per l'identità di Bézout, si ha:

$$m\mathbb{Z} + n\mathbb{Z} = \{am + bn | a, b \in \mathbb{Z}\} = \{dx | x \in \mathbb{Z}\}$$

Consideriamo ora  $n = p_1^{e_1} \dots p_r^{e_r}$ , possiamo considerare:

$$\sqrt{n\mathbb{Z}} = p_1 \dots p_r \mathbb{Z}$$

poiché:

$$\sqrt{n\mathbb{Z}} = \{x \in \mathbb{Z} | x^k \in n\mathbb{Z}, k \in \mathbb{N}\} = \{x \in \mathbb{Z} | n \mid x^k, k \in \mathbb{N}\}$$

ma  $n \mid x^k \implies p_i \mid x^k, \forall i \in \{1, \dots, r\}$ , ovvero  $p_1 \dots p_r \mid x \implies x \in p_1 \dots p_r \mathbb{Z}$ .  
Viceversa  $x = p_1 \dots p_r m \in \sqrt{n\mathbb{Z}}$  perché, detto  $e = \max e_i$ :

$$x^e = p_1^e \dots p_r^e m^e = ny \in n\mathbb{Z}$$

quindi ad esempio:

$$\sqrt{100\mathbb{Z}} = 10\mathbb{Z}$$

Infine, osserviamo che:

$$(m\mathbb{Z} : n\mathbb{Z}) = \frac{m}{(m, n)}\mathbb{Z}$$

quindi ad esempio:

$$(75\mathbb{Z} : 18\mathbb{Z}) = \frac{75}{(75, 18)} = 25\mathbb{Z}$$

questo poiché:

$$(75\mathbb{Z} : 18\mathbb{Z}) = \{x \in \mathbb{Z} | 18x\mathbb{Z} \subset 75\mathbb{Z}\} = 25\mathbb{Z}$$

infatti  $18x\mathbb{Z} \subset 75\mathbb{Z} \iff 75 \mid 18x \iff 25 \mid 6x \iff 25 \mid x$ .

**Proposizione 2.26** (Proprietà ideali propri)

Valgono i seguenti fatti:

- (1) Dato  $I \subset A$  ideale,  $I$  è un **ideale proprio** ( $I \subsetneq A$ ) se e solo se  $I \cap A^* = \emptyset$ .
- (2)  $A$  è un campo se e solo se gli unici ideali di  $A$  sono  $\{0\}$  e  $A$ .

*Dimostrazione.* Dimostriamo singolarmente i fatti:

- (1) Se  $I \cap A^* = \emptyset$ , poiché vale sempre che  $1 \in A^*$ , allora c'è almeno un elemento di  $A$  che non sta nell'ideale, quindi  $I \subsetneq A$ . Viceversa, sia  $I$  ideale proprio e supponiamo  $x \in I \cap A^*$ , allora  $x$  è invertibile, dunque  $\exists y \in A$  tale che  $xy = 1$ , ma:

$$1 = \underbrace{x}_{\in I} \underbrace{y}_{\in A} \in I \implies a \cdot 1 \in I^{36} \quad \forall a \in A \implies A \subset I$$

che è assurdo in quanto avevamo supposto  $I \subset A$ , dunque  $I \cap A^* = \emptyset$ .

- (2)  $A$  è un campo se e solo se  $A^* = A \setminus \{0\}$ , ma per il punto (1) l'unico elemento fuori da  $A^*$  è 0, dunque  $I = \{0\}$  e  $I = A$  sono gli unici ideali che possiamo avere.

□

<sup>36</sup>In pratica se c'è l'identità in  $I$  c'è esattamente ogni elemento dell'anello che contiene l'ideale.



## §2.3 Anelli quoziente e omomorfismi di anelli

**Definizione 2.27.** Dati  $A$  e  $B$  anelli,  $f : A \longrightarrow B$  è un **omomorfismo di anelli** se:

- $f(a_1 + a_2) = f(a_1) + f(a_2), \forall a_1, a_2 \in A.$
- $f(a_1 a_2) = f(a_1) f(a_2), \forall a_1, a_2 \in A.$

**Osservazione 2.28** — Se  $A$  e  $B$  sono anelli commutativi con identità in genere si richiede anche:

$$f(1_A) = 1_B$$

poiché tale condizione non è già implicata da altro; ad esempio:

$$f(a) = f(1_A a) = f(1_A) f(a) \implies f(a) - f(1_A) f(a) = (1_B - f(1_A)) f(a) = 0$$

ma non abbiamo la legge di cancellazione in quanto non è detto che  $A$  sia un dominio d'integrità. Se  $B$  è un dominio e  $f(a) \neq 0$ , allora, da quanto detto sopra segue  $f(1_A) = 1_B$ , ma se  $f(A) \subset D(B)$  non è detto che  $f(1_A) = 1_B$ .

**Definizione 2.29.** Sia  $A$  un anello e  $I \subseteq A$  un suo ideale, il gruppo quoziente  $(A/I, +)$  ha anche una struttura di anello con l'operazione:

$$(a + I) \cdot (b + I) \stackrel{\text{def}}{=} ab + I$$

**Osservazione 2.30** — Si verifica facilmente che l'operazione è ben definita, infatti, presi:

$$a + I = a' + I \quad \text{e} \quad b + I = b' + I$$

segue:

$$(a' + I) \cdot (b' + I) = a'b' + I = (a + I)(b + I) + I = ab + I$$

**Osservazione 2.31** — Si verifica facilmente che  $(A/I, +, \cdot)$  è un anello.

**Osservazione 2.32** — Possiamo definire una proiezione all'anello quoziente:

$$\pi_I : A \longrightarrow A/I : a \longmapsto a + I$$

con  $\pi_I$  omomorfismo di anelli surgettivo e  $\ker \pi_I = I$ .

### Proposizione 2.33

Gli ideali sono tutti e soli i nuclei degli omomorfismi di anello definiti su  $A$ .

*Dimostrazione.* Sia  $\varphi : A \longrightarrow B$  un omomorfismo di anelli, allora  $\ker \varphi$  è un ideale di  $A$ , infatti  $\ker \varphi < A$  perché  $\varphi$  è in particolare un omomorfismo di gruppi, inoltre,  $\forall a \in A$  si ha che:

$$ax \in \ker \varphi \quad \forall x \in \ker \varphi$$

in quanto  $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$ ; dunque i nuclei degli omomorfismi di anelli sono ideali. Viceversa, tutti gli ideali sono nuclei degli omomorfismi di proiezione al quoziente  $\pi_I$ .  $\square$

**Teorema 2.34** (Teorema di Omomorfismo di Anelli)

Dati  $A, B$  anelli e  $f : A \longrightarrow B$  omomorfismo (di anelli), esiste un unico omomorfismo (di anelli)  $\varphi$  che fa commutare il diagramma:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \curvearrowright \varphi & \nearrow \\ A/\ker f & & \end{array}$$

cioè tale che  $f = \varphi \circ \pi$ , con  $\varphi$  iniettivo e  $\text{Im } \varphi = \text{Im } f$ .

*Dimostrazione.* Per il Teorema di Omomorfismo i gruppi, essendo  $f$  in particolare un omomorfismo di gruppi, posto  $I = \ker f$ , sappiamo che esiste ed è unico l'omomorfismo:

$$\varphi : A/I \longrightarrow B$$

tale che  $f = \varphi \circ \pi_I$ , con  $\varphi$  è iniettivo e  $\text{Im } \varphi = \text{Im } f$ . Non ci resta altro da fare che verificare che  $\varphi$  è anche un omomorfismo di anelli:

$$\varphi((a+I)(b+I)) = \varphi(ab+I) = f(ab) \quad \forall a, b \in A$$

viceversa:

$$f(ab) = f(a)f(b) = \varphi(a+I)\varphi(b+I) \quad \forall a, b \in A$$

dove la seconda uguaglianza è vera per ipotesi.  $\square$

**Lemma 2.35** (Gli ideali si comportano come i sottogruppi normali con gli omomorfismi)

Dato  $f : A \longrightarrow B$  omomorfismo di anelli vale che:

- (1)  $\forall J \subset B$  ideale si ha  $f^{-1}(J)$  è un ideale di  $A$ .
- (2) Se  $f$  è surgettiva  $\forall I \subset A$  ideale si ha  $f(I)$  ideale di  $B$

*Dimostrazione.* Dimostriamo le proposizioni:

- (1) Sappiamo già che  $f^{-1}(J)$  è un sottogruppo di  $A$ , verifichiamo che valga la proprietà di assorbimento, ovvero:

$$af^{-1}(J) \subset f^{-1}(J) \quad \forall a \in A$$

sia  $x \in f^{-1}(J) \implies f(x) \in J$ , allora:

$$\underbrace{f(a)}_{\in B} \underbrace{f(x)}_{\in J} = f(ax) \in J \quad \forall x \in f^{-1}(J)$$

da cui  $ax \in f^{-1}(J)$ .

- (2) Sappiamo che  $f(I)$  è un sottogruppo di  $B$ , verifichiamo l'assorbimento, sia  $b \in B$ , poiché  $f$  è surgettiva esiste  $a \in A$  tale che  $b = f(a)$ , dunque:

$$bf(x) = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I)$$

□

**Teorema 2.36** (Teorema di Corrispondenza tra Ideali)

Sia  $I \subset A$  un ideale e  $\pi_I$  la proiezione all'anello quoziente modulo  $I$ ,  $\pi_I$  induce una corrispondenza biunivoca tra gli ideali di  $A/I$  e gli ideali di  $A$  che contengono  $I$ , e tale corrispondenza preserva l'ordinamento.

*Dimostrazione.* Per il Teorema di Corrispondenza tra sottogruppi abbiamo già la bigezione tra questi, dobbiamo tuttavia verificare che restringendo la corrispondenza agli ideali questa associ ancora un ideale di  $A$  ad un ideale di  $A/I$  e viceversa, cioè l'immagine e la controimmagine di un ideale mediante  $\pi_I$  è ancora un ideale (in particolare, per la Corrispondenza tra Sottogruppi sappiamo già che le controimmagini contengono l'ideale per il quale si quozienta). Siano:

$$X = \{J \subseteq A \text{ ideale} \mid I \subset J\} \quad \text{e} \quad Y = \{\mathcal{J} \subset A/I \mid \mathcal{J} \text{ ideale}\}$$

per il [Lemma 2.35](#), essendo  $\pi_I$  surgettivo, si ha che le immagini e la controimmagini via  $\pi_I$ :

$$J \mapsto \pi_I(J) \quad \text{e} \quad \mathcal{J} \mapsto \pi_I^{-1}(\mathcal{J})$$

sono ideali, e ciò conclude la dimostrazione. □

**Esempio 2.37**

Se nel [Lemma 2.35](#)  $f$  non fosse surgettiva, allora l'immagine di un ideale non sarebbe un ideale, ad esempio presa:

$$f : \mathbb{Z} \hookrightarrow \mathbb{Q} : (2) \mapsto 2\mathbb{Z}$$

con  $2\mathbb{Z}$  che non è un ideale di  $\mathbb{Q}$  perché  $\mathbb{Q}$  è un campo e quindi i suoi ideali sono soltanto  $\{0\}$  e  $\mathbb{Q}$ .

**Definizione 2.38.** Dato un omomorfismo di anelli  $f : A \longrightarrow B$  e un ideale  $I \subset A$  definiamo **estensione** di  $I$  a  $B$  via  $f$  l'ideale generato in  $B$  da  $f(I)$ :

$$(f(I)) = f(I)B = IB$$

**Definizione 2.39.** Dato un omomorfismo di anelli  $f : A \longrightarrow B$  e un ideale  $J \subset B$  definiamo **contrazione** di  $J$  ad  $A$  via  $f$  l'ideale  $f^{-1}(J)$ .

**Osservazione 2.40** — Gli omomorfismi sono sostanzialmente inclusioni a meno di isomorfismo, conoscendo la corrispondenza tra ideali indotta da  $\pi_I$  osserviamo che:

$$A \hookrightarrow B : I \mapsto IB$$

che manda ogni ideale nella propria estensione ad un **sovranello** e:

$$J \mapsto J \cap A$$

che manda ogni ideale di  $B$  nella propria contrazione ad un **sottoanello** fanno sì che l'applicazione:

$$\varphi : A \hookrightarrow B \longrightarrow B/J$$

sia tale che:

$$\ker \varphi = \{a \in A \mid \varphi(a) = a + J = J\} = \{a \in A \mid a \in J\} = J \cap A = \pi_I^{-1}(J)$$

da cui si ha anche che:

$$\frac{A}{J \cap A} \hookrightarrow B/J$$

per il Primo Teorema di Omomorfismo.

**Osservazione 2.41** — Dal **Teorema di Omomorfismo di Anelli** si deducono anche il secondo ed il terzo teorema di omomorfismo, ovvero:

$$\frac{A/I}{J/I} \cong A/J \quad \text{e} \quad \frac{I+J}{J} \cong \frac{I}{I \cap J}$$

dove in entrambi i casi gli isomorfismi sono di anelli.

## §2.4 Prodotto diretto di anelli

**Definizione 2.42.** Dati gli anelli  $A, B$  il prodotto cartesiano  $A \times B$  può essere dotato di una struttura di anello con le operazioni:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{e} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

$\forall a_1, a_2 \in A, \forall b_1, b_2 \in B$ , l'insieme  $A \times B$  con queste operazioni si dice **prodotto diretto** di anelli.

### Teorema 2.43 (Teorema Cinese Del Resto Per Anelli)

Dato  $A$  anello commutativo con unità,  $I, J$  suoi ideali, allora la mappa di doppia proiezione:

$$f : A \longrightarrow A/I \times A/J : a \longmapsto (a + I, a + J)$$

è un omomorfismo di anelli, con  $\ker f = I \cap J$ . Inoltre,  $I + J = A$  se e solo se  $f$  è surgettiva, ed in tal caso si ottiene:

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

*Dimostrazione.* Verifichiamo in primis che  $f$  sia un omomorfismo di anelli:

$$f(a+b) = ((a+b) + I, (a+b) + J) = (a + I, a + J) + (b + I, b + J) = f(a) + f(b) \quad \forall a, b \in A$$

dove la terza uguaglianza è assicurata dalla struttura di anello del quoziente; analogamente:

$$f(ab) = (ab + I, ab + J) = (a + I, a + J)(b + I, b + J) = f(a)f(b) \quad \forall a, b \in A$$

Osserviamo ora che:

$$\ker f = \{a \in A \mid f(a) = (a + I, a + J) = (I, J)\} = \{a \in A \mid a \in I, a \in J\} = I \cap J$$

Verifichiamo separatamente le due implicazioni della seconda parte del teorema:

- Supponiamo che  $I + J = A$ , ovvero che esistono  $i$  e  $j$  tali che  $i + j = 1$ <sup>37</sup>, e verifichiamo che  $f$  è surgettiva. Per verificare che  $f$  è surgettiva dobbiamo far vedere che:

$$\forall a, b \in A, \exists x \in A : f(x) = (a + I, b + J)$$

per ipotesi sappiamo che  $x \in A \implies x \in I + J$  quindi possiamo prendere  $x = bi + aj \in A$ , per  $i \in I$  e  $j \in J$ , dunque:

$$f(x) = (\underbrace{bi}_{\in I} + aj + I, bi + \underbrace{aj}_{\in J} + J) = (aj + I, bi + J)$$

da cui, osservando che  $j = 1 - i$  e  $i = 1 - j$  per ipotesi abbiamo:

$$(aj + I, bi + J) = (a(1 - i) + I, b(1 - j) + J) = (a + I, b + J)$$

e pertanto abbiamo ottenuto  $f(x) = (a + I, b + J)$ .

<sup>37</sup>Poiché l'identità è in  $I + J$ , allora per la proprietà di assorbimento ogni altro elemento di  $A$  è in  $I + J$ .

- Supponiamo ora che  $f$  sia surgettiva e proviamo che  $I + J = A$ . Se  $f$  è surgettiva abbiamo che:

$$\exists i \in A : f(i) = (I, 1 + J)$$

dunque per tale  $i$  si ha che:

$$i \in I \quad \text{e} \quad i \equiv 1 \pmod{J}$$

da cui si ricava che:  $\underbrace{i}_{\in I} = 1 + \underbrace{j}_{\in J} \implies 1 \in I + J \implies I + J = A$ .

Per il Primo Teorema di Omomorfismo abbiamo a questo punto che se  $f$  è surgettiva (ed equivalentemente  $I + J = A$ ), allora:

$$\frac{A}{\ker f} \cong A/I \times A/J \implies \frac{A}{I \cap J} \cong A/I \times A/J$$

D'altra parte, per l'Osservazione 2.24, essendo  $I + J = A$ , allora  $I \cap J = IJ$ , da cui la tesi:

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

□

**Osservazione 2.44** — Per il Teorema Cinese Del Resto tra gruppi sapevamo che:

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \iff (m, n) = 1$$

per il Teorema Cinese Del Resto tra anelli ora sappiamo che:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

con  $\ker f = m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$ , da cui:

$$\mathbb{Z}/[m, n]\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

avevamo visto che  $f$  è surgettiva se e solo se  $(m, n) = 1$ , ed in questo modo  $[m, n] = mn$  (o equivalentemente  $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z} = \mathbb{Z}$ ), dunque:

$$\mathbb{Z}/[m, n]\mathbb{Z} = \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

pertanto la nuova versione del Teorema Cinese del Resto è una generalizzazione della precedente.

## §2.5 Ideali primi e massimali

**Definizione 2.45.** Sia  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato e sia  $X \subset \mathcal{F}$  un suo sottoinsieme, diciamo che  $M \in \mathcal{F}$  è un **maggiorante** per  $X$  se:

$$A \leq M \quad \forall A \in X$$

**Definizione 2.46.** Sia  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato, diciamo che  $A \in \mathcal{F}$  è un elemento **massimale** per  $\mathcal{F}$  se:

$$\forall B \in \mathcal{F} : A \leq B \implies A = B$$

**Definizione 2.47.** Sia  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato, diciamo che  $A \in \mathcal{F}$  si dice **massimo** per  $\mathcal{F}$  se:

$$\forall B \in \mathcal{F} : B \leq A$$

**Definizione 2.48.** Sia  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato, una **catena** di  $\mathcal{F}$  è un sottoinsieme di  $\mathcal{F}$  totalmente ordinato.

**Definizione 2.49.** Sia  $(\mathcal{F}, \leq)$  un insieme parzialmente ordinato,  $(\mathcal{F}, \leq)$  si dice **induttivo** se ogni catena di  $\mathcal{F}$  ammette un maggiorante in  $\mathcal{F}$ .

### Lemma 2.50 (Lemma di Zorn)

Sia  $(\mathcal{F}, \leq)$  un insieme non vuoto, parzialmente ordinato e induttivo, allora  $\mathcal{F}$  contiene elementi massimali.

**Osservazione 2.51** — Spesso il **Lemma di Zorn** viene usato su famiglie  $\mathcal{F}$  di ideali ordinati secondo la relazione di inclusione  $\subseteq$ .

**Definizione 2.52.** Dato un ideale proprio  $I \subsetneq A$ ,  $I$  si dice **primo** se:

$$xy \in I \implies x \in I \vee y \in I \quad \forall x, y \in A$$

ovvero se ogni volta che contiene un prodotto, contiene uno dei due fattori.

**Definizione 2.53.** Un ideale  $I$  si dice **massimale** se è un elemento massimale della famiglia  $\mathcal{F}$  di tutti gli ideali propri di  $A$ , ovvero:

$$I \text{ è massimale} \iff \forall J \subsetneq A : I \subseteq J \implies I = J$$

### Esempio 2.54 (Ideali primi di $\mathbb{Z}$ )

Gli ideali primi di  $\mathbb{Z}$  sono  $(p)$  con  $p$  primo, infatti:

$$xy \in (p) \iff p \mid xy \iff p \mid x \vee p \mid y$$

ovvero se  $x \in (p)$  o  $y \in (p)$ . Se consideriamo invece  $(m)$ , con  $m$  non primo, dunque riducibile  $m = ab$ , con  $1 < a < m$  e  $1 < b < m$ , allora:

$$ab \in (m) \quad \text{ma} \quad a \notin (m) \quad \text{e} \quad b \notin (m)$$

dunque  $(m)$  non è primo.

**Proposizione 2.55** (Proprietà degli Ideali Massimali)

Dato un anello  $A$  allora:

- (1) Ogni ideale proprio di  $A$  è contenuto in un ideale massimale.
- (2) Ogni elemento non invertibile di  $A$  è contenuto in un ideale massimale.

*Dimostrazione.* Verifichiamo le affermazioni:

1. Sia  $I \subsetneq A$  un ideale proprio e sia  $\mathcal{F}$  la famiglia di tutti gli ideali propri che lo contengono:

$$\mathcal{F} = \{J \subsetneq A \mid I \subseteq J\}$$

osserviamo che  $I \in \mathcal{F} \implies \mathcal{F} \neq \emptyset$ , inoltre  $(\mathcal{F}, \subseteq)$  è induttivo, infatti, detta  $\mathcal{C}$  una catena, essa sarà un sottoinsieme di  $\mathcal{F}$  totalmente ordinato della forma:

$$\mathcal{C} = \{J_n\}^{38} \subseteq \mathcal{F}$$

allora posta  $\bigcup J_n^{39} = J \in \mathcal{F}$ , verifichiamo che  $J$  è maggiorante di  $\mathcal{C}$ . Si ha che:

- $\forall J_n \in \mathcal{C} : J_n \subseteq J$ , segue ovviamente da come abbiamo definito  $J$ , avendolo costruito come l'unione di tutti i  $J_n$ .
- $J \in \mathcal{F}$ , poiché  $I \subset J_n \subset J$ ,  $\forall J_n \in \mathcal{F}$ , e infine  $J$  è un ideale proprio, infatti, se per assurdo fosse  $1 \in J = \bigcup J_n \implies \exists n$  tale che  $1 \in J_n \subsetneq A$  che è assurdo (se un ideale contenesse l'identità del prodotto, allora conterrebbe tutti gli elementi dell'anello).

Dunque ogni catena  $\mathcal{C}$  di  $\mathcal{F}$  ammette maggiorante<sup>40</sup>, pertanto  $\mathcal{F}$  è induttivo e vale il [Lemma di Zorn](#), per il quale la famiglia  $\mathcal{F}$  ammette almeno un elemento massimale  $M$ .

Resta da verificare che tale elemento massimale  $M$  sia un ideale massimale dell'anello (poiché abbiamo dimostrato che è massimale per la famiglia  $\mathcal{F}$  degli ideali che ne contengono uno proprio, la quale ovviamente non è la famiglia di tutti gli ideali propri di  $A$ ), ciò segue subito osservando che, supponendo  $L \subsetneq A$  ideale proprio con  $M \subseteq L$ , allora:

$$I \subseteq M \subseteq L \implies L \in \mathcal{F}$$

dunque  $L$  è un elemento della famiglia  $\mathcal{F}$ , e per la massimalità di  $M$  in  $\mathcal{F}$ , segue che  $M = L$ .

2. Segue immediatamente dal punto (1), infatti, sia  $x \in A \setminus A^*$ , allora per la [Proposizione 2.26](#) l'ideale generato da  $x$  è proprio,  $(x) \subsetneq A$ , e quindi vale il punto (1) appena dimostrato:

$$(x) \subseteq M \implies x \in M$$

con  $M$  ideale massimale di  $A$ .

□

<sup>38</sup>I vari  $J_i$  sono contenuti tutti uno dentro l'altro "in catena".

<sup>39</sup>Andrebbe dimostrato che l'unione di ideali in catena, analogamente a quanto accade per i sottogruppi, è un ideale.

<sup>40</sup>Abbiamo verificato addirittura che tale maggiorante sia un massimo della catena.



**Proposizione 2.56** (Caratterizzazione degli ideali primi e massimali)

Dato un ideale proprio di  $I \subsetneq A$ , allora:

- (1)  $I$  è primo se e solo se  $A/I$  è un dominio.
- (2)  $I$  è massimale se e solo se  $A/I$  è un campo.

*Dimostrazione.* Verifichiamo le affermazioni:

- (1) Presi  $x, y \in A$ , per definizione abbiamo che  $I$  è primo se e solo se  $xy \in I \implies x \in I$  o  $y \in I$ , d'altra parte,  $A/I$  è un dominio se e solo se:

$$(x + I)(y + I) = xy + I = I \iff xy \in I \implies x \in I \text{ o } y \in I$$

ovvero se e solo se, quando un prodotto di elementi si annulla (quindi fa la classe laterale neutra in questo caso) uno dei due elementi è già nella classe laterale neutra dell'anello quoziente (quindi è già l'unico elemento neutro del prodotto, come richiesto dal fatto che l'anello sia un dominio), ma come si vede ciò è equivalente a dire che  $I$  è primo.

- (2) Per il (2) della [Proposizione 2.26](#)  $A/I$  è un campo se e solo se gli unici ideali che contiene sono quelli impropri,  $\overline{(0)}$  e  $A/I$ , dunque per il [Teorema di Corrispondenza](#) ciò è equivalente a dire che gli ideali di  $A$  che contengono  $I$  sono soltanto  $A$  ed  $I$  stesso <sup>41</sup>, ovvero  $I$  è un ideale massimale di  $A$ .

□

**Corollario 2.57** (Caratterizzazione degli ideali primi e massimali 2)

Dato  $A$  un anello si ha:

- (1)  $A$  è un dominio se e solo se  $(0)$  è un ideale primo.
- (2)  $A$  è un campo se e solo se  $(0)$  è un ideale massimale.
- (3)  $I$  massimale  $\implies I$  primo.

*Dimostrazione.* Proviamo le affermazioni:

- (1) Per l'(1) della [Proposizione 2.56](#) sappiamo che  $(0)$  è primo se e solo se  $A/(0)$  è un dominio, ma:

$$A/(0) \cong A$$

da cui segue che  $A$  è un dominio.

- (2) Per il punto (2) della [Proposizione 2.56](#) sappiamo che  $(0)$  è massimale se e solo se  $A/(0)$  è un campo, ma:

$$A/(0) \cong A$$

da cui segue che  $A$  è un campo.

<sup>41</sup>Infatti si ha che  $\pi_I^{-1}(A/I) = A$  e  $\pi_I^{-1}(\overline{(0)}) = I$ .

- (3) Per quanto detto nel (2) della [Proposizione 2.56](#),  $I$  è massimale se e solo se  $A/I$  è un campo, in particolare ciò significa che  $A/I$  è un dominio d'integrità, ma per l'(1) della [Proposizione 2.56](#) ciò è equivalente a dire che  $I$  sia primo.

□

**Esempio 2.58** ( $\mathbb{Z}$  è un dominio ma non un campo)

Si osserva che l'ideale  $(0)$  è un ideale primo (poiché  $xy \in (0) \iff xy = 0 \implies x \in (0) \text{ o } y \in (0)$ , poiché  $\mathbb{Z}$  è un dominio), ma non massimale, infatti:

$$(0) \subset (m) \quad \forall m \in \mathbb{Z}$$

**Corollario 2.59**

La corrispondenza biunivoca tra ideali per mezzo della proiezione:

$$\pi_I : A \longrightarrow A/I$$

conserva ideali primi e massimali.<sup>a</sup>

<sup>a</sup>Ovviamente gli ideali considerati devono contenere  $I$ , altrimenti non c'è nulla da preservare in arrivo.

*Dimostrazione.* Osserviamo preliminarmente che si ha  $I \subseteq J \subseteq A$ , dunque nella proiezione  $\pi_I$  si ha che:

$$J \longmapsto \pi_I(J) = J/I$$

Dobbiamo dimostrare che  $J$  è primo (massimale) in  $A$  se e solo se  $J/I$  è primo (massimale) in  $A/I$ . Per quanto detto nella [Proposizione 2.56](#)  $J$  primo (massimale) è equivalente al fatto che  $A/J$  sia un dominio (campo), e, ugualmente deve essere che  $\frac{A/I}{J/I}$  è un dominio (campo) ma dal Secondo Teorema di Omomorfismo di Anelli si ha:

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

che in entrambi i casi verifica la tesi.

□

## §2.6 Anello delle frazioni di un dominio

**Definizione 2.60.** Consideriamo un anello commutativo con identità  $A$ , che sia un dominio di integrità. Sia  $S \subset A$  con le seguenti proprietà:

- $0 \notin S$ .
- $1 \in S$ .
- $S$  è moltiplicativamente chiuso:  $xy \in S, \forall x, y \in S$ .

Il sottoinsieme  $S$  con queste proprietà si dice **parte moltiplicativa** di  $A$ .

**Definizione 2.61.** Dato un anello commutativo con identità  $A$ , che sia un dominio di integrità, e  $S$  la sua parte moltiplicativa, allora possiamo definire l'insieme delle **frazioni di un dominio**:

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

con la relazione  $\sim$  data da  $\frac{a}{s} \sim \frac{b}{t} \iff at = bs$ .<sup>42</sup>

**Osservazione 2.62** — La relazione  $\sim$  usata nella definizione precedente è una relazione di equivalenza, infatti:

- $\sim$  è riflessiva in quanto  $\frac{a}{s} \sim \frac{a}{s} \iff as = sa$ , che è vero in quanto abbiamo supposto  $A$  commutativo.
- $\sim$  è simmetrica in quanto  $\frac{a}{s} \sim \frac{b}{t} \iff at = bs \iff \frac{b}{t} \sim \frac{a}{s}$ .
- $\sim$  è transitiva in quanto, dati  $\frac{a}{s} \sim \frac{b}{t}$  e  $\frac{b}{t} \sim \frac{c}{u}$  abbiamo che:

$$at = bs \quad \text{e} \quad bu = tc$$

da cui, moltiplicando la prima per  $u$  si ha:

$$aut = bus = tcu \implies aut = cts \iff t(au - cs) = 0$$

essendo per ipotesi  $A$  un dominio<sup>a</sup> e  $t \in S$  (dunque  $t \neq 0$ ) segue:

$$au = cs \iff \frac{a}{s} \sim \frac{c}{u}$$

<sup>a</sup>È importante notare che qui stiamo usando il fatto che  $A$  è un dominio.

<sup>42</sup>Alternativamente possiamo scrivere la relazione come:  $(a, s) \sim (b, t) \iff at = bs$ , ed indicare con  $\frac{a}{s}$  la classe di equivalenza dei due elementi.

**Proposizione 2.63** (Anello delle frazioni di un dominio)

L'insieme delle frazioni di un dominio munito con le operazioni di:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{e} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

è un anello commutativo con identità.<sup>a</sup>

<sup>a</sup>Con l'identità data dall'elemento  $1/1$ .

*Dimostrazione.* Bisogna verificare in primis che le operazioni sono ben definite (in quanto le abbiamo definite tra classi di equivalenza), consideriamo  $\frac{a}{s} \sim \frac{a'}{s'}$  e  $\frac{b}{t} \sim \frac{b'}{t'}$ , vogliamo verificare che le due somme:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{e} \quad \frac{a'}{s'} + \frac{b'}{t'} = \frac{a't' + b's'}{s't'}$$

diano lo stesso risultato; per ipotesi sappiamo che  $as' = a's$  e  $bt' = b't$ , osserviamo che l'uguaglianza tra le due somme è vera se e solo se:

$$(at + bs)s't' = (a't' + b's')st$$

sviluppando l'LHS otteniamo:

$$att's' + bss't' = a'stt' + b'tss' = (a't' + b's')st$$

che dimostra che l'operazione  $+$  è ben definita.<sup>43</sup> □

**Esempio 2.64** (Anello delle frazioni di  $\mathbb{Z}$ )

Preso  $A = \mathbb{Z}$  e  $S = \{10^k\}_{k \geq 0}$  (si verifica facilmente che  $S$  rispetta le tre proprietà richieste dalla definizione) abbiamo che l'anello delle frazioni di  $\mathbb{Z}$  è dato da:

$$S^{-1}A = \left\{ \frac{z}{10^k} \mid z \in \mathbb{Z}, k \geq 0 \right\}$$

con ad esempio  $\frac{5}{10} = \frac{1}{2} \in S^{-1}A$ .

**Osservazione 2.65** — Nel caso dell'esempio precedente si osserva che  $\frac{2}{1} \in S^{-1}$  ed è invertibile:

$$\frac{2}{1} \cdot \frac{5}{10} = \frac{1}{1}$$

**Proposizione 2.66** ( $S^{-1}A$  come estensione di  $A$ )

Dato un dominio  $A$  e il suo anello delle frazioni, l'applicazione:

$$f : A \longrightarrow S^{-1}A : a \longmapsto \frac{a}{1}$$

è un omomorfismo iniettivo di anelli.<sup>a</sup>

<sup>a</sup>Dunque  $A \subset S^{-1}A$ , cioè  $S^{-1}A$  è un'estensione di  $A$ .

<sup>43</sup>Le restanti (lunghe e noiose) 9 verifiche verranno aggiunte in seguito :).

*Dimostrazione.* Verifichiamo che  $f$  sia un omomorfismo di anelli:

$$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b) \quad \forall a, b \in A$$

e analogamente:

$$f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a)f(b) \quad \forall a, b \in A$$

Per l'iniettività studiamo il nucleo:

$$\ker f = \left\{ a \in A \mid f(a) = \frac{a}{1} = \frac{0}{1} \right\}^{44} = \{a \in A \mid a \cdot 1 = 0 \cdot 1 = 0\} = \{0\}$$

dunque l'omomorfismo è iniiettivo.  $\square$

**Osservazione 2.67** ( $S = A \setminus \{0\}$ ) — Se  $A$  è un dominio, allora  $S = A \setminus \{0\}$ <sup>a</sup> è una parte moltiplicativa, infatti,  $\forall x, y \in S$ , ovvero  $x \neq 0$  e  $y \neq 0$ , dunque  $xy \in S$ ,  $xy \neq 0$ .

<sup>a</sup>Sarebbe  $A^*$  se  $A$  fosse finito.

**Definizione 2.68.** Dato un dominio  $A$ , definiamo **campo dei quozienti** di  $A$ :

$$S^{-1}A = Q(A)$$

l'anello delle frazioni con parte moltiplicativa  $S = A \setminus \{0\}$ .

**Proposizione 2.69** ( $A \subset Q(A)$ )

Dato  $A$  dominio e la sua parte moltiplicativa  $S = A \setminus \{0\}$ , l'anello delle frazioni  $S^{-1}A = Q(A)$  è il più piccolo campo che contiene  $A$ .

*Dimostrazione.* Verifichiamo prima che  $Q(A)$  è un campo e poi la tesi:

- Per verificare che  $Q(A)$  sia un campo, ci basta verificare che esistono gli inversi moltiplicativi, e ciò segue immediatamente dal fatto che  $\forall a \in A$ ,  $a \neq 0$ , allora  $\frac{1}{a} \in Q(A)$  (in questo modo tutti gli elementi di  $A$ , eccetto lo 0, possono essere scritti come  $\frac{1}{a}$ ) ed è tale per cui:

$$\frac{a}{1} \cdot \frac{1}{a} = \frac{1}{1}$$

- Per la [Proposizione 2.66](#) sappiamo già che  $A \subset S^{-1}A$ , ed ora abbiamo dimostrato che  $S^{-1}A$  è un campo, ci resta da verificare che  $S^{-1}A (= Q(A))$  sia effettivamente il più piccolo campo che contiene  $A$ . Sia  $K$  è un campo tale che  $A \subset K$ , allora  $\frac{1}{a} \in K$ ,  $\forall a \in A \setminus \{0\}$ , ovvero  $K$  contiene tutti gli inversi degli elementi di  $A$ , allora,  $\forall b \in A$ ,  $\forall a \in A \setminus \{0\}$ , cioè  $K$  contiene tutti gli elementi di  $S^{-1}A$ :

$$\frac{b}{a} \in K \implies Q(A) = S^{-1}A \subset K$$

pertanto, essendo contenuto in ogni campo che contiene  $A$ , e contenendolo a sua volta,  $Q(A)$  è il più piccolo campo che contiene  $A$ .  $\square$

<sup>44</sup>Ricordiamo che  $0/1$  è l'elemento neutro di  $S^{-1}A$ .

### Esempio 2.70

Vediamo alcuni esempi di anelli delle frazioni di domini e campi quoziente:

- Consideriamo  $A = \mathbb{Z}$ ,  $S_1 = \{10^k\}_{k \geq 0}$  e  $S_0 = A \setminus \{0\}$ , allora si ha che:

$$\mathbb{Z} \subset S_1^{-1}\mathbb{Z} \subset S_0^{-1}\mathbb{Z} = Q(\mathbb{Z}) = \mathbb{Q}$$

- Considerando  $A = K[x]$  si ha che:

$$Q(A) = K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

- Sia  $A$  un dominio e  $P \subset A$  un suo ideale primo, possiamo considerare  $S = A \setminus P$  che è una parte moltiplicativa, in quanto  $0 \notin S$ ,  $1 \in S$  e  $\forall x, y \in S$  si ha:

$$x, y \notin P \implies xy \notin P$$

poiché  $P$  è primo, dunque  $xy \in A \setminus P = S$ . In questo caso indichiamo  $S^{-1}A = A_P$  e prende il nome di **localizzato** dell'anello  $A$  all'ideale  $P$ .

**Osservazione 2.71** — Dato il localizzato di  $A$  a  $P$ ,  $A_P$ , si osserva che esso è un **anello locale**, ovvero un anello che ha un unico ideale massimale.

### Esempio 2.72 (Localizzato di un ideale primo)

Se consideriamo  $A = \mathbb{Z}$  e  $P = 2\mathbb{Z}$ , allora la parte moltiplicativa è data da  $S = \mathbb{Z} \setminus 2\mathbb{Z}$  (i numeri dispari), da cui abbiamo che:

$$S^{-1}\mathbb{Z} = \mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \equiv 1 \pmod{2} \right\}$$

**Esercizio 2.73.** Dati  $A = \mathbb{Z}$ ,  $P = 2\mathbb{Z}$  e  $S = \mathbb{Z} \setminus 2\mathbb{Z}$ , verificare che l'ideale  $(2)\mathbb{Z}_{(2)}$  è l'unico ideale massimale di  $\mathbb{Z}_{(2)}$ .

*Soluzione.* La tesi è equivalente a mostrare che  $\mathbb{Z}_{(2)}^* = \mathbb{Z}_{(2)} \setminus (2)\mathbb{Z}_{(2)}$ . Infatti, sappiamo già che  $(2)\mathbb{Z}_{(2)}$  è un ideale, mentre qualunque ideale non contenuto in esso contiene necessariamente un elemento invertibile ed è perciò non proprio. Se  $\frac{a}{b} \notin (2)\mathbb{Z}_{(2)}$  allora sia  $a$  che  $b$  sono dispari, dunque  $\frac{b}{a} \in \mathbb{Z}_{(2)}$  ed è chiaramente l'inverso di  $\frac{a}{b}$ . Viceversa se  $\frac{a}{b}$  è invertibile esiste  $\frac{c}{d} \in \mathbb{Z}_{(2)}$  tale che  $\frac{ac}{bd} = 1$ , cioè  $ac = bd$ . Se uno tra  $a$  e  $c$  fosse pari lo sarebbe anche  $bd$ , e poiché  $2$  è primo uno tra  $b$  e  $d$  sarebbe pari, contraddicendo la definizione di  $\mathbb{Z}_{(2)}$ . Dunque  $\frac{a}{b} \in \mathbb{Z}_{(2)} \setminus (2)\mathbb{Z}_{(2)}$ .<sup>45</sup>  $\square$

<sup>45</sup>Dimostrazione proposta da Davide Ranieri.

**Osservazione 2.74 (Elementi invertibili di  $S^{-1}A$ )** — Osserviamo che gli invertibili dell'anello  $S^{-1}A$  sono:

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \mid \frac{s}{a} \in S^{-1}A \right\}$$

ovvero esistono  $b \in A$  e  $t \in S$  tali che  $\frac{s}{a} = \frac{b}{t} \iff st = ab \in S$  (cioè esiste una scrittura di questo tipo in  $S^{-1}A$ , ma poiché non è detto che  $a$  appartenga ad  $S$ , sappiamo che, per quanto scritto, almeno un suo multiplo c'è), dunque:

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \mid \exists b \in A \text{ t.c. } ab \in S \right\}$$

Ad esempio, nel caso di  $A = \mathbb{Z}$  e  $S = \{10^k\}_{k \geq 0}$ , abbiamo che:

$$\frac{5}{10} = \frac{1}{2} \in (S^{-1}A)^* \quad \text{ma} \quad 2 \notin S$$

dunque  $2 \in (S^{-1}A)^*$ , poiché il suo inverso,  $\frac{1}{2} = \frac{5}{10}$ , ha una scrittura che rispetta la proprietà richiesta dall'insieme (e tale scrittura è appunto un multiplo di quella iniziale).

**Osservazione 2.75 (Ideali di  $S^{-1}A$ )** — Sia  $I \subset A$  un ideale di  $A$ , possiamo costruire l'insieme:

$$S^{-1}I = \left\{ \frac{x}{s} \in S^{-1}A \mid x \in I, s \in S \right\} \cong \frac{I \times S}{\sim}$$

per tale insieme valgono le proprietà espresse dalla proposizione seguente.

**Proposizione 2.76 (Ideali di  $S^{-1}A$ )**

Sia  $I \subset A$  e sia  $S^{-1}A$  l'insieme costruito come sopra, allora:

- (1)  $S^{-1}I$  è un ideale di  $S^{-1}A$ .
- (2)  $\forall J \subset S^{-1}A, \exists I \subset A$  tale che  $J = S^{-1}I$  (cioè ogni ideale di  $S^{-1}A$  si ottiene da un ideale di  $A$ , considerandone il relativo anello delle frazioni).
- (3)  $S^{-1}I$  è un ideale proprio di  $S^{-1}A$  se e solo se  $I \cap S = \emptyset$ .
- (4) Sia  $P$  un ideale primo di  $A$ , con  $P \cap S = \emptyset$ , allora  $S^{-1}P$  è un ideale primo di  $S^{-1}A$ .

*Dimostrazione.* Dimostriamo le singole affermazioni:

- (1) Per verificare che  $S^{-1}I$  sia un ideale verifichiamo prima la chiusura per somma:

$$\frac{x}{s} + \frac{y}{t} = \frac{\overbrace{xt + ys}^{\in I}}{\underbrace{st}_{\in S}} \in S^{-1}I \quad \forall x, y \in I$$

dove l'appartenenza del numeratore deriva dal fatto che  $x, y$  siano elementi di un ideale. Per verificare la proprietà di assorbimento osserviamo che:

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{\overbrace{ax}^{\in I}}{\underbrace{st}_{\in S}} \in S^{-1}I \quad \forall \frac{a}{s} \in S^{-1}A$$

- (2) Sia  $J \subset S^{-1}A$  un ideale, per quanto detto nella [Proposizione 2.66](#), sappiamo che  $S^{-1}A$  è un'estensione di  $A$ , inoltre se consideriamo  $f^{-1}(J)$ , che per il [Lemma 2.35](#), sappiamo essere un ideale, ed in particolare una contrazione di  $J$  ad  $A$ , abbiamo che:

$$f^{-1}(J) = J \cap A = I \subset A$$

vogliamo mostrare che vale  $J = S^{-1}I$ . Osserviamo che  $\forall x \in I$  si ha  $f(x) = \frac{x}{1} \in J$ , dunque:

$$\underbrace{\frac{1}{s}}_{\in S^{-1}A} \cdot \frac{x}{1} = \frac{x}{s} \in J \implies S^{-1}I \subseteq J$$

cioè per assorbimento di  $J$  ci sono tutti gli elementi di  $S^{-1}I$ . Viceversa si ha che  $\forall \frac{x}{s} \in J$  possiamo scrivere:

$$\frac{x}{1} = \frac{x}{s} \cdot \frac{s}{1} \in J \implies x = f^{-1}\left(\frac{x}{1}\right) \in I$$

ovvero il numeratore di ogni elemento in  $J$  è un elemento di  $I$ , dunque considerando l'anello delle frazioni  $S^{-1}I$  esso contiene tutte quelle di  $J$ , da cui si conclude  $\frac{x}{s} \in S^{-1}I \implies J \subseteq S^{-1}I$ .

- (3) Dimostriamo la negazione<sup>46</sup>, ovvero  $S^{-1}I$  non proprio equivale a  $S^{-1}I = S^{-1}A$ , ma essendo il primo un ideale questo è vero se e solo se:

$$\frac{1}{1} \in S^{-1}I \iff \exists x \in I, \exists s \in S : \frac{1}{1} = \frac{x}{s}$$

che, per la relazione definita sugli anelli di frazioni è equivalente a chiedere che  $I \ni x = s \in S \iff I \cap S \neq \emptyset$ .

- (4) Sia  $P$  un ideale primo, se fosse  $P \cap S \neq \emptyset$ , allora per quanto visto al punto (3) non sarebbe proprio (e dunque nemmeno primo), viceversa, se  $P \cap S = \emptyset$  vogliamo dimostrare che  $S^{-1}P$  primo in  $S^{-1}A$ ; consideriamo:

$$\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}P$$

ciò è equivalentemente al fatto che  $\exists \sigma \in S$  e  $\exists p \in P$  tali per cui:

$$\frac{ab}{st} = \frac{p}{\sigma} \iff ab\sigma = \underbrace{p}_{\in P} st \in P \implies ab\sigma \in P$$

ma, essendo per ipotesi che  $\sigma \in P$  e  $P \cap S = \emptyset$ , allora  $ab \in P$ , e poiché  $P$  è primo si deve avere  $a \in P$  o  $b \in P$ , e quindi la frazione di uno dei due deve essere quella in  $S^{-1}P$ :  $\frac{a}{s} \in S^{-1}P$  o  $\frac{b}{t} \in S^{-1}P$  e quindi  $S^{-1}P$  primo.

□

<sup>46</sup>Poiché trattandosi di un'equivalenza logica va bene lo stesso.



## §2.7 Divisibilità nei domini

**Definizione 2.77.** Sia  $A$  un dominio e siano  $a, b \in A$ , con  $a \neq 0$ , si dice che  $a \mid b$  ( $a$  divide  $b$ ) se:

$$\exists c \in A : b = ac$$

**Osservazione 2.78** — Osserviamo che  $a \mid b \iff (b) \subseteq (a)$ , infatti:

$$a \mid b \iff \exists c \in A : b = ac \iff b \in (a) \iff (b) \subseteq (a)$$

**Definizione 2.79.** Dato  $A$  dominio e  $a, a'$ , diciamo che  $a$  ed  $a'$  sono **associati**,  $a \sim a'$ , se vale una delle seguenti tre condizioni equivalenti:

- (i)  $a \mid a'$  e  $a' \mid a$ .
- (ii)  $\exists u \in A^*$  tale che  $a = ua'$ .
- (iii)  $(a) = (a')$ .

**Osservazione 2.80 (Equivalenza delle condizioni)** — Osserviamo che le tre condizioni date sono equivalenti, infatti, per quanto riguarda (i) e (iii) si ha:

$$a \mid a' \iff (a') \subseteq (a) \quad \text{e} \quad a' \mid a \iff (a) \subseteq (a')$$

dunque se sono vere entrambe le condizioni (i) e (iii) sono equivalenti. Dobbiamo da verificare che (i)  $\implies$  (ii), dalle due divisibilità segue che:

$$a' = xa \quad \text{e} \quad a = ya' \implies a = yxa \implies a(1 - xy) = 0$$

poiché  $a \neq 0$ , ed  $A$  dominio per ipotesi si ha che  $xy = 1 \implies y \in A^*$ , ovvero la (ii). Viceversa, assumiamo (ii) e deduciamo (iii):<sup>a</sup>

$$a = ua' \implies a \in (a') \implies (a') \subseteq (a)$$

con  $u \in A^*$ , pertanto  $\exists v \in A^*$  tale che  $uv = vu = 1$ , moltiplicando la prima relazione per  $v$  si ottiene:

$$a' = va \implies a' \in (a) \implies (a) \subseteq (a')$$

e si conclude  $(a) = (a')$ .

<sup>a</sup>A questo punto sappiamo che già che (i) e (iii) sono equivalenti, quindi non è necessario fare verifiche distinte.

**Definizione 2.81.** Dati  $a, b \in A$  dominio, non entrambi nulli, diciamo che  $d \in A$  è un **massimo comun divisore** per  $a$  e  $b$  se:

- (1)  $d \mid a$  e  $d \mid b$ .
- (2)  $\forall x \in A$  tale che  $x \mid a$  o  $x \mid b$ , allora  $x \mid d$ .

**Proposizione 2.82** (Gli M.C.D. di due elementi in un dominio sono associati)

Dati  $d, d' \in A$ , essi sono due massimi comun divisori di una stessa coppia di elementi  $a$  e  $b$  di  $A$ ,  $d = (a, b)$  e  $d' = (a, b)$ , se e solo se sono associati,  $d \sim d'$ .

*Dimostrazione.* Se  $d$  e  $d'$  sono due massimi comun divisori di  $a$  e  $b$ , allora vale che:

$$d \mid a \wedge d \mid b \quad \text{e} \quad x \mid a \wedge x \mid b \implies x \mid d$$

e contemporaneamente:

$$d' \mid a \wedge d' \mid b \quad \text{e} \quad x \mid a \wedge x \mid b \implies x \mid d'$$

dunque, considerando  $d$ , esso deve essere diviso da  $d'$  in quanto massimo comune divisore:

$$d = ud'$$

e simmetricamente:

$$d' = vd$$

da cui, sfruttando il fatto che  $A$  è un dominio segue:

$$d = ud' = uvd \implies d(1 - uv) = 0 \implies uv = 1 \implies u, v \in A^*$$

e quindi  $d \sim d'$  per definizione. □

**Definizione 2.83.** Dato un dominio  $A$  e  $x \in A$ , con  $x \notin A^* \cup \{0\}$ ,  $x$  si dice **primo** se  $\forall a, b \in A$ :

$$x \mid ab \implies x \mid a \vee x \mid b$$

**Definizione 2.84.** Dato un dominio  $A$  e  $x \in A$ , con  $x \notin A^* \cup \{0\}$ ,  $x$  si dice **irriducibile** se  $\forall a, b \in A$ :

$$x = ab \implies a \in A^* \vee b \in A^*$$

**Proposizione 2.85** (primo  $\implies$  irriducibile)

Dato  $A$  dominio, se  $x$  è primo, allora è irriducibile.

*Dimostrazione.* Supponiamo che:

$$x = ab$$

essendo  $x$  primo, allora  $x \mid a$  o  $x \mid b$ , assumiamo (WLOG) che  $x \mid a$ , allora:

$$a = xc \implies x = bcx \implies x(1 - bc) = 0$$

poiché  $A$  è un dominio, e poiché  $x \neq 0$  per ipotesi segue che:

$$bc = 1 \implies b, c \in A^*$$

in particolare ciò significa che  $x$  è irriducibile, in quanto scrivendolo come  $x = ab$ , abbiamo verificato che  $b \in A^*$ . □

**Proposizione 2.86** (Caratterizzazione di primi ed irriducibili in domini)

Dato un dominio  $A$  si ha che:

- (1)  $x$  è primo se e solo se  $(x)$  è un ideale primo non nullo.
- (2)  $x$  è irriducibile se e solo se  $(x)$  è un ideale massimale nell'insieme degli ideali principali.

*Dimostrazione.* Verifichiamo entrambe le proprietà:

- (1) Sia  $(x)$  un ideale primo, ovvero:

$$ab \in (x) \iff a \in (x) \vee b \in (x)$$

ciò è equivalente al richiedere che  $x \mid a$  o  $x \mid b$ , ovvero che  $x$  sia primo in  $A$ .

- (2) Dimostriamo separatamente le due implicazioni. Sia  $x$  irriducibile e supponiamo che sia  $(x) \subseteq (y) \subsetneq A$ , dunque  $\exists z \in A$  tale che  $x = yz$ , sappiamo che  $y \notin A^*$  (altrimenti sarebbe l'ideale contenebbe l'identità e avremmo  $(y) = A$ ), poiché  $x$  deve essere irriducibile segue necessariamente che  $z \in A^*$  e quindi  $x \sim y$ , cioè:

$$(x) = (y)$$

pertanto  $(x)$  è massimale tra gli ideali principali. Per il viceversa dimostriamo la contronominale; sia  $x$  riducibile, allora:

$$x = yz \quad \text{con } y, z \notin A^*$$

e per quanto detto segue che:

$$(x) \subsetneq (y) \subsetneq A$$

dove la seconda inclusione non può essere un'uguaglianza in quanto  $y \notin A^* \implies 1 \notin (y)$ , mentre la prima segue dal fatto che  $z \notin A^*$  (e quindi  $x$  e  $y$  non sono associati), pertanto  $(x)$  non è massimale tra gli ideali principali.

□

### Esempio 2.87

Osserviamo che se  $x$  è primo nel dominio d'integrità  $A = K[x, y]$ , allora:

$$A/(x) \cong K[y]$$

che sappiamo essere un dominio, dunque per la [Proposizione 2.56](#)  $(x)$  è primo. Poiché  $x$  è primo è anche irriducibile, quindi  $(x)$  è massimale tra gli ideali principali di  $A$ , ma non è un ideale massimale di  $A$  in quanto  $K[y]$  non è un campo, infatti:

$$(x) \subsetneq (x, y) \subsetneq A$$

ovvero  $(x)$  non è massimale in quanto è contenuto nell'ideale proprio  $(x, y)$ .

## §2.8 Domini euclidei (ED)

**Definizione 2.88.** Un dominio di integrità  $A$  si dice **dominio euclideo** (ED) se esiste una funzione:

$$d : A \setminus \{0\} \longrightarrow \mathbb{N}$$

detta **grado**, con le seguenti proprietà:

- (i)  $d(x) \leq d(xy)$ ,  $\forall x, y \in A \setminus \{0\}$ .
- (ii)  $\forall x \in A, \forall y \in A \setminus \{0\}, \exists q, r \in A$  tali che:

$$x = yq + r$$

con  $d(r) < d(y)$ <sup>47</sup> oppure  $r = 0$ .

**Osservazione 2.89** — In un dominio euclideo ogni elemento si può "ben approssimare" con un multiplo di ogni altro elemento. La funzione grado serve per dire cosa significa esattamente "approssimare bene".

### Esempio 2.90 (Domini Euclidei)

Vediamo alcuni esempi di domini euclidei:

- (1)  $(\mathbb{Z}, |\cdot|)$  è un dominio euclideo, infatti sappiamo che per le proprietà del valore assoluto vale che:

$$|xy| = |x||y| \geq |x| \quad \forall y \neq 0$$

ed esiste la divisione euclidea con il resto:

$$\forall x, y \in \mathbb{Z}, \exists q, r \in \mathbb{Z} : x = qy + r$$

con  $|r| < |y|$  oppure  $r = 0$ , la prima condizione posta non ci assicura l'unicità (infatti possiamo approssimare sia dal basso che dall'alto prendendo anche resti negativi), ma poiché sappiamo che in realtà vale:

$$0 \leq r < |y|$$

allora tale scrittura è unica.

- (2)  $(K[x], \deg)$  è un dominio euclideo, infatti:

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x) \geq \deg f(x)$$

e vale la divisione euclidea tra polinomi con resto:

$$\forall f(x), g(x) \in K[x], \exists q(x), r(x) \in K[x] : f(x) = g(x)q(x) + r(x)$$

con  $\deg r(x) < \deg g(x)$  oppure  $r(x) = 0$ .

- (3)  $(\mathbb{Z}[i], N)$ , l'anello degli **interi di Gauss**,  $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ , con la norma data da:

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N} : (a + ib) \alpha \longmapsto N(\alpha) = \alpha \bar{\alpha} = a^2 + b^2$$

<sup>47</sup>Ciò non assicura l'unicità di  $q$  ed  $r$ , ma non è richiesto dalla definizione.

Osserviamo che  $\mathbb{Z}[i] \subset \mathbb{Q}(i) \subset \mathbb{C}$ , dunque  $\mathbb{Z}[i]$  è un dominio. Osserviamo inoltre che valgono le proprietà richieste dalla definizione di dominio euclideo per la norma definita in precedenza:

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 \geq |\alpha|^2 = N(\alpha)$$

che è vera in quanto  $|\beta|^2 = x^2 + y^2 \geq 1$ . Per la proprietà (ii), vorremmo che  $\forall \alpha, \beta \in \mathbb{Z}[i]$ , con  $\beta \neq 0$ , si può "approssimare"  $\alpha$  con un multiplo di  $\beta$ ; abbiamo che  $\frac{\alpha}{\beta} \in \mathbb{C}$ , ma in generale non in  $\mathbb{Z}[i]$ , se  $\frac{\alpha}{\beta} \in \mathbb{Z}[i]$ , vogliamo trovare semplicemente il valore del rapporto in  $\mathbb{Z}[i]$  (ed abbiamo che  $r = 0$ ), se  $\frac{\alpha}{\beta} \notin \mathbb{Z}[i]$ , allora vogliamo scrivere:

$$\alpha = \beta q + r \quad \text{con} \quad N(r) < N(\beta)$$

Osserviamo il reticolo formato dai multipli di  $\beta$  nel piano complesso:<sup>48</sup>

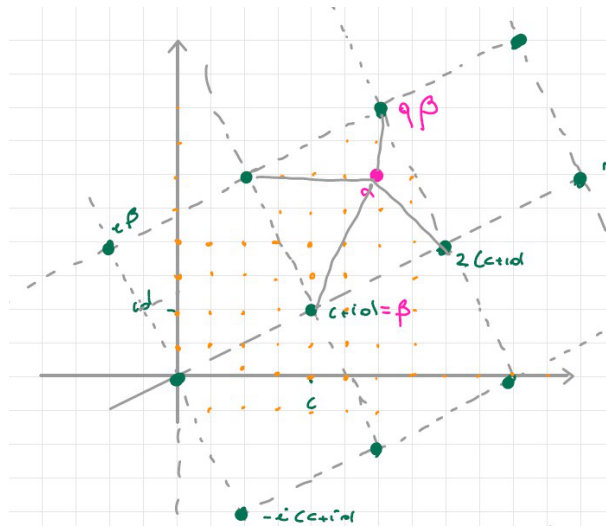


Figura 1: Reticolo dei multipli interi di  $\beta$  nel piano complesso.

Come si osserva  $\alpha$  cade in un quadrato (compreso il bordo) e del quale  $q\beta$  è il multiplo di  $\beta$  più vicino ad  $\alpha$ , pertanto, scelto  $q\beta$  abbiamo:

$$r = \alpha - q\beta$$

con  $N(r) < \frac{1}{2}$  diagonale quadrato  $<$  lato  $= N(\beta)$ .

### Proposizione 2.91 (Algoritmo di Euclide)

Dato un dominio euclideo  $A$ ,  $\forall a, b \in A$  non entrambi nulli esiste l'MCD  $(a, b)$ , determinato mediante l'algoritmo di Euclide.

*Dimostrazione.* Poiché in un dominio euclideo esiste una funzione grado (che è appunto il caso generale del valore assoluto) ed è possibile la divisione euclidea con resto per definizione, allora vale l'Algoritmo di Euclide con la stessa dimostrazione già vista per  $\mathbb{Z}$ , e con in questo caso l'applicazione grado generica al posto del valore assoluto:

<sup>48</sup>Immagine provvisoria, non appena ho tempo la disegno in TikZ.

- **L'algoritmo termina:** L'algoritmo termina perché la successione dei resti  $r_n$  è una successione a termini in  $\mathbb{N}$  strettamente decrescente, pertanto è definitivamente costante (in questo caso 0).
- **Correttezza dell'algoritmo:** Si dimostra l'algoritmo per induzione sul numero degli  $N$  passi richiesti. Sia  $\mathcal{P}(n)$  : "Se l'algoritmo termina in  $N$  passi, allora funziona.", per  $N = 1$ , si ha che:

$$a = qb + 0$$

con  $b = r_0$  (ovvero  $b \mid a$ ), e quindi  $(a, b) = r_0$ . Supponiamo per ipotesi induttiva che l'Algoritmo di Euclide funzioni per ogni numero di passi  $m \leq N - 1$  e proviamo che è vero per  $N$ . Sia:

$$\begin{cases} a = qb + r_1 & 0 \leq r_1 < |b| \\ r_0 = q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ \vdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_n r_n + 0 \end{cases}$$

possiamo applicare l'algoritmo di Euclide per  $(r_0, r_1)$  (in tal modo si ha una sequenza di  $N - 1$  passi) ed ottenere  $r_n = (b, r_1)$ :

$$\begin{cases} r_0 = q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ \vdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_n r_n + 0 \end{cases}$$

da cui  $r_n = (b, r_1) = (b, a - q_0 b) = (a, b)$ , dove l'ultima uguaglianza è giustificata dalla proprietà dell'M.C.D.

□

### Proposizione 2.92 (Elementi invertibili)

Dato un dominio euclideo  $A$ , gli elementi di grado minimo sono gli elementi di  $A^*$ .

*Dimostrazione.* Consideriamo  $d(A \setminus \{0\}) \subset \mathbb{N}$ , ovvero l'immagine del dominio euclideo mediante l'applicazione grado, tale immagine è non vuota<sup>49</sup> ed è un sottoinsieme di  $\mathbb{N}$ , pertanto, per il Principio del Minimo ammette elemento minimo  $d_0$ , sia  $x \in A \setminus \{0\}$  un elemento nella controimmagine di  $d_0$ , quindi tale che  $d(x) = d_0$ , tale elemento è quindi di grado minimo, vediamo che è invertibile. Sappiamo che  $\forall y \in A \setminus \{0\}$  possiamo fare la divisione euclidea per  $x$ :

$$y = qx + r$$

ed in questo caso non può essere che  $d(r) < d(x) = d_0$ , in quanto abbiamo supposto  $d_0$  minimo, dunque l'unica possibilità è che  $r = 0$  e  $y = qx$ , in particolare, per  $y = 1$ ,  $\exists q \in A$  tale che:

$$1 = qx \implies x \in A^*$$

<sup>49</sup>Praticamente è ovvio, altrimenti non avrebbe nemmeno senso parlare di  $A$  come dominio.

Viceversa, sia  $x \in A^*$ , allora  $(x) = A$  (poiché in  $(x)$  vi è 1), pertanto,  $\forall a \in A$ :

$$a = qx \quad q \in A$$

inoltre, sappiamo per le proprietà del grado che  $d(x) \leq d(qx)$ ,  $\forall q \in A \setminus \{0\}$ , ovvero:

$$d(x) \leq d(a) \quad \forall a \in A$$

quindi  $x$  è un elemento di grado minimo. □

### Proposizione 2.93 (Ideali di un dominio euclideo)

Dato un dominio euclideo  $A$ , tutti gli ideali di  $A$  sono principali<sup>a</sup> e generati da un elemento di grado minimo.

<sup>a</sup>Quindi ogni dominio euclideo è un PID.

*Dimostrazione.* Sia  $I \subset A$  un ideale, se  $I = \{0\}$ , allora è principale, altrimenti, preso  $I \neq \{0\}$ , vogliamo mostrare che  $I$  è generato da un singolo elemento di grado minimo. Sia  $x \in I$  un elemento di grado minimo (esiste perché  $d(I) \subset \mathbb{N}$  e non vuoto), allora è ovvio che  $(x) \subseteq I$ , viceversa, si ha che  $\forall a \in A$  si può fare la divisione euclidea per  $x$ :

$$a = qx + r \quad d(r) < d(x) \vee r = 0$$

da cui segue che  $r = a - qx \in I$  da cui  $d(x) \leq d(r) \implies r = 0$ , ovvero:

$$a = qx \in (x) \implies I \subseteq (x)$$

□

## §2.9 Domini a ideali principali (PID)

**Definizione 2.94.** Un dominio  $A$  si dice a **ideali principali** (PID) se ogni ideale di  $A$  è principale:

$$\forall I \subseteq A, I \text{ ideale}, \exists x \in I : I = (x)$$

### Proposizione 2.95 (Ideali primi di un PID)

Dato un dominio ad ideali principali  $A$ , gli unici ideali primi di  $A$  sono  $(0)$  e gli ideali massimali.

*Dimostrazione.* Dall'(1) del [Corollario 2.57](#) sappiamo che il fatto che  $A$  sia un dominio è equivalente al fatto che  $(0)$  sia un ideale primo, inoltre, dal (3) del [Corollario 2.57](#) sappiamo anche che tutti gli ideali massimali di un anello sono primi.

Viceversa, vogliamo dimostrare che gli ideali primi diversi da  $(0)$  di un dominio a ideali principali sono solo quelli massimali; sia  $P$  un ideale primo diverso da  $(0)$ , essendo in un PID si ha che  $P = (x)$ , verifichiamo che  $P$  è massimale osservando che, essendo  $A$  un dominio, per l'(1) della [Proposizione 2.86](#),  $P$  è primo se e solo se  $x$  è primo, e dunque  $x$  irriducibile (è vero in ogni dominio per la [Proposizione 2.58](#)). Essendo  $x$  irriducibile segue che  $(x)$  è massimale tra gli ideali principali di  $A$  (per il (2) della [Proposizione 2.86](#)), e poiché  $A$  è un PID (dunque tutti gli ideali sono principali), allora  $(x)$  è un ideale massimale per  $A$ .  $\square$

**Osservazione 2.96 (M.C.D. nei PID)** — Se  $A$  è un PID e  $x, y \in A$ , non entrambi nulli, osserviamo che l'ideale generato da  $x$  e  $y$  deve essere tale che:

$$(x, y) = (d)$$

con  $d$  un M.C.D.<sup>a</sup> di  $x$  e  $y$ . Infatti:

$$x \in (d) \quad \text{e} \quad y \in (d)$$

dunque  $d \mid x$  e  $d \mid y$ , inoltre, se  $c \mid x$  e  $c \mid y$ , allora  $x, y \in (c)$ , da cui:

$$(d) = (x, y) \subseteq (c) \implies d \in (c) \implies c \mid d$$

dunque  $d$  è un M.C.D. tra  $x$  ed  $y$ .

<sup>a</sup>M.C.D. a meno di prodotto per elementi di  $A^*$ .



## §2.10 Domini a fattorizzazione unica (UFD)

**Definizione 2.97.** Dato  $A$  un dominio, esso si dice **a fattorizzazione unica** (UFD) se  $\forall x \in A$ ,  $x \notin A^* \setminus \{0\}$  si scrive in modo unico, a meno dell'ordine di fattori e di moltiplicazione per elementi invertibili, come prodotto di elementi irriducibili.

### Esempio 2.98 (Esempi di UFD)

Esempi noti di UFD sono il dominio degli interi  $\mathbb{Z}$ , i polinomi in  $\mathbb{Z}[x]$  e in generale polinomi in un'ordinata a coefficienti in un campo  $K[x]$ .

### Proposizione 2.99 (UFD $\Rightarrow$ $\exists$ M.C.D.)

Sia  $A$  un dominio a fattorizzazione unica, allora presi  $a, b \in A$ , non entrambi nulli, esiste M.C.D.  $(a, b)$ .

*Dimostrazione.* Sia  $d$  il prodotto dei fattori irriducibili comuni fra  $a$  e  $b$ , presi con il minimo esponente con cui compaiono, allora per verifica diretta si mostra che  $d$  è l'M.C.D.<sup>50</sup>  $\square$

**Osservazione 2.100** — Osserviamo che nei tre tipi di domini analizzati esiste sempre l'M.C.D., ma con delle differenze:

- Se  $A$  è un dominio euclideo (ED): con l'algoritmo di Euclide si può determinare l'M.C.D. di due elementi:

$$d = (a, b) \quad a, b \in A$$

e i coefficienti  $x_0, y_0 \in A$  per i quali vale l'identità di Bézout:

$$d = ax_0 + by_0$$

- Se  $A$  è un dominio a ideali principali (PID): sappiamo che presi due elementi si ha:

$$(a, b) = (d) \quad a, b, d \in A$$

con  $d$  che è l'M.C.D. tra  $a$  e  $b$ , ma non disponiamo di un algoritmo "facile" per poterlo determinare, tuttavia esistono  $x_0, y_0 \in A$  tali che:

$$d = ax_0 + by_0$$

e ciò deriva semplicemente dal fatto che  $d \in (a, b)$ , dunque si può scrivere come loro combinazione lineare (ugualmente però non disponiamo di algoritmi "facili" per poter determinare  $x_0$  e  $y_0$ ).

- Se  $A$  è un dominio a fattorizzazione unica (UFD): allora  $\forall a, b \in A$  non entrambi nulli, esiste  $d = \text{M.C.D.}(a, b)$ , ma **non è detto che**  $(d) = (a, b)$  e quindi neppure che  $d = ax_0 + by_0$ . Infatti, sicuramente è vero che  $(a, b) \subset (d)$ , ma non

<sup>50</sup>Si tratta praticamente solo di verifiche formali, pertanto conto di aggiungerla in seguito.

è detto che valga il contenimento opposto, il quale vale solo se  $d = ax_0 + by_0$ .  
Ad esempio, preso l'UFD  $\mathbb{Z}[x]$ , l'ideale:

$$I = (2, x)$$

è tale che  $\text{M.C.D.}(2, x) = 1$ , ma  $1 \notin (2, x)$ , perché se non fosse così avremmo:

$$1 = 2a(x) + xb(x)$$

che per  $x = 0$  porta a:

$$1 = 2a(0) + 0 \implies 2 \mid 1$$

che è assurdo.

### Teorema 2.101 (Caratterizzazione degli UFD)

Dato un dominio  $A$ , sono fatti equivalenti:

- (1)  $A$  è un UFD.
- (2) Valgono le due condizioni seguenti:
  - (i) Ogni elemento irriducibile è primo.
  - (ii) Ogni catena discendente di divisibilità è stazionaria, ovvero se  $\{a_i\} \subset A$ , con:

$$a_{i+1} \mid a_i \quad \forall i \geq 0$$

allora  $\exists n_0$  tale che  $a_i \sim a_{n_0}$ ,  $\forall i \geq n_0$ .

**Osservazione 2.102** — La condizione (i) permette di dimostrare che la fattorizzazione in primi è unica, dunque è equivalente a questo fatto; mentre, la condizione (ii) permette di dimostrare l'esistenza della fattorizzazione, e quindi vi è equivalente, pertanto il teorema dice che essere un UFD è equivalente al fatto che in un dominio valga il teorema di fattorizzazione unica.

**Osservazione 2.103** — Osserviamo che la condizione (ii) può essere riformulata equivalentemente come: ogni catena ascendente di ideali principali è stazionaria, ovvero, considerata  $\{(a_i)\}_{i \geq 0}$ , catena ascendente di ideali di  $A$ :

$$(a_1) \subseteq (a_2) \subseteq \dots$$

allora  $\exists n_0$  tale che  $(a_i) = (a_{n_0})$ ,  $\forall i \geq n_0$ .<sup>a</sup>

<sup>a</sup>Tra l'altro ciò, estendendo la condizione di stazionarietà ad ogni catena di ideali (quindi non solo principali), definisce un **anello noetheriano**.

### Corollario 2.104 ( $A \text{ PID} \implies A \text{ UFD}$ )

Se  $A$  è un dominio a ideali principali, allora è anche un dominio a fattorizzazione unica.

*Dimostrazione.* Per dimostrare il corollario ci basta verificare che per ogni PID valgono le condizioni (i) e (ii) del [Teorema 2.101](#), e ciò è equivalente al dire che ogni PID è un UFD. Sia  $A$  un PID, e sia  $x \in A$  un elemento irriducibile, per quanto visto nella [Proposizione 2.95](#) l'ideale  $(x)$  è massimale in  $A$ , ma dalla (3) del [Corollario 2.57](#), sappiamo quindi che  $(x)$  è primo, e poiché siamo in un dominio vale la (1) della [Proposizione 2.86](#) che ci assicura che  $x$  è primo, dunque vale la (i).

Consideriamo ora una catena ascendente di ideali (principali):

$$(a_1) \subseteq (a_2) \subseteq \dots$$

e sia:

$$I = \bigcup_{i \geq 0} (a_i)$$

tale unione di ideali in catena è un ideale<sup>51</sup> di  $A$ , ed è pertanto principale, dunque  $I = (a)$ . Osserviamo che  $a$  appartiene all'unione, per cui  $a \in (a_{n_0})$ , e quindi:

$$I = (a) \subseteq (a_{n_0})$$

ma d'altra parte avevamo detto che  $I$  è l'unione di tutti gli ideali principali di  $A$ , quindi  $(a_{n_0}) \subseteq (a) = I$ , dunque  $I = (a_{n_0})$ ; a questo punto sappiamo che:

$$(a_i) \subset (a_{n_0}) \quad \forall i \geq 0$$

dove si ha  $(a_i) = (a_{n_0})$  quando vi è anche il contenimento opposto, e ciò avviene, poiché stiamo considerando ideali in catena,  $\forall i \geq n_0 \implies \{(a_i)\}$  è stazionaria e quindi è verificata la (ii).  $\square$

**Osservazione 2.105** — L'ultimo corollario ci permette di poter mettere in relazione i vari tipi di domini d'integrità:

$$\underbrace{\text{ED}}_{\text{Domini euclidei}} \subset \underbrace{\text{PID}}_{\text{Domini a ideali principali}} \subset \underbrace{\text{UFD}}_{\text{Domini a fattorizzazione unica}}$$

### Esempio 2.106 (Anello senza la (ii))

Consideriamo l'estensione  $K[\{x^{\frac{1}{n}}\}_{n \geq 1}]$ , essa non è un UFD, in quanto non vale la (ii) dell'[Teorema 2.101](#):

$$x^{\frac{1}{2^{n+1}}} \mid x^{\frac{1}{2^n}} \mid \dots \mid x^{\frac{1}{4}} \mid x^{\frac{1}{2}} \mid x$$

dove tale catena non è definitivamente stazionaria (il successivo può sempre dividere il precedente) dunque non esiste la fattorizzazione di  $x$ .

<sup>51</sup>Come già osservato in precedenza ciò andrebbe dimostrato.

**Esempio 2.107** (Anello senza la (i))

Consideriamo l'anello  $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{-5}) \subset \mathbb{C}$ , tale anello non è un UFD poiché non vale la (i), infatti, ad esempio, 2 è irriducibile ma non primo in  $\mathbb{Z}[\sqrt{-5}]$ :

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \implies N(2) = (a^2 + 5b^2)(c^2 + 5d^2)$$

da cui possiamo dedurre che le uniche possibilità sono  $a = \pm 2, c = \pm 1, b = 0, d = 0$  (oppure invertiti), pertanto 2 è irriducibile, ma non è primo perché:

$$2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad \text{ma} \quad 2 \nmid (1 + \sqrt{-5}), (1 - \sqrt{-5})$$

poiché,  $\alpha = \frac{1 \pm \sqrt{-5}}{2} = \frac{1}{2} \pm \frac{\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$ . In  $\mathbb{Z}[\sqrt{-5}]$  abbiamo quindi due fattorizzazioni distinte per 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})^a$$

<sup>a</sup>Per essere precisi dovremmo verificare che  $2, 3, 1 \pm \sqrt{-5}$  sono irriducibili in  $\mathbb{Z}[\sqrt{-5}]$ .

**Osservazione 2.108** —  $\mathbb{Z}[\sqrt{-5}]$  non essendo un UFD, non è neppure un PID, infatti, ad esempio, l'ideale  $(2, 1 + \sqrt{-5})$  non è principale.

**Teorema 2.109** ( $A$  UFD  $\implies A[x]$  UFD)

Se  $A$  è un dominio a fattorizzazione unica, allora anche  $A[x]$  è un anello a fattorizzazione unica.

**Corollario 2.110** ( $A$  UFD  $\implies A[x_1, \dots, x_n]$  UFD)

Se  $A$  un dominio a fattorizzazione unica, allora anche  $A[x_1, \dots, x_n]$  è un anello a fattorizzazione unica.

*Dimostrazione.* Dal [Teorema 2.109](#) segue il caso base  $A[x]$ , per induzione si suppone vera la tesi per  $A[x_1, \dots, x_{n-1}] = B$ , e poi si considera  $B[x_n]$ , che è un UFD per il caso iniziale, dunque la tesi è vera per induzione.  $\square$

**Osservazione 2.111** (Schema della dimostrazione del Teorema 2.109) — La dimostrazione del [Teorema 2.109](#) si articola in tre tappe:

- (1)  $A[x]$  dominio.
- (2) Ogni irriducibile di  $A[x]$  è primo (condizione (i)).
- (3) Ogni catena discendente di divisibilità è stazionaria (condizione (ii)).

Da cui si conclude per il [Teorema di Caratterizzazione degli UFD](#).

*Dimostrazione.* Iniziamo quindi verificando il primo punto come segue.

- (1) Siano  $f(x), g(x) \in A[x] \setminus \{0\}$ , e  $\deg f(x) = n \geq 0$ ,  $\deg g(x) = m \geq 0$ , essendo  $a_n, b_m \neq 0$ , segue che  $a_n b_m \neq 0$  poiché per ipotesi  $A$  un dominio di integrità, pertanto  $f(x) \cdot g(x) \neq 0$  se  $f(x), g(x) \neq 0 \implies A[x]$  è un dominio d'integrità.

**Osservazione 2.112** — Osserviamo anche che da ciò discende che  $(A[x])^* = A^*$ , infatti, considerando  $f(x) \in (A[x])^*$ ,  $\exists g(x) \in A[x]$  tale che:

$$f(x)g(x) = 1 \implies \deg f(x) + \deg g(x) = 0$$

ovvero  $\deg f(x) = \deg g(x) = 0$ , per cui  $f(x), g(x) \in A$ , ed in particolare  $f(x) = a, g(x) = b$ , pertanto:

$$ab = 1 \implies f(x) \in A^*$$

□

Per verificare la condizione (i) dobbiamo prima caratterizzare gli irriducibili di  $A[x]$ , e fare ciò abbiamo bisogno del Lemma di Gauss.

**Definizione 2.113.** Dato  $A$  un UFD e  $f(x) \in A[x]$ , con  $f(x) = \sum_{i=0}^n a_i x^i$ , si dice **contenuto** di  $f(x)$  l'M.C.D. dei suoi coefficienti:

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

**Osservazione 2.114** — Il contenuto di un polinomio a coefficienti in un UFD è definito a meno di associati.

**Definizione 2.115.** Dato  $A$  un UFD e  $f(x) \in A[x]$ ,  $f(x)$  si dice **primitivo** se  $c(f(x)) \sim 1$ .

**Osservazione 2.116** — Ovviamente dato  $f(x) \in A[x]$  si ha che:

$$f(x) = c(f(x))f'(x) \quad c(f'(x)) = 1$$

dove  $f'(x) \in A[x]$  e:

$$f'(x) = \sum_{i=0}^n \frac{a_i}{d} x^i \quad \frac{a_i}{d} \in A, \left( \frac{a_0}{d}, \dots, \frac{a_n}{d} \right) = 1$$

#### Lemma 2.117 (Lemma di Gauss)

Dati  $f(x), g(x) \in A[x]$ , allora:

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

*Dimostrazione.* Distinguiamo due casi:

- Se  $c(f(x)) = c(g(x)) = 1$ , dunque  $f(x)$  e  $g(x)$  sono primitivi, vogliamo verificare che  $c(f(x)g(x)) = 1$ ; se  $f(x)g(x)$  non fosse primitivo (ovvero associato ad 1) allora  $c(f(x)g(x))$  non sarebbe invertibile (gli elementi invertibili sono associati ad 1),

ovvero esisterebbe  $p$  primo tale che  $p \mid c(f(x)g(x))$ , consideriamo la proiezione modulo  $(p)$ :

$$\pi_{(p)} : A[x] \longrightarrow \frac{A}{(p)}[x] : f(x) \longmapsto \overline{f(x)}$$

con  $\overline{f(x)} \neq 0$  in quanto  $p \nmid c(f(x))$ , analogamente  $\pi_{(p)}(g(x)) = \overline{g(x)} \neq 0$ , poiché  $p \nmid c(g(x))$ , ma  $\pi_{(p)}(f(x)g(x)) = \overline{f(x)}\overline{g(x)} = 0$ , perché avevamo supposto che  $p \mid c(f(x)g(x))$ , ma questo è assurdo in quanto  $\frac{A}{(p)}$  è un dominio e quindi, per quanto detto,  $A$  dominio  $\implies A[x]$  dominio, ovvero  $\frac{A}{(p)}[x]$  è un dominio, da cui  $c(f(x)g(x)) = 1$ .

- Consideriamo ora il caso generale, sia  $f(x) = c(f(x))f'(x)$ , con  $f'(x)$  primitivo, e analogamente  $g(x) = c(g(x))g'(x)$ , con  $g'(x)$  primitivo, abbiamo che:

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

dove  $h'(x) = g'(x)f'(x)$  è primitivo perché prodotto di polinomi primitivi, dunque:

$$h(x) = c(h(x))h'(x)$$

e uguagliando i contenuti si ha:

$$\underbrace{c(h(x))c(h'(x))}_{=1} = c(f(x))c(g(x))\underbrace{c(g'(x)f'(x))}_{=1} \implies c(h(x)) = c(f(x)g(x)) = c(f(x))c(g(x))$$

□

### Corollario 2.118

Siano  $f(x), g(x) \in A[x]$ , 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  $A[x]$ .

*Dimostrazione.* Per ipotesi sappiamo che  $f(x) \mid g(x)$  in  $K[x]$ , ovvero  $\exists h(x) \in K[x]$  tale che  $g(x) = f(x)h(x)$ , allora  $\exists d \in A$  tale che:

$$h_1(x) = dh(x) \in A[x]$$

(stiamo "cancellando" il denominatore), dunque:

$$dg(x) = f(x)h_1(x) \in A[x]$$

da cui per il [Lemma di Gauss](#):

$$dc(g(x)) = c(f(x)h_1(x)) = c(f(x))c(h_1(x)) = c(h_1(x)) \implies d \mid c(h_1(x))$$

dove abbiamo usato nell'ultimo passaggio il fatto che  $c(f(x)) = 1$ , dunque abbiamo  $\frac{h_1(x)}{d} = h(x) \in A[x]$  e quindi la divisibilità iniziale era anche in  $A[x]$ . □

### Corollario 2.119

Sia  $f(x) \in A[x]$  e  $f(x) = g(x)h(x)$  in  $K[x]$  (con  $K$  campo dei quozienti di  $A$ ), con  $\deg f(x), \deg g(x) \geq 1$ , allora esiste  $\delta \in K^*$  tale che  $g_1(x) = \delta g(x) \in A[x]$ ,  $h_1(x) = \delta^{-1}h(x) \in A[x]$  e  $f(x) = g_1(x)h_1(x)$ .

*Dimostrazione.* Analogamente a quanto fatto per il corollario precedente, sappiamo che  $\exists d \in A$  tale che  $g_1(x) = dg(x) \in A[x]$  (stiamo di nuovo "eliminando" i denominatori, ad esempio moltiplicando per l'm.c.m.), dunque:

$$f(x) = dg(x)d^{-1}h(x) = g_1(x)(d^{-1}h(x)) = c(g_1(x))g'_1(x)(d^{-1}h(x))$$

con  $g'_1(x) \in A[x]$  primitivo (dividendo per il contenuto, che è un invertibile di  $A$ , siamo rimasti in  $A[x]$ ), pertanto abbiamo:

$$f(x) = g'_1(x) \underbrace{(c(g_1(x))d^{-1}h(x))}_{\in K[x]}$$

ovvero  $g'_1(x) \mid f(x)$  in  $K[x]$ , ma allora per il [Corollario 2.118](#) segue che  $g'_1(x) \mid f(x)$  in  $A[x]$ , dunque:

$$h_1(x) = \underbrace{\frac{c(g_1(x))}{d}}_{=\delta^{-1}} h(x)$$

abbiamo quindi determinato  $\delta$  e  $\delta^{-1}$  richiesti dalla tesi.  $\square$

**Osservazione 2.120** — Il teorema non ci dice altro che se  $f(x)$  è riducibile in  $K[x]$ , allora è riducibile anche in  $A[x]$ , con polinomi dello stesso grado (per la precisione associati a quelli iniziali).<sup>a</sup>

<sup>a</sup>In [Aritmetica](#), avevamo trattato il caso particolare del Lemma di Gauss applicato a  $\mathbb{Q}[x]$  e  $\mathbb{Z}[x]$ .

### Esempio 2.121

Un esempio del discorso appena fatto è rappresentato dalla fattorizzazione di un polinomio in  $\mathbb{Q}[x]$  e  $\mathbb{Z}[x]$ :

$$(x^2 - 1) = \left(\frac{100}{7}x + \frac{100}{7}\right) \left(\frac{7}{100}x - \frac{7}{100}\right) = (x+1)(x-1)$$

### Teorema 2.122 (Caratterizzazione degli irriducibili di $A[x]$ )

Dato  $A$  UFD, gli elementi irriducibili di  $A[x]$  sono tutti e soli quelli che soddisfano una tra le seguenti:

- (1)  $f(x) \in A$  irriducibile in  $A$ .
- (2)  $f(x) \in A[x]$ , con  $\deg f(x) \geq 1$ ,  $c(f(x)) = 1$  e  $f(x)$  irriducibile in  $K[x]$  (anello dei polinomi a coefficienti nel campo dei quozienti di  $A$ ).

*Dimostrazione.* Distinguiamo i due casi:

1. Se  $f(x) \in A$ , dunque è costante, allora, come già osservato in precedenza, si ha:

$$f(x) = g(x)h(x) \implies \deg g(x) + \deg h(x) = \deg f(x) = 0$$

dove l'implicazione è data dal fatto che siamo in un dominio, dunque segue che  $\deg g(x) = \deg h(x) = 0$ , pertanto  $g(x), h(x) \in A$ , per cui  $f(x)$  è irriducibile in  $A[x]$  se e sole  $f(x)$  è irriducibile in  $A$  (che è la stessa cosa che avevamo già osservato dicendo che  $(A[x])^* = A^*$ ).

2. Sia  $f(x)$  con  $\deg f(x) \geq 1$ . Supponiamo che  $f(x)$  sia irriducibile in  $A[x]$ , abbiamo che:

$$f(x) = c(f(x))f'(x)$$

con  $c(f(x))$  invertibile in  $A[x]$ ,  $c(f(x)) \in (A[x])^* = A^*$  (per quanto detto al punto (1)), d'altra parte, sia  $f(x) = g(x)h(x)$  in  $K[x]$ , allora per il [Corollario 2.119](#), possiamo scriverlo come prodotto di polinomi dello stesso grado in  $A[x]$ :

$$f(x) = g_1(x)h_1(x) \quad \text{con} \quad \deg g_1(x) = \deg g(x), \deg h_1(x) = \deg h(x)$$

poiché  $f(x)$  è irriducibile in  $A[x]$  deve essere che  $g_1(x)$  o  $h_1(x)$  sono invertibili. Abbiamo quindi che  $\deg g_1(x) = 0$  o  $\deg h_1(x) = 0$ , da cui  $\deg g(x) = 0$  o  $\deg h(x) = 0$ , ovvero  $g(x) \in (K[x])^*$  o  $h(x) \in (K[x])^*$ , dunque  $f(x)$  è irriducibile in  $K[x]$ . Verifichiamo il viceversa, sia  $f(x)$  primitivo ed irriducibile in  $K[x]$ , e sia  $f(x) = g(x)h(x)$  in  $A[x]$  (e anche in  $K[x]$ ), poiché  $f(x)$  è irriducibile in  $K[x]$   $g(x)$  o  $h(x)$  sono invertibili in  $K[x]$  e quindi costanti, supponiamo quindi ad esempio che sia  $g(x) \in A$ , da ciò segue che:

$$1 = c(f(x)) = c(g(x)h(x)) = c(g(x))c(h(x)) = gc(h(x))$$

dove nell'ultima uguaglianza abbiamo usato il fatto che, essendo  $g(x)$  costante, allora è uguale al suo contenuto, dunque  $g \in A^*(= (A[x])^*)$ , pertanto  $f(x)$  è irriducibile in  $A[x]$ .

□

### Proposizione 2.123 (Condizione (i) per $A[x]$ )

Dato  $A$  UFD, in  $A[x]$  ogni irriducibile è primo.

*Dimostrazione.* Sia  $f(x) \in A[x]$  irriducibile, per dimostrare che è primo bisogna verificare che  $\forall g(x), h(x) \in A[x]$  si ha che:

$$f(x) \mid g(x)h(x) \implies f(x) \mid g(x) \quad \text{o} \quad f(x) \mid h(x) \quad \text{in } A[x]$$

Distinguiamo due casi:

- Se  $\deg f(x) = 0$ , ovvero  $f(x) = f \in A$ , dunque se  $f$  è irriducibile in  $A$ , essendo  $A$  UFD, allora  $f$  è primo in  $A$ ; infatti abbiamo che:

$$f \mid gh \implies f = c(f) \mid c(gh) = c(g)c(h) \implies f \mid c(g) = g \quad \text{o} \quad f \mid c(h) = h$$

dunque  $f$  primo.



- Sia  $f(x)$  primitivo e irriducibile in  $K[x]$ , con  $\deg f(x) \geq 1$ , si osserva che  $K[x]$  è euclideo, dunque  $f(x)$  è primo in  $K[x]$  (poiché avevamo detto che  $ED \subset UFD$ ), dunque se:

$$f(x) \mid g(x)h(x) \quad \text{in } A[x]$$

allora  $f(x) \mid g(x)$  o  $f(x) \mid h(x)$  in  $K[x]$ . Avendo supposto che  $f(x)$  è primitivo, allora per il [Corollario 2.118](#):

$$f(x) \mid g(x)h(x) \quad \text{in } A[x]$$

□

### Proposizione 2.124 (Condizione (ii) per $A[x]$ )

Sia  $\{f_n(x)\}$  una successione di elementi di  $A[x]$  tale che:

$$f_{i+1}(x) \mid f_i(x)$$

allora è stazionaria, ovvero  $\exists n_0$  tale che  $f_i(x) \sim f_{n_0}(x)$ ,  $\forall i \geq n_0$ .

*Dimostrazione.* Si osserva che per il [Lemma di Gauss](#) si ha che:

$$f(x) \mid g(x) \implies c(f(x)) \mid c(g(x)) \quad \text{e} \quad f'(x) \mid g'(x)$$

infatti, se  $g(x) = f(x)h(x) \implies c(g(x))g'(x) = c(f(x))f'(x)c(h(x))c'(x)$ , ma per quanto detto  $c(g(x)) = c(f(x)h(x)) = c(f(x))c(h(x))$ , da cui  $f'(x) \mid g'(x)$ . Alla successione  $\{f_i(x)\}$  possiamo quindi associare le successioni  $\{c(f_i(x))\}$  e  $\{f'_i(x)\}$ , per quanto abbiamo detto si ha:

$$c(f_{i+1}(x)) \mid c(f_i(x)) \quad \text{e} \quad f'_{i+1}(x) \mid f'_i(x) \quad \forall i \geq 0$$

dove la successione  $\{c(f_i(x))\}$  è stazionaria, in quanto è una catena discendente di divisibilità dell'UFD  $A$ , dunque:

$$\exists m_0 : c(f_i(x)) \sim c(f_{m_0}(x)) \quad \forall i \geq m_0$$

Consideriamo ora  $\{f'_i(x)\}$  e associamo a questa la successione  $\{\deg f'_i(x)\}$ , ma dalla condizione:

$$f'_{i+1}(x) \mid f'_i(x) \implies \deg f'_{i+1}(x) \leq \deg f'_i(x)$$

dunque  $\{\deg f'_i(x)\}$  è una successione di numeri naturali decrescente, pertanto si stabilizza:

$$\exists d_0 : \deg f'_i(x) \leq \deg f'_{d_0}(x) \quad \forall i \geq d_0$$

pertanto  $\forall i \geq d_0$  abbiamo che  $f'_i(x)$  e  $\deg f'_{i+1}(x)$  hanno lo stesso grado e  $f'_i(x) \mid f'_{d_0}(x)$ , cioè differiscono per una costante, ma essendo entrambi primitivi la costante deve essere un'unità, per cui:

$$f'_i(x) \sim f'_{d_0}(x) \quad \forall i \geq d_0$$

dunque, detto  $n_0 = \max\{m_0, d_0\}$ ,  $\forall i \geq n_0$  vale contemporaneamente che:

$$c(f_i(x)) \sim c(f_{m_0}(x)) \quad \text{e} \quad f'_i(x) \sim f'_{d_0}(x)$$

da cui la tesi:

$$f_i(x) = c(f_i(x))f'_i(x) \sim c(f_{n_0}(x))f'_{n_0}(x) \quad \forall i \geq n_0$$

□

Con la dimostrazione di quest'ultima proposizione abbiamo concluso la dimostrazione del [Teorema di Caratterizzazione degli UFD](#).

**Osservazione 2.125** — Osserviamo che in generale se  $A$  è un PID, allora non è sempre vero che  $A[x]$  sia un PID, ad esempio nel caso di  $\mathbb{Z}$  sappiamo che  $\mathbb{Z}[x]$  non è un PID, in quanto, ad esempio, l'ideale  $I = (2, x)$  non è principale. Analogamente, in generale se  $A$  è un ED, allora non è sempre vero che  $A[x]$  sia un ED, anche qui come controesempio possiamo considerare il caso di  $\mathbb{Z}$  e  $\mathbb{Z}[x]$ .

**Osservazione 2.126** — Se  $K$  è un campo, allora abbiamo che  $K[x]$  è euclideo, mentre  $K[x, y]$  è un UFD (poiché vale sempre il [Teorema di Caratterizzazione degli UFD](#), e  $K[x]$  è un UFD), ma  $K[x, y]$  non è un PID, in quanto ad esempio  $I = (x, y)$  non è principale.

**Esercizio 2.127.** Dimostrare che dato  $K[x, y]$  campo, l'ideale  $I = (x, y)$  non è principale.

*Soluzione.*

□

**Proposizione 2.128** (Criterio di irriducibilità Eisenstein)

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

- (1)  $p \nmid a_n$ .
- (2)  $p \mid a_i, \forall i \in \{0, \dots, n-1\}$ .
- (3)  $p^2 \nmid a_0$ .

Allora  $f(x)$  è irriducibile in  $A[x]$  (e in  $K[x]$ , con  $K$  campo dei quozienti di  $A$ ).

*Dimostrazione.* La dimostrazione è identica a quella già trattata in [Aritmetica](#), con la sola differenza che in questo caso utilizziamo un UFD generico al posto di  $\mathbb{Z}$ .

Supponiamo per assurdo che  $f(x)$ , con  $\deg(f(x)) = n$  sia riducibile, allora:

$$f(x) = g(x)h(x)$$

con  $\deg f(x) = m \geq 1$ ,  $\deg(h(x)) = n - m \geq 1$ . Possiamo applicare la proiezione al quoziente modulo  $(p)$ , e per le ipotesi si ha:

$$\overline{f(x)} = \overline{a_n}x^n (\neq \overline{0})$$

e inoltre:

$$\pi_{(p)}(f(x)) = \pi_{(p)}(g(x))\pi_{(p)}(h(x))$$

con:

$$\pi_{(p)}(g(x)) = \overline{b_m}x^m + \dots + \overline{b_0} \quad \text{e} \quad \pi_{(p)}(h(x)) = \overline{c_{n-m}}x^{n-m} + \dots + \overline{c_0}$$

Si ha che  $\pi_{(p)}(f(x)) \in \frac{A}{(p)}[x]$  (che è un campo), quindi UFD, da ciò segue che  $\pi_{(p)}(g(x))$  e  $\pi_{(p)}(h(x))$  sono fattori del polinomio  $\overline{a_n}x^n$ , da cui segue, per la definizione di prodotto tra polinomi che:

$$\pi_{(p)}(g(x)) = \overline{b_m}x^m \quad \text{e} \quad \pi_{(p)}(h(x)) = \overline{c_{n-m}}x^{n-m}$$

ma da ciò segue che  $b_0 \equiv c_0 \equiv 0 \pmod{p}$ , da cui  $a_0 \equiv b_0 c_0 \equiv 0 \pmod{p^2}$ , ovvero  $p^2 \mid a_0$ , ma ciò è assurdo. □

## §2.11 Terne pitagoriche

**Definizione 2.129.** Si definiscono **terne pitagoriche** le terne di soluzioni intere dell'equazione:

$$x^2 + y^2 = z^2 \quad x, y, z \in \mathbb{Z}$$

con  $(x, y, z) = 1$ .

Osserviamo che possiamo riformulare il problema negli interi di Gauss nel modo che segue:

$$x^2 + y^2 = (x + iy)(x - iy) = z^2$$

dunque determinare le terne pitagoriche significa risolvere questo problema moltiplicativo in  $\mathbb{Z}[i]$ .

**Osservazione 2.130 —** Osserviamo che la coprimalità dei tre fattori la implica anche a coppie:  $(x, y, z) = 1 \implies (x, y) = (x, z) = (y, z) = 1$ .

**Osservazione 2.131 —** Abbiamo che  $x \not\equiv y \pmod{2}$ , infatti, studiando l'equazione modulo 4:

$$x^2 + y^2 \equiv z^2 \pmod{4}$$

dove essendo un quadrato modulo 4 abbiamo che  $z^2 \in \{0, 1\}$ , dunque  $x^2, y^2 \in \{0, 1\}$ , ma non possono essere contemporaneamente pari, altrimenti avremmo che  $(x, y) \neq 1$ , e neppure contemporaneamente dispari, altrimenti la somma dei loro quadrati modulo 4 sarebbe 2, pertanto  $x$  ed  $y$  sono uno pari e l'altro dispari.

**Osservazione 2.132 —** Consideriamo l'ideale  $I = (x + iy, x - iy)$ , verifichiamo che  $I = (1)$ , o equivalentemente che  $x + iy$  e  $x - iy$  sono coprimi (abbiamo visto che in un ED l'ideale generato da due elementi è quello generato dal loro M.C.D.). Osserviamo che:

$$2x = (x + iy) + (x - iy) \in I$$

Analogamente, considerando la differenza si ha  $2y \in I$  e, considerando il prodotto,  $x^2 + y^2 \in I$ ; poiché  $x$  ed  $y$  hanno diversa parità,  $x^2 + y^2$  è dispari, mentre  $2x$  è pari, dunque si ha che:

$$1 \in (2x, 2y, x^2 + y^2) \subset \mathbb{Z} \subset \mathbb{Z}[i]$$

infatti, se non ci fosse 1,  $\exists p$  tale che  $p \mid 2x$ ,  $p \mid 2y$ , da cui  $p = 2$  (in quanto  $(x, y) = 1$ ), ma  $2 = p \nmid x^2 + y^2$ , che però è dispari, dunque:

$$I = (1)$$

o equivalentemente  $x + iy$  e  $x - iy$  sono coprimi e quindi entrambi dei quadrati a meno di unità.

**Osservazione 2.133 (Invertibili di  $\mathbb{Z}[i]$ )** — Osserviamo che gli elementi di  $(\mathbb{Z}[i])^*$  sono gli  $u \in \mathbb{Z}[i]$  tali per cui  $\exists v \in \mathbb{Z}[i]$ :

$$uv = 1 \stackrel{a}{\implies} v = \bar{u} \implies u\bar{u} = 1$$

ovvero  $u = \varepsilon + i\delta \in \mathbb{Z}[i]$  dove:

$$u\bar{u} = \varepsilon^2 + \delta^2 = 1$$

che ha per soluzioni:

$$\begin{cases} \varepsilon = \pm 1 \\ \delta = 0 \end{cases} \quad \text{e} \quad \begin{cases} \varepsilon = 0 \\ \delta = \pm 1 \end{cases}$$

dunque  $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$ .

<sup>a</sup>Stiamo usando il fatto che nei complessi il prodotto fa 1 se è tra elementi coniugati.

Allora, per quanto detto sappiamo che:

$$x + iy = u\alpha^2 \quad \alpha \in \mathbb{Z}[i], u \in \{\pm 1, \pm i\}$$

e analogamente:

$$x - iy = \bar{u}\bar{\alpha}^2 \quad \bar{\alpha} \in \mathbb{Z}[i], \bar{u} \in \{\pm 1, \pm i\}$$

Considerando  $\alpha = a + ib$  si ottiene:

$$x + iy = u(a^2 - b^2 - 2iab)$$

distinguiamo ora due casi:

- Se  $u = \pm 1$ , allora si ottiene:

$$\begin{cases} x = \pm(a^2 - b^2) \\ y = \mp 2ab \\ z = \pm(a^2 + b^2) \end{cases}$$

- Se  $u = \pm i$ , allora si ottiene:

$$\begin{cases} x = \mp 2ab \\ z = \pm(a^2 - b^2 - 2) \\ y = \pm(a^2 + b^2) \end{cases}$$

che forniscono la parametrizzazione delle terne pitagoriche e rispondono al problema iniziale di determinarle.

**Osservazione 2.134 (Ultimo teorema di Fermat)** — Il procedimento risolutivo appena utilizzato nel caso delle terne pitagoriche non può essere generalizzato al caso dell'equazione:

$$x^n + y^n = z^n \quad n \geq 3$$

inizialmente, possiamo considerare solo il caso in cui  $n = p$ , infatti, se non ci fossero soluzioni nemmeno nel caso di un primo, non potremmo trovarle nel caso generale. Distinguiamo due casi:

- Se  $p \nmid xyz$ , abbiamo  $x^p + y^p = z^p$  che può essere fattorizzata:

$$(x + y)(x + \zeta_p y) \dots (x + \zeta_p^{p-1} y) = z^p \quad \text{in } \mathbb{Z}[\zeta_p]$$

si può dimostrare in questo caso che i fattori sono a due a due coprimi, ma da ciò non possiamo concludere che sono tutte potenze  $p$ -esime (altrimenti a questo punto potremmo dimostrare che non esistono soluzioni), perché in generale  $\mathbb{Z}[\zeta_p]$  **non** è un UFD, ad esempio per  $p = 23$  non è vero<sup>a</sup>.

- Se  $p$  divide esattamente uno tra  $x, y$  e  $z$ , ma non discutiamo ora questo caso.

<sup>a</sup>Ed anzi è proprio il più piccolo primo per il quale non funziona.

## §3 Campi

### §3.1 Riepilogo sulle estensioni di campi

**Definizione 3.1.** Dato un campo  $K$  ed una sua estensione  $L$ ,  $\alpha \in L$  si dice **algebrico** su  $K$  se:

$$\exists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$$

**Definizione 3.2.** Dato un campo  $K$  ed una sua estensione  $L$ ,  $\alpha \in L$  si dice **trascendente** su  $K$  se non è algebrico, ovvero:

$$\nexists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$$

**Definizione 3.3.** Dato un campo  $K$ , una sua estensione  $L$ , e  $\alpha \in L$ , possiamo definire l'**omomorfismo di valutazione** di  $\alpha$  su  $K[x]$  come:

$$\varphi_\alpha : K[x] \longrightarrow K[\alpha] (\subset L) : f(x) \longmapsto f(\alpha)$$

Per tale omomorfismo vale il diagramma:

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_\alpha} & K[\alpha] (\subset L) \\ \pi_{\ker \varphi_\alpha} \downarrow & \nearrow \varphi_\alpha & \\ \frac{K[x]}{\ker \varphi_\alpha} & & \end{array}$$

Da cui abbiamo che:

$$K[\alpha] \cong \frac{K[x]}{\ker \varphi_\alpha}$$

dove  $K[\alpha]$  è un dominio perché è un sottoanello di un campo, dunque  $\ker \varphi_\alpha \subset K[x]$  è un ideale primo (per l'(1) della [Proposizione 2.56](#)).

**Osservazione 3.4 —** Ricordiamo che, data un'estensione  $K \subset L$ , si ha per  $\alpha \in L$  che:

- $\alpha$  è trascendente su  $K \iff \ker \varphi_\alpha = \{0\} \iff \varphi_\alpha$  è iniettivo  $\iff K[x] \cong K[\alpha]$ .
- $\alpha$  è algebrico su  $K \iff \ker \varphi_\alpha \neq \{0\} \iff \varphi_\alpha$  non è iniettivo.

Se consideriamo  $\alpha \in L$  algebrico su  $K[x]$ , dunque  $\ker \varphi_\alpha \neq \{0\}$ , poiché  $K[x]$  è un PID, allora  $\ker \varphi_\alpha$  è un ideale massimale di  $K[x]$  (poiché vale la [Proposizione 2.95](#)), dunque  $\frac{K[x]}{\ker \varphi_\alpha}$  è un campo, e lo è quindi  $K[\alpha]$ , di conseguenza, coincide col suo campo dei quozienti<sup>52</sup>  $K[\alpha] = K(\alpha)$ .

**Osservazione 3.5 —** Poiché  $K[x]$  è un PID, si ha che  $\ker \varphi_\alpha = (\mu_\alpha(x))$ , con  $\mu_\alpha(x) \in \ker \varphi_\alpha$ , ed essendo un ideale massimale  $\mu_\alpha(x)$  è irriducibile in  $K[x]$  ([Proposizione 2.86](#)). Inoltre, scegliamo  $\mu_\alpha(x)$  come l'unico generatore monico, infatti essendo  $K[x]$  anche un ED, per la [Proposizione 2.93](#) sappiamo che i suoi ideali sono generati da elementi di grado minimo, e tali elementi differiscono per un elemento di  $K \setminus \{0\}$ .

<sup>52</sup>Volendo per la [Proposizione 2.69](#).

**Definizione 3.6.** Data l'estensione  $L/K$  ( $K \subseteq L$ ), si dice **grado** di  $L/K$ :

$$[L : K] = \dim_K L$$

se  $[L : K] < +\infty$ , diciamo che  $L/K$  è un'estensione **finita** (o di **grado finito**).

**Proposizione 3.7** (Grado di un'estensione semplice)

Data l'estensione  $L/K$  e  $\alpha \in L$ , allora il grado dell'estensione semplice  $K \subseteq K(\alpha)$  è dato da:

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

*Dimostrazione.* Osserviamo che per quanto già detto,  $\alpha$  è trascendente su  $K$  se e solo se  $\ker \varphi_\alpha = \{0\}$  (a questo punto abbiamo già concluso la dimostrazione della prima parte), quindi se e solo se l'omomorfismo di valutazione è iniettivo, ed essendo surgettivo per definizione, si ha che:

$$K[x] \cong K[\alpha] \iff K(x) \cong K(\alpha)$$

Analogamente, per quanto detto,  $\alpha$  algebrico su  $K$  è equivalente a dire:

$$K(\alpha) \cong K[\alpha] \cong \frac{K[x]}{(\mu_\alpha(x))}$$

con l'isomorfismo che manda la base  $\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$  di  $\frac{K[x]}{(\mu_\alpha(x))}$ , in  $\{1, \alpha, \dots, \alpha^{n-1}\}$ , ovvero la  $K$ -base di  $K(\alpha)$ , da cui segue che:

$$\dim_K K(\alpha) = n = \deg \mu_\alpha(x)$$

□

**Proposizione 3.8** (Proprietà delle torri di estensioni)

Data una torre di estensioni  $K \subset F \subset L$ ,  $F/K$  è finita se e solo se  $F/L$  e  $L/K$  sono finite e inoltre:

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

*Dimostrazione.* La dimostrazione è identica a quella già vista in **Aritmetica**. Siano  $[F : K] = n$  e  $[L : F] = m$ , verifichiamo che  $[L : K] = nm$ ; per definizione sappiamo che  $[F : K] = n$  ovvero  $F$  è un  $K$ -spazio vettoriale con  $\dim_K F = n$ , e ugualmente,  $[L : F] = m$  ovvero  $L$  è un  $F$ -spazio vettoriale con  $\dim_F L = m$ , possiamo considerare allora una  $K$ -base di  $F$ ,  $\{v_1, \dots, v_n\}$ , ed una  $F$ -base di  $L$ ,  $\{w_1, \dots, w_m\}$ , per dimostrare la tesi, dobbiamo dimostrare che  $\dim_K L = nm$ , ovvero  $L$  ammette una  $K$ -base di cardinalità  $nm$ . Consideriamo l'insieme  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$ , come si osserva facilmente, esso ha cardinalità  $nm$ , dimostriamo quindi che tale insieme è una  $K$ -base di  $L$ , per fare ciò verifichiamo separatamente che gli elementi di  $\{v_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  generano tutti gli elementi di  $L$  e che sono tra loro linearmente indipendenti:

- Sia  $\alpha \in L$ , poiché  $L$  è per ipotesi un  $F$ -spazio vettoriale, quindi  $L = \langle w_1, \dots, w_m \rangle_F$ , si ha che:

$$\alpha = \sum_{j=1}^m \lambda_j w_j \quad \lambda_j \in F$$

d'altra parte, poiché  $F$  è un  $K$ -spazio vettoriale, quindi  $F = \langle w_1, \dots, w_m \rangle_K$ , si ha che:

$$\lambda_j = \sum_{i=1}^n a_{ji} w_i \quad a_{ji} \in K$$

e sostituendo si ottiene:

$$\alpha = \sum_{j=1}^m \left( \sum_{i=1}^n a_{ji} w_i \right) w_j = \sum_{j=1}^m \sum_{i=1}^n a_{ji} w_i w_j \quad a_{ji} \in K$$

e quindi l'insieme  $\{w_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  genera  $L$  su  $K$ <sup>53</sup>.

- Per dimostrare che l'insieme  $\{w_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  è costituito da elementi linearmente indipendenti, è sufficiente mostrare che la somma:

$$\sum_{j=1}^m \sum_{i=1}^n a_{ji} w_i w_j = 0$$

se e solo se sono nulli tutti i coefficienti  $a_{ji}$ . Scriviamo esplicitamente la somma esterna:

$$\left( \sum_{i=1}^n a_{1i} w_i \right) w_1 + \left( \sum_{i=1}^n a_{2i} w_i \right) w_2 + \dots + \left( \sum_{i=1}^n a_{mi} w_i \right) w_m = 0$$

i prodotti  $a_{ji} w_i$ , essendo  $w_i \in F$  e  $a_i \in K$ , sono contenuti in  $F$ , pertanto, la somma appena scritta è una combinazione lineare dei  $w_j$  (della  $F$ -base di  $L$ ), che sappiamo essere linearmente indipendenti su  $F$  (perché appunto sono una base di  $L$ ), quindi la somma fa 0 se e solo se i coefficienti sono tutti nulli, ovvero:

$$\sum_{i=1}^n a_{1i} w_i = \dots = \sum_{i=1}^n a_{mi} w_i = 0$$

essendo  $\{w_1, \dots, w_n\}$  una  $K$ -base di  $F$ , le singole somme  $\sum_{i=1}^n a_{ji} w_i$  sono nulle se e solo se  $a_{ji} = 0$ ,  $\forall i \in \{1, \dots, n\}$ , quindi la somma iniziale è nulla se e solo se  $a_{ji} = 0$ ,  $\forall i \in \{1, \dots, n\}$ ,  $\forall j \in \{1, \dots, m\}$ , quindi gli elementi di  $\{w_i w_j\}_{i=1, \dots, n}^{j=1, \dots, m}$  sono linearmente indipendenti.  $\square$

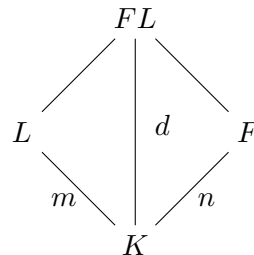
### Proposizione 3.9 (Proprietà del composto di estensioni)

Date due torri di estensioni di  $K$ ,  $K \subset L \subset FL$  e  $K \subset F \subset FL$ , con  $[L : K] = m$  e  $[F : K] = n$ , allora  $[FL : K] = d < +\infty$  e  $[m, n] \mid d$ .

<sup>53</sup>Ovviamente tutti i prodotti  $w_i w_j$  sono contenuti in  $L$  per le proprietà di campo e perché appartengono a sottocampi del campo considerato.



*Dimostrazione.* Per dimostrare la proposizione, osserviamo che, avendo supposto  $n, m < +\infty$ , allora possiamo considerare  $FL$  come  $L$ -spazio vettoriale con un insieme di generatori di  $n$  elementi, da cui si ricava che  $FL$  è anche un  $K$ -spazio vettoriale di dimensione finita; per la precisione applicando due volte il [Teorema delle torri di estensioni](#) all'estensione:



otteniamo che  $m \mid d$  e  $n \mid d$ , da cui la tesi.  $\square$

**Definizione 3.10.** Un'estensione  $L/K$  si dice **algebraica** se  $\forall \alpha \in L$ ,  $\alpha$  è algebrico su  $K$ .

**Proposizione 3.11** (Estensione finita  $\implies$  algebraica)

Ogni estensione di grado finito è algebraica.

*Dimostrazione.* Vogliamo verificare che  $\forall \alpha \in L$ ,  $\alpha$  è algebrico su  $K$ , abbiamo che la torre:

$$K \subseteq K(\alpha) \subseteq L$$

è finita per ipotesi ( $[L : K] < +\infty$ ), pertanto la sottoestensione  $K \subseteq K(\alpha)$  è a sua volta finita (volendo per il [Teorema delle torri](#)), quindi per la [Proposizione 3.7](#)  $\alpha$  è algebrico su  $K$  (poiché siamo nel caso di un'estensione semplice), ed essendo vero per ogni  $\alpha$ , allora  $L$  è un'estensione algebraica di  $K$ .  $\square$

**Proposizione 3.12** (Campo delle estensioni algebriche)

Data un'estensione  $L/K$ , sia  $A = \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}$ , allora  $A$  è un campo (ed ovviamente è un'estensione algebraica di  $K$ ).

*Dimostrazione.* Verifichiamo che  $A$  sia un campo; siano  $\alpha, \beta \in A$ , allora  $[K(\alpha) : K] < +\infty$  e  $[K(\beta) : K] < +\infty$ , consideriamo la torre:

$$K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta)$$

la prima estensione è finita per ipotesi, mentre la seconda è finita per la [Proposizione 3.9](#) in quanto estensione composta da  $K(\alpha)$  e  $K(\beta)$  (entrambe semplici e quindi finite perché algebriche, per la [Proposizione 3.7](#)). Essendo dunque  $K \subseteq K(\alpha, \beta)$  un'estensione finita, per la [Proposizione 3.11](#) è algebraica, quindi tutti gli elementi  $\alpha \pm \beta$ ,  $\alpha\beta$  e  $\frac{1}{\beta}$  sono algebrici su  $K$ , pertanto  $A$  è un campo.  $\square$

**Osservazione 3.13** — Il viceversa della [Proposizione 3.11](#) in generale è falso; non lo è nel caso in cui l'estensione sia semplice, come visto nella [Proposizione 3.7](#).

**Esempio 3.14** (Estensione algebrica non finita)

Consideriamo l'estensione  $\mathbb{Q} \subset \mathbb{C}$ , e l'insieme  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ , costruito come nella [Proposizione 3.12](#), che è un'estensione algebrica di  $\mathbb{Q}$ . Verifichiamo che  $[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$ ; consideriamo la torre:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}} \quad \forall n \geq 2$$

l'estensione  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2})$  ha grado  $n$ , in quanto il suo polinomio minimo è il 2-Eisenstein:

$$\mu_{\sqrt[n]{2}}(x) = x^n - 2$$

per il [Teorema delle torri](#):

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \geq n \quad \forall n \geq 2$$

dunque l'estensione  $\mathbb{Q} \subset \overline{\mathbb{Q}}$  ha grado  $+\infty$ , in quanto ha grado maggiore di  $n$  definitivamente.

**Osservazione 3.15** — Ricordiamo che avevamo definito un'estensione **finitamente generata** una scrittura del tipo  $L = K(\alpha_1, \dots, \alpha_n)$  che può essere definita equivalentemente come:

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1) \dots (\alpha_n) = \{p(\alpha_1, \dots, \alpha_n) \mid p(x_1, \dots, x_n) \in K[x_1, \dots, x_n]\}$$

con  $\alpha_1, \dots, \alpha_n$  algebrici su  $K$ , o anche come il più piccolo campo che contiene  $K$  e gli elementi  $\alpha_1, \dots, \alpha_n$ :

$$K(\alpha_1, \dots, \alpha_n) = \bigcap_{\substack{K \subseteq M \subseteq L \\ \alpha_1, \dots, \alpha_n \in M}} M$$

**Proposizione 3.16** (Estensione algebrica e finitamente generata  $\implies$  finita)

Sia  $L/K$  finitamente generata da elementi algebrici,  $L = K(\alpha_1, \dots, \alpha_n)$ , allora  $L/K$  è finita.

*Dimostrazione.* Possiamo dimostrare la tesi per induzione; per  $n = 1$ , la tesi è vera per la [Proposizione 3.7](#), in quanto abbiamo un'estensione semplice ed algebrica, che dunque è finita. Supponiamo la tesi vera per  $n - 1$ , abbiamo che:

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$$

consideriamo la torre:

$$K \subset K(\alpha_1, \dots, \alpha_{n-1}) \subset K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$$

dove la prima estensione è finita per ipotesi induttiva, mentre la seconda perché estensione semplice ed algebrica su un campo più piccolo (quindi vale la [Proposizione 3.7](#)), o alternativamente perché estensione composta di estensioni finite per quanto già detto, quindi vale [Proposizione 3.9](#); pertanto per  $L/K$  è finita per ogni  $n \in \mathbb{N}$ .  $\square$

**Osservazione 3.17** — Della [Proposizione 3.16](#) vale anche il viceversa, infatti, presa un'estensione finita  $[L : K] = n$ , consideriamo  $v_1, \dots, v_n$  una  $K$ -base di  $L$ , allora è vero che è finitamente generata:

$$L = \langle v_1, \dots, v_n \rangle_K = K(v_1, \dots, v_n)$$

dunque si può affermare che **un'estensione è finita se e solo se è finitamente generata da elementi algebrici**.

**Proposizione 3.18** (Proprietà delle estensioni algebriche rispetto a torri e composto)

Valgono le seguenti proprietà per le estensioni algebriche:

- (1) Data una torre di estensioni  $K \subset L \subset F$ ,  $F/K$  è algebrica se e solo se  $F/L$  e  $L/K$  sono algebriche.
- (2) Date due estensioni  $L/K$  e  $M/K$  esse sono algebriche se e solo se l'estensione composta  $LM/K$  è algebrica.

**Osservazione 3.19** (Sulla definizione di estensione composta) — Dati  $L, M \subset \Omega$  sottocampi dello stesso campo  $\Omega$ , abbiamo che il composto è:

$$LM = L(M) = M(L)$$

ovvero il più piccolo sottocampo di  $\Omega$  che contiene sia  $L$  che  $M$ . Se  $K$  ed  $L$  sono finitamente generati:

$$L = K(\alpha_1, \dots, \alpha_n) \quad \text{e} \quad M = K(\beta_1, \dots, \beta_m)$$

allora il loro composto è dato da:

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

*Dimostrazione.* Proviamo le due affermazioni:

- (1) La prima implicazione segue quasi immediatamente, infatti, se  $F/K$  è algebrica, allora  $\forall \alpha \in F$ ,  $\alpha$  è algebrico su  $K$ , dunque tutti gli  $\alpha \in L \subset F$  sono algebrici su  $K$  perché elementi anche di  $F$ , pertanto  $L$  è algebrico su  $K$ ; inoltre,  $F$  è algebrico su  $L$  perché contiene  $K$ , dunque **tutti gli elementi di  $F$  sono già algebrici** su  $K$  (un campo più piccolo) e quindi lo saranno anche in un campo più grande. Viceversa sia  $\alpha \in F$ , per ipotesi sappiamo che  $F/L$  e  $L/K$  sono algebriche, quindi  $\alpha$  è algebrico su  $L$ , dunque:

$$\exists f(x) \in L[x] \setminus \{0\} : f(\alpha) = 0 \quad \text{con} \quad f(x) = \sum_{i=0}^n a_i x^i$$

consideriamo  $L_0 = K(a_0, \dots, a_n)$  (essendo un'estensione algebrica per ipotesi, ciò, come detto nell'[Osservazione 3.17](#), è equivalente a dire che è un'estensione finitamente generata da elementi algebrici su  $K$ ), si ha per costruzione che  $f(x) \in L_0[x]$ , dunque  $\alpha$  è algebrico su  $L_0$ :

$$K \subset L_0 \subset L_0(\alpha)$$

dove la prima estensione è finitamente generata ed algebrica (perché  $\forall a_i \in L$ ,  $a_i$  è algebrico su  $K$ ), pertanto è finita per la [Proposizione 3.16](#), inoltre la seconda estensione è a sua volta finita perché algebrica (quindi vale la [Proposizione 3.11](#)), di conseguenza, per il [Teorema delle torri](#), la torre di estensione è finita,  $[L_0(\alpha) : K] < +\infty$ , dunque, sempre per la [Proposizione 3.11](#)  $L_0(\alpha)/K$  è algebrica. Abbiamo quindi dimostrato che  $\alpha \in F$  è algebrico su  $K$ ,  $\forall \alpha \in F$ , dunque  $F/K$  è algebrica.

- (2) Sia  $LM/K$  algebrica e sia  $\alpha \in M \subset LM$ , allora è algebrico su  $K$ , in quanto tutti gli elementi di  $LM$  già lo erano, dunque non stiamo facendo altro che prendere una sottoestensione di un'estensione algebrica, che quindi sarà a sua volta algebrica, ovvero  $M/K$  algebrica; in maniera identica  $L/K$  è anch'essa algebrica.

Supponiamo ora che  $L/K$  e  $M/K$  siano algebriche, consideriamo  $\alpha \in LM = L(M)$ , ovvero  $\alpha = \sum_{i=1}^n \lambda_i m_i$ , con  $\lambda_i \in L$  e  $m_i \in M$ , dunque:

$$\alpha \in F = K(\lambda_1, \dots, \lambda_n, m_1, \dots, m_n)$$

dove tale estensione è algebrica (perché tutti gli elementi che abbiamo aggiunto sono algebrici), quindi per la [Proposizione 3.16](#) è finita, e dunque  $\alpha$  è algebrico su  $K$ ,  $\forall \alpha \in LM$ , da cui la tesi.

□

### §3.2 Chiusura algebrica di un campo

**Definizione 3.20.** Un campo  $\Omega$  si dice **algebricamente chiuso** se ogni polinomio  $f(x) \in \Omega[x]$  non costante ha almeno una radice in  $\Omega$ .

#### Esempio 3.21

Per il Teorema Fondamentale dell'Algebra  $\mathbb{C}$  è algebricamente chiuso.

**Osservazione 3.22** — Se  $\Omega$  è algebricamente chiuso gli unici polinomi irriducibili di  $\Omega[x]$  sono quelli di grado 1.

**Definizione 3.23.** Data l'estensione  $\Omega/K$ ,  $\Omega$  è una **chiusura algebrica** di  $K$  se:

- $\Omega$  è algebricamente chiuso.
- $\Omega/K$  è un'estensione algebrica.

#### Esempio 3.24

Osserviamo che:

- (1)  $\mathbb{C}$  è la chiusura algebrica di  $\mathbb{R}$ .
- (2)  $\mathbb{C}$  non è la chiusura algebrica di  $\mathbb{Q}$ , poiché non tutti gli elementi di  $\mathbb{C}$  sono algebrici su  $\mathbb{Q}$ .

#### Teorema 3.25 (Esistenza e unicità della chiusura algebrica)

Sia  $K$  un campo, allora esiste sempre una sua chiusura algebrica. Inoltre due qualsiasi chiusure algebriche su  $K$  sono isomorfe.<sup>a</sup>

<sup>a</sup>Nel senso che gli isomorfismi tra le varie chiusure algebriche fissano  $K$ .

#### Esempio 3.26

Consideriamo  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ è algebrico su } \mathbb{Q}\}$ , tale insieme è un campo, per quanto asserito nella [Proposizione 3.12](#), ed è per una chiusura algebrica di  $\mathbb{Q}$ , infatti  $\overline{\mathbb{Q}}/\mathbb{Q}$  è un'estensione algebrica per definizione. Verifichiamo che  $\overline{\mathbb{Q}}$  è algebricamente chiuso; sia  $f(x) \in \overline{\mathbb{Q}}[x]$  non costante, allora  $f(x)$  ammette almeno una radice  $\alpha \in \mathbb{C}$ , poiché  $f(x) \in \overline{\mathbb{Q}}[x] \subset \mathbb{C}[x]$  e  $\mathbb{C}$  è algebricamente chiuso. Per mostrare che  $\alpha \in \overline{\mathbb{Q}}$ , bisogna dimostrare che  $\alpha$  è algebrico su  $\mathbb{Q}$ , consideriamo la torre:

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}(\alpha)$$

la prima estensione è algebrica per quanto già discusso, la seconda è algebrica perché semplice ([Proposizione 3.7](#)), dunque per [torri](#)  $\alpha$  è algebrico su  $\mathbb{Q}$ , inoltre  $\alpha \in \mathbb{C}$ , per cui  $\alpha \in \overline{\mathbb{Q}}$  che quindi è algebricamente chiuso, perché quanto detto vale per qualunque polinomio in  $\overline{\mathbb{Q}}[x]$ .

**Osservazione 3.27** — L'argomento dell'esempio precedente può essere utilizzato per costruire  $\overline{K}$  chiusura algebrica di  $K$  ogni volta che si ha:

$$K \subset \Omega$$

con  $\Omega$  algebricamente chiuso, definendo  $\overline{K} = \{\alpha \in \Omega \mid \alpha \text{ è algebrico su } K\}$ , da cui  $\overline{K}$  chiusura algebrica di  $K$  (infatti  $\overline{K}$  è un'estensione algebrica di  $K$  per definizione, ed iterando il ragionamento precedente si mostra come sia anche algebricamente chiuso).

**Definizione 3.28.** Sia  $f(x) \in K[x]$ , con  $\deg f(x) \geq 1$ , e siano  $\alpha_1, \dots, \alpha_n \in \overline{K}$  le radici di  $f(x)$ , si definisce **campo di spezzamento** di  $f(x)$  su  $K$  il sottocampo di  $\overline{K}$ :

$$K(\alpha_1, \dots, \alpha_n)$$

**Osservazione 3.29** — La definizione di campo di spezzamento può essere estesa ad una famiglia di polinomi  $\mathcal{F} = \{f_i(x) \mid i \in I\} \subset K[x]$ , infatti, dato l'insieme delle radici di un polinomio  $f_i(x)$  della famiglia,  $\{\alpha_{ij}\}_{i \in I}^{j=1, \dots, n_i}$ , il campo di spezzamento di  $\mathcal{F}$  su  $K$  è dato da:

$$K(\{\alpha_{ij}\}_{j=1, \dots, n_i \mid i \in I})$$

Tale estensione della definizione risulta necessaria soltanto nel caso di famiglie infinite di polinomi, infatti nel caso finito è sufficiente considerare il campo di spezzamento dell'unico polinomio prodotto di tutti gli altri (prodotto che non è definito nel caso di una famiglia infinita).

**Esempio 3.30** (Campo di spezzamento di  $x^3 - 2$ )

Consideriamo  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ , le radici di  $f(x)$  in  $\mathbb{C}[x]$  sono  $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3$  e  $\sqrt[3]{2}\zeta_3^2$ , dunque il campo di spezzamento di  $f(x)$  su  $\mathbb{Q}$  è dato da :

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

dove l'ultima uguaglianza andrebbe verificata mediante doppio contenimento.

**Esempio 3.31** (Campo di spezzamento di  $x^n - 1$ )

Consideriamo  $\Phi_n(x) = x^n - 1 \in \mathbb{Q}[x]$ , le radici di  $\Phi_n(x)$  in  $\mathbb{C}[x]$  sono gli elementi del gruppo  $\langle \zeta_n \rangle = \{\alpha \in \mathbb{C} \mid \alpha^n = 1\}$ , con  $\zeta_n$  radice  $n$ -esima primitiva di 1, pertanto  $\mathbb{Q}(\zeta_n)$  è il campo di spezzamento del polinomio ciclotomico  $n$ -esimo:

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$$

Ci poniamo ora il seguente problema: dato un campo  $K$ , la sua chiusura algebrica  $\overline{K}$  e  $\alpha \in \overline{K}$  (algebrico su  $K$ ), vogliamo sapere in quanti modi si può immergere  $K(\alpha)$  in  $\overline{K}$  con:

$$\varphi : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

**Osservazione 3.32 (Omomorfismi da campi)** — Osserviamo che in generale un omomorfismo definito su un campo può avere solo nucleo banale, infatti, esso è in particolare un omomorfismo tra anelli, dunque il nucleo è un ideale, ma per la (2) della [Proposizione 2.26](#) gli unici ideali di un campo sono se stesso e  $\{0\}$ , dunque il nucleo o è tutto o è banale, pertanto gli unici omomorfismi possibili da un campo sono o iniettivi o nulli.

Possiamo rispondere alla domanda iniziale per mezzo della seguente proposizione.

**Proposizione 3.33** (Numero di estensioni via identità di  $K(\alpha)$  a  $\overline{K}$ )

Dato un campo  $K$  ed  $\alpha \in \overline{K}$ , con  $\overline{K}$  chiusura algebrica di  $K$ , detto  $k$  il numero di radici distinte di  $\mu_\alpha(x)$  in  $\overline{K}$ , allora:

$$\exists \varphi_1, \dots, \varphi_k : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = id_K$$

ovvero esistono esattamente  $k$  estensioni distinte da  $K(\alpha)$  a  $\overline{K}$ .

*Dimostrazione.* Per quanto detto sull'omomorfismo di valutazione sappiamo che  $K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))}$ , dunque, determinando un omomorfismo da  $K[x]$  ad  $\overline{K}$  possiamo applicare il [Primo Teorema di Omomorfismo](#). Sia dunque:

$$\tilde{\varphi} : K[x] \longrightarrow \overline{K} : x \longmapsto \beta, p(x) \longmapsto p(\beta) \quad \forall \beta \in \overline{K}$$

per tale omomorfismo abbiamo che  $(\mu_\alpha(x)) \subset \ker \tilde{\varphi} \iff \mu_\alpha(x) \in \ker \tilde{\varphi}$  (per le proprietà degli ideali), quindi se e solo se  $\mu_\alpha(\beta) = 0$ , quindi per tutte le radici di  $\mu_\alpha(x)$  in  $\overline{K}$  si ha che:

$$\begin{array}{ccc} K[x] & \xrightarrow{\tilde{\varphi}} & \overline{K} \\ \pi_{(\mu_\alpha(x))} \downarrow & \nearrow \varphi & \\ K(\alpha) \cong \frac{K[x]}{(\mu_\alpha(x))} & & \end{array}$$

dove  $\varphi$  è un omomorfismo per il [Primo Teorema di Omomorfismo](#), ed è iniettivo (per quanto già visto nell'[Osservazione 3.32](#)) perché omomorfismo **non nullo** tra campi (ad esempio perché  $1 \mapsto 1$ ). Si osserva infine che le  $\varphi_i$  sono distinte perché danno diversa immagine quando calcolate su  $x$ .  $\square$

Dalla proposizione appena dimostrata ci poniamo un secondo problema, quello di contare il numero di radici di  $\mu_\alpha(x)$  in  $\overline{K}$ , essendo  $\overline{K}$  algebricamente chiuso, allora il numero delle radici del polinomio, ciascuna contata con la propria molteplicità, è dato da  $\deg \mu_\alpha(x) = n$ , a questo punto, per determinare se  $\mu_\alpha(x)$  abbia o meno radici multiple possiamo fare uso del criterio che segue.

**Teorema 3.34** (Criterio della Derivata)

Sia  $f(x) \in K[x]$ ,  $f(x)$ , allora  $f(x)$  ha radici multiple in  $\overline{K}$  se e solo se  $(f(x), f'(x)) \neq 1$ . Inoltre se  $f(x)$  è irriducibile in  $K[x]$ , allora  $f(x)$  ha radici multiple se e solo se  $f'(x) = 0$ .

*Dimostrazione.* Il primo fatto è stato trattato in **Aritmetica**, quindi non ne forniremo qui una dimostrazione. Per il secondo fatto si può osservare che  $f(x) \in K[x] \implies f'(x) \in K[x]$ , da cui  $(f(x), f'(x)) \in K[x]$  (perché si ottiene mediante l'Algoritmo di Euclide), e se  $f(x)$  è irriducibile in  $K[x]$  l'M.C.D. fa 1 oppure  $f(x)$ ; dove il secondo caso si realizza se e solo se  $f'(x) = 0$  (dato che  $\deg f'(x) < \deg f(x)$ ).  $\square$

Dunque se in  $K[x]$  i polinomi irriducibili non hanno derivata nulla, allora il numero delle loro radici distinte coincide con il loro grado.

**Definizione 3.35.** Un campo  $K$  tale per cui tutti i polinomi irriducibili in  $K[x]$  hanno derivata non nulla prende il nome di **campo perfetto**.

**Osservazione 3.36 (Campi perfetti)** — Osserviamo che:

- Se  $\text{char } K = 0$ , allora  $K$  è un campo perfetto, infatti, detto  $f(x) = \sum_{i=0}^n a_i x^i$ , allora  $f'(x) = \sum_{i=0}^{n-1} i a_i x^i$ ,  $\forall n \geq 1$ , ovvero la derivata di un polinomio non costante non può essere mai nulla.
- $\mathbb{F}_{p^n}$  è perfetto  $\forall p$  primo,  $\forall n \geq 1$ .
- Al contrario possiamo vedere che per campi con caratteristica diversa da 0 esistono polinomi irriducibili con derivata nulla, sia  $K = \mathbb{F}_p(t)$  e  $f(x) = x^p - t \in K[x]$ , abbiamo che  $f'(x) = p x^{p-1} = 0$ , possiamo verificare che  $f(x)$  è irriducibile in  $K[x]$ . Osserviamo che:

$$f(x) \in \mathbb{F}_p[t][x] := A[x]$$

dove  $A$  UFD (essendo un ED), dunque per il **Lemma di Gauss** verificare che  $f(x)$  è irriducibile in  $K[x] = \mathbb{F}_p(t)[x]$  è equivalente a verificare che sia irriducibile in  $A[x] = \mathbb{F}_p[t][x]$ . In  $A[x]$ , essendo UFD vale il **Criterio di Eisenstein**, dunque  $f(x)$  è irriducibile rispetto all'ideale  $P = (t)$ , che è primo in quanto massimale, infatti  $\frac{A}{(t)} \cong \mathbb{F}_p$ . Inoltre se  $\alpha \in \bar{K}$  è una radice di  $f(x)$ , abbiamo che  $f(\alpha) = \alpha^p - t = 0 \implies t = \alpha^p$ , da cui:

$$f(x) = x^p - \alpha^p = (x - \alpha)^p$$

dove nell'ultima uguaglianza abbiamo usato il lemma del Binomio Ingenuo, pertanto in realtà  $f(x)$  ha un'unica radice in  $\bar{K}$ .

Ci limiteremo (assumendolo anche senza ripeterlo ogni volta) ai campi perfetti, pertanto un polinomio irriducibile di  $K[x]$  di grado  $n$  avrà esattamente  $n$  radici distinte in  $\bar{K}$ .

**Proposizione 3.37** (Numero di estensioni di  $K(\alpha)$  a  $\bar{K}$ )

Dato  $\alpha \in \bar{K}$ , con  $[K(\alpha) : K] = n$ , si ha che  $\forall \varphi : K \hookrightarrow \bar{K}$  immersione, esistono esattamente  $n$  estensioni a  $K(\alpha)$ , cioè:

$$\exists \varphi_1, \dots, \varphi_n : K(\alpha) \hookrightarrow \bar{K} \quad \text{con} \quad \varphi_i|_K = \varphi$$



**Osservazione 3.38** — Abbiamo già visto che ciò è vero se  $\varphi = id_K$ , nella [Proposizione 3.33](#), la nuova proposizione ci permette di contare il numero di estensioni di un omomorfismo da  $K$  in  $\overline{K}$  ad uno da  $K(\alpha)$  in  $\overline{K}$ . Ad esempio, dato  $K = \mathbb{Q}(\sqrt[3]{2})$  e l'omomorfismo:

$$\varphi : K \hookrightarrow \overline{K} : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$$

ci chiediamo quanti sono gli omomorfismi:

$$\varphi_i : K(\zeta_3) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = \varphi$$

cioè che quando ristretti a  $K$  si comportano come  $\varphi$ .

*Dimostrazione.* In analogia con quanto fatto nella dimostrazione della [Proposizione 3.33](#), consideriamo:

$$\tilde{\varphi} : K[x] \longrightarrow \overline{K} : x \mapsto \beta : p(x) \mapsto p(\beta) \quad \text{con} \quad \varphi_i|_K = \varphi$$

per tale omomorfismo abbiamo che  $(\mu_\alpha(x)) \subseteq \ker \tilde{\varphi} \iff \tilde{\varphi}(\mu_\alpha(x)) = 0 \iff \varphi(\mu_\alpha(x))(\beta) = 0$ , dunque applichiamo  $\varphi$  ai coefficienti di  $\mu_\alpha(x)$  (prima venivano lasciati fissi perché usavamo l'identità) e poi valutiamo il nuovo polinomio in  $\beta$ , pertanto  $\beta$  deve essere una radice di  $\varphi(\mu_\alpha(x))$ , dunque le estensioni di  $\varphi$  a  $K(\alpha)$  sono tante quante le radici distinte di  $\varphi(\mu_\alpha(x))$  in  $\overline{K}$ .

Poiché  $\mu_\alpha(x)$  è irriducibile per definizione, allora  $\varphi(\mu_\alpha(x))$  è irriducibile, inoltre,  $\deg \mu_\alpha(x) = \deg \varphi(\mu_\alpha(x))$  (poiché l'omomorfismo è iniettivo), pertanto, essendo il campo perfetto il numero di radici distinte di  $\varphi(\mu_\alpha(x))$  è uguale al suo grado, e quindi a quello di  $\mu_\alpha(x)$ .  $\square$

**Corollario 3.39** (Numero di estensioni a  $\overline{K}$  di un'estensione qualsiasi)

Sia  $E/K$  un'estensione, con  $[E : K] = n$ , allora  $\forall \varphi : K \hookrightarrow \overline{K}$  immersione, esistono  $n$  immersioni:

$$\varphi_1, \dots, \varphi_n : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = \varphi$$

*Dimostrazione.* La dimostrazione segue facilmente per induzione, infatti per  $n = 1$  abbiamo che l'estensione è semplice e quindi vale la [Proposizione 3.37](#); per  $n > 1$  consideriamo  $\alpha \in E \setminus K$  per il quale si ha la torre di estensioni:

$$K \subset K(\alpha) \subset E$$

con  $[K(\alpha) : K] = m$  e  $[E : K(\alpha)] = d$ . Se  $m = n$ , allora  $E = K(\alpha)$  e siamo ancora nel caso precedente; se  $1 < m < n \implies d < n$ , essendo  $n = md$  (in pratica stiamo supponendo di aver già messo nell'estensione almeno un nuovo elemento), dunque per la [Proposizione 3.37](#)  $\varphi$  si estende in  $m$  modi a  $K(\alpha)$ :

$$\varphi_1, \dots, \varphi_m : K(\alpha) \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = \varphi$$

Ogni  $\varphi_i : K(\alpha) \hookrightarrow \overline{K}$  si estende a sua volta per ipotesi induttiva:

$$\varphi_{i1}, \dots, \varphi_{id} : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_{ij}|_{K(\alpha)} = \varphi_i$$

dunque abbiamo  $\{\varphi_{ij}\}_{i=1, \dots, m}^{j=1, \dots, d} : E \hookrightarrow \overline{K}$ , ovvero  $md = n$  estensioni, con  $\varphi_{ij}|_{K(\alpha)} = \varphi_i$ , per cui  $\varphi_{ij}|_K = \varphi_i|_K = \varphi$ , quindi tutte le  $n$  estensioni funzionano.  $\square$

### §3.3 Estensioni normali

**Definizione 3.40.** Dato  $\alpha \in \overline{K}$ , diciamo che i **coniugati** di  $\alpha$  su  $K$  sono le radici del polinomio minimo di  $\alpha$  su  $K$ .

**Definizione 3.41.** Data un'estensione algebrica  $K \subset L$ , essa si dice **separabile** se il polinomio minimo di ogni elemento è un **polinomio separabile**, ovvero se ha radici tutte distinte in un suo campo di spezzamento.<sup>54</sup>

Nella trattazione di teoria di campi di queste dispense considereremo soltanto estensioni separabili.

#### Esempio 3.42

Sia  $f(x) = x^3 - 2$ , tale polinomio coincide con  $\mu_{\sqrt[3]{2}/\mathbb{Q}}(x)$ , ovvero il polinomio minimo di  $\alpha = \sqrt[3]{2}$  su  $\mathbb{Q}$ , vogliamo studiare le immersioni di  $\mathbb{Q}(\alpha)$  in  $\overline{\mathbb{Q}}$ :

$$\varphi : \mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}} \quad \text{con} \quad \varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

dati i coniugati di  $\alpha$  (dunque le radici di  $\mu_{\alpha/\mathbb{Q}}$ ):  $\alpha, \alpha\zeta_3, \alpha\zeta_3^2$ , il nostro omomorfismo deve mandare ogni radice in un'altra, dunque abbiamo più possibilità:

$$\varphi(\alpha) = \begin{cases} \alpha \\ \alpha\zeta_3 \\ \alpha\zeta_3^2 \end{cases}$$

pertanto in base alla scelta di  $\varphi(\alpha)$  abbiamo le possibilità:

$$\varphi(\mathbb{Q}(\alpha)) = \mathbb{Q}(\varphi(\alpha)) = \begin{cases} \mathbb{Q}(\alpha) \\ \mathbb{Q}(\alpha\zeta_3) \\ \mathbb{Q}(\alpha\zeta_3^2) \end{cases}$$

da cui  $\mathbb{Q}(\alpha)$  è isomorfo su  $\mathbb{Q}$  (o si dice anche i tre isomorfismi fissano  $\mathbb{Q}$  puntualmente) a questi tre campi (distinti), ciò è in accordo con la [Proposizione 3.33](#).

<sup>54</sup>Questa definizione è stata aggiunta per completezza al materiale della professoressa, infatti verrà citata successivamente qualche volta, pertanto, sebbene non vi sarà una trattazione ulteriore a riguardo, ho ritenuto opportuno aggiungerla qui.

### Esempio 3.43

Sia  $p$  un primo e consideriamo il campo ciclotomico  $p$ -esimo  $\mathbb{Q}(\zeta_p)$ ; per tale campo abbiamo che:

$$\mu_{\zeta_p/\mathbb{Q}}(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$$

il quale è irriducibile perché è traslato di un  $p$ -Eisenstein, pertanto i coniugati di  $\zeta_p$  sono  $\zeta_p^i$ , con  $1 \leq i < p$  (ovvero sono  $p - 1$ ), da cui:

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p - 1$$

Le immersioni di  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  sono del tipo:

$$\varphi_i : \mathbb{Q}(\zeta_p) \longrightarrow \overline{\mathbb{Q}} : \zeta_p \longmapsto \zeta_p^i \quad \text{con} \quad \varphi_i|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

ed abbiamo quindi  $p - 1$  possibili immersioni, ancora una volta in accordo con la [Proposizione 3.33](#), per cui abbiamo:

$$\varphi_i(\mathbb{Q}(\zeta_p)) = \mathbb{Q}(\varphi_i(\zeta_p)) = \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p) \quad \forall i \in \{1, \dots, p - 1\}$$

dove l'ultima uguaglianza deriva dal fatto che  $\mathbb{Q}(\zeta_p^i) \subseteq \mathbb{Q}(\zeta_p)$  e  $\mu_{\zeta_p^i}(x) = \mu_{\zeta_p}(x)$ , dunque abbiamo un contenimento di estensioni che hanno lo stesso grado, quindi sono la stessa estensione.

**Definizione 3.44.** Un'estensione algebrica  $F/K$  si dice **normale** se:

$$\forall \varphi : F \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

si ha che  $\varphi(F) = F$ , ovvero l'estensione viene fissata da ogni immersione del campo di partenza nella sua chiusura algebrica.

### Esempio 3.45 (Estensione normale)

Alcuni esempi di estensioni normali possono essere:

- $\mathbb{Q}(\zeta_p)$  è un'estensione normale su  $\mathbb{Q}$ .
- Detto  $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ , allora l'estensione  $F/\mathbb{Q}$  è normale, infatti data:

$$\varphi : F \hookrightarrow \overline{\mathbb{Q}} \quad \text{con} \quad \varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$$

con:

$$\varphi(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = \mathbb{Q}(\varphi(\sqrt[3]{2}), \varphi(\zeta_3)) = {}^a \mathbb{Q}(\sqrt[3]{2}\zeta_3^i, \zeta_3^j) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

per  $i \in \{0, 1, 2\}$  e  $j \in \{1, 2\}$  (dunque abbiamo 6 immersioni, come previsto dall'[Corollario 3.39](#)), quindi abbiamo  $F$  invariante rispetto a  $\varphi$ , per cui  $F/\mathbb{Q}$  è un'estensione normale.

<sup>a</sup>Le immagini di entrambi gli elementi devono essere loro coniugati per quanto detto in precedenza.

**Proposizione 3.46** (Caratterizzazione delle estensioni normali)

Sia  $F/K$  un'estensione algebrica (finita)<sup>a</sup>, sono fatti equivalenti:

- (1)  $F/K$  normale.
- (2) Ogni polinomio irriducibile  $f(x) \in K[x]$  che ha una radice in  $F$  ha tutte le sue radici in  $F$ .
- (3)  $F$  è il campo di spezzamento su  $K$  di una famiglia di polinomi di  $K[x]$ .

<sup>a</sup>La proposizione è vera anche senza questa ipotesi, ma la dimostriamo solo in questo caso.

*Dimostrazione.* Verifichiamo le varie equivalenze:

- (1)  $\implies$  (2): sia  $f(x) \in K[x]$  e siano  $\alpha_1, \dots, \alpha_n \in \overline{K}$  le radici di  $F$ , per ipotesi sappiamo che  $f(x)$  ha almeno una radice in  $F$ , supponiamo sia  $\alpha_1$ , allora  $K(\alpha_1) \subset F$ , dunque  $\forall i \in \{1, \dots, n\}$  consideriamo le immersioni:

$$\varphi_i : K(\alpha_1) \hookrightarrow K(\alpha_i) \subseteq \overline{K} : \alpha_1 \mapsto \alpha_i \quad \text{con} \quad \varphi_i|_K = id_K$$

esse esistono sempre per la [Proposizione 3.33](#), inoltre,  $\forall i \in \{1, \dots, n\}$  sia  $\tilde{\varphi}_i$  un'estensione di  $\varphi_i$  a  $F$ , cioè ogni immersione di  $K(\alpha_i)$  si estende ad  $F$  in tanti modi quanti il grado  $[F : K(\alpha_1)]$ , pertanto, fissata un'estensione di  $\varphi_i$ :

$$\tilde{\varphi}_i : (K(\alpha_i) \subset) F \longrightarrow \overline{K} \quad \text{con} \quad \tilde{\varphi}_i|_{K(\alpha_1)} = \varphi_i \implies \tilde{\varphi}_i|_K = id_K$$

cioè  $\tilde{\varphi}_i$  si restringe a  $K$  proprio come  $\varphi_i$ , da cui, essendo  $F/K$  normale, si ha che  $\tilde{\varphi}_i(F) = F$ , ma in particolare ciò significa che dalla radice  $\alpha_1$  di  $f(x)$ , che va nei suoi coniugati mediante  $\tilde{\varphi}_i$ , otteniamo tutte le altre radici dentro  $F$ :

$$\tilde{\varphi}_i(\alpha_1) = \varphi_i(\alpha_1) = \alpha_i \in F \quad \forall i \in \{1, \dots, n\}$$

che prova la tesi.

- (2)  $\implies$  (3): Consideriamo  $F_0$  il campo di spezzamento su  $K$  della famiglia di polinomi:

$$\mathcal{F} = \{\mu_\alpha(x) | \alpha \in F, \mu_\alpha(x) \text{ polinomio minimo di } \alpha \text{ su } K\}$$

abbiamo che  $F \subseteq F_0$ , poiché abbiamo aggiunto tutte le radici di tutti i polinomi minimi di tutti gli elementi di  $F$ , dunque  $F_0$  contiene almeno  $F$ . D'altra parte:

$$F_0 = K(\beta | \beta \text{ radice di } \mu_\alpha(x) \in \mathcal{F})$$

dove  $\mu_\alpha(x)$  è irriducibile su  $K[x]$  e  $\alpha$  è una sua radice in  $F$ , dunque per ipotesi  $F$  contiene tutte le radici  $\beta$  di  $\mu_\alpha(x)$ ,  $\forall \mu_\alpha(x) \in \mathcal{F}$ , ovvero  $F_0 \subseteq F$ , quindi  $F = F_0$ , per cui  $F$  è proprio il campo di spezzamento dei polinomi della famiglia  $\mathcal{F}$ .

- (3)  $\implies$  (1): Consideriamo:

$$\varphi : F \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

vogliamo dimostrare che  $\varphi(F) = F$ , avendo per ipotesi che  $F$  è il campo di spezzamento di:

$$\mathcal{F} = \{f_1(x), \dots, f_k(x)\}$$

per cui  $\{\alpha_{ij}\}_{j=1,\dots,n_i}$  sono le radici di  $f_i(x)$ , dunque possiamo riscrivere  $F$  come:

$$F = K(\{\alpha_{ij}\} | i = 1, \dots, k, j = 1, \dots, n_i)^{55}$$

Sappiamo che per ogni  $i$  e  $j$ , poiché  $\varphi$  è un'immersione deve mandare le radici in loro coniugati, dunque  $\varphi(\alpha_{ij}) = \alpha_{ij'}$  (ovvero un'altra radice dello stesso polinomio  $f_i(x) \in K[x]$ , con  $\mu_{\alpha_{ij}}(x) \mid f_i(x)$ ), da cui abbiamo che:

$$\begin{aligned} \varphi(F) &= \varphi(K(\{\alpha_{ij}\} | i = 1, \dots, k, j = 1, \dots, n_i)) = \\ &= K(\varphi(\alpha_{ij}) | i = 1, \dots, k, j = 1, \dots, n_i) \subset F \end{aligned}$$

dove il contenimento segue dal fatto che abbiamo soltanto permutato gli elementi  $\{\alpha_{ij}\}$ , per cui  $K \subset \varphi(F) \subset F$ , ma poiché  $F$  e  $\varphi(F)$  hanno lo stesso grado finito su  $K$ , allora  $\varphi(F) = F$ .

□

### Esempio 3.47 (Ogni estensione di grado 2 è normale)

Sia  $F/K$  un'estensione, supponiamo di essere in caratteristica diversa da 2<sup>a</sup>, con  $[F : K] = 2$  e sia  $\alpha \in F \setminus K \implies F = K(\alpha)$  abbiamo che quindi il polinomio minimo è della forma:

$$\mu_{\alpha}(x) = x^2 + bx + c \in K[x]$$

con:

$$\alpha_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2} \implies \alpha = \frac{-b + \sqrt{\Delta}}{2} \implies F = K(\alpha) = K(\sqrt{\Delta})$$

infatti si verifica facilmente che  $\alpha_1, \alpha_2 \in K(\sqrt{\Delta}) = F$ , ovvero  $F$  è il campo di spezzamento di  $\mu_{\alpha/K}(x)$ , pertanto per la (3) della [Proposizione 3.46](#)  $F/K$  è normale.

<sup>a</sup>Per la precisione, l'osservazione funziona anche in questo caso, infatti l'unico polinomio di grado 2 irriducibile in un campo di caratteristica 2 può essere solo  $x^2 + x + 1$  (dato che tutti quei campi estendono  $\mathbb{F}_2$ ) e per questo si verifica che se  $\alpha$  è una radice,  $\alpha + 1$  è l'altra radice e quindi effettivamente l'estensione è sempre di grado 2.

### Esempio 3.48 (Estensione non normale)

L'estensione  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  non è normale, infatti, preso  $f(x) = x^3 - 2$  irriducibile su  $\mathbb{Q}$  abbiamo in  $\mathbb{Q}(\sqrt[3]{2})$  una sola radice di  $f(x)$  e non tutte, pertanto tale estensione non può essere normale.

### Proposizione 3.49 (Proprietà delle estensioni normali rispetto a composto ed intersezione)

Date due estensioni  $F/K$  e  $L/K$  in una fissata chiusura algebrica  $\bar{K}$  normali, allora  $FL/K$  e  $F \cap L/K$  sono normali.

<sup>55</sup>Potremmo anche considerare il campo di spezzamento del polinomio prodotto dei precedenti, ma le radici sarebbero sempre le stesse.

*Dimostrazione.* La proprietà del composto segue immediatamente dal fatto che l'immersione nella chiusura algebrica:

$$\varphi : FL \longrightarrow \overline{K} \quad \text{con} \quad \varphi|_K = id_K$$

è un omomorfismo, per cui:

$$\varphi(FL) = {}^{56}\varphi(F)\varphi(L) = FL$$

dunque  $FL$  è un'estensione normale. Analogamente per l'intersezione abbiamo:

$$\varphi(F \cap L) = {}^{57}\varphi(F) \cap \varphi(L) = F \cap L$$

ed in questo caso stiamo estendendo  $\varphi$  sia ad  $L$  sia ad  $F$ . □

**Proposizione 3.50** (Proprietà delle estensioni normali rispetto alle torri)

Data una torre di estensioni  $K \subset F \subset L$  in una fissata chiusura algebrica  $\overline{K}$ , se  $L/K$  è normale, allora  $L/F$  è normale.<sup>a</sup>

<sup>a</sup>In generale  $F/K$  non è normale.

*Dimostrazione.* Per ipotesi sappiamo che:

$$\forall \varphi : F \hookrightarrow \overline{K} \quad \text{con} \quad \varphi|_F = id_F$$

essendo  $K \subset F$ , allora  $id_F$  include già  $id_K$ , quindi  $\varphi|_F = id_F \implies \varphi|_K = id_K$ , dato che  $L/K$  è normale, abbiamo  $\varphi(L) = L$  per tutte le immersioni  $\varphi$  di  $L$  che fissano  $K$ , ma abbiamo visti che le immersioni che fissano  $F$  fissano  $K$  dunque  $\varphi(L) = L$  anche in questo caso, pertanto  $L/F$  è normale.

*Dimostrazione alternativa.*<sup>58</sup>  $L/K$  normale significa che è campo di spezzamento di una famiglia di polinomi in  $K[x] \subseteq F[x]$ , quindi  $L$  è il campo di spezzamento della stessa famiglia vista come polinomi in  $F$ . □

**Osservazione 3.51** — Prendendo  $K = \mathbb{Q}$ ,  $F = \mathbb{Q}(\sqrt[3]{2})$  e  $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ , abbiamo che  $L/K$  è normale in quanto tutte le radici del polinomio minimo dei due elementi sono in  $L$ , ma per lo stesso motivo  $F/K$  non è normale.

<sup>56</sup>Ciò deriva dal fatto che gli elementi di  $FL$  sono combinazioni polinomiali degli elementi di  $F$  e di  $L$ .

<sup>57</sup>Ciò andrebbe verificato, ma è abbastanza semplice.

<sup>58</sup>Proposta da Francesco Sorce.

**Osservazione 3.52** — Osserviamo che il viceversa della [Proposizione 3.50](#) è falso, presa ad esempio la torre:

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ | 2 \\ \mathbb{Q}(\sqrt{2}) \\ | 2 \\ \mathbb{Q} \end{array}$$

entrambe le estensioni sono normali, poiché di grado 2, ma la torre non è normale perché  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  contiene solo due radici di  $x^4 - 2$ .

### §3.4 Gruppo di Galois

**Definizione 3.53.** Un'estensione  $E/K$  si dice **estensione di Galois** se è normale e separabile.

In queste dispense tratteremo soltanto il caso di estensioni di Galois finite. Poiché  $E/K$  è normale possiamo considerare l'insieme:

$$\{\varphi : E \hookrightarrow \overline{K} \mid \varphi|_K = id_K\}$$

considerando ora lo stesso insieme, poiché l'estensione è normale, dunque  $\varphi(E) = E$  per ogni  $\varphi$ , possiamo restringere l'insieme di arrivo degli omomorfismi ottenendo:

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

i  $K$ -automorfismi di  $E$ , cioè gli automorfismi dell'estensione che fissano  $K$ , tale insieme con l'operazione di composizione forma il **gruppo di Galois**:

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

con:

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

#### Proposizione 3.54

Il gruppo di Galois dell'estensione di Galois  $E/K$ ,  $\text{Gal}(E/K)$  è un gruppo.

*Dimostrazione.* Essendo un sottoinsieme del gruppo degli automorfismi di un campo, è sufficiente mostrare che un sottogruppo, dunque date  $\varphi, \psi \in \text{Gal}(E/K)$ , allora si verifica che  $\varphi \circ \psi \in \text{Gal}(E/K)$ , inoltre, essendo automorfismi sono invertibili e i loro inversi sono ancora automorfismi, dunque:

$$\forall \varphi \in \text{Gal}(E/K) \implies \varphi^{-1} \in \text{Gal}(E/K)$$

□

#### Proposizione 3.55

Dato  $f(x) \in K[x]$  irriducibile di grado  $n$  e detto  $F$  il suo campo di spezzamento su  $K$ , allora:

$$n \mid [F : K] \mid n!$$

e  $\text{Gal}(F/K) \hookrightarrow S_n$ .

*Dimostrazione.* Dette  $\alpha_1, \dots, \alpha_n$  le radici di  $f(x)$  in  $\overline{K}$ , allora  $F = K(\alpha_1, \dots, \alpha_n)$ , da cui si ha la torre:

$$K \subseteq K(\alpha_1) \subseteq F \implies n = [K(\alpha_1) : K] \mid [F : K] = |\text{Gal}(F/K)|$$

dove la divisibilità segue ovviamente dal **Teorema delle torri**. Consideriamo ora:

$$\phi : \text{Gal}(F/K) \longrightarrow S(\{\alpha_1, \dots, \alpha_n\}) \cong S_n : \varphi \longmapsto \varphi|_{\{\alpha_1, \dots, \alpha_n\}}$$

Osserviamo che:



- **$\phi$  è ben definita**: poiché  $\forall \varphi \in \text{Gal}\left(\frac{F}{K}\right)$ ,  $\varphi$  permuta le radici di  $f(x)$  poiché manda ciascuna in un suo coniugato.

- **$\phi$  è un omomorfismo**: si verifica direttamente che:

$$\phi(\varphi \circ \psi) = (\varphi \circ \psi)|_{\{\alpha_1, \dots, \alpha_n\}} = \varphi(\psi|_{\{\alpha_1, \dots, \alpha_n\}}) = \varphi|_{\{\alpha_1, \dots, \alpha_n\}} \circ \psi|_{\{\alpha_1, \dots, \alpha_n\}}$$

$\forall \phi, \psi \in \text{Gal}\left(\frac{F}{K}\right)$ , in questo caso stiamo restringendo  $\varphi$  alle radici perché  $\psi$  sulle radici ha immagine nelle radici, per quanto detto sopra.

- **$\phi$  è iniettiva**: poiché, avendo dimostrato che è un omomorfismo possiamo studiarne il nucleo:

$$\ker \phi = \left\{ \varphi \in \text{Gal}\left(\frac{F}{K}\right) \mid \varphi(\alpha_i) = id(\alpha_i) = \alpha_i, \forall i \in \{1, \dots, n\} \right\} = \{id\}$$

dove l'ultima uguaglianza è data dal fatto che se  $\varphi$  fissa tutti i generatori di  $\frac{F}{K}$ , l'unica possibilità è che sia l'identità (banalmente perché stiamo considerando funzioni che permutano delle radici, dunque ce n'è una sola che le lascia tutte fisse ed è l'identità). In alternativa si poteva anche osservare che  $\varphi$  è in particolare  $K$  lineare e le radici formano una base su  $K$  di  $F$ , dunque dato che  $\varphi$  coincide con l'identità su queste essa è l'identità.

□

**Osservazione 3.56** — Con la dimostrazione precedente abbiamo anche visto che il gruppo di Galois agisce fedelmente su  $\{\alpha_1, \dots, \alpha_n\}$ . Inoltre tale azione è transitiva perché ha un'unica orbita:

$$\text{Orb}(\alpha_1) = \left\{ \varphi(\alpha_1) \mid \varphi \in \text{Gal}\left(\frac{F}{K}\right) \right\} = \{\alpha_1, \dots, \alpha_n\}$$

infatti, essendo  $[K(\alpha_1) : K] = n$ , allora ho esattamente  $n$  immersioni che permutano i coniugati (ognuna delle quali si può estendere ad  $F$ ):

$$\forall i \in \{1, \dots, n\}, \exists \psi_i : K(\alpha_1) \longrightarrow K(\alpha_i) \subset \overline{K} : \alpha_1 \longmapsto \alpha_i$$

e per tali immersioni abbiamo appunto che l'unica orbita è quella vista sopra.

### Esempio 3.57 (Gruppo di Galois)

Sia  $K$  un campo e  $f(x) \in K[x]$  irriducibile, con  $F$  campo di spezzamento di  $f(x)$  su  $K$ , studiamo il gruppo di Galois di  $F/K$  al variare del grado di  $f(x)$ :

- Se  $\deg f(x) = 2$ , allora  $[F : K] = 2$ , per la [Proposizione 3.55](#), dunque  $\text{Gal}(F/K) \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $\text{Gal}(F/K) = \{id, \varphi\}$ , dove, essendo  $F = K(\sqrt{\Delta})$  abbiamo che:

$$id : a + b\sqrt{\Delta} \mapsto a + b\sqrt{\Delta} \quad \text{e} \quad \varphi : a + b\sqrt{\Delta} \mapsto a - b\sqrt{\Delta}$$

o analogamente, se fosse  $f(x) = (x - \alpha_1)(x - \alpha_2)$  le applicazioni sarebbero state tali che  $id : \alpha_1 \mapsto \alpha_1$  e  $\varphi : \alpha_1 \mapsto \alpha_2$ .

- Se  $\deg f(x) = 3$ , allora  $3 \mid [F : K] \mid 6$ , per la [Proposizione 3.55](#) sappiamo che  $\text{Gal}(F/K) \leq S_3$  pertanto:

$$\text{Gal}(F/K) \cong \begin{cases} A_3 \cong \mathbb{Z}/3\mathbb{Z} \\ S_3 \end{cases}$$

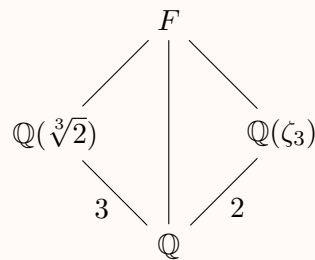
Discutiamo di seguito entrambi i casi con due esempi.

### Esempio 3.58

Se fosse  $f(x) = x^3 - 2$ , con  $K = \mathbb{Q}$  e  $F = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \implies [F : K] = 6$  e quindi  $\text{Gal}(F/K) \cong S_3$ ; per quanto detto sulle immersioni sappiamo che qualsiasi automorfismo del gruppo di Galois deve mandare un elemento nei suoi coniugati, quindi abbiamo in totale appunto 6 possibili immersioni al variare di  $\varphi$ :

$$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\zeta_3^i \quad \text{e} \quad \varphi(\zeta_3) = \zeta_3^j \quad \text{con} \quad i \in \{0, 1, 2\}, j \in \{0, 1\}$$

Necessariamente  $\varphi$  deve verificare le relazioni sopra<sup>a</sup> che danno al più 6 possibili  $\varphi$ . Poiché il grado è 6, tutte e 6 funzionano cioè si estendono ad  $F$ , ciò perché:



ovvero  $[F : \mathbb{Q}] = [Q(\sqrt[3]{2}) : \mathbb{Q}][Q(\zeta_3) : \mathbb{Q}] = 6$ .

<sup>a</sup>E per la precisione, affinché il discorso fatto sopra funzioni gli elementi devono essere algebricamente indipendenti.

**Esempio 3.59** (Vi sconsiglio caldamente di leggere quest'esempio prima che l'abbia riscritto)

<sup>a</sup> Consideriamo  $f(x) = x^3 + x^2 - 2x - 1$ , ovvero il polinomio minimo di  $\zeta_7 + \zeta_7^{-1}$  su  $\mathbb{Q}$  e  $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ , che è normale, quindi di Galois<sup>b</sup>, abbiamo quindi che:

$$\text{Gal}\left(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}\right) \cong \mathcal{A}_3$$

verifichiamo quanto appena detto. Abbiamo che  $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$ , pertanto:

$$\text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right) = \{\varphi : \zeta_7 \mapsto \zeta_7^i \mid (i, 7) = 1\}$$

Osserviamo che il polinomio scritto sopra è proprio il polinomio minimo di  $\alpha = \zeta_7 + \zeta_7^{-1} \in \mathbb{Q}(\zeta_7)$ , infatti per l'appartenenza appena citata sappiamo che tutte le radici di  $\mu_{\zeta_7 + \zeta_7^{-1}}(x)$  stanno in  $\mathbb{Q}(\zeta_7)$ , ed esse sono:

$$\{\varphi(\alpha) \mid \varphi \in \text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)\}$$

le radici sono queste poiché, data la torre:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_7)$$

le immersioni  $\psi$  mandano  $\alpha$  in una qualsiasi radice coniugata di  $\mu_\alpha(x)$ , per cui l'insieme:

$$\{\psi(\alpha)\}$$

che, al variare delle immersioni  $\psi$  di  $\mathbb{Q}(\alpha)$  in  $\overline{\mathbb{Q}}$ , è l'insieme delle radici di  $\mu_\alpha(x)$ , dunque possiamo scrivere:

$$\mu_\alpha(x) = \prod_{\psi} (x - \psi(\alpha))$$

D'altra parte ogni immersione  $\psi$  si estende ad uno  $\varphi \in \text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)$  e  $\forall \varphi \in \text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)$ , sappiamo che  $\varphi(\alpha)$  sarà ancora una radice di  $\mu_\alpha(x)$ , pertanto abbiamo:

$$\{\text{radici di } \mu_\alpha(x)\} = \{\psi(\alpha)\}_{\psi: \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}} = \{\varphi(\alpha)\}_{\varphi \in \text{Gal}\left(\mathbb{Q}(\zeta_7)/\mathbb{Q}\right)}$$

infine abbiamo che:

$$\{\text{radici di } \mu_\alpha(x)\} = \{\varphi(\zeta_7 + \zeta_7^{-1}) = \zeta_7^i + \zeta_7^{-i} \mid i = 1, \dots, 6\} = \{\zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2}, \zeta_7^3 + \zeta_7^{-3}\}$$

ciò dimostra l'assunto iniziale  $[\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) : \mathbb{Q}] = \deg \mu_{\zeta_7 + \zeta_7^{-1}}(x) = 3$ . Per concludere osserviamo che l'estensione è di Galois perché è il campo di spezzamento di  $\mu_{\zeta_7 + \zeta_7^{-1}}(x)$  in quanto:

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 2 \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$$

e analogamente:

$$\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1}) \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$$

si può verificare che in tal modo, con qualche calcolo, è possibile trovare l'espressione di  $\mu_\alpha(x)$ .

<sup>a</sup>Questo è l'esercizio risolto dalla Del Corso con la spiegazione più contorta in assoluto, prometto di riscriverlo per bene nella prima revisione.

<sup>b</sup>Ciò sempre in virtù del fatto che stiamo lavorando soltanto su estensioni separabili.

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

#### Proposizione 3.60 (L'estensione $\mathbb{F}_{q^d}/\mathbb{F}_q$ )

Data l'estensione  $\mathbb{F}_{q^d}/\mathbb{F}_q$ , con  $q = p^r$ , essa è normale.

*Dimostrazione.* Osserviamo che:

$$\forall \varphi : \mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}_p}$$

$\varphi(\mathbb{F}_{p^n})$  è un sottocampo di  $\overline{\mathbb{F}_p}$  con  $p^n$  elementi (essendo  $\varphi$  iniettiva), e per l'unicità dei campi con  $p^n$  elementi deve essere necessariamente che  $\varphi(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}$ , pertanto l'estensione è normale.<sup>59</sup>  $\square$

**Osservazione 3.61** — Osserviamo che tutte le estensioni di campi finiti sono normali, infatti, considerando la torre:

$$\begin{array}{c} \mathbb{F}_{p^n} = \mathbb{F}_{q^d} \\ \text{NOR.} \left( \begin{array}{c} \text{NOR.} \\ \mathbb{F}_q = \mathbb{F}_{p^r} \end{array} \right) \\ \mathbb{F}_p \end{array}$$

dove per quanto detto  $\mathbb{F}_{p^n}/\mathbb{F}_p$  è normale, dunque per la [Proposizione 3.50](#) tutte le estensioni di campi finiti sono normali.

**Definizione 3.62.** Si dice **automorfismo di Frobenius** l'automorfismo:

$$\phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \mapsto x^q$$

#### Teorema 3.63 (Gruppo di Galois di estensioni di campi finiti)

Il gruppo di Galois  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , con  $q = p^r$ , è generato dall'automorfismo di Frobenius  $\phi$  di  $\mathbb{F}_{q^d}$ :

$$\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \phi \rangle$$

con  $\phi$  automorfismo di Frobenius del campo  $\mathbb{F}_{q^d}$ :

$$\phi : \mathbb{F}_{q^d} \xrightarrow{\sim} \mathbb{F}_{q^d} : x \mapsto x^q$$

*Dimostrazione.* Per prima cosa verifichiamo che  $\phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ ;  $\phi$  è un omomorfismo di anelli in quanto:

$$\phi(\alpha + \beta) = (\alpha + \beta)^q = \alpha^q + \beta^q = \phi(\alpha) + \phi(\beta) \quad \forall \alpha, \beta \in \mathbb{F}_{q^d}$$

<sup>59</sup>Alternativamente si ricorda che in [Aritmetica](#), avevamo costruito tutte le estensioni  $\mathbb{F}_{p^n}$  di campi finiti  $\mathbb{F}_p$ , come campi di spezzamento del polinomio  $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ .

dove l'ultima uguaglianza segue dal fatto che  $q = p^r$ , dunque siamo in caratteristica  $p$  e vale il Lemma del Binomio Ingenuo. Analogamente:

$$\phi(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \phi(\alpha)\phi(\beta) \quad \forall \alpha, \beta \in \mathbb{F}_{q^d}$$

si verifica facilmente inoltre che è iniettivo e surgettivo.  $\forall \alpha \in \mathbb{F}_q$  si ha che  $\phi(\alpha) = \alpha^q = \alpha$  (perché stiamo considerando elementi di  $\mathbb{F}_q$ ), dunque  $\phi$  è un automorfismo di  $\mathbb{F}_{q^d}$  che lascia fisso  $\mathbb{F}_q$ , pertanto  $\phi \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , per definizione. Osserviamo che per ipotesi  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  è un gruppo di ordine  $d$  e quindi ovviamente  $\text{ord } \phi = k \mid d$ ; d'altra parte se  $\phi^k = \text{id}$ ,  $\forall \alpha \in \mathbb{F}_{q^d}$  si ha che:

$$\phi^k(\alpha) = \alpha^{q^k} = \alpha$$

cioè il polinomio  $f(x) = x^{q^k} - x$  ha come radici tutti i  $q^d$  elementi di  $\mathbb{F}_{q^d}$ , pertanto abbiamo:

$$\deg f(x) = q^k \geq q^d = |\mathbb{F}_{q^d}| \implies k \geq d$$

da cui  $k = d$  e quindi la tesi:

$$\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \phi \rangle$$

□

### Esempio 3.64

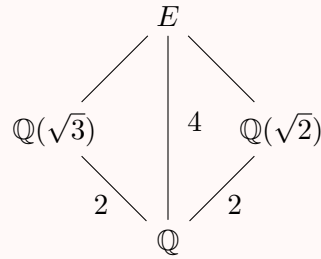
Consideriamo  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ , abbiamo che le estensioni alla chiusura algebrica via identità:

$$\varphi : E \hookrightarrow \overline{\mathbb{Q}}$$

sono determinate dalle immagini di  $\sqrt{2}$  e  $\sqrt{3}$ , dunque abbiamo:

$$\varphi = \begin{cases} \sqrt{2} \mapsto \pm\sqrt{2} \\ \sqrt{3} \mapsto \pm\sqrt{3} \end{cases}$$

da cui il diagramma:



dove il composto e le due estensioni semplici sono normali (perché di grado 2); le quattro immersioni possibili sono:

$$\begin{aligned} id = \varphi_1 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} & \varphi_2 &= \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} & \varphi_3 &= \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \\ \varphi_4 &= \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \end{aligned}$$

con  $\varphi_i(E) = E$ ,  $\forall i = 1, \dots, 4$ . Il gruppo di Galois è dato da  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , poiché ha ordine 4, e tutti gli elementi, esclusa l'identità, hanno ordine 2. Si verifica facilmente via contenimenti che  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ , tuttavia possiamo anche osservare a questo punto che, data la torre:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq E$$

di grado 4, abbiamo che:

$$\begin{aligned} \varphi_1(\sqrt{2} + \sqrt{3}) &= \sqrt{2} + \sqrt{3} & \varphi_2(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} + \sqrt{3} \\ \varphi_3(\sqrt{2} + \sqrt{3}) &= \sqrt{2} - \sqrt{3} & \varphi_4(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} - \sqrt{3} \end{aligned}$$

$\gamma = \sqrt{2} + \sqrt{3}$  ha quattro immagini distinte<sup>a</sup> attraverso le immersioni del gruppo di Galois, e mediante questo  $\gamma$  viene mandato in suoi coniugati su  $\mathbb{Q}$ ; dunque il polinomio minimo di  $\gamma$  su  $\mathbb{Q}$  ha almeno grado 4, ma per la torre precedente ciò significa che  $\mathbb{Q}(\gamma) = E$ .

<sup>a</sup>Per essere precisi ciò significa che, data la base  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  di  $E$ , per mezzo di questa si verifica che tutte e quattro quelle immagini hanno scrittura unica e distinta.

**Osservazione 3.65** — In questo caso abbiamo assunto direttamente che  $\deg \mu_\gamma(x) = 4$ , perché  $\deg \mu_\gamma = \#\{\psi : \mathbb{Q}(\gamma) \hookrightarrow \overline{\mathbb{Q}}\}$  e ogni  $\psi$  si estende ad  $E$ , via:

$$\varphi_i : E \hookrightarrow \overline{\mathbb{Q}}$$

pertanto  $\{\varphi_i(\gamma)\}$  è l'insieme dei coniugati di  $\gamma$  su  $\mathbb{Q}$ .

### §3.6 Teorema dell'elemento primitivo

#### Teorema 3.66 (Teorema dell'elemento primitivo)

Sia  $K$  un campo e sia  $E/K$  un'estensione finita (e separabile), allora  $E/K$  è semplice, cioè:

$$\exists \gamma \in E : E = K(\gamma)$$

*Dimostrazione.* Distinguiamo due casi:

- **$K$  campo infinito:** Per ipotesi abbiamo che  $E/K$  è finita, dunque per la [Proposizione 3.16](#), ciò è equivalente al dire che  $E$  è finitamente generata da elementi algebrici,  $E = K(\alpha_1, \dots, \alpha_n)$ , dimostriamo per induzione che  $E/K$  è semplice. Per  $n = 2$  (trattiamo solo di questo caso in quanto una volta dimostrata la tesi per  $n = 2$ , basterà come al solito aggiungere un altro alla volta e procedere per induzione usando il caso  $n = 2$  come fatto che rende vero il passo induttivo<sup>60</sup>) abbiamo  $E = K(\alpha, \beta)$ , sia  $[E : K] = n$ , allora per il [Corollario 3.35](#):

$$\exists \varphi_1, \dots, \varphi_n : E \hookrightarrow \overline{K} \quad \text{con} \quad \varphi_i|_K = id_K$$

sia  $x$  un'indeterminata, consideriamo i polinomi  $\alpha + \beta x$ , possiamo definire il polinomio:

$$F(x) = \prod_{i < j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)) \in \overline{K}[x]^{61}$$

con  $\deg F(x) \leq \binom{n}{2}$  e  $F(x) \neq 0$  in quanto se un fattore fosse 0, quindi  $\varphi_i(\alpha) + x\varphi_i(\beta) = \varphi_j(\alpha) + x\varphi_j(\beta)$ , da cui  $x(\varphi_i(\beta) - \varphi_j(\beta)) + \varphi_i(\alpha) - \varphi_j(\alpha) = 0$ , per il principio di identità dei polinomi avremmo:

$$\begin{cases} \varphi_i(\beta) - \varphi_j(\beta) = 0 \\ \varphi_i(\alpha) - \varphi_j(\alpha) = 0 \end{cases} \iff \begin{cases} \varphi_i(\beta) = \varphi_j(\beta) \\ \varphi_i(\alpha) = \varphi_j(\alpha) \end{cases}$$

da cui  $\varphi_i \equiv \varphi_j$  perché  $E = K(\alpha, \beta)$  (infatti due immersioni in cui i generatori coincidono sono la stessa immersione), ma ciò è assurdo, in quanto avevamo assunto  $i < j$ . Dunque il polinomio è non nullo ed ha grado limitato, sappiamo quindi che  $F(x)$  ha al più  $\deg F(x)$  radici in  $\overline{K}$  e poiché  $K$  è un campo infinito, allora  $\exists t \in K$  tale che  $F(t) \neq 0$ , dunque:

$$F(t) = \prod_{i < j} (\underbrace{\varphi_i(\alpha) + t\varphi_i(\beta)}_{=\varphi_i(\alpha+t\beta)} - \underbrace{\varphi_j(\alpha) + t\varphi_j(\beta)}_{=\varphi_j(\alpha+t\beta)}) \neq 0$$

da ciò abbiamo che:

$$\varphi_i(\alpha + t\beta) \neq \varphi_j(\alpha + t\beta) \quad \forall i \neq j$$

quindi  $\gamma = \alpha + t\beta$  ha  $n$  coniugati, pertanto  $[K(\gamma) : K] = n \implies E = K(\gamma)$  (ovvero le due estensioni dello stesso campo hanno lo stesso grado e quindi coincidono).

<sup>60</sup>Andrebbe dimostrato anche il caso  $n = 1$ , ma è banale.

<sup>61</sup>È come se applicassimo  $\varphi_i$  al polinomio  $\alpha + \beta x$  e poi vi sottraessimo  $\varphi_j$  applicata allo stesso.



- $K$  campo finito: Se  $E/K$  è finita, allora  $E$  è finito, da cui, per la nota proprietà sui sottogruppi moltiplicativi di un campo finito, sia che  $E^*$  è un sottogruppo moltiplicativo finito di  $E$  ed è ciclico,  $E^* = \langle \gamma \rangle$ , ma per un altro teorema noto da **Aritmetica**, si ha che  $E = K(\gamma)$ .

□

### §3.7 Teorema di corrispondenza di Galois

Data l'estensione di Galois (finita)  $L/K$  e  $H < \text{Gal}(L/K)$  sottogruppo, definiamo la scrittura  $L^H$  come:

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

ovvero il sottocampo<sup>62</sup> di  $L$  di tutti gli elementi fissati da tutti i  $K$ -automorfismi del sottogruppo  $H$ . Si osserva che per tale sottocampo si ha che:

$$K \subseteq L^H \subseteq L$$

la seconda inclusione segue immediatamente dalla definizione, la prima deriva dal fatto che essendo i  $K$ -automorfismi in particolare delle immersioni di  $L$  in  $\bar{K}$  via identità (per come è definito il gruppo di Galois), allora almeno tutti gli elementi del campo  $K$  devono essere fissati per definizione.

**Lemma 3.67** (Il campo fissato è quello base  $\iff$  fissiamo rispetto a tutto il gruppo di Galois)

Sia  $L/M$  un'estensione di Galois e  $H < \text{Gal}(L/M)$ , allora:

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

*Dimostrazione.* Dimostriamo separatamente le due implicazioni:

- Supponiamo che  $G = \text{Gal}(L/M)$  e dimostriamo che  $L^G = M$ . Se  $M \subsetneq L^G$ , allora  $[L^G : M] > 1$ , quindi:

$$\exists \varphi : L^G \longrightarrow \bar{M} \quad \text{con} \quad \varphi|_M = id_M$$

con  $\varphi \neq id$  in quanto il grado è maggiore di 1, per cui non c'è solo l'identità tra le immersioni; a questo punto sappiamo dalla [Proposizione 3.39](#) che l'immersione si può estendere ad un campo più grande, dunque sia:

$$\tilde{\varphi} : L \longrightarrow \bar{M} \quad \text{con} \quad \tilde{\varphi}|_{L^G} = \varphi$$

dove  $\tilde{\varphi}|_M = \varphi|_M = id$ . D'altra parte abbiamo per ipotesi che  $L/M$  è normale, dunque  $\tilde{\varphi}(L) = L$ , quindi:  $\tilde{\varphi} \in \text{Gal}(L/M)$  (perché è un automorfismo che fissa puntualmente  $L$  e si restringe all'identità su  $M$ ), da ciò abbiamo che  $\tilde{\varphi}$  fissa puntualmente  $L^G$ , che è assurdo perché avevamo supposto il grado dell'estensione maggiore di 1 (quindi con un elemento non fissato da  $\tilde{\varphi}$ ).

- Essendo  $L/M$  un'estensione finita, per il [Teorema dell'elemento primitivo](#)  $L = M(\alpha)$ , sia  $H \leq G$  e consideriamo:

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)) \quad \text{con} \quad \deg f(x) = |H|$$

<sup>62</sup>Andrebbe verificato che è un campo.

si ha  $f(x) \in L^H[x]$ , poiché, se consideriamo  $\rho \in H$ , allora si ha:

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

dove l'ultima uguagliando deriva dal fatto che anche  $\rho$  è un elemento di  $H$ , e dunque l'unica cosa che fa è permutare gli elementi dell'insieme stesso. Se  $H = G$  abbiamo  $|G| = [L : M] = [M(\alpha) : M] = \deg \mu_{\alpha/M}(x) \geq \deg f(x) = |H|$ , in quanto  $f(x) \in L^M[x] = M[x]$  per ipotesi e  $f(\alpha) = 0$ , da cui  $\mu_{\alpha}(x) \mid f(x)$  e quindi la tesi  $H = G$ .

□

### Lemma 3.68

Data l'estensione  $L/K$  di Galois e  $H < \text{Gal}(L/K)$ , sia  $\sigma \in \text{Gal}(L/K)$ , allora:

$$L^{\sigma H \sigma^{-1}} = \sigma(L^H)$$

*Dimostrazione.* Ricordando che  $L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\}$ , abbiamo che:

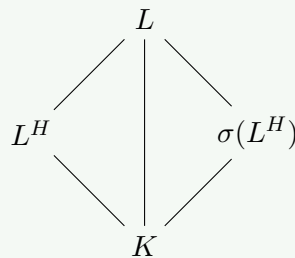
$$\sigma(L^H) = \{\sigma(\alpha) \mid \alpha \in L^H\} = \underbrace{\{\sigma(\alpha) \mid \varphi(\alpha) = \alpha, \forall \varphi \in H\}}_{=\beta}$$

da cui:

$$\begin{aligned} \sigma(L^H) &= \{\beta \in L \mid (\varphi \circ \sigma^{-1})(\beta) = \sigma^{-1}(\beta), \forall \varphi \in H\} = \\ &= \{\beta \in L \mid (\sigma \circ \varphi \circ \sigma^{-1})(\beta) = \beta, \forall \varphi \in H\} = L^{\sigma H \sigma^{-1}} \end{aligned}$$

□

**Osservazione 3.69** — Non è detto che  $\sigma(L^H)$  faccia  $L^H$ , tuttavia sarà sempre una sottoestensione di  $L/K$ , poiché  $L$  è ancora fissato, quindi in generale abbiamo:



**Teorema 3.70** (Teorema di Corrispondenza di Galois)

Data l'estensione di Galois (finita)  $L/K$  c'è una corrispondenza biunivoca tra l'insieme delle sottoestensioni di  $L/K$  e l'insieme dei sottogruppi di  $\text{Gal}(L/K)$ . Inoltre  $H \triangleleft G$  se e solo se  $L^H/K$  è normale, ed in tal caso abbiamo:

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

*Dimostrazione.* Detto  $\mathcal{E}_{L/K} = \{F|K \subseteq F \subseteq L\}$  l'insieme delle sottoestensioni di  $L/K$  e  $\mathcal{G}_{L/K} = \{H < \text{Gal}(L/K)\}$  l'insieme dei sottogruppi del gruppo di Galois dell'estensione, allora essi sono in bigezione:

$$\mathcal{E}_{L/K} \longleftrightarrow \mathcal{G}_{L/K}$$

mediante le applicazioni:

$$\alpha : \mathcal{E}_{L/K} \longrightarrow \mathcal{G}_{L/K} : F \longmapsto \text{Gal}\left(\frac{L}{F}\right)^{63}$$

e:

$$\beta : \mathcal{G}_{L/K} \longrightarrow \mathcal{E}_{L/K} : H \longmapsto L^H$$

Si osserva che essendo  $L^H$  un campo e  $K \subseteq L^H \subseteq L$  per definizione, allora  $\beta$  è ben definita; osserviamo anche che si ha:

$$\text{Gal}\left(\frac{L}{F}\right) < \text{Gal}\left(\frac{L}{K}\right)$$

perché un automorfismo di  $F$  che fissa puntualmente  $F$ , ovviamente fissa puntualmente anche il suo sottoinsieme  $K$ , dunque l'immagine via  $\alpha$  di  $F$  sta in  $\mathcal{G}$ , pertanto  $\alpha$  è ben definita. Verifichiamo ora che  $\alpha$  e  $\beta$  descrivono una bigezione tra  $\mathcal{E}_{L/K}$  e  $\mathcal{G}_{L/K}$ , mostriamo che sono una l'inversa dell'altra:

$$\beta \circ \alpha(F) = \beta\left(\text{Gal}\left(\frac{L}{F}\right)\right) = L^{\text{Gal}\left(\frac{L}{F}\right)} = F \quad \forall F \in \mathcal{E}_{L/K}$$

dove l'ultima uguaglianza è garantita dal [Lemma 3.67](#), in quanto stiamo considerando il campo fissato da tutto il gruppo di Galois  $\text{Gal}\left(\frac{L}{F}\right)$ . Viceversa:

$$\alpha \circ \beta(H) = \alpha(L^H) = \text{Gal}\left(\frac{L}{L^H}\right) = H \quad \forall H \in \mathcal{G}_{L/K}$$

infatti,  $H < \text{Gal}\left(\frac{L}{L^H}\right)$  in quanto tutti gli elementi di  $L^H$  sono fissati dagli elementi di  $H$  per definizione e quindi  $H \subseteq \text{Gal}\left(\frac{L}{L^H}\right)$ ; d'altra parte  $\text{Gal}\left(\frac{L}{L^H}\right) \subseteq H$ , perché, detto  $L^H = M$ , abbiamo  $H \subseteq \text{Gal}\left(\frac{L}{M}\right)$  e  $L^H = M$ , dunque per il [Lemma 3.67](#) segue che  $H = \text{Gal}\left(\frac{L}{L^H}\right)$ .

<sup>63</sup>Per la precisione, avendo assunto che estensione normale e di Galois siano la stessa cosa e che  $L/K$  sia di Galois, allora  $L/F$  è di Galois, mentre non è detto che  $F/K$  lo sia, per la [Proposizione 3.50](#), ed essendo di Galois ciò ci permette di usare la corrispondenza scritta sopra.

Verifichiamo ora la seconda parte del teorema; sappiamo che  $H \triangleleft \text{Gal}(L/K) \iff gHg^{-1} = H, \forall \sigma \in \text{Gal}(L/K)$  e per il [Lemma 3.68](#) abbiamo che:

$$\sigma(L^H) = L^{\sigma H \sigma^{-1}} = L^H \quad \forall \sigma \in \text{Gal}(L/K)$$

e ciò è equivalente al dire che  $L^H/K$  è normale, perché,  $\forall \psi : L^H \hookrightarrow \overline{K}$ , con  $\psi|_K = id_K$ , si ha che  $\psi(L^H) = L^H$ , poiché ogni  $\psi$  si estende a  $L$  e quindi:

$$\forall \varphi \in \text{Gal}(L/K), \exists \sigma \in \text{Gal}(L/K) : \sigma|_{L^H} = \psi$$

Infine, resta da verificare che  $\text{Gal}(L^H/K) \cong G/H$ , consideriamo l'omomorfismo di restrizione:

$$\Gamma : \text{Gal}(L/K) \longrightarrow \text{Gal}(L^H/K) : \varphi \longmapsto \varphi|_{L^H}$$

esso è ovviamente surgettivo perché ogni  $\psi \in \text{Gal}(L^H/K)$  si estende ad  $L$ , ed inoltre:

$$\begin{aligned} \ker \Gamma &= \left\{ \varphi \in \text{Gal}(L/K) \mid \varphi|_{L^H} = id \right\} = \left\{ \varphi \in \text{Gal}(L/K) \mid \varphi(\alpha) = \alpha, \forall \alpha \in L^H \right\} = \\ &= \text{Gal}(L/L^H) \cong H \end{aligned}$$

□

**Osservazione 3.71** — Il teorema ci dice che, data ad esempio la torre:

$$\begin{array}{c} L \\ \left| \begin{array}{c} H \\ L^H \\ G/H \end{array} \right. \\ K \end{array} \quad \text{con } G \text{ a sinistra della parentesi}$$

dove  $G$  è il gruppo di Galois di  $L/K$ . Essendo anche  $L/L^H$  di Galois per ipotesi, e detto  $H$  il suo gruppo di Galois, allora, per il teorema precedente, se  $H \triangleleft G$ , si ha che anche  $L^H/K$  è di Galois ed il suo gruppo di Galois è  $G/H$ .

**Proposizione 3.72** (Proprietà della corrispondenza di Galois)

Dati  $H, S < \text{Gal}(L/K)$ , allora valgono le seguenti:

- (1)  $H \leq S \iff L^H \supset L^S$ .
- (2)  $L^{H \cap S} = L^H L^S$ .<sup>a</sup>
- (3)  $L^{\langle S, H \rangle} = L^H \cap L^S$ .

<sup>a</sup>Intendiamo il composto dei due campi.

*Dimostrazione.* Dimostriamo le affermazione:

- (1) "Ovvio".
- (2) Osserviamo che  $H \cap S \subset H, S$ , dunque  $L^{H \cap S} \supset L^H, L^S$ , per il punto (1); pertanto un campo che contiene entrambi i sottocampi conterrà anche il composto,  $L^{H \cap S} \supset L^H L^S$ . D'altra parte  $L^H L^S \subset L \implies \exists N \leq \text{Gal}\left(\frac{L}{K}\right)$  tale che  $L^H L^S = L^N$ , per il [Teorema di corrispondenza di Galois](#), inoltre:

$$\text{Gal}\left(\frac{L}{L^N}\right) = N \subset \left( \underbrace{\text{Gal}\left(\frac{L}{L^H}\right)}_{=H \cap S} \cap \text{Gal}\left(\frac{L}{L^S}\right) \right)$$

da cui  $N \subset H \cap S \iff L^N \supset L^{H \cap S}$ .

- (3) Abbiamo che  $H \subseteq \langle H, S \rangle$  e  $S \subseteq \langle H, S \rangle$ , da cui  $L^S, L^H \supseteq L^{\langle H, S \rangle}$ , da cui  $L^{\langle H, S \rangle} \subseteq L^H \cap L^S$ .

Viceversa sia  $\alpha \in L^H \cap L^S$ , allora  $\varphi(\alpha) = \alpha, \forall \varphi \in H, S$ , quindi  $\alpha$  è fissato dai generatori del gruppo  $\langle H, S \rangle$ , pertanto  $\alpha$  è fissato da tutti gli elementi di  $\langle H, S \rangle$ , da cui la tesi:

$$L^H \cap L^S \subseteq L^{\langle H, S \rangle}$$

□