# Complementi di Algebra 1

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

Leonardo Migliorini
l.migliorini@studenti.unipi.it
Università di Pisa

Gabriel Antonio Videtta
g.videtta1@studenti.unipi.it
Università di Pisa

Anno Accademico 2022-23

# Indice

## Premessa

Il seguente scritto è una mia rielaborazione delle note del corso di Algebra 1 tenuto dalla prof.ssa Del Corso e dal prof. Lombardo nell'anno accademico 2022-23, con alcune aggiunte relative all'anno accademico 2023-24. **Queste dispense non sono state revisionate dai suddetti professori**.

In particolare, queste dispense contengono soltanto gli appunti delle lezioni complementari del prof. Lombardo (per le note delle lezioni della professoressa Del Corso si rimanda agli Appunti di Algebra 1). L'ordine degli argomenti è pressoché lo stesso di quello seguito a lezione. Chiunque volesse aiutare a migliorare questi appunti può farlo segnalando eventuali errori e/o imprecisioni alle mail dei due autori.

## Ringraziamenti

Si ringraziano Diego Monaco, Niccolò Nannicini, Pietro Crovetto, Leonardo Alfani, Daniele Lapadula, Francesco Sorce, Alessandro Moretti, Matteo Gori, Lorenzo Bonetti e **Rubens Martino**.

# §1 Gruppi

## §1.1 Insiemi di generatori

**Definizione 1.1.** Dati un gruppo $G$ e $x_1, \ldots, x_n$ elementi di $G$, chiamiamo **sottogruppo generato** da $x_1, \ldots, x_n$ il più piccolo sottogruppo $\langle x_1, \ldots x_n \rangle$ di $G$ contenente $x_1, \ldots, x_n$, cioè

$$\langle x_1, \ldots, x_n \rangle = \bigcap_{\substack{H \leqslant G \\ \{x_1, \ldots, x_n\} \subseteq H}} H$$

**Osservazione 1.2** — La definizione è ben posta, infatti l'intersezione avviene su una famiglia non vuota di insiemi dal momento che $G$ è un sottogruppo di se stesso contenente $x_1, \ldots, x_n$. Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi $x_1, \ldots, x_n$.

La definizione data non dà informazioni su come sono fatti gli elementi di $\langle x_1, \ldots, x_n \rangle$, cerchiamo quindi di caratterizzare in modo diverso tale sottogruppo. Poiché chiuso per l'operazione indotta da $G$, $\langle x_1, \ldots, x_n \rangle$ deve contenere tutti i prodotti finiti, in qualsiasi ordine, delle potenze di $x_1, \ldots, x_n$, cioè deve contenere l'insieme

$$\{g_1^{\pm 1} \ldots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}$$

**Proposizione 1.3**

Dati un gruppo $G$ e $x_1, \ldots, x_n$ elementi di $G$, allora

$$\langle x_1 \ldots x_n \rangle = \{g_1^{\pm 1} \ldots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}$$

*Dimostrazione.* Poniamo $S = \{g_1^{\pm 1} \ldots g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}$, mostriamo che $S$ è un sottogruppo di $G$. Effettivamente $e \in S$ in quanto è prodotto di nessuna potenza di $x_1, \ldots, x_n$, il prodotto di due elementi di $S$ è ancora un elemento di $S$ in quanto prodotto finito di potenze di $x_1, \ldots, x_n$ e l'inverso di un elemento $g_1^{\pm 1} \ldots g_r^{\pm 1} \in S$ è $(g_1^{\pm 1} \ldots g_r^{\pm 1})^{-1} = g_r^{\mp 1} \ldots g_1^{\mp 1}$, che è un elemento di $S$. Abbiamo quindi che $S$ è un sottogruppo di $G$ contenente $x_1, \ldots, x_n$, pertanto $\langle x_1, \ldots, x_n \rangle \subseteq S$ per minimalità di $\langle x_1, \ldots, x_n \rangle$. D'altra parte, per quanto osservato sopra abbiamo che tutti gli elementi della forma $g_1^{\pm 1} \ldots g_r^{\pm 1}$ con $r \in \mathbb{N}$, $g_i \in \{x_1, \ldots, x_n\}$ per ogni $i \in \{1, \ldots, r\}$ devono essere contenuti in $\langle x_1, \ldots, x_n \rangle$, pertanto i due sottogruppi coincidono. $\square$

**Osservazione 1.4** — Se $G$ è un gruppo ciclico, esiste allora $x \in G$ tale che $\langle x \rangle = G$, cioè tutti gli elementi di $G$ sono potenze di $x$.

Diciamo che $x_1, \ldots, x_n \in G$ sono **generatori** per $G$, o che l'insieme $\{x_1, \ldots, x_n\}$ **genera** $G$, se $\langle x_1, \ldots, x_n \rangle = G$.

## §1.2 Gruppi liberi e presentazioni

**Definizione 1.5.** Si definisce il **gruppo libero** su $n$ generatori il gruppo $F_n$ tale per cui:

$$F_n = \langle x_1, \ldots, x_n \rangle = \{x_{i_1}^{\pm 1} \cdots x_{i_k}^{\pm 1} \mid i_j \in \{1, \ldots, n\},\, k \in \mathbb{N}\}/\sim$$

dove[1] $a \sim b$ se e solo se eliminando le scritture $x_i x_i^{-1}$ o $x_i^{-1} x_i$ da $a$ e $b$ si ottengono in successione gli stessi simboli. L'operazione di questo gruppo è la concatenazione (ossia il prodotto tra $x_i$ e $x_j$ è per definizione $x_i x_j$) e la stringa vuota è per definizione l'identità, indicata con $e$. Per convenzione si denota $x \cdots x$ ripetuto $k$ volte come $x^k$ e si pone $x^{-k} := (x^{-1})^k$, facendo valere le usuali proprietà delle potenze.

**Osservazione 1.6** (Costruzione del gruppo $F(S)$) — In generale, dato un insieme $S$, si definisce il gruppo libero $F(S)$ come il gruppo libero ottenuto dalle scritture finite di $S$ a meno di equivalenza per $\sim$. Se $S$ è finito e $|S| = n$, allora $F(S) \cong F_n$, dove l'isomorfismo è costruito mandando ordinatamente i generatori di $F(S)$ in $x_1$, ..., $x_n$.

Per i gruppi liberi vale la **proprietà universale**, ossia $\mathrm{Hom}(F_n, G)$ è in bigezione con $G^n$ tramite la mappa che associa un omomorfismo $\varphi$ alla $n$-upla $(\varphi(x_1), \ldots, \varphi(x_n))$, la cui inversa associa una $n$-upla $(g_1, \ldots, g_n)$ ad un unico omomorfismo tale per cui $\varphi(x_i) = g_i$. Questi gruppi, infatti, non presentano alcuna relazione tra i propri generatori, e dunque gli omomorfismi presentati sono sempre ben definiti.

**Definizione 1.7.** Si dice che un gruppo $G$ ammette una **presentazione** se esiste un insieme $S$ di generatori di $G$ e un sottoinsieme $R$ di $F(S)$ tale per cui:

$$G \cong F(S) \big/ N$$

dove $N$ è il più piccolo sottogruppo normale di $F(S)$ contenente $R$, ossia la *chiusura normale* di $R$. In particolare $G$ ammette una presentazione finita se $S$ e $R$ sono finiti.

Se $G$ ammette una presentazione, allora esiste un omomorfismo surgettivo $\varphi : F(S) \to G$ tale per cui $\varphi$ ristretto a $S$ sia l'identità[2] e per cui $\ker \varphi = N$.

In tal caso, è decisamente più facile descrivere gli omomorfismi da $G$ a un qualsiasi altro gruppo $H$. Infatti, poiché $G \cong F(S) \big/ N$, esiste una bigezione, secondo il Primo Teorema di Omomorfismo, tra $\mathrm{Hom}(G, H)$ e gli omomorfismi di $\mathrm{Hom}(F(S), H)$ tali per cui $N$ sia contenuto nel nucleo; affinché $N$ sia contenuto nel nucleo è però sufficiente vi sia contenuto $R$, dacché $N$ è la chiusura normale di $R$. Pertanto $R$ rappresenta in un certo senso un insieme di "relazioni tra i generatori" che devono essere rispettate affinché l'omomorfismo sia ben definito, e così si dice che $R$ è l'insieme dei **relatori** di $G$. Si scrive allora la presentazione di $G$ come:

$$G \cong F(S) \big/ N = \langle S \mid R \rangle$$

Talvolta per $R$ si scrive un insieme di identità $a_1 = b_1$, sottintendendo che $a_1 b_1^{-1}$ appartiene ad $R$.

[1] Si verifica facilmente che la relazione $\sim$ è di equivalenza.
[2] A livello astratto $S$ in $F(S)$ è solo una scrittura simbolica, quello che si intende è che si associa al simbolo $s \in S$ l'effettivo elemento $s$ in $G$.

**Esempio 1.8**

Si illustrano alcuni esempi di presentazione:

- $\mathbb{Z} \cong \langle x_1 \rangle = F_1$
- $\mathbb{Z}/n\mathbb{Z} \cong \langle x \mid x^n = e \rangle$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle x, y \mid x^2 = y^2 = e, [x, y] = e \rangle$
- $(\mathbb{Z}/2\mathbb{Z})^3 \cong \langle x, y, z \mid x^2 = y^2 = z^2 = e, [x, y] = [y, z] = [z, x] = e \rangle$
- $\mathrm{D}_n \cong \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$

## §1.3 Automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$

Dato $p$ un primo, vogliamo determinare quanti sono gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$. Per fare ciò è conveniente osservare che $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ è un campo e che $(\mathbb{Z}/p\mathbb{Z})^n$ è dunque uno spazio vettoriale, dove il prodotto per scalari $\cdot : \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n$ è tale per cui:

$$(\overline{\lambda}, v) \longmapsto \overline{\lambda} v$$

con $\overline{\lambda} v = \underbrace{v + \ldots + v}_{\tilde{\lambda} \text{ volte}}$ e $\tilde{\lambda}$ un qualsiasi rappresentante di $\overline{\lambda}$.

Tale prodotto è ben definito. Se infatti $\lambda, \lambda' \in \mathbb{Z}$ sono tali per cui $\overline{\lambda} = \overline{\lambda'}$, cioè esiste $k \in \mathbb{Z}$ tale che $\lambda = \lambda' + kp$, allora

$$\overline{\lambda'} v = \underbrace{v + \ldots + v}_{\lambda' \text{ volte}} = \underbrace{v + \ldots + v}_{\lambda + kp \text{ volte}} = \underbrace{v + \ldots + v}_{\lambda \text{ volte}}$$

Per come abbiamo è definito il prodotto per scalari su $(\mathbb{Z}/p\mathbb{Z})^n$, si osserva che per ogni $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ vale che $\varphi(\lambda v) = \lambda \varphi(v)$ per ogni $\lambda \in \mathbb{Z}/p\mathbb{Z}$. Pertanto vale la seguente uguaglianza insiemistica

$$\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = \operatorname{GL}((\mathbb{Z}/p\mathbb{Z})^n) = \{\varphi : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \mid \varphi \text{ isomorfismo di sp. vett.}\}$$

Poiché $\operatorname{GL}((\mathbb{Z}/p\mathbb{Z})^n) \cong \operatorname{GL}_n(\mathbb{Z}/p\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z}) \mid \det M \neq 0\}$, possiamo rappresentare ogni automorfismo di $(\mathbb{Z}/p\mathbb{Z})^n$ con una matrice invertibile di taglia $n \times n$ a coefficienti in $\mathbb{Z}/p\mathbb{Z}$.

**Proposizione 1.9**

Dato $p$ un primo, allora

$$\left|\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)\right| = \prod_{i=0}^{n-1} (p^n - p^i)$$

*Dimostrazione.* Osserviamo che un elemento di $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ deve necessariamente mandare una base di $(\mathbb{Z}/p\mathbb{Z})^n$ in un'altra base, e si determina univocamente in questo modo. Sia $\{v_1, \ldots, v_n\}$ una base di $(\mathbb{Z}/p\mathbb{Z})^n$ e sia $\varphi \in \operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$. Consideriamo $\varphi(v_1)$: $\varphi(v_1)$ può assumere qualsiasi valore non nullo, pertanto abbiamo $(p^n - 1)$ possibilità per la sua immagine. Per quanto riguarda $v_2$, $\varphi(v_2)$ può assumere qualsiasi valore non nullo che non sia multiplo di $\varphi(v_1)$, e quindi $p^n - p$ valori. Analogamente $\varphi(v_3)$ può assumere qualsiasi valore non nullo che non appartenga a $\operatorname{Span}(\varphi(v_1), \varphi(v_2))$, che consta di $p^2$ elementi, e così via. Iterando questo ragionamento fino a $\varphi(v_n)$, che può essere scelto in $p^n - p^{n-1}$ modi, si ottiene la tesi. $\square$

## §1.4 Gruppo diedrale

### §1.4.1 Elementi del gruppo

**Definizione 1.10.** Dato $n \geq 3$ un numero naturale, si può considerare un poligono regolare di $n$ vertici centrato nell'origine del piano $\mathbb{R}^2$. Si definisce il **gruppo diedrale** su $n$ vertici, detto $\mathrm{D}_n$, come il gruppo delle isometrie[3] di $\mathbb{R}^2$ che fissano il poligono, cioè che mandano i vertici in se stessi. Per $n = 2$, si definisce $\mathrm{D}_2$ come il gruppo delle isometrie che mandano un segmento in se stesso.

**Osservazione 1.11 —** $\mathrm{D}_n$ è un gruppo, in quanto l'applicazione identità che fissa tutti i vertici è un'isometria dal poligono in se stesso, la composizione di isometrie è un'isometria e un'isometria ammette sempre un'inversa[a], che è anch'essa un'isometria.

[a] In particolare, $\mathrm{D}_n$ si immerge sempre in $\mathrm{O}(2)$, il gruppo delle matrici ortogonali di taglia $2 \times 2$ a coefficienti in $\mathbb{R}$, dal momento che queste rappresentano esattamente le isometrie del piano. Una matrice $M$ di $\mathrm{O}(2)$ è tale per cui $MM^\top = M^\top M = I_2$, e quindi $\det(M) \in \{\pm 1\}$. In particolare $M$ è invertibile, e la sua inversa appartiene ancora a $\mathrm{O}(2)$.

**Osservazione 1.12 —** Una rotazione di angolo[a] $\frac{2\pi}{n}$ è un elemento di $\mathrm{D}_n$, così come una simmetria rispetto a un asse.

[a] Per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario.

Proseguendo con questa intuizione geometrica, indicheremo con $r$ una rotazione di angolo $\frac{2\pi}{n}$ e con $s$ una simmetria rispetto a un qualsiasi asse. Si osserva facilmente che $\operatorname{ord}(r) = n$ e $\operatorname{ord}(s) = 2$.

**Definizione 1.13.** Data $r \in \mathrm{D}_n$ una rotazione di ordine $n$, indichiamo con $\mathcal{R}$ il **sottogruppo delle rotazioni** $\langle r \rangle$.

**Osservazione 1.14 —** Il sottogruppo $\mathcal{R}$ contiene tutte le rotazioni di $\mathrm{D}_n$. Se infatti $r'$ è una rotazione di angolo $\frac{2k\pi}{n}$ con $k \in \mathbb{Z}$, allora $r^k = r'$, e quindi $r' \in \mathcal{R}$.

Inoltre, $\mathcal{R}$ si immerge in $\mathrm{SO}(2)$, il gruppo delle matrici ortogonali speciali, ossia delle matrici ortogonali con determinante 1. Se infatti $r$ è un elemento di $\mathcal{R}$, $r$ è rappresentato da una matrice della seguente forma

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

che ha infatti come determinante $\cos^2(\theta) + \sin^2(\theta) = 1$.

Per determinare come sono fatti gli elementi di $\mathrm{D}_n$, studiamo il sottogruppo $\langle r, s \rangle$. Sicuramente $\langle r, s \rangle$ contiene il sottogruppo $\mathcal{R}$ e tutti gli elementi della forma $sr^k$, $sr^k s$, $sr^k sr^h$, e così via. Vogliamo mostrare che in effetti $\mathrm{D}_n$ è generato da $r$ e $s$.

[3] In particolare tutte queste isometrie sono lineari, dal momento che devono mappare l'origine in se stessa.

**Osservazione 1.15** — Gli elementi della forma $r^k$ e $sr^h$ sono distinti per ogni $h, k \in \mathbb{Z}$. Infatti, presi come elementi di base di $\mathbb{R}^2$ un vettore $v_1$ che giace sull'asse di simmetria di $s$ e un vettore $v_2$ perpendicolare ad esso, $s$ si rappresenta in tale base come la matrice

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

e quindi $s$ corrisponde a una matrice di determinante $-1$. In particolare, $\det : \mathrm{O}(2) \to \{\pm 1\}$ è un omomorfismo di gruppi tale per cui $\ker \det = \mathrm{SO}(2)$, in cui si immerge $\mathcal{R}$. In particolare, per il Primo Teorema di Omomorfismo vale che

$$\mathrm{O}(2) / \mathrm{SO}(2) \cong \{\pm 1\}$$

e quindi esistono solo due classi laterali di $\mathrm{O}(2) / \mathrm{SO}(2)$.

In particolare ogni simmetria della forma $sr^k$ si identifica come elemento di $s\,\mathrm{SO}(2) \neq \mathrm{SO}(2)$. Dal momento allora che $\det(r^k) = 1$ e $\det(sr^h) = -1$, questi elementi sono distinti.

**Lemma 1.16**

Per ogni rotazione $r \in \mathrm{D}_n$ e per ogni simmetria $s \in \mathrm{D}_n$ vale

$$srs^{-1} = r^{-1}$$

*Dimostrazione.* Senza perdita di generalità possiamo supporre che $r$ sia la rotazione di angolo $\frac{2\pi}{n}$ e che $s$ sia la simmetria (rispetto all'asse $y$) che a ogni punto $x$ del piano associa il punto $-x$. Possiamo rappresentare rispettivamente $r$ e $s$ tramite le matrici

$$\begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \qquad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Svolgendo esplicitamente il prodotto si ottiene quindi che

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} =$$

$$= \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(-\frac{2\pi}{n}\right) & -\sin\left(-\frac{2\pi}{n}\right) \\ \sin\left(-\frac{2\pi}{n}\right) & \cos\left(-\frac{2\pi}{n}\right) \end{pmatrix}$$

che è la matrice associata alla rotazione di angolo $-\frac{2\pi}{n}$, cioè $r^{-1}$. □

**Proposizione 1.17**

Se $n \geq 3$ allora $|\mathrm{D}_n| = 2n$.

*Dimostrazione.* Indicando con 0, ..., $n-1$ i vettori degli $n$ vertici di un poligono regolare di $n$ lati, notiamo che un elemento $g \in \mathrm{D}_n$ è univocamente determinato da $g(0)$ e $g(1)$, rappresentando questi una base di vettori per $\mathbb{R}^2$. Infatti 0 e 1, per $n \geq 3$, sono linearmente indipendenti. In particolare, fissato $g(0)$, per il quale abbiamo $n$ possibili scelte, abbiamo al massimo due valori per $g(1)$, cioè $g(0)+1$ o $g(0)-1$ (opportunamente normalizzati modulo $n$). Pertanto possiamo determinare $g$ in al più $2n$ modi, e quindi $|\mathrm{D}_n| \leq 2n$. Ricordando adesso che $\mathrm{D}_n$ contiene gli elementi della forma $r^k$ e $sr^h$ al variare di $h, k \in \mathbb{Z}$, mostriamo che questi sono esattamente $2n$, e dunque che generano anche $\mathrm{D}_n$. Gli elementi $r^k$ appartengono al gruppo ciclico $\mathcal{R}$ di ordine $n$, pertanto sono $n$ elementi distinti, inoltre

$$sr^i = sr^j \iff r^i = r^j \iff i \equiv j \pmod n$$

e dunque anche questi sono $n$ elementi distinti. Poiché gli insiemi $\mathcal{R}$ e $\{sr^h \mid h \in \mathbb{Z}\}$ sono disgiunti (Osservazione 1.15), si ricava che $|\mathrm{D}_n| = 2n$. □

**Osservazione 1.18** — Abbiamo mostrato che effettivamente $\mathrm{D}_n = \langle r, s \rangle$, quindi i suoi elementi sono tutti della forma $r^k$, $sr^h$ al variare di $h, k \in \mathbb{Z}$. In particolare gli elementi distinti di $\mathrm{D}_n$ sono tutti gli $r^k$ e i $sr^h$ con $1 \leq r, k \leq n-1$, insieme all'identità.

**Osservazione 1.19** — Il risultato è valido anche per $\mathrm{D}_2$, ma con motivazioni leggermente differenti. Se consideriamo il segmento nel piano $\mathbb{R}^2$ giacente sulla retta $y = 0$ che congiunge $(1, 0)$ e $(-1, 0)$, ogni isometria di $\mathrm{D}_2$ è tale per cui $e_1$ può essere mappato in sé stesso o in $-e_1$, e analogamente può essere mappato anche $e_2$. Pertanto anche in $\mathrm{D}_2$ vi sono al più $2 \cdot 2 = 4$ isometrie. Dal momento che l'identità, la rotazione di angolo $\pi$, la simmetria lungo la retta $y = 0$ e la simmetria lungo $x = 0$ sono isometrie, $\mathrm{D}_2$ contiene quindi esattamente quattro elementi: l'identità e tre elementi di ordine 2. Essendo composto da $4 = 2^2$ elementi e non essendo ciclico, si conclude infine che $\mathrm{D}_2$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong V$, il gruppo di Klein.

### §1.4.2 Sottogruppi

Consideriamo un sottogruppo $H \leqslant \mathrm{D}_n$. Distinguiamo il caso in cui $H \subseteq \mathcal{R}$ e il caso in cui $H \nsubseteq \mathcal{R}$. Nel primo caso, se $|H| = d$, vale allora che $d \mid n$ e che $H$ è l'unico sottogruppo di $\mathcal{R}$ di ordine $d$, essendo $\mathcal{R}$ ciclico. In particolare varrebbe $H = \langle r^{\frac{n}{d}} \rangle$.

Studiamo ora quindi il caso in cui $H \nsubseteq \mathcal{R}$. Innanzitutto si osserva che $\mathcal{R} \trianglelefteq \mathrm{D}_n$ dal momento che $[\mathrm{D}_n : \mathcal{R}] = 2$. Pertanto ${}^{\mathrm{D}_n}\!/\!_{\mathcal{R}}$ è un gruppo, ed essendo composto da due soli elementi è isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : \mathrm{D}_n \longrightarrow {}^{\mathrm{D}_n}\!/\!_{\mathcal{R}} : g \mapsto g\mathcal{R}$$

Dal momento che $H \nsubseteq \mathcal{R}$, esiste $sr^h \in H$ tale per cui $sr^h \notin \mathcal{R}$, e quindi $\pi_{\mathcal{R}}(sr^h) \neq \mathcal{R}$. In particolare vale allora che $\pi_{\mathcal{R}}(H) \nsubseteq \{\mathcal{R}\}$. Allora, poiché i sottogruppi di ${}^{\mathrm{D}_n}\!/\!_{\mathcal{R}}$ sono solo $\{\mathcal{R}\}$ e ${}^{\mathrm{D}_n}\!/\!_{\mathcal{R}}$, deve valere $\pi_{\mathcal{R}}(H) = {}^{\mathrm{D}_n}\!/\!_{\mathcal{R}}$. Allora, per il Primo Teorema di Omomorfismo, vale che $\ker \pi_{\mathcal{R}|H} = \ker \pi_{\mathcal{R}} \cap H = \mathcal{R} \cap H$ è isomorfo a $\pi_{\mathcal{R}}(H) = {}^{\mathrm{D}_n}\!/\!_{\mathcal{R}} \cong \mathbb{Z}/2\mathbb{Z}$. Da quest'ultima osservazione si ricava quindi che $|H \cap \mathcal{R}| = \frac{1}{2}|H|$.

Dato che $\mathcal{R} \cap H \subseteq \mathcal{R}$, esiste $k \in \mathbb{Z}$ tale per cui $H \cap \mathcal{R} = \langle r^k \rangle$. In particolare $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono entrambi contenuti in $H$, e così anche $\langle r^k, sr^h \rangle$.

**Proposizione 1.20**

Dato $H \leqslant \mathrm{D}_n$ un sottogruppo tale per cui $H \nsubseteq \mathcal{R}$, se $r$ è un generatore di $\mathcal{R}$ tale per cui $H \cap \mathcal{R} = \langle r^k \rangle$ e $sr^h$ è una simmetria di $H$, allora

$$H = \langle r^k \rangle \cdot \langle sr^h \rangle = \{xy \mid x \in \langle r^k \rangle, y \in \langle sr^h \rangle\}$$

*Dimostrazione.* Per quanto visto sopra vale $|\langle r^k \rangle| = \frac{1}{2}|H|$. Inoltre si osserva facilmente che $\operatorname{ord}(sr^h) = 2$:

$$(sr^h)^2 = sr^h sr^h = (srs)^h r^h = (srs^{-1})^h r^h = r^{-h} r^h = e$$

Pertanto $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Inoltre $\langle sr^h \rangle \subseteq N_{\mathrm{D}_n}(\langle r^k \rangle)$; infatti per ogni $m \in \mathbb{Z}$ vale che:

$$(sr^h) r^{mk} (sr^h)^{-1} = sr^{h+mk} sr^h = r^{-h-mk} r^h = r^{-mk} \in \langle r^k \rangle$$

Quindi $\langle r^k \rangle \cdot \langle sr^h \rangle$ è effettivamente un sottogruppo di $\mathrm{D}_n$[4]. Poiché $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono contenuti in $H$, anche $\langle r^k \rangle \cdot \langle sr^h \rangle$ è contenuto in $H$. Infine si verifica che

$$|\langle r^k \rangle \cdot \langle sr^h \rangle| = \frac{1}{2}|H| \cdot 2 = |H|$$

in quanto $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$[5]. Pertanto i due sottogruppi coincidono. □

**Osservazione 1.21** — Per $k \mid n$ e $0 \leq h < k$, i sottogruppi $H_{k,h} = \langle r^k, sr^h \rangle$ e $H = \langle r^k \rangle \cdot \langle sr^h \rangle$ coincidono. Infatti $H_{k,h} \subseteq H$ in quanto $r^k, sr^h$ sono elementi di $H$; d'altra parte $H \subseteq H_{k,h}$ in quanto $H_{k,h}$ contiene tutti i prodotti finiti delle potenze di $r^k$ e $sr^h$.

**Osservazione 1.22** — Per $k \mid n$ e $0 \leq h < k$, $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$. Infatti $\langle r^k, sr^h \rangle \subseteq \langle r^k, sr^{h+k} \rangle$ in quanto $sr^h = (sr^{h+k})r^{-k}$ è un elemento del secondo gruppo. Analogamente $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$ in quanto $sr^{h+k} = (sr^h)r^k$ è un elemento del primo gruppo.

**Teorema 1.23** (Classificazione dei sottogruppi di $\mathrm{D}_n$)

I sottogruppi di $\mathrm{D}_n$ sono della forma

(1) $\langle r^k \rangle$ con $k \mid n$,

(2) $\langle r^k, sr^h \rangle$ con $k \mid n$ e $0 \leq h < k$,

con $r \in \mathcal{R}$ e $s$ una simmetria. Inoltre tali sottogruppi sono tutti distinti.

*Dimostrazione.* La classificazione è sicuramente completa, dal momento che ogni sottogruppo della forma $\langle r^k \rangle$ può ridursi a $\langle r^{k \bmod n} \rangle$, e analogamente $\langle r^k, sr^h \rangle$ è uguale a $\langle r^{k \bmod n}, sr^{h \bmod (k \bmod n)} \rangle$. Consideriamo $H, K \leqslant \mathrm{D}_n$ due sottogruppi, abbiamo tre casi:

[4] Dati $H$, $K$ sottogruppi di un gruppo $G$, se $H \subseteq N_G(K)$, allora $HK = KH$, e quindi $HK$ è un sottogruppo di $G$.

[5] Si ricorda che se $H$ e $K$ sono sottogruppi finiti di un gruppo $G$ allora vale che $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

- se $H = \langle r^k \rangle$ e $K = \langle r^m \rangle$ con $k$, $m \mid n$, allora $H = K$ se e solo se $m = k$;
- se $H = \langle r^k \rangle$ e $K = \langle r^m, sr^h \rangle$, allora $H$ e $K$ sono distinti dal momento che $sr^h$ non può appartenere ad $H$, essendo una rotazione;
- se $H = \langle r^k, sr^h \rangle$ e $K = \langle r^m, sr^l \rangle$, considerando le intersezioni $H \cap \mathcal{R} = \langle r^k \rangle$ e $K \cap \mathcal{R} = \langle r^m \rangle$. Allora, se $H = K$, anche $H \cap \mathcal{R}$ è uguale a $K \cap \mathcal{R}$, e quindi $k = m$. Inoltre, $sr^h$ deve appartenere a $K = \langle r^m, sr^l \rangle = \langle r^m \rangle \langle sr^l \rangle$, e quindi, dacché $sr^h$ è una simmetria, esiste $t \in \mathbb{Z}$ tale per cui

  $$sr^h = (r^m)^t sr^l = sr^{-mt+l}$$

  da cui ricaviamo che $h \equiv l - mt \pmod{n}$, e quindi $h \equiv l \pmod{m}$; in particolare, se $h$ e $l$ sono minori di $m$, deve valere $k = l$.

Quindi la classificazione è unica e completa. □

**Lemma 1.24**
Dati un gruppo $G$ e $A, B$ due sottogruppi tali che $A \leqslant B \leqslant G$, se $B \trianglelefteq G$ e $A$ è caratteristico in $B$ allora $A \trianglelefteq G$.

*Dimostrazione.* Fissato $g \in G$, consideriamo l'omomorfismo di coniugio

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

poiché $B \trianglelefteq G$ è ben definita la restrizione $\varphi_{g|B} \in \mathrm{Aut}(B)$[6]. Dal momento che $A$ è un sottogruppo caratteristico di $B$ abbiamo che $\varphi_{g|B}(A) = \varphi_g(A) = A$. Pertanto $A \trianglelefteq G$. □

**Corollario 1.25**
Ogni sottogruppo di $\mathcal{R}$ è normale in $\mathrm{D}_n$.

*Dimostrazione.* Siano $\langle r^k \rangle$ un sottogruppo di $\mathcal{R}$ e $\varphi \in \mathrm{Aut}(\mathcal{R})$, allora $\varphi(\langle r^k \rangle) = \langle r^k \rangle$ in quanto $\varphi$ preserva l'ordine dei sottogruppi e $\langle r^k \rangle$ è l'unico sottogruppo di $\mathcal{R}$ di tale ordine, dacché $\mathcal{R}$ è ciclico. Pertanto $\langle r^k \rangle$ è caratteristico in $\mathcal{R}$. Poiché $\mathcal{R}$ è un sottogruppo normale di $\mathrm{D}_n$, per il Lemma 1.24 abbiamo $\langle r^k \rangle \trianglelefteq \mathrm{D}_n$. □

**Osservazione 1.26** — A dire il vero, $\mathcal{R} = \langle r \rangle$ non solo è normale in $\mathrm{D}_n$, ma è anche per $n \geq 3$. Infatti per ogni $\varphi \in \mathrm{Aut}(\mathrm{D}_n)$ allora $\mathrm{ord}(\varphi(r)) = \mathrm{ord}(r) = n$. Se $\varphi(r)$ non appartenesse a $\mathcal{R}$, avremmo $\mathrm{ord}(\varphi(r)) = 2$, assurdo dacché $n \geq 3$.

Questo non è vero per $\mathrm{D}_2$. Sia infatti $\varphi : \mathrm{D}_2 \to \mathrm{D}_2$ l'omomorfismo univocamente determinato da

$$r \mapsto s, \quad s \mapsto r$$

Tale omomorfismo è ben definito dal momento che $\varphi(s)\varphi(r)\varphi(s) = rsr = s = s^{-1} = \varphi(r^{-1})$, ed è in particolare un elemento di $\mathrm{Aut}(\mathrm{D}_2)$, dal momento che $\ker \varphi$ è banale. Si osserva inoltre che $\mathrm{Aut}(\mathrm{D}_2) \cong \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathcal{S}_3$.

[6] In generale $\varphi_{g|B}$ non è un coniugio di $B$, poiché $g$ non appartiene necessariamente a $B$.

**Corollario 1.27**
Per $k \mid n$ e $0 \leq h < k$, il sottogruppo $H_{k,h} = \langle r^k, sr^h \rangle$ è normale in $\mathrm{D}_n$ se e solo se $r, s \in N_{\mathrm{D}_n}(H_{k,h})$.

*Dimostrazione.*

- Se $H_{k,h} \trianglelefteq \mathrm{D}_n$ allora $N_{\mathrm{D}_n}(H_{k,h}) = \mathrm{D}_n$, e dunque $r, s \in N_{\mathrm{D}_n}(H_{k,h})$;
- se $r, s \in N_{\mathrm{D}_n}(H_{k,h})$, dacché il normalizzatore è un sottogruppo di $D_n$, si osserva che $\mathrm{D}_n = \langle r, s \rangle \subseteq N_{D_n}(H_{k,h})$, e dunque che $H_{k,h} \trianglelefteq \mathrm{D}_n$.

□

Si calcolano adesso i sottogruppi normali di $\mathrm{D}_n$. Come visto prima, i sottogruppi di $\mathcal{R}$ sono tutti normali. Resta da verificare quali sottogruppi di $\mathrm{D}_n$ sono normali tra quelli della forma $\langle r^k, sr^h \rangle$ con $k \mid n$ e $0 \leq h \leq k-1$. Sia $H$ un tale sottogruppo. Allora, per il corollario precedente, $H$ è normale se e solo se $rHr^{-1} = H$ e $sHs^{-1} = H$.

Si verifica facilmente che $rHr^{-1} = r\langle r^k, sr^h \rangle r^{-1} = \langle r^k, rsr^{h-1} \rangle = \langle r^k, sr^{h-2} \rangle$. Quest'ultimo sottogruppo è uguale ad $H$ se e solo se $h - 2 \equiv h \pmod{k}$, e quindi se e solo se $k \mid 2$. Pertanto $k$ è uguale ad 1 o 2. Per $k = 1$, l'unico sottogruppo considerato è $\langle r, s \rangle = \mathrm{D}_n$, che è banalmente normale.

Si considera d'ora in poi il caso $k = 2$. Dal momento che $k \mid n$, questo implica che $n$ sia pari. Pertanto, se $n$ è dispari, non esistono sottogruppi normali che non siano sottogruppi di $\mathcal{R}$ o che non siano $\mathrm{D}_n$ stesso. Si applica il coniugio ad $H$ tramite la simmetria $s$: $sHs^{-1} = s\langle r^2, sr^h \rangle s^{-1} = \langle r^{-2}, s^2r^hs \rangle = \langle r^2, sr^{-h} \rangle$. Quest'ultimo sottogruppo è uguale ad $H$ se e solo se $-h$ è congruo ad $h$ modulo 2, e quindi sempre. Pertanto, per $n$ pari, sono sottogruppi normali anche $\langle r^2, sr \rangle$ e $\langle r^2, s \rangle$.

Si riassume la classificazione dei sottogruppi normali di $\mathrm{D}_n$ nella seguente lista:

- se $n$ è dispari, i sottogruppi normali di $\mathrm{D}_n$ sono $\mathrm{D}_n$ stesso, $\{\mathrm{id}\}$ e i sottogruppi di $\mathcal{R}$,
- se $n$ è dispari, sono sottogruppi normali di $\mathrm{D}_n$ i sottogruppi elencati nel caso in cui $n$ sia pari insieme a $\langle r^2, sr \rangle$ e $\langle r^2, s \rangle$.

**Osservazione 1.28** — I sottogruppi aggiuntivi che appaiono nel caso in cui $n$ sia pari corrispondono al fatto che in un poligono con un numero pari di lati gli assi di simmetria sono per metà passanti per i lati e metà passanti per i vertici opposti. Al contrario, per un poligono con un numero dispari di lati gli assi di simmetria sono tutti passanti per i lati.

### §1.4.3 Classi di coniugio

Consideriamo la classe di coniugio di $r^h$. Chiaramente ogni elemento di $\mathcal{R}$ commuta con $r^h$ e dunque stabilizza $r$ tramite l'azione di coniugio. Se si considera invece $sr^k$ con $0 \leq k \leq n-1$, allora si verifica che $sr^kr^h(sr^k)^{-1} = sr^kr^hr^{-k}s = sr^hs = r^{-h}$. Pertanto $\mathcal{C}\ell(r^h) = \{r^h, r^{-h}\}$. In particolare $\mathcal{C}\ell(r^h)$ ha sempre due elementi distinti, a meno che

$r^h = r^{-h}$. Quest'ultima identità si verifica solo nel caso in cui $r^{2h} = \mathrm{id}$, e quindi se e solo se

$$\frac{n}{(n,h)} = 2$$

da cui si osserva facilmente che $n$ deve essere pari. In tal caso, detto $n = 2m$, vale che

$$\frac{2m}{(2m,h)} = 2 \iff \frac{m}{(2m,h)} = 1 \iff m = (2m,h)$$

e quindi $m$ deve dividere $h$. Dal momento che $h \leq n-1 = 2m-1$, deve per forza valere $h = m$, e quindi $h = \frac{n}{2}$. Se dunque $n$ è pari, $\mathcal{C}\ell(r^{\frac{n}{2}})$ è composta da un singolo elemento e quindi $r^{\frac{n}{2}}$ appartiene a $Z(\mathrm{D}_n)$.

**Osservazione 1.29 —** Se $n$ è pari, $r^{\frac{n}{2}}$ rappresenta la rotazione di 180°, che commuta con ogni isometria del piano. Infatti, nella base canonica di $\mathbb{R}^2$, tale rotazione è rappresentata dalla matrice $-I_2$, che commuta con ogni matrice di $\mathcal{M}_2(\mathbb{R})$.

Consideriamo adesso la classe di coniugio di $sr^h$. Si verifica facilmente che $r^k sr^h r^{-k} = sr^{h-2k}$ e che $sr^k sr^h sr^k = s^2 r^{h-k} sr^k = sr^{2k-h}$. Pertanto vale che

$$\mathcal{C}\ell(sr^h) = \{sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z}\}$$

I due elementi elencati rappresentano in realtà la stessa sequenza di esponenti, dal momento che $h - 2(h-k) = 2k - h$. Quindi vale che

$$\mathcal{C}\ell(sr^h) = \{sr^{h-2k} \mid k \in \mathbb{Z}\}$$

**Osservazione 1.30 —** Si studiano le simmetrie di $\mathcal{C}\ell(sr^h)$. La simmetria $sr^t$ appartiene a $\mathcal{C}\ell(sr^h)$ se e solo se $x \in \mathbb{Z}$ tale per cui $sr^{h-2x} = sr^t$ e quindi se e solo se $h - 2x \equiv t \pmod n$. Quest'ultima equazione è equivalente a $2x \equiv h - t \pmod n$ ed ha soluzione se e solo se $(2,n) \mid h - t$. Se $n$ è dispari, tale soluzione ha sempre soluzione, se invece $n$ è pari, $(2,n)$ è uguale a 2 e quindi $sr^t \in \mathcal{C}\ell(sr^h)$ se e solo se $t$ ha la stessa parità di $h$.

Riassumendo, se $n$ è dispari, $\mathcal{C}\ell(sr^h) = \mathrm{D}_n \setminus \mathcal{R}$ e dunque contiene tutte le simmetrie; se invece $n$ è pari, $\mathcal{C}\ell(sr^h)$ contiene solo le simmetrie $sr^t$ con $t \equiv h \pmod 2$. Geometricamente questo è equivalente a osservare che, se $n$ è dispari, tutti gli assi di simmetria passano per i vertici (e dunque appartengono alla stessa classe) e che, se $n$ è pari, vi sono due classi di assi di simmetria: quelli passanti solo per i vertici e quelli passanti per il punto medio dei segmenti del poligono regolare considerato.

**Osservazione 1.31 —** Per $n \geq 3$ si osserva che $\mathcal{C}\ell(sr^h)$ non è mai composto da un singolo elemento, e dunque $sr^h \notin Z(\mathrm{D}_n)$. Pertanto si conclude facilmente che $\mathrm{D}_n$ ha centro banale per $n \geq 3$ dispari e che $Z(\mathrm{D}_n) = \left\{\mathrm{id}, r^{\frac{n}{2}}\right\}$ per $n \geq 3$ pari.

### §1.4.4 Legge di gruppo e omomorfismi

In questa sezione si ricava la presentazione di $\mathrm{D}_n$ cercando di descrivere un elemento $s^a r^b$ di $\mathrm{D}_n$ come elemento $(a,b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ con una nuova opportuna operazione di gruppo. Infatti vale che

$$s^{a_1} r^{b_1} \cdot s^{a_2} r^{b_2} = s^{a_1+a_2} r^{(-1)^{a_2} b_1 + b_2}$$

e quindi tale operazione di gruppo sarà descritta dalla relazione[7]

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, (-1)^{a_2} b_1 + b_2)$$

Usando il risultato appena ottenuto si possono descrivere gli omomorfismi da $\mathrm{D}_n$ in un qualsiasi gruppo $G$. Poiché ogni elemento $g \in \mathrm{D}_n$ si scrive come $s^a r^b$, un omomorfismo $\varphi \in \mathrm{Hom}(\mathrm{D}_n, G)$ è chiaramente determinato in modo univoco da $\varphi(r)$ e $\varphi(s)$. Detti $x = \varphi(s)$ e $y = \varphi(r)$, necessariamente $\mathrm{ord}(x) \mid 2$ e $\mathrm{ord}(y) \mid n$, dacché $x^2 = \varphi(s^2) = \varphi(\mathrm{id}) = e_G$ e $y^n = \varphi(r^n) = \varphi(\mathrm{id}) = e_G$. Inoltre deve valere la seguente relazione

$$xyx^{-1} = \varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(srs^{-1}) = \varphi(r^{-1}) = \varphi(r)^{-1} = y^{-1}$$

Mostriamo che effettivamente queste condizioni sono sufficienti affinché un omomorfismo $\varphi : \mathrm{D}_n \to G$ sia ben definito.

**Proposizione 1.32**

Dati un gruppo $G$ e un'applicazione

$$\varphi : \mathrm{D}_n \longrightarrow G : s^a r^b \longmapsto x^a y^b$$

con $x$, $y \in G$, allora $\varphi$ è un omomorfismo se e solo se $x^2 = e_G$, $y^n = e_G$ e $xyx^{-1} = y^{-1}$.

*Dimostrazione.* Mostriamo che tali condizioni sono sufficienti affinché $\varphi$ sia un omomorfismo. Poiché $x^m = x^{-m}$ per ogni $m \in \mathbb{Z}$, fissati $a_1$, $a_2$, $b_1$, $b_2 \in \mathbb{Z}$ ricaviamo che

$$\begin{aligned}(x^{a_1} y^{b_1})(x^{a_2} y^{b_2}) &= x^{a_1} x^{a_2} (x^{a_2} y^{b_1} x^{-a_2}) y^{b_2} = x^{a_1+a_2} \varphi_{x^{a_2}}(y^{b_1}) y^{b_2} = \\ &= x^{a_1+a_2} (\varphi(\varphi_{s^{a_2}}(r)))^{b_1} y^{b_2} = x^{a_1+a_2} y^{(-1)^{a_2} b_1} y^{b_2} = x^{a_1+a_2} y^{(-1)^{a_2} b_1 + b_2}\end{aligned}$$

dove con $\varphi_g$ si indica l'automorfismo di coniugio per $g$. Allora si verifica facilmente che $\varphi$ è un omomorfismo. Infatti per ogni $h_1$, $h_2$, $k_1$, $k_2 \in \mathbb{Z}$ vale che

$$\begin{aligned}\varphi((s^{h_1} r^{k_1})(s^{h_2} r^{k_2})) &= \varphi(s^{h_1+h_2} r^{(-1)^{h_2} k_1 + k_2}) = \\ &= x^{h_1+h_2} y^{(-1)^{h_2} k_1 + k_2} = (x^{h_1} y^{k_1})(x^{h_2} y^{k_2}) = \varphi(s^{h_1} r^{h_2}) \varphi(s^{h_2} r^{h_2})\end{aligned}$$

□

**Osservazione 1.33** — Le condizioni $\mathrm{D}_n = \langle r, s \rangle$, $\mathrm{ord}(r) = n$, $\mathrm{ord}(s) = 2$ e $srs^{-1} = r^{-1}$ determinano in modo univoco la struttura astratta di $\mathrm{D}_n$. Pertanto la presentazione desiderata di $\mathrm{D}_n$ è la seguente

$$\langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$$

[7] Questa operazione è esattamente quella che si ottiene considerando il prodotto semidiretto $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, dove $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ è univocamente determinata dalla relazione $[1] \mapsto -\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$. Più avanti si dimostrerà che in effetti $\mathrm{D}_n$ è proprio isomorfo a questo gruppo.

### §1.4.5 Automorfismi

Studiamo separatamente gli automorfismi di $D_n$ per $n \geqslant 3$ e di $D_2$.
Per $n \geqslant 3$ consideriamo $\varphi \in \mathrm{Aut}(D_n)$, poiché $D_n = \langle r, s\rangle$ è sufficiente studiare le immagini di $r, s$ per determinare $\varphi$. Osserviamo che necessariamente $\varphi(r) = r^k$ con $(n, k) = 1$, infatti $\varphi$ deve preservare l'ordine di $r$ e la sua immagine deve essere un generatore di $\mathcal{R}$, in quanto $\mathcal{R}$ è caratteristico in $D_n$ e isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Per quanto riguarda $\varphi(s)$, se $n$ è dispari allora le simmetrie sono gli unici elementi di ordine 2, pertanto $\varphi(s) = sr^h$ con $0 \leq h < n$. Se $n$ è pari abbiamo apparentemente due possibilità:

(1) $\varphi(s) = sr^h$, con $0 \leq h < n$;

(2) $\varphi(s) = r^{\frac{n}{2}}$, se $n$ è pari.

D'altra parte, se fosse $\varphi(s) = r^{\frac{n}{2}}$ allora $\varphi$ non sarebbe né iniettiva né surgettiva, pertanto $\varphi(s) = sr^h$ con $0 \leq h \leq n$. Verifichiamo che $\varphi$ è un omomorfismo, per la caratterizzazione che abbiamo dato sopra è sufficiente verificare che $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)^{-1}$:

$$\varphi(s)\varphi(r)\varphi(s)^{-1} = (sr^h)r^k(sr^h)^{-1} = sr^{h+k}r^{-h}s = sr^ks^{-1} = r^{-k} = \varphi(r)^{-1}$$

Inoltre $\varphi$ è surgettiva, infatti $r^k, sr^h \in \mathrm{Im}\varphi$, cioè

$$\langle r^k, sr^h\rangle = \langle r, sr^h\rangle = \langle s, r\rangle = D_n \subseteq \mathrm{Im}\varphi$$

da cui $\mathrm{Im}\varphi = D_n$. Poiché $D_n$ è finito abbiamo che $\varphi$ è un automorfismo. Gli automorfismi di $D_n = \langle r, s\rangle$ quindi sono tutti e soli gli omomorfismi da $D_n$ in $D_n$ che mandano $r$ in un generatore di $\mathcal{R}$, che sono $\phi(n)$, e $s$ in un'altra simmetria, che sono $n$, pertanto $|\mathrm{Aut}(D_n)| = n\phi(n)$.

Per $n = 2$, sappiamo che $D_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$, pertanto

$$\mathrm{Aut}(D_2) \cong \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong \mathcal{S}_3$$

Alternativamente possiamo considerare $(\mathbb{Z}/2\mathbb{Z})^2$ come spazio vettoriale su $\mathbb{F}_2$, pertanto abbiamo

$$\mathrm{Aut}(D_2) \cong GL_2(\mathbb{F}_2)$$

Per quanto visto nella sezione (1.2), $GL_2(\mathbb{F}_2)$ contiene $(4-1)(4-2) = 6$ elementi, inoltre $GL_2$ non è un gruppo commutativo (con l'operazione di prodotto tra matrici), pertanto $GL_2(\mathbb{F}_2) \cong \mathcal{S}_3$. In particolare, gli elementi di $GL_2(\mathbb{F}_2)$ sono:

- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, che è l'identità del gruppo;
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, che sono gli elementi di ordine 2 corrispondenti alle trasposizioni;
- $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ che sono gli elementi di ordine 3 corrispondenti ai 3-cicli.

## §1.5 Automorfismi di un prodotto diretto

Consideriamo due gruppi finiti $H, K$, studiamo il gruppo degli automorfismi di $H \times K$. Chiaramente esiste un'inclusione di $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ data dall'omomorfismo

$$\iota : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \hookrightarrow \mathrm{Aut}(H \times K) : (\varphi_1, \varphi_2) \longmapsto \varphi_1 \times \varphi_2$$

con

$$\varphi_1 \times \varphi_2 : H \times K \longrightarrow H \times K : (g_1, g_2) \longmapsto (\varphi_1(g_1), \varphi_2(g_2))$$

Mostriamo che $\iota$ è ben definita e che è effettivamente un omomorfismo iniettivo:

- per ogni $(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2), (h_1, h_2) \in H \times K$ abbiamo

$$(\varphi_1 \times \varphi_2)((g_1, g_2)(h_1, h_2)) = (\varphi_1(g_1h_1), \varphi_2(g_2h_2)) = (\varphi_1(g_1)\varphi_1(h_1), \varphi_2(g_2)\varphi_2(h_2)) = \\ = (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(h_1), \varphi_2(h_2)) = ((\varphi_1 \times \varphi_2)(g_1, g_2))((\varphi_1 \times \varphi_2)(h_1, h_2))$$

  cioè $\varphi_1 \times \varphi_2$ è un omomorfismo. Inoltre

$$\ker(\varphi_1 \times \varphi_2) = \{(g_1, g_2) \in H \times K \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K)\} = \{(e_H, e_K)\}$$

  quindi $\varphi_1 \times \varphi_2 \in \mathrm{Aut}(H \times K)$ in quanto $H \times K$ è finito, pertanto $\iota$ è ben definita;

- per ogni $(\varphi_1, \varphi_2), (\psi_1, \psi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2) \in H \times K$ abbiamo

$$\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2))(g_1, g_2) = \iota(\varphi_1\psi_1, \varphi_2\psi_2)(g_1, g_2) = (\varphi_1\psi_1 \times \varphi_2\psi_2)(g_1, g_2) = \\ = (\varphi_1(\psi_1(g_1)), \varphi_2(\psi_2(g_2))) = (\varphi_1 \times \varphi_2)(\psi_1(g_1), \psi_2(g_2)) = \\ = ((\varphi_1 \times \varphi_2)(\psi_1 \times \psi_2))(g_1, g_2) = (\iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2))(g_1, g_2)$$

  cioè $\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2)) = \iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2)$, quindi $\iota$ è un omomorfismo;

- $\iota$ è iniettiva, infatti

$$\ker \iota = \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid \iota(\varphi_1, \varphi_2) = id_{\mathrm{Aut}(H \times K)}\} = \\ = \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid (\varphi_1(g_1), \varphi_2(g_2)) = (g_1, g_2)\ \forall (g_1, g_2) \in H \times K\} = \\ = \{(id_{\mathrm{Aut}(H)}, id_{\mathrm{Aut}(K)})\} = \{id_{\mathrm{Aut}(H) \times \mathrm{Aut}(K)}\}$$

**Proposizione 1.34**

Dati due gruppi finiti $H, K$, $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$ se e solo se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

*Dimostrazione.* Sia $\iota$ l'immersione da $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ definita come sopra, se $\iota$ è surgettiva allora ogni elemento di $\mathrm{Aut}(H \times K)$ può essere scritto come $\varphi_1 \times \varphi_2$ con $\varphi_1 \in \mathrm{Aut}(H)$ e $\varphi_2 \in \mathrm{Aut}(K)$. Allora abbiamo

$$(\varphi_1 \times \varphi_2)(H \times \{e_K\}) = (\varphi_1(H), \varphi_2(\{e_K\})) = H \times \{e_K\}$$

$$(\varphi_1 \times \varphi_2)(\{e_H\} \times K) = (\varphi_1(\{e_H\}), \varphi_2(K)) = \{e_H\} \times K$$

cioè $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$. Viceversa, se i due sottogruppi sono caratteristici, dato $\varphi \in \mathrm{Aut}(H \times K)$ poniamo $\varphi_1 \in \mathrm{Aut}(H)$ tale che $\varphi(g_1, e_K) = (\varphi_1(g_1), e_K)$ e $\varphi_2 \in \mathrm{Aut}(K)$ tale che $\varphi(e_H, g_2) = (e_H, \varphi_2(g_2))$ per ogni $g_1 \in H$, per ogni

$g_2 \in K$ (questo possiamo farlo in quanto $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici). Allora abbiamo

$$\begin{aligned}\varphi(g_1, g_2) = \varphi((g_1, e_K)(e_H, g_2)) = \varphi(g_1, e_K)\varphi(e_H, g_2) = \\ = (\varphi_1(g_1), e_K)(e_H, \varphi_2(g_2)) = (\varphi_1(g_1), \varphi_2(g_2)) = (\varphi_1 \times \varphi_2)(g_1, g_2)\end{aligned}$$

cioè $\iota$ è surgettiva e quindi un isomorfismo tra $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ e $\mathrm{Aut}(H \times K)$. $\square$

**Esempio 1.35**

Consideriamo il gruppo $G = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, osserviamo che il sottogruppo $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ è caratteristico in quanto un automorfismo $\varphi$ di $G$ deve preservare gli ordini degli elementi, in particolare quello di un generatore, quindi l'immagine di un generatore è un altro generatore del sottogruppo. Poiché gli elementi di $G$ di ordine finito sono tutti della forma $(0, d)$ abbiamo che $\varphi(\{0\} \times \mathbb{Z}/n\mathbb{Z}) = \{0\} \times \mathbb{Z}/n\mathbb{Z}$. Viceversa, l'immagine di $\varphi$ su un generatore di $\mathbb{Z} \times \{0\}$, ad esempio $\varphi(1, 0)$, è della forma $(a, b)$, e questo implica che $\mathbb{Z} \times \{0\}$ non è caratteristico. Se $\varphi$ è surgettivo, necessariamente esiste $(x, y) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tale che $\varphi(x, y) = (\pm 1, 0)$, da cui, posti $\varphi(1, 0) = (a, b)$ e $\varphi(0, 1) = (0, d)$ con $n$ e $d$ coprimi, abbiamo

$$\begin{aligned}\varphi(x, y) = \varphi(x(1, 0) + y(0, 1)) = x\varphi(1, 0) + y\varphi(0, 1) = \\ = x(a, b) + y(0, d) = (xa, xb + yd) = (\pm 1, 0) \iff a = \pm 1\end{aligned}$$

Viceversa, se $a = \pm 1$ allora $\varphi$ è surgettiva, infatti per ogni $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, scegliendo $x = x_0 a$ e $y \equiv d^{-1}(y_0 - x_0 ab) \pmod{n}$ abbiamo

$$\varphi(x, y) = (x_0 a^2, x_0 ab + dd^{-1}(y_0 - x_0 ab)) = (x_0, y_0)$$

e questo ci permette di concludere che $\mathbb{Z} \times \{0\}$ non è un sottogruppo caratteristico. In questo caso abbiamo solo un'immersione del gruppo $\mathrm{Aut}(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ dentro a $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$, in quanto gli automorfismi che mandano $(\pm 1, 0)$ in $(a, b)$ con $a = \pm 1$ e $b \neq 0$ non possono essere ristretti ad automorfismi di $\mathbb{Z} \times \{0\}$.

È utile riuscire a determinare se i sottogruppi $H \times \{e_K\}$, $\{e_H\} \times K$ sono caratteristici in $H \times K$, da cui il seguente risultato:

**Proposizione 1.36**

Dati due gruppi finiti $H, K$, se $(|H|, |K|) = 1$ allora $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

*Dimostrazione.* Posti $n = |H|$, $m = |K|$, consideriamo l'insieme

$$S = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^n = (e_H, e_K)\}$$

Osserviamo che $H \times \{e_K\} = S$, infatti $H \times \{e_K\} \subseteq S$ in quanto tutti gli elementi di $H \times \{e_K\}$ hanno ordine che divide $n$. D'altra parte dato $(g_1, g_2) \in S$, se $\mathrm{ord}(g_1, g_2) \mid n$ allora $\mathrm{ord}(g_1) \mid n$ e $\mathrm{ord}(g_2) \mid n$, ma $\mathrm{ord}(g_2) \mid m$ per il Teorema di Lagrange, quindi $\mathrm{ord}(g_2) = 1$ e $S \subseteq H \times \{e_K\}$, da cui l'uguaglianza. Con un ragionamento analogo possiamo caratterizzare $\{e_H\} \times K$ come

$$\{e_H\} \times K = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^m = (e_H, e_K)\}$$

Poiché un automorfismo di $H \times K$ deve preservare gli ordini degli elementi, per la caratterizzazione data abbiamo che i due sottogruppi sono caratteristici. □

**Corollario 1.37**

Se $m, n \geqslant 2$ sono interi coprimi allora

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$$

## §1.6 Gruppo derivato

**Definizione 1.38.** Dati un gruppo $G$ e $x, y$ elementi di $G$, chiamiamo **commutatore** di $x$ e $y$ l'elemento $[x, y] = xyx^{-1}y^{-1}$. Chiamiamo **sottogruppo derivato** di $G$, oppure **sottogruppo dei commutatori** di $G$ il sottogruppo

$$G' = \langle \{[x, y] \mid x, y \in G\} \rangle$$

**Osservazione 1.39** — $[x, y] = e$ se e solo se $x$ e $y$ commutano.

**Proposizione 1.40**
Dato un gruppo $G$, valgono i seguenti fatti:

(1) $G'$ è un sottogruppo caratteristico di $G$;

(2) ${}^{G}\!/_{G'}$ è un gruppo abeliano;

(3) dato $A$ un gruppo abeliano e $\varphi \in \mathrm{Hom}(G, A)$, allora $G' \subseteq \ker \varphi$.

*Dimostrazione.* Mostriamo le affermazioni singolarmente:

(1) consideriamo $\varphi \in \mathrm{Aut}(G)$, poiché $\varphi$ preserva la struttura di gruppo è sufficiente descrivere come $\varphi$ agisce sui generatori di $G'$ per determinare $\varphi(G')$. Fissati $x, y \in G$ abbiamo

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in G'$$

pertanto $\varphi(G') \subseteq G'$, da cui l'uguaglianza in quanto $\varphi$ è bigettiva;

(2) dati $x, y \in G$, $xG' \cdot yG' = yG' \cdot xG'$ se e solo se $xyG' = yxG'$, che è equivalente a richiedere $xyx^{-1}y^{-1} \in G'$. Dato che effettivamente $xyx^{-1}y^{-1} = [x, y]$ è un elemento di $G'$ abbiamo che ${}^{G}\!/_{G'}$ è abeliano;

(3) dati $x, y \in G$, abbiamo

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$$

e questo coincide con l'identità di $A$ in quanto $A$ è abeliano. Poiché l'immagine di $\varphi$ è un sottogruppo di $A$ allora $G' \subseteq \ker \varphi$, in quanto il commutatore di ogni coppia di elementi di $G$ è contenuto in $\ker \varphi$.

□

**Osservazione 1.41** — Come conseguenza del Primo Teorema di Omomorfismo abbiamo che ${}^{G}\!/_{G'}$ è il "più grande" quoziente abeliano di $G$, o analogamente che $G'$ è il "più piccolo" sottogruppo di $G$ che produce un quoziente abeliano. In questo senso, $G'$ misura quanto è abeliano il gruppo $G$.

**Osservazione 1.42 —** Dato $A$ un gruppo abeliano, il Primo Teorema di Omomorfismo produce una bigezione naturale tra $\mathrm{Hom}(G, A)$ e $\mathrm{Hom}\left({}^{G}\!/_{G'}, A\right)$. Consideriamo infatti $\varphi \in \mathrm{Hom}(G, A)$, $\pi_{G'} : G \longrightarrow {}^{G}\!/_{G'}$ la proiezione al quoziente e $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$, il Teorema fornisce un'unico omomorfismo $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$ che rende commutativo il diagramma

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi_{G'}"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\ {}^{G}\!/_{G'} \arrow[ur, hook, "\overline{\varphi}"'] & \end{tikzcd}$$

Viceversa, dato un omomorfismo $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$ otteniamo un'unico omomorfismo $\varphi : G \longrightarrow A$ con la composizione $\overline{\varphi} \circ \pi_{G'}$.

**Esempio 1.43**

Consideriamo il gruppo $\mathcal{S}_3$, chiaramente $(\mathcal{S}_3)' \neq \{id\}$ in quanto ${}^{\mathcal{S}_3}\!/_{\langle id \rangle} \cong \mathcal{S}_3$ che non è abeliano, pertanto abbiamo due possibilità: $(\mathcal{S}_3)' = \mathcal{S}_3$ oppure $(\mathcal{S}_3)' = \langle (1\ 2\ 3) \rangle$[a]. D'altra parte ${}^{\mathcal{S}_3}\!/_{\langle (1\ 2\ 3) \rangle}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, che è abeliano, pertanto $(\mathcal{S}_3)'$ è contenuto in $\langle (1\ 2\ 3) \rangle$, da cui necessariamente $(\mathcal{S}_3)' = \langle (1\ 2\ 3) \rangle$. Più in generale vedremo che $(\mathcal{S}_n)' = \mathcal{A}_n$, dove $\mathcal{A}_n$ è il sottogruppo di $\mathcal{S}_n$ delle permutazioni pari (sappiamo già che $(\mathcal{S}_n)' \subseteq \mathcal{A}_n$ in quanto ${}^{\mathcal{S}_n}\!/_{\mathcal{A}_n} \cong \mathbb{Z}/2\mathbb{Z}$).

[a] Gli unici sottogruppi normali di $\mathcal{S}_3$ sono $\{id\}$, $\langle (1\ 2\ 3) \rangle$, $\mathcal{S}_3$.

## §1.7 Azioni di gruppo

### §1.7.1 Azioni transitive

**Definizione 1.44.** Siano $G$ un gruppo e $X$ un insieme, un'azione

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

si dice **transitiva** se per ogni $x, y \in X$ esiste $g \in G$ tale che $\varphi_g(x) = y$, equivalentemente se $\operatorname{Orb}(x) = X$ per ogni $x \in X$. Diciamo anche che G **agisce transitivamente** su $X$ tramite $\varphi$.

**Lemma 1.45**

Dato $G$ un gruppo finito e $H \lneq G$ un suo sottogruppo proprio, allora

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

*Dimostrazione.* Poniamo $K = \bigcup_{g \in G} gHg^{-1}$, osserviamo che gli elementi della forma $xHx^{-1}$ con $x \in N_G(H)$ contribuiscono una sola volta all'unione, in quanto $xHx^{-1} = H$, pertanto $K$ è unione di $[G : N_G(H)] = \dfrac{|G|}{|N_G(H)|}$ elementi distinti[8]. Poiché $H \subseteq N_G(H)$ e $|gHg^{-1}| = |H|$ per ogni $g \in G$, possiamo stimare la cardinalità di $K$ nel seguente modo

$$|K| \leq \frac{|G|}{|N_G(H)|}|H| \leq \frac{|G|}{|H|}|H| = |G|.$$

D'altra parte, per il Principio di Inclusione-Esclusione abbiamo che $|K|$ è somma delle cardinalità dei singoli termini dell'unione se e solo se l'unione è disgiunta, ma questo è falso in quanto ogni classe di coniugio di $H$ contiene l'identità del gruppo, quindi $|K| < |G|$, cioè $G \neq K$. □

**Proposizione 1.46**

Dati un gruppo $G$ e un insieme $X$, se

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

è un'azione transitiva valgono i seguenti fatti:

(1) per ogni $x, y \in X$ esiste $g \in G$ tale che $g \operatorname{St}(x) g^{-1} = \operatorname{St}(y)$;

(2) se $|X| \geqslant 2$ e $G$ è finito allora esiste $g \in G$ che agisce su $X$ senza punti fissi, cioè tale che $\varphi_g(x) \neq x$ per ogni $x \in X$.

*Dimostrazione.* Mostriamo i due fatti singolarmente:

[8] Infatti, se $X = \{N \mid N \leqslant G\}$ e $\varphi$ è l'azione di coniugio su $X$, per ogni $N \in X$ abbiamo $\operatorname{St}(N) = N_G(N)$ e $\operatorname{Orb}(N) = \mathcal{C}\ell(N) = \{gNg^{-1} \mid g \in G\}$. Vale quindi la relazione $|G| = |\mathcal{C}\ell(N)| \cdot |N_G(N)|$.

(1) sia $g \in G$ tale che $\varphi_g(x) = y$, dato $h \in g \operatorname{St}(x) g^{-1}$ esiste $w \in \operatorname{St}(x)$ tale che $h = gwg^{-1}$. Allora

$$\varphi_h(y) = \varphi_{gwg^{-1}}(y) = \varphi_g(\varphi_w(\varphi_g^{-1}(y))) = \varphi_g(\varphi_w(x)) = \varphi_g(x) = y$$

pertanto $g \operatorname{St}(x) g^{-1} \subseteq \operatorname{St}(y)$. Osservando che $\varphi_{g^{-1}}(y) = x$ e ragionando in modo simmetrico otteniamo l'inclusione $g^{-1} \operatorname{St}(y) g \subseteq \operatorname{St}(x)$, da cui $g \operatorname{St}(x) g^{-1} = \operatorname{St}(y)$;

(2) un elemento $g \in G$ con tali proprietà non può essere contenuto nello stabilizzatore di nessun elemento di $X$, cioè cerchiamo $g \in G$ tale che

$$g \in \bigcap_{x \in X} \operatorname{St}(x)^{\mathcal{C}}$$

che è equivalente a

$$g \notin \bigcup_{x \in X} \operatorname{St}(x) = \bigcup_{h \in G} h \operatorname{St}(x_0) h^{-1}$$

per il fatto precedente, fissato $x_0 \in G$. Osserviamo che $\operatorname{St}(x_0) \neq G$, infatti se fosse $\operatorname{St}(x_0) = G$ avremmo

$$|\operatorname{Orb}(x_0)| = \frac{|G|}{|\operatorname{St}(x_0)|} = 1$$

ma questo è assurdo in quanto $\operatorname{Orb}(x_0) = X$ per la transitività di $\varphi$ e $|X| \geqslant 2$. Allora per il Lemma 1.40 abbiamo

$$G \neq \bigcup_{h \in G} h \operatorname{St}(x_0) h^{-1}$$

pertanto esiste almeno un elemento $g \in G$ con la proprietà voluta.

□

**Osservazione 1.47** — Se $\varphi$ è l'azione di un gruppo $G$ su un insieme $X$, restringendo $\varphi$ all'orbita di un elemento $x \in X$ otteniamo per definizione un'azione transitiva su $\operatorname{Orb}(x)$. Pertanto gli stabilizzatori degli elementi di $\operatorname{Orb}(x)$ sono tra loro coniugati.

**Proposizione 1.48**

Dato $G$ un gruppo finito e $H \lneq G$ un sottogruppo proprio, se $[G : H] = p$ con $p$ il più piccolo primo che divide l'ordine di $G$ allora $H$ è normale in $G$.

*Dimostrazione.* Consideriamo l'azione di $G$ sull'insieme quoziente ${}^{G}\!/_{H}$

$$\psi : G \longrightarrow \mathcal{S}\left({}^{G}\!/_{H}\right) : g \longmapsto \psi_g$$

con

$$\psi_g : {}^{G}\!/_{H} \longrightarrow {}^{G}\!/_{H} : g'H \longmapsto gg'H$$

Poiché l'immagine di $\psi$ è un sottogruppo di $\mathcal{S}\left({}^{G}\!/_{H}\right)$, che è isomorfo a $S_p$, abbiamo che $|\mathrm{Im}\psi| \mid p!$, inoltre $|\mathrm{Im}\psi| = \dfrac{|G|}{|\ker \psi|}$ come conseguenza del Primo Teorema di Omomorfismo. Pertanto $|\mathrm{Im}\psi| \mid (p!, |G|) = p$, in quanto $p$ è il più piccolo primo che divide $|G|$, quindi

$|\mathrm{Im}\psi| \in \{1, p\}$. D'altra parte osserviamo che $\psi$ è un'azione transitiva, infatti per ogni $g_1, g_2 \in G$ abbiamo $\psi_{g_2 g_1^{-1}}(g_1 H) = g_2 g_1^{-1} g_1 H = g_2 H$, pertanto non è possibile $\mathrm{Im}\psi = \{id\}$, da cui $|\mathrm{Im}\psi| = p$ e $[G : \ker\psi] = p$. Consideriamo il nucleo di $\psi$

$$\ker\psi = \{g \in G \mid gg'H = g'H \ \forall g' \in G\}$$

nel caso particolare $g' = e$ otteniamo l'inclusione

$$\ker\psi \subseteq \{g \in G \mid gH = H\} = H$$

in quanto stiamo indebolendo la condizione di appartenenza all'insieme. Poiché $[G : \ker\psi] = [G : H] = p$ e $G$ è un gruppo finito abbiamo che effettivamente $\ker\psi = H$, cioè $H$ è normale in $G$. □

### §1.7.2 Teorema di Cauchy e Piccolo Teorema di Fermat

Vediamo una dimostrazione alternativa del Teorema di Cauchy e del Piccolo Teorema di Fermat, di cui ricordiamo gli enunciati, che fa uso del concetto di azione.

**Teorema 1.49** (Teorema di Cauchy)
Dato un gruppo $G$ e un numero primo $p$, se $p \mid |G|$ allora esiste $g \in G$ tale che $\mathrm{ord}(g) = p$.

**Teorema 1.50** (Piccolo Teorema di Fermat)
Dato un numero primo $p$, se $n \in \mathbb{Z}$ è coprimo con $p$ allora $n^{p-1} \equiv 1 \pmod p$.

Dati un gruppo $G$ e un numero primo $p$, consideriamo l'insieme

$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \ldots g_p = e\}$$

osserviamo che $|X| = |G|^{p-1}$, possiamo infatti scegliere liberamente i primi $p-1$ elementi di ogni $p$-upla, che ne determinano l'ultimo in modo univoco (per unicità dell'inverso). Definiamo un'azione di $\mathbb{Z}/p\mathbb{Z}$ su $X$ nel seguente modo:

$$\psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{S}(X) : a \longmapsto \psi_a$$

con

$$\psi_a : X \longrightarrow X : (g_1, \ldots, g_p) \longmapsto (g_{1+a}, \ldots, g_p, g_1, \ldots, g_a)$$

Fissato $x \in X$, poiché la cardinalità di $\mathrm{Orb}(x)$ divide l'ordine di $\mathbb{Z}/p\mathbb{Z}$ abbiamo che $|\mathrm{Orb}(x)| \in \{1, p\}$, in particolare le orbite di cardinalità 1 sono date dalle $p$-uple della forma $(g, \ldots, g)$ con $g^p = e$. Poniamo $S = \{g \in G \mid \mathrm{ord}(g) = p\}$ e $\mathcal{R}$ un insieme di rappresentanti per la relazione di equivalenza indotta da $\psi$, poiché le orbite degli elementi di $X$ formano una partizione dell'insieme abbiamo

$$|G|^{p-1} = |X| = \sum_{x \in \mathcal{R}} |\mathrm{Orb}(x)| = 1 + |S| + \sum_{x \in \mathcal{R} \setminus S} |\mathrm{Orb}(x)|$$

dove l'ultimo termine della somma è divisibile per $p$. Distinguiamo quindi due casi:

- se $p \mid |G|$, riducendo modulo $p$ la formula sopra otteniamo $|S| \equiv -1 \pmod p$, in particolare esiste almeno un elemento di ordine $p$ (Teorema di Cauchy);

- se $G = \mathbb{Z}/n\mathbb{Z}$ con $p$ e $n$ coprimi, $\mathbb{Z}/n\mathbb{Z}$ non contiene elementi di ordine $p$, pertanto riducendo modulo $p$ la formula sopra otteniamo $n^{p-1} \equiv 1 \pmod p$ (Piccolo Teorema di Fermat).

**Esercizio 1.51.** Mostrare che i gruppi di ordine 15 sono ciclici.

*Soluzione.* Sia $G$ un gruppo di ordine 15, poiché 5 è un primo che divide $|G|$ esiste $h \in G$ tale che $\mathrm{ord}(h) = 5$ per il Teorema di Cauchy. Inoltre, posto $H = \langle h \rangle$, abbiamo che $[G : H] = 3$ e quindi, dato che 3 è il più piccolo primo che divide $|G|$, $H$ è un sottogruppo normale di $G$. Mostriamo che $H \subseteq Z(G)$, questo è equivalente a richiedere che l'omomorfismo

$$\varphi : G \longrightarrow \mathrm{Aut}(H) : g \longmapsto \varphi_{g|H}$$

dove $\varphi_g$ è il coniugio per $g$, abbia come unico elemento dell'immagine l'applicazione

$$id_H : H \longrightarrow H : h \longmapsto h$$

Poiché $H \cong \mathbb{Z}/5\mathbb{Z}$, abbiamo $\mathrm{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$, d'altra parte $|\mathrm{Im}\varphi_{|H}|$ divide $(|G|, |\mathrm{Aut}(H)|) = 1$, pertanto $|\mathrm{Im}\varphi| = 1$ e l'omomorfismo è banale, cioè $H \subseteq Z(G)$. Diamo adesso due modi per concludere l'esercizio:

(1) osserviamo che se $G$ è un gruppo abeliano, cioè se $Z(G) = G$, allora abbiamo che $G$ è ciclico. Infatti posto $k \in G$ un elemento di ordine 3 (che esiste in virtù del Teorema di Cauchy), abbiamo che $\mathrm{ord}(hk) = \mathrm{ord}(h)\,\mathrm{ord}(k) = 15$ in quanto i due elementi hanno ordine coprimo. D'altra parte, se $G$ non fosse abeliano allora avremmo necessariamente $Z(G) = H$, quindi ${}^{G}\!/_{Z(G)}$ sarebbe ciclico in quanto di ordine 3, pertanto $G$ sarebbe un gruppo abeliano, da cui la tesi per quanto appena detto;

(2) sia $k \in G$ un elemento di ordine 3, consideriamo il centralizzatore di $k$

$$Z_G(k) = \{x \in G \mid xk = kx\}$$

Osserviamo che $k \in Z_G(k)$ e $Z(G) \subseteq Z_G(k)$, pertanto $h$ è un elemento di $Z_G(k)$. Abbiamo quindi che $\mathrm{ord}(h) \mid |Z_G(k)|$ e $\mathrm{ord}(k) \mid |Z_G(k)|$, da cui $|Z_G(k)| = 15$. Abbiamo che tutti gli elementi di ordine 3 sono contenuti nel centro di $G$, che quindi coincide con $G$. Allora $G$ è ciclico in quanto abeliano e contenente un elemento di ordine 3 e uno di ordine 5, quindi uno di ordine 15.

□

**Osservazione 1.52** — In generale dati $x, y \in G$, se $x$ e $y$ commutano e $(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$, allora $\mathrm{ord}(xy) = [\mathrm{ord}(x), \mathrm{ord}(y)]$ anche se $G$ non è un gruppo abeliano.

**Esercizio 1.53.** Dato $d$ un numero dispari, mostrare che ogni gruppo di ordine $2d$ ammette un sottogruppo normale di indice 2.

*Soluzione.* Consideriamo la rappresentazione regolare a sinistra di $G$

$$\lambda : G \longrightarrow \mathcal{S}(G) : g \longmapsto \lambda_g$$

con

$$\lambda_g : G \longrightarrow G : x \longmapsto gx$$

Fissato un isomorfismo $\psi : \mathcal{S}(G) \longrightarrow S_{2d}$ poniamo $\varphi = \psi \circ \lambda : G \longrightarrow S_{2d}$, $\varphi$ è un omomorfismo iniettivo (infatti nella dimostrazione del Teorema di Cayley abbiamo visto che $\lambda$ è un omomorfismo iniettivo). Consideriamo il sottogruppo $\varphi^{-1}(\mathcal{A}_{2d})$, mostriamo che il suo indice in $G$ è al più 2: posta $\pi_{\mathcal{A}_{2d}}$ la proiezione al quoziente

$$\pi_{\mathcal{A}_{2d}} : \mathcal{S}_{2d} \longrightarrow {S_{2d}}/{\mathcal{A}_{2d}} \cong \mathbb{Z}/2\mathbb{Z}$$

possiamo caratterizzare $\varphi^{-1}(\mathcal{A}_{2d})$ come

$$\varphi^{-1}(\mathcal{A}_{2d}) = \{g \in G \mid \varphi(g) \in \mathcal{A}_{2d}\} = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$$

pertanto $\varphi^{-1}(\mathcal{A}_{2d}) \trianglelefteq G$. Per il Primo Teorema di Omomorfismo abbiamo che esiste un omomorfismo iniettivo da ${G}/{\ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)}$ in $\mathbb{Z}/2\mathbb{Z}$, da cui $[G : \ker(\pi_{\mathcal{A}_{2d}})] \leq 2$. Tale sottogruppo ha indice 1 se e solo se $G = \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)$, cioè $\varphi(G) \subseteq \mathcal{A}_{2d}$, mostriamo che in effetti esiste un elemento di $G$ la cui immagine tramite $\varphi$ è una permutazione dispari. Consideriamo $g \in G$ un elemento di ordine 2, poiché $\varphi$ è un omomorfismo iniettivo abbiamo che $\mathrm{ord}(\varphi(g)) = \mathrm{ord}(g) = 2$, pertanto la permutazione $\varphi(g)$ ha una decomposizione in $d$ 2-cicli, cioè è dispari. Pertanto $G \neq \varphi^{-1}(\mathcal{A}_{2d})$, da cui $[G : \varphi^{-1}(\mathcal{A}_{2d})] = 2$, □

Possiamo generalizzare il ragionamento appena usato nel seguente risultato

**Proposizione 1.54**
Dato un gruppo $G$ e $H \lneq G$ un sottogruppo tale che $[G : H] = 2$, se $K$ è un sottogruppo di $G$ allora $H \cap K$ ha indice 1 o 2 in $K$, cioè $[K : H \cap K] \in \{1, 2\}$.

*Dimostrazione.* Distinguiamo due casi:

- se $K \subseteq H$ allora $H \cap K = K$, da cui $[K : H \cap K] = 1$;
- se $K \nsubseteq H$ consideriamo la proiezione

  $$\pi_H : G \longrightarrow {G}/{H} : g \longmapsto gH$$

  Poiché ${G}/{H} \cong \mathbb{Z}/2\mathbb{Z}$ abbiamo che gli unici sottogruppi del quoziente sono $\{H\}$ e ${G}/{H}$, pertanto $\pi_H(K) = {G}/{H}$. Osserviamo che $\ker \pi_{H|K} = \ker \pi_H \cap K$, per il Primo Teorema di Omomorfismo allora ${K}/{H \cap K} \cong \mathbb{Z}/2\mathbb{Z}$, cioè $[K : H \cap K] = 2$.

□

### §1.7.3 Teorema di Poincaré

Vediamo un risultato che sarà utile nel futuro, che permette di esibire, se esistono, sottogruppi normali non banali di un gruppo finito.

**Teorema 1.55** (Teorema di Poincaré)
Dato un gruppo $G$ finito e $H \leqslant G$ un suo sottogruppo, se $[G : H] = n$ allora esiste un sottogruppo normale $N \triangleleft G$ tale che:

(1) $N \leqslant H \leqslant G$;

(2) $n \mid [G : N] \mid n!$.

*Dimostrazione.* Consideriamo l'azione di $G$ su ${G}/{H}$

$$\psi : G \longrightarrow \mathcal{S}\left({G}/{H}\right) : g \longmapsto \psi_g$$

con

$$\psi_g : {G}/{H} \longrightarrow {G}/{H} : g'H \longmapsto gg'H$$

(1) Consideriamo il nucleo di $\psi$

$$\ker \psi = \{g \in G \mid gg'H = g'H \ \forall g' \in G\}$$

nel caso particolare $g' = e$ otteniamo l'inclusione

$$\ker \psi \subseteq \{g \in G \mid gH = H\} = H$$

in quanto stiamo indebolendo la condizione di appartenenza all'insieme, pertanto $\ker \psi \leqslant H$;

(2) poiché $\ker \psi \leqslant H$ abbiamo $[G : H] \mid [G : \ker \psi]$, cioè $n \mid [G : \ker \psi]$. Dal Primo Teorema di Omomorfismo abbiamo che ${G}/{\ker \psi} \cong \mathrm{Im}\psi$, che è un sottogruppo di $\mathcal{S}\left({G}/{H}\right) \cong \mathcal{S}_n$, pertanto $[G : \ker \psi] \mid n!$.

Poiché $\ker \psi$ è normale in $G$ abbiamo che $N = \ker \psi$ è un sottogruppo con le proprietà cercate. □

**Osservazione 1.56 —** In particolare, se $G$ ha un sottogruppo di indice $n$ e $n! < |G|$ allora $G$ ammette sottogruppi normali non banali.

## §1.8 Gruppo simmetrico

### §1.8.1 Generatori di $\mathcal{S}_n$

Esibiamo alcuni insiemi di generatori per $\mathcal{S}_n$:

- $\{(i\ j) \mid i, j \in \{1, \ldots, n\}, i < j\}$, abbiamo visto che ogni permutazione può essere scritta come prodotto di trasposizioni;
- $\{(1\ j) \mid j \in \{2, \ldots, n\}\}$, infatti per ogni $i < j$ abbiamo
$$(i\ j) = (1\ i)(1\ j)(1\ i)$$
- $\{(i\ i+1) \mid i \in \{1, \ldots, n-1\}\}$, infatti per ogni $j$ abbiamo
$$(1\ j) = (j-1\ j)(1\ j-1)(j-1\ j)$$
- $\{(1\ 2), (1\ 2\ \ldots\ n)\}$, infatti per ogni $i$ abbiamo
$$(i\ i+1) = (1\ \ldots\ n)^{i-1}(1\ 2)(1\ \ldots\ n)^{1-i}$$

**Osservazione 1.57** — Non è vero in generale che una trasposizione e un $n$-ciclo generano $\mathcal{S}_n$, consideriamo ad esempio $\langle \sigma, \rho \rangle \leqslant \mathcal{S}_4$ con $\sigma = (1\ 2\ 3\ 4)$, $\rho = (2\ 4)$. Abbiamo $\sigma^4 = \rho^2 = 1$ e $\rho\sigma\rho^{-1} = (1\ 4\ 3\ 2) = \sigma^{-1}$, pertanto $\langle \sigma, \rho \rangle$ è isomorfo a un quoziente di $D_4$. D'altra parte $\langle \sigma \rangle \cap \langle \rho \rangle = \{id\}$ e $\rho \in N_{\mathcal{S}_4}(\sigma)$, pertanto $\langle \sigma, \rho \rangle = \langle \sigma \rangle \langle \rho \rangle$ e $|\langle \sigma, \rho \rangle| = 8$, pertanto è isomorfo a $D_4$.

### §1.8.2 Sottogruppi abeliani massimali di $\mathcal{S}_n$

Vogliamo studiare i sottogruppi abeliani di $\mathcal{S}_n$, caratterizzando in particolare i suoi sottogruppi abeliani massimali.

**Definizione 1.58.** Un sottogruppo $G \leqslant \mathcal{S}_n$ si dice **transitivo** se l'azione
$$\varphi : G \longrightarrow \mathcal{S}_n : \sigma \longmapsto \sigma$$
indotta da $G$ su $\{1, \ldots, n\}$ è transitiva, cioè se per ogni $i, j \in \{1, \ldots, n\}$ esiste $\sigma \in G$ tale che $\sigma(i) = j$.

**Lemma 1.59**
Dato $G$ un sottogruppo abeliano di $\mathcal{S}_n$, se $G$ è transitivo allora $|G| = n$.

*Dimostrazione.* Consideriamo l'azione di $G$ su $\{1, \ldots, n\}$
$$\psi : G \longrightarrow \mathcal{S}_n : \sigma \longmapsto \sigma$$
poiché $G$ è transitivo, per la Proposizione 1.41 gli stabilizzatori degli elementi di $\{1, \ldots, n\}$ sono tra loro coniugati. D'altra parte, poiché lo stabilizzatore è un sottogruppo di $G$, che è un gruppo abeliano, la restrizione del coniugio agli stabilizzatori coincide con

l'applicazione identità, da cui $\mathrm{St}(i) = \mathrm{St}(j)$ per ogni $i, j \in \{1, \ldots, n\}$. Osserviamo infine che

$$\bigcap_{i=1}^{n} \mathrm{St}(i) = \{id_{\mathcal{S}_n}\}$$

in quanto $id_{\mathcal{S}_n}$ è l'unica permutazione che fissa tutti gli elementi di $\{1, \ldots, n\}$, pertanto $\mathrm{St}(i) = \{id_{\mathcal{S}_n}\}$ per ogni $i \in \{1, \ldots, n\}$. Fissato $i \in \{1, \ldots, n\}$, abbiamo

$$|G| = |\operatorname{Orb}(i)| \cdot |\operatorname{St}(i)| = |\operatorname{Orb}(i)| = n$$

in quanto $G$ è transitivo. □

**Lemma 1.60**

Se $a_1, \ldots, a_k$ sono interi positivi tali che $\sum_{i=1}^{k} a_i = 3m$, con $m \geqslant k$ intero, allora $\prod_{i=1}^{k} a_i \leq 3^m$, e vale l'uguaglianza se e solo se $k = m$ e $a_i = 3$ per ogni $i \in \{1, \ldots, k\}$.

*Dimostrazione.* Senza perdita di generalità, a meno di aumentare $k$ possiamo supporre $a_i \in \{1, 2, 3\}$ per ogni $i \in \{1, \ldots, k\}$, infatti se uno degli $a_i$ è uguale a 4 possiamo sostituirlo con $2 + 2$, se uno degli $a_i$ è uguale a 5 possiamo sostituirlo con $2 + (a_i - 2)$ e così via (queste sostituzioni mantengono inalterato il valore della somma). In particolare abbiamo che $a_i \leqslant 3$ per ogni $i \in \{1, \ldots, n\}$, pertanto

$$\prod_{i=1}^{k} a_i \leq 3^k \leq 3^m$$

inoltre se $k = m$ e tutti gli $a_i$ sono uguali a 3 abbiamo chiaramente

$$\prod_{i=1}^{k} a_i = 3^k = 3^m$$

Viceversa, se il prodotto degli $a_i$ è uguale a $3^m$ allora necessariamente $k = m$ e $a_i = 3$ per ogni $i \in \{1, \ldots, k\}$ in quanto possiamo supporre $a_i \in \{1, 2, 3\}$ senza perdita di generalità. □

**Lemma 1.61**

Dati $\sigma, \tau \in \mathcal{S}_n$, se $\sigma = (x_1 \ \ldots \ x_k)$ è un $k$-ciclo allora

$$\tau\sigma\tau^{-1} = (\tau(x_1) \ \ldots \ \tau(x_k))$$

*Dimostrazione.*

$$(\tau\sigma\tau^{-1})(\tau(x_i)) = (\tau\sigma)(x_i) = \tau(x_{i+1})$$

per ogni $i \in \{1, \ldots, k\}$, pertanto

$$\tau\sigma\tau^{-1} = (\tau(x_1) \ \ldots \ \tau(x_k))$$

□

**Esercizio 1.62.** Posto $n = 3m$, mostrare che la massima cardinalità di un sottogruppo abeliano di $\mathcal{S}_n$ è $3^m$ e caratterizzare la sua classe di isomorfismo.

*Soluzione.* Per prima cosa, osserviamo che $\mathcal{S}_n$ contiene sottogruppi abeliani di cardinalità $3m$, ad esempio

$$\langle (1\ 2\ 3)\rangle \cdot \langle (4\ 5\ 6)\rangle \cdot \ldots \cdot \langle (n-2\ n-1\ n)\rangle$$

è un sottogruppo abeliano di $\mathcal{S}_n$ di cardinalità $3^m$, essendo isomorfo a

$$\langle (1\ 2\ 3)\rangle \times \langle (4\ 5\ 6)\rangle \times \ldots \times \langle (n-2\ n-1\ n)\rangle$$

Sia $G$ un sottogruppo abeliano di $\mathcal{S}_n$ di ordine massimo, data

$$\psi : G \longrightarrow \mathcal{S}_n : \sigma \longmapsto \sigma$$

l'azione naturale di $G$ su $\{1, \ldots, n\}$ chiamiamo $\Omega_1, \ldots, \Omega_k$ le orbite. Consideriamo le mappe $\varphi_i : G \longrightarrow \mathcal{S}(\Omega_i)$ tali che, data $\sigma \in G$ e fissata $\rho_1 \ldots \rho_k$ una sua decomposizione in cicli disgiunti, $\varphi_i(\sigma) = \rho_i$, poniamo $G_i = \mathrm{Im}\varphi_i = \mathrm{Im}\psi \cap \mathcal{S}(\Omega_i)$. Possiamo quindi costruire l'omomorfismo

$$\varphi : G \longrightarrow G_1 \times \ldots \times G_k : g \longmapsto (\varphi_1(g), \ldots, \varphi_k(g))$$

che è iniettivo in quanto

$$\varphi(\sigma) = id \iff \varphi_i(\sigma) = id_{\mathcal{S}(\Omega_i)} \iff \sigma_{|\Omega_i} = id_{\mathcal{S}(\Omega_i)}$$

per ogni $i \in \{1, \ldots, k\}$, che è equivalente a $\sigma = id_{\mathcal{S}_n}$ dato che le orbite ricoprono $\{1, \ldots, n\}$, da cui $\ker \varphi = \{id_{\mathcal{S}_n}\}$. Osserviamo adesso che ogni $G_i$ è un gruppo abeliano poiché immagine omomorfa di $G$, che è un gruppo abeliano, inoltre è transitivo sull'orbita $\Omega_i$ per costruzione, pertanto per il Lemma 1.54 abbiamo $|G_i| = |\Omega_i|$ per ogni $i \in \{1, \ldots, k\}$. Vale quindi la seguente disuguaglianza, data dall'iniettività di $\varphi$

$$|G| \leqslant \prod_{i=1}^{k} |G_i| = \prod_{i=1}^{k} |\Omega_i|$$

D'altra parte

$$3m = \sum_{i=1}^{k} |\Omega_i|$$

pertanto per il Lemma 1.55 abbiamo $|G| \leq 3^m$, ma questa è effettivamente un'uguaglianza in quanto $\mathcal{S}_n$ contiene almeno un sottogruppo abeliano di ordine $3^m$ e $G$ ha ordine massimo. Sempre per il Lemma 1.55 allora $k = m$ e $|\Omega_i| = 3$ per ogni $i \in \{1, \ldots, k\}$. Abbiamo quindi che $\varphi$ è un isomorfismo e che $G_1 \times \ldots \times G_k$ è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^k$, pertanto $G$ è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^k$. □

**Osservazione 1.63 —** Se $a_1, \ldots, a_k$ sono interi tali che

$$3m + 2 = \sum_{i=1}^{k} a_i$$

ragionando come nella dimostrazione del Lemma 1.55 possiamo scrivere

$$3m + 2 = 2 + \sum_{i=1}^{k-1} a_i$$

da cui ricaviamo

$$\prod_{i=1}^{k} a_i \leqslant 2 \cdot 3^m$$

Inoltre questa è un'uguaglianza se e solo se esiste $j \in \{1, \ldots, k\}$ tale che $a_j = 2$, $a_i = 3$ per ogni $i \in \{1, \ldots, k\} \setminus \{j\}$ e $k = m$. Ragionando come sopra otteniamo $|G| \leqslant 2 \cdot 3^m$, d'altra parte osserviamo che $\mathcal{S}_n$ contiene un sottogruppo abeliano

$$\langle (1\ 2\ 3) \rangle \cdot \ldots \cdot \langle (3m-2\ 3m-1\ 3m) \rangle \cdot \langle (3m+1\ 3m+2) \rangle$$

di ordine $2 \cdot 3^m$ poiché isomorfo a

$$\langle (1\ 2\ 3) \rangle \times \ldots \times \langle (3m-2\ 3m-1\ 3m) \rangle \times \langle (3m+1\ 3m+2) \rangle$$

pertanto $|G| = 2 \cdot 3^m$ e $G \cong (\mathbb{Z}/3\mathbb{Z})^m \times \mathbb{Z}/2\mathbb{Z}$. Se $n = 3m+1$, ragionando in modo simile abbiamo che la somma delle cardinalità delle orbite $\Omega_1, \ldots, \Omega_k$ è $3m+1$ e il loro prodotto è minore o uguale a $4 \times 3^{m-1}$, da cui $|G| \leq 4 \cdot 3^{m-1}$. D'altra parte $\mathcal{S}_n$ contiene almeno due tipi di sottogruppi abeliani di ordine $3m+1$, uno isomorfo a $(\mathbb{Z}/3\mathbb{Z})^{m-1} \times \mathbb{Z}/4\mathbb{Z}$ e uno isomorfo a $(\mathbb{Z}/3\mathbb{Z})^{m-1} \times V_4$, dove

$$V_4 = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), id\}$$

è un sottogruppo abeliano non ciclico di $\mathcal{S}_4$, chiamato **gruppo di Klein** o **Klein 4-group**. Pertanto un sottogruppo abeliano di ordine massimo deve avere una di queste due forme.

**Osservazione 1.64** — I sottogruppi di $\mathcal{S}_n$ di questo tipo sono tutti coniugati tra loro, infatti se

$$G = \langle (x_1\ x_2\ x_3) \rangle \cdot \ldots \cdot \langle (x_{n-2}\ x_{n-1}\ x_n) \rangle$$
$$G' = \langle (y_1\ y_2\ y_3) \rangle \cdot \ldots \cdot \langle (y_{n-2}\ y_{n-1}\ y_n) \rangle$$

sono due sottogruppi abeliani di $\mathcal{S}_n$ di ordine massimo (per semplicità supponiamo $n = 3m$, gli altri due casi si studiano in modo analogo) consideriamo $\sigma \in \mathcal{S}_n$ tale che $\sigma(y_i) = x_i$ per ogni $i \in \{1, \ldots, n\}$, è sufficiente mostrare che i generatori delle componenti del prodotto sono tra loro coniugate. Infatti, per il Lemma 1.56 abbiamo

$$\sigma (x_i\ x_{i+1}\ x_{i+2}) \sigma^{-1} = (\sigma(x_i)\ \sigma(x_{i+1})\ \sigma(x_{i+2})) = (y_i\ y_{i+1}\ y_{i+2})$$

per ogni $i \in \{1, \ldots, n-2\}$, pertanto $G$ e $G'$ sono coniugati.

### §1.8.3 Classi di coniugio in $\mathcal{A}_n$

Studiamo le classi di coniugio in $\mathcal{A}_n$. In particolare, fissato $\sigma \in \mathcal{A}_n$, vogliamo determinare una relazione tra $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$ e $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$. Poiché valgono $|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n}(\sigma)|$ e $Z_{\mathcal{A}_n}(\sigma) = Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n$, abbiamo

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2} \frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n|}$$

Dato che $[\mathcal{S}_n : \mathcal{A}_n] = 2$, per la Proposizione 1.49 abbiamo $[Z_{\mathcal{S}_n}(\sigma) : Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n] \in \{1, 2\}$, distinguiamo quindi due casi:

- $|Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n| = \frac{1}{2}|Z_{\mathcal{S}_n}(\sigma)|$;
- $|Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n| = |Z_{\mathcal{S}_n}(\sigma)|$.

Nel primo caso otteniamo

$$|\mathcal{C}\ell_{\mathcal{A}_n}| = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n|} = \frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = |\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)|$$

poiché $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$ abbiamo che le due classi coincidono. In particolare questo succede se $Z_{\mathcal{S}_n}(\sigma) \nsubseteq \mathcal{A}_n$.

Nel secondo caso invece, che si verifica se $Z_{\mathcal{S}_n}(\sigma) \subseteq \mathcal{A}_n$,

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma) \cap \mathcal{A}_n|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)|$$

Più precisamente, abbiamo $\mathcal{C}\ell_{\mathcal{S}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$ per ogni $\tau$ permutazione dispari. Infatti $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1}) \subseteq \mathcal{C}\ell_{\mathcal{S}_n}(\sigma)$ (i coniugati di $\tau\sigma\tau^{-1}$ sono anche coniugati di $\sigma$), d'altra parte per ogni $\rho \in \mathcal{S}_n$ abbiamo $\rho\sigma\rho^{-1} \in \mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$ se $\rho$ è pari, $\rho\sigma\rho^{-1} = (\rho\tau^{-1})(\tau\sigma\tau^{-1})(\rho\tau^{-1})^{-1} \in \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$ se $\rho$ è dispari, da cui l'uguaglianza. Abbiamo altri due casi:

- $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})|$;
- $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})|$.

Tuttavia se fosse $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})|$ avremmo $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$, che è assurdo in quanto $\tau\sigma\tau^{-1} \notin \mathcal{C}\ell_{\mathcal{A}_n}(\sigma)$, pertanto

$$|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\tau\sigma\tau^{-1})| = \frac{1}{2}|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)|$$

Poiché $|\mathcal{C}\ell_{\mathcal{S}_n}(\sigma)| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| + |\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})|$, per il Principio di Inclusione-Esclusione abbiamo che l'unione è disgiunta, cioè

$$\mathcal{C}\ell_{\mathcal{S}_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \sqcup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$$

### §1.8.4 Studio di $\mathcal{S}_5$

Consideriamo gli elementi di $\mathcal{S}_5$ $\sigma = (1\ 2\ 3\ 4\ 5), \tau = (2\ 5)(3\ 4)$, studiamo il sottogruppo $H = \langle \sigma, \tau \rangle$, in particolare siamo interessati a determinare una regola di commutazione per $\sigma$ e $\tau$. Osserviamo che

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5)) = (1\ 5\ 4\ 3\ 2)$$

e che questo coincide con $\sigma^{-1}$. Abbiamo quindi che $H$ è generato da un elemento $\tau$ di ordine 2 e da un elemento $\sigma$ di ordine 5 che soddisfano la relazione $\tau\sigma\tau^{-1} = \sigma^{-1}$, pertanto $H$ è isomorfo a un sottogruppo del gruppo diedrale $D_5$. D'altra parte, da questa relazione ricaviamo che $\langle \tau \rangle \subseteq N_{\mathcal{S}_5}(\langle \sigma \rangle)$, pertanto possiamo scrivere $H = \langle \sigma \rangle \cdot \langle \tau \rangle$ in quanto $\langle \sigma \rangle \cdot \langle \tau \rangle$ è un sottogruppo di $H$ che ha la sua stessa cardinalità. In particolare otteniamo che $|H| = 10 = |D_5|$, quindi $H \cong D_5$.

Abbiamo visto che le classi di coniugio in un gruppo simmetrico su $n$ elementi sono parametrizzate dalle partizioni di $n$

| Partizioni di 5 | Cardinalità della classe di coniugio associata |
|---|---|
| 5 | $\binom{5}{5}4! = 4! = 24$ |
| 4 + 1 | $\binom{5}{4}3! = 30$ |
| 3 + 2 | $\binom{5}{3}2!\binom{2}{2}1! = 20$ |
| 3 + 1 + 1 | $\binom{5}{3}2! = 20$ |
| 2 + 2 + 1 | $\frac{1}{2}\binom{5}{2}1!\binom{3}{2}1! = 15$ |
| 2 + 1 + 1 + 1 | $\binom{5}{2}1! = 10$ |
| 1 + 1 + 1 + 1 + 1 | 1 |

(Nel calcolo della cardinalità della classe associata alla partizione 2 + 2 + 1 dividiamo per 2 in quanto contiamo i cicli a meno dell'ordine, e le coppie di trasposizioni che stiamo considerando commutano). Di queste, le permutazioni che appartengono a $\mathcal{A}_5$ sono quelle la cui classe di coniugio è associata alle partizioni 5, 3 + 1 + 1, 2 + 2 + 1, 1 + 1 + 1 + 1 + 1, cioè le permutazioni $\sigma, \tau, \rho$ aventi una decomposizione in cicli disgiunti della forma

$$\sigma = (a_1\ a_2\ a_3\ a_4\ a_5)$$

$$\tau = (b_1\ b_2\ b_3)$$

$$\rho = (c_1\ c_2)(d_1\ d_2)$$

e l'identità. Vediamo come sono fatte le loro classi di coniugio in $\mathcal{A}_5$. Chiaramente $\mathcal{C}\ell_{\mathcal{A}_n}(id) = \mathcal{C}\ell_{\mathcal{S}_n}(id) = \{id\}$, studiamo quindi le classi di $\sigma, \tau, \rho$ fissate come sopra.

- $Z_{\mathcal{S}_5}(\sigma) = \langle (a_1\ a_2\ a_3\ a_4\ a_5) \rangle$, infatti

  $$|Z_{\mathcal{S}_5}(\sigma)| = \frac{|\mathcal{S}_5|}{|\mathcal{C}\ell_{\mathcal{S}_5}(\sigma)|} = \frac{5!}{4!} = 5$$

  Allora $Z_{\mathcal{S}_5}(\sigma)$ contiene solo permutazioni pari, fissata $\psi$ una permutazione dispari la sua classe di coniugio in $\mathcal{S}_5$ si scrive come

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma) \sqcup \mathcal{C}\ell_{\mathcal{A}_5}(\psi\sigma\psi^{-1})$$

- $Z_{\mathcal{S}_5}(\tau)$ non è contenuto in $\mathcal{A}_5$, infatti una trasposizione $\psi$ disgiunta da $\tau$ è una permutazione dispari che appartiene al centralizzatore. Pertanto

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\tau) = \mathcal{C}\ell_{\mathcal{A}_5}(\tau)$$

- $Z_{\mathcal{S}_5}(\rho)$ non è contenuto in $\mathcal{A}_5$, infatti la trasposizione $(c_1\ c_2)$ è una permutazione dispari che commuta con $\rho$ (infatti $(c_1\ c_2)$ e $(d_1\ d_2)$ commutano in quanto cicli disgiunti e $(c_1\ c_2)$ commuta con se stessa). Pertanto

  $$\mathcal{C}\ell_{\mathcal{S}_5}(\rho) = \mathcal{C}\ell_{\mathcal{A}_5}(\rho)$$

### §1.8.5 Sottogruppi normali di $\mathcal{A}_n$

Esibiamo alcuni insiemi di generatori per $\mathcal{A}_n$:

- $\{(i\ j)(k\ l) \mid i \neq j, k \neq l\}$, infatti ogni elemento di $\mathcal{A}_n$ può essere scritto come prodotto di coppie di trasposizioni in quanto permutazione pari;
- $\{(i\ j\ k) \mid i, j, k \text{ distinti}\}$. Infatti se $\{i, j\} = \{k, l\}$ allora $(i\ j)(k\ l) = id$ è un elemento generato dall'insieme, se invece $|\{i, j\} \cap \{k, l\}| = 1$, ad esempio $j = k$, abbiamo $(i\ j)(k\ l) = (i\ j)(j\ l) = (i\ j\ l)$, che è un elemento generato dall'insieme. Nel caso $\{i, j\} \cap \{k, l\} = \emptyset$ abbiamo $(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l)$, che è un elemento generato dall'insieme. Possiamo quindi ottenere il precedente insieme di generatori a partire da questo;

**Definizione 1.65.** Un gruppo non banale $G$ si dice **semplice** se i suoi unici sottogruppi normali sono $\{e\}$ e $G$.

**Proposizione 1.66**

$\mathcal{A}_5$ è un gruppo semplice.

*Dimostrazione.* Ricordiamo le cardinalità delle classi di coniugio in $\mathcal{A}_5$:

| Rappresentante della classe | Cardinalità della classe |
|---|---|
| $(1\ 2\ 3\ 4\ 5)$ | 12 |
| $(2\ 1\ 3\ 4\ 5)$ | 12 |
| $(1\ 2)(3\ 4)$ | 15 |
| $(1\ 2\ 3)$ | 20 |
| $id$ | 1 |

In generale, un sottogruppo è normale se e solo se è unione disgiunta delle classi di coniugio dei suoi elementi, quindi la cardinalità di $N \trianglelefteq \mathcal{A}_5$ deve essere somma di alcuni termini nella seconda colonna, compreso 1. D'altra parte $|N| \mid |\mathcal{A}_5| = 60$, da cui $|N| = 1$ oppure $|N| = 60$. Pertanto $\mathcal{A}_5$ è semplice. □

**Lemma 1.67**

Dati un gruppo $G$ e $N \trianglelefteq G$ un sottogruppo normale di indice finito, $N$ contiene ogni elemento di $G$ il cui ordine è coprimo con $[G : N]$.

*Dimostrazione.* Sia $g \in G$ tale che $(\operatorname{ord}(g), [G : N]) = 1$, consideriamo la proiezione

$$\pi_N : G \longrightarrow {}^{G}\!/_{N} (x \longmapsto xN)$$

Poiché $\pi_N$ è un omomorfismo abbiamo $\operatorname{ord}(\pi_N(g)) \mid (\operatorname{ord}(g), [G : N]) = 1$, pertanto $\pi_N(g) = N$, cioè $g \in N$. □

Diamo adesso una dimostrazione alternativa della semplicità di $\mathcal{A}_5$.

*Dimostrazione.* Consideriamo un sottogruppo normale $N \trianglelefteq \mathcal{A}_5$. Distinguiamo tre casi:

- se $2 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.62 $N$ contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 2, cioè le permutazioni della forma $(a\ b)(c\ d)$ con $a \neq b$ e $c \neq d$, da cui $N = \mathcal{A}_5$ in quanto contiene un suo insieme di generatori;
- se $3 \nmid [\mathcal{A}_5 : N]$, per il Lemma 1.62 $N$ contiene tutti gli elementi di $\mathcal{A}_5$ di ordine 3, cioè i 3-cicli, da cui $N = \mathcal{A}_5$ in quanto contiene un suo insieme di generatori;
- se $6 \mid [\mathcal{A}_5 : N]$ allora $|N| \mid 10$, ma l'unica classe di coniugio di $\mathcal{A}_5$ di cardinalità minore di 10 è $\{id\}$, pertanto $N = \{id\}$.

Quindi $\mathcal{A}_5$ è semplice. □

In effetti vale un risultato più generale

**Proposizione 1.68**

$\mathcal{A}_n$ è un gruppo semplice per $n \geq 5$.

*Dimostrazione.* Procediamo per induzione su $n$, per $n = 5$ la tesi è garantita dalla Proposizione 1.61, supponiamo quindi che $\mathcal{A}_n$ sia un gruppo semplice e mostriamo che anche $\mathcal{A}_{n+1}$ lo è. Consideriamo un sottogruppo normale $N \trianglelefteq \mathcal{A}_{n+1}$ e i sottogruppi

$$H_i = \{\sigma \in \mathcal{A}_{n+1} \mid \sigma(i) = i\},\ i \in \{1, \dots, n+1\}$$

questi sono tutti isomorfi a $\mathcal{A}_n$ (infatti gli elementi di $H_i$ sono tutte e sole le permutazioni pari su $n+1$ elementi che fissano l'$i$-esimo, cioè sono permutazioni pari su $n$ elementi). Notiamo che l'azione naturale di $\mathcal{A}_{n+1}$ su $\{1, \dots, n+1\}$

$$\psi : \mathcal{A}_{n+1} \longrightarrow S_{n+1} : \sigma \longmapsto \sigma$$

è transitiva, infatti per $i, j \in \{1, \dots, n+1\}$ distinti la permutazione pari $\rho = (i\ j)(h\ k)$, con $(i\ j)$ disgiunta da $(h\ k)$, è tale che $\rho(i) = j$. Per costruzione vale $\mathrm{St}(i) = H_i$ per ogni $i \in \{1, \dots, n+1\}$, pertanto per la Proposizione 1.41 abbiamo che gli $H_i$ sono tutti coniugati.
Fissato $i \in \{1, \dots, n+1\}$, consideriamo $N \cap H_i$: questo è un sottogruppo normale di $H_i$, infatti per ogni $h \in H_i$ si ha $h(N \cap H_i)h^{-1} = N \cap H_i$ in quanto $N$ è normale in $\mathcal{A}_{n+1}$ e $h \in H_i$, d'altra parte $H_i \cong \mathcal{A}_n$ è un gruppo semplice per ipotesi induttiva, pertanto $N \cap H_i$ coincide con $\{id\}$ oppure con $H_i$.
Se $N \cap H_i = H_i$ allora $H_i \subseteq N$, pertanto $N$ contiene almeno un 3-ciclo $(i\ j\ k)$ e tutti i suoi coniugati in $\mathcal{A}_{n+1}$. Notiamo che una trasposizione $(a\ b)$ disgiunta da $(i\ j\ k)$ (che esiste in quanto $n \geq 5$) è una permutazione dispari in $Z_{S_{n+1}}((i\ j\ k))$, pertanto $\mathcal{C}\ell_{\mathcal{A}_{n+1}}((i\ j\ k)) = \mathcal{C}\ell_{S_{n+1}}((i\ j\ k))$ e $N$ contiene l'insieme dei 3-cicli di $S_{n+1}$, quindi $N = \mathcal{A}_{n+1}$ dal momento che contiene un suo insieme di generatori.
Altrimenti $N \cap H_i = \{id\}$ per ogni $i \in \{1, \dots, n+1\}$, cioè l'unico elemento di $N$ avente almeno un punto fisso è l'identità, vogliamo mostrare che in effetti $N = \{id\}$. Osserviamo che se $\sigma \in N$ ha una decomposizione in cicli disgiunti della forma

$$\sigma = (x_1^{(1)}\ \dots\ x_{l_1}^{(1)}) \dots (x_1^{(k)}\ \dots\ x_{l_k}^{(k)})$$

con $l_1 \leqslant l_2 \leqslant \dots \leqslant l_k$, allora i suoi cicli hanno tutti la stessa lunghezza, cioè $l_i = l_j$ per ogni $i, j \in \{1, \dots, n+1\}$. Infatti, posto $r = \min\{l_i \mid 1 \leqslant i \leqslant k\} = l_1$, abbiamo

$$\sigma^{l_1} = id \cdot (x_1^{(2)}\ \dots\ x_{l_2}^{(2)})^{l_1} \dots (x_1^{(k)}\ \dots\ x_{l_k}^{(k)})^{l_1}$$

Poiché $\sigma^{l_1}$ ha almeno un punto fisso, esiste $i \in \{1, \dots, n+1\}$ tale che $\sigma^{l_1} \in N \cap H_i = \{id\}$, cioè $\sigma^{l_1} = id$. Pertanto $l_1 = l_2 = \dots = l_k$. Fissata $\sigma \in N$ possiamo quindi scrivere $\sigma = \sigma_1 \dots \sigma_k$, dove $\sigma_i$ sono $l$-cicli disgiunti con $l = \dfrac{n+1}{k}$. Supponiamo per assurdo $N \neq \{id\}$, distinguiamo tre casi:

- se $k = 1$ abbiamo $l = n+1$, cioè $\sigma$ è un $n+1$-ciclo. Scriviamo $\sigma = (a_1 \ \dots \ a_l)$ e consideriamo la permutazione pari $\tau = (a_1 \ a_2)(a_3 \ a_4)$, poiché $N$ è normale in $\mathcal{A}_{n+1}$ contiene
$$\tau\sigma\tau^{-1} = (a_2 \ a_1 \ a_4 \ a_3 \ a_5 \ a_6 \ \dots \ a_l)$$
Consideriamo $\rho = (\tau\sigma\tau^{-1})\sigma \in N$, notiamo che $\rho \neq id$ in quanto
$$\rho(a_4) = (\tau\sigma\tau^{-1})(\sigma(a_4)) = (\tau\sigma\tau^{-1})(a_5) = a_6 \neq a_4$$
d'altra parte $a_1$ è un punto fisso per $\rho$, che è assurdo;

- se $k > 1$ e $l > 2$, poiché $\sigma_1^{-1}$ è un $l$-ciclo disgiunto da $\sigma_2, \dots, \sigma_k$ la permutazione $\rho = \sigma_1^{-1}\sigma_2 \dots \sigma_k$ è un elemento di $N$. Consideriamo $\alpha = \rho\sigma \in N$, osserviamo che
$$\alpha = \sigma_2^2 \dots \sigma_k^2 \neq id$$
in quanto $\operatorname{ord}(\sigma_i) = l > 2$ per ogni $i \in \{1, \dots, k\}$, tuttavia $a_1$ è un punto fisso per $\alpha$, che è assurdo;

- se $k > 1$ e $l = 2$, scriviamo $\sigma$ come prodotto di $k$ trasposizioni disgiunte
$$\sigma = (a_1 \ b_1) \dots (a_k \ b_k)$$
Consideriamo la permutazione pari $\tau = (a_1 \ a_2 \ b_1)$, poiché $N$ è normale in $\mathcal{A}_{n+1}$ contiene
$$\rho = \tau\sigma\tau^{-1} = (a_2 \ a_1)(b_1 \ b_2)(a_3 \ b_3) \dots (a_k \ b_k)$$
e anche la permutazione
$$\alpha = \rho\sigma = ((a_2 \ a_1)(b_1 \ b_2))((a_1 \ b_1)(a_2 \ b_2)) = (a_1 \ b_2)(a_2 \ b_1) \neq id$$
ma $a_3$ è un punto fisso per $\alpha$, che è assurdo.

Pertanto $N = \{id\}$, cioè $\mathcal{A}_{n+1}$ è un gruppo semplice. □

**Corollario 1.69**
L'insieme $X = \{\sigma \in \mathcal{S}_n \mid \sigma \text{ è un 5-ciclo}\}$ genera $\mathcal{A}_n$ per $n \geqslant 5$.

*Dimostrazione.* Sia $\sigma \in X$ un 5-ciclo, per ogni $\tau \in \mathcal{A}_n$ abbiamo che $\tau\sigma\tau^{-1}$ è ancora un elemento di $X$, pertanto $\langle X \rangle$ è un sottogruppo normale di $\mathcal{A}_n$, da cui $\langle X \rangle = \mathcal{A}_n$ in quanto diverso da $\{id\}$. □

### §1.8.6 Sottogruppi normali di $\mathcal{S}_n$

**Lemma 1.70**

Per $n \geq 3$ il centro di $\mathcal{S}_n$ è banale, cioè $Z(\mathcal{S}_n) = \{id\}$.

*Dimostrazione.* Sia $\sigma \in Z(\mathcal{S}_n) \setminus \{id\}$, allora esistono distinti $x, y \in \{1, \dots, n\}$ tali che $\sigma(x) = y$. Fissiamo $z \in \{1, \dots, n\} \setminus \{x, y\}$ e consideriamo la permutazione $\tau = (y\ z)$, abbiamo

$$(\tau\sigma)(x) = z \quad (\sigma\tau)(x) = y$$

che è assurdo in quanto $y \neq z$. Pertanto $Z(\mathcal{S}_n) = \{id\}$. □

**Proposizione 1.71**

Per $n \geq 5$, gli unici sottogruppi normali di $\mathcal{S}_n$ sono $\{id\}$, $\mathcal{A}_n$ e $\mathcal{S}_n$.

*Dimostrazione.* Sia $N$ un sottogruppo normale di $\mathcal{S}_n$, consideriamo $K = N \cap \mathcal{A}_n$. $K$ è normale in $\mathcal{A}_n$, pertanto $K = \{id\}$ oppure $K = \mathcal{A}_n$, distinguiamo 2 casi:

- se $K = \mathcal{A}_n$ allora $\mathcal{A}_n \leqslant N$: per il Teorema di Corrispondenza i sottogruppi di $\mathcal{S}_n$ contenenti $\mathcal{A}_n$ sono in bigezione con i sottogruppi di ${}^{\mathcal{S}_n}\!/_{\mathcal{A}_n} \cong \mathbb{Z}/2\mathbb{Z}$, pertanto $N = \mathcal{A}_n$ oppure $N = \mathcal{S}_n$;

- se $K = \{id\}$, poiché $[\mathcal{S}_n : \mathcal{A}_n] = 2$ per la Proposizione 1.49 vale $[N : K] \in \{1, 2\}$, da cui $|N| \leq 2$. Se $|N| = 1$ allora $N = \{id\}$, se $|N| = 2$ consideriamo l'azione di coniugio di $\mathcal{S}_n = N_{\mathcal{S}_n}(N)$ su $N$

$$\varphi : N_{\mathcal{S}_n}(N) \longrightarrow Aut(N) : g \longmapsto \varphi_g$$

dove $\varphi_g$ è la mappa

$$\varphi_g : N \longrightarrow N : h \longmapsto ghg^{-1}$$

il nucleo di $\varphi$ coincide con $Z_{\mathcal{S}_n}(N)$. Per il Primo Teorema di Omomorfismo allora abbiamo un omomorfismo iniettivo

$$\psi : \frac{N_{\mathcal{S}_n}(N)}{Z_{\mathcal{S}_n}(N)} \hookrightarrow \mathrm{Aut}(N)$$

Poiché $|N| = 2$ abbiamo $N \cong \mathbb{Z}/2\mathbb{Z}$, pertanto $\mathrm{Aut}(N) = \{id\}$. Dato che $N_{\mathcal{S}_n}(N) = \mathcal{S}_n$ per la normalità di $N$ questo implica che sia $Z_{\mathcal{S}_n}(N) = \mathcal{S}_n$, cioè che $N \subseteq Z(\mathcal{S}_n)$, ma questo è assurdo in quanto $Z(\mathcal{S}_n) = \{id\}$ per il Lemma 1.65.

□

**Osservazione 1.72** — L'enunciato è vero anche per $n = 3$ con la stessa dimostrazione, infatti $\mathcal{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ è un gruppo semplice, mentre per $n = 4$ è falso. Infatti $\mathcal{A}_4$ non è semplice, e il sottogruppo di Klein

$$V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

è un suo sottogruppo normale non banale. Notiamo che $V_4$ è normale in $\mathcal{S}_4$ in quanto unione delle classi di coniugio di tutti i suoi elementi.

### §1.8.7 Sottogruppi isomorfi a $S_{n-1}$

[9]

Abbiamo osservato più volte che $S_{n-1}$ si immerge naturalmente in $\mathcal{S}_n$, vediamo adesso un risultato che generalizza questo fatto ad alcuni sottogruppi di $\mathcal{S}_n$.

**Proposizione 1.73**

Dato un sottogruppo $H \leqslant \mathcal{S}_n$ con $n \geq 5$, se $[\mathcal{S}_n : H] = n$ allora $H$ è isomorfo a $S_{n-1}$.

*Dimostrazione.* Consideriamo l'azione di moltiplicazione a sinistra di $\mathcal{S}_n$ sull'insieme quoziente $\mathcal{S}_n/H$:

$$\varphi : \mathcal{S}_n \longrightarrow \mathcal{S}\left(\mathcal{S}_n/H\right) \cong \mathcal{S}_n$$

tale azione è transitiva in quanto per ogni $\sigma, \rho \in \mathcal{S}_n$ vale

$$\varphi(\sigma\rho^{-1})(\rho H) = \sigma\rho\rho^{-1}H = \sigma H$$

in particolare $\ker\varphi \neq \mathcal{S}_n$. Poiché $\ker\varphi \trianglelefteq \mathcal{S}_n$ allora il nucleo di $\varphi$ è banale oppure è $\mathcal{A}_n$. D'altra parte se fosse $\ker\varphi = \mathcal{A}_n$ avremmo $|\mathrm{Im}\varphi| = 2$, pertanto l'orbita di ogni elemento di $\mathcal{S}_n/H$ contiene al più due elementi, ma questo è assurdo in quanto per la transitività di $\varphi$ si ha $\mathrm{Orb}(\rho H) = \mathcal{S}_n/H$ per ogni $\rho \in \mathcal{S}_n$, che contiene almeno 5 elementi. Pertanto $\ker\varphi = \{id\}$, cioè $\varphi$ è un omomorfismo iniettivo e in particolare un isomorfismo. Notiamo che $H$ è lo stabilizzatore della classe $H$, infatti

$$\mathrm{St}(H) = \{\sigma \in \mathcal{S}_n \mid \sigma H = H\} = \{\sigma \in H\} = H$$

pertanto $\varphi(H)$ è lo stabilizzatore di un elemento di $\mathcal{S}_n/H$ per l'azione naturale di $\mathcal{S}\left(\mathcal{S}_n/H\right)$ su $\mathcal{S}_n/H$. Tramite la corrispondenza tra $\mathcal{S}_n/H$ e $\{1, \ldots, n\}$ possiamo identificare $\varphi(H)$ con le permutazioni di $\mathcal{S}_n$ che fissano un elemento di $\{1, \ldots, n\}$, che a loro volta costituiscono un gruppo isomorfo a $S_{n-1}$, pertanto $H \cong S_{n-1}$. □

Utilizzando il seguente teorema (di cui non diamo la dimostrazione) possiamo dire qualcosa di più forte nei casi $n \neq 2$ e $n \neq 6$.

**Teorema 1.74**

Per $n \notin \{2, 6\}$ i gruppi $\mathcal{S}_n$ e $\mathrm{Aut}(\mathcal{S}_n)$ sono isomorfi, e l'isomorfismo è dato dall'azione di coniugio

$$\varphi : \mathcal{S}_n \longrightarrow \mathrm{Aut}(\mathcal{S}_n) : \sigma \longmapsto \varphi_\sigma$$

**Osservazione 1.75** — In particolare gli automorfismi di $\mathcal{S}_n$ sono tutti interni nei casi $n \notin \{2, 6\}$, cioè sono coniugi per elementi di $\mathcal{S}_n$

Con le stesse notazioni di sopra chiamiamo $\varphi'$ l'isomorfismo tra $\mathcal{S}\left(\mathcal{S}_n/H\right)$ e $\mathcal{S}_n$, componendo $\varphi'$ con $\varphi$ otteniamo un isomorfismo

$$\psi : \mathcal{S}_n \longrightarrow \mathcal{S}_n$$

[9] Non sono sicuro di essere stato chiarissimo in questa sezione, se ci sono dei passi che ritenete poco comprensibili fatemelo sapere :)

che, per $n \notin \{2, 6\}$, è il coniugio per un elemento di $\mathcal{S}_n$. Abbiamo quindi che $\psi(H)$ è lo stabilizzatore di un elemento per l'azione naturale di $\mathcal{S}_n$ su $\{1, \ldots, n\}$, ma allora anche $H$ è uno stabilizzatore per tale azione in quanto coniugato a $\psi(H)$[10].Pertanto i sottogruppi di $\mathcal{S}_n$ isomorfi a $S_{n-1}$ sono tra loro coniugati e ognuno è lo stabilizzatore di un elemento per l'azione naturale di $\mathcal{S}_n$ su $\{1, \ldots, n\}$.

### §1.8.8 Costruzione di un automorfismo esterno di $\mathcal{S}_6$

Abbiamo visto che i casi $n = 2$ e $n = 6$ sono gli unici per cui non vale che $\mathcal{S}_n \cong \operatorname{Aut}(\mathcal{S}_n)$. Per $n = 2$ il motivo è semplice, infatti essendo $\mathcal{S}_2$ isomorfo a $\mathbb{Z}/2\mathbb{Z}$ il suo gruppo di automorfismi è banale, per $n = 6$ invece abbiamo che gli automorfismi di $\mathcal{S}_6$ non sono tutti elementi di $\operatorname{Inn}(\mathcal{S}_n)$, vogliamo quindi esibire un automorfismo di $\mathcal{S}_6$ che non sia interno.

Iniziamo osservando che $\mathcal{S}_5$ contiene 6 5-Sylow, infatti tali sottogruppi sono isomorfi a $\mathbb{Z}/5\mathbb{Z}$ e, essendo i 5-cicli gli unici elementi di ordine 5, $\mathcal{S}_5$ ne contiene esattamente

$$\frac{1}{\phi(5)}\binom{5}{5}4! = 6$$

Posto $X = \{P_1, \ldots, P_6\}$ l'insieme dei 5-Sylow di $\mathcal{S}_5$, consideriamo l'azione di coniugio di $\mathcal{S}_5$ su $X$

$$\varphi : \mathcal{S}_5 \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_6$$

dove l'isomorfismo tra $\mathcal{S}(X)$ e $\mathcal{S}_6$ è dato dall'associare $P_i$ a $i$, poniamo $\Phi$ la composizione di $\varphi$ con tale isomorfismo, notiamo che $\Phi$ è un'immersione di $\mathcal{S}_5$ in $\mathcal{S}_6$. L'azione $\varphi$ è transitiva in quanto i 5-Sylow di $\mathcal{S}_5$ sono tutti coniugati, pertanto $\ker\varphi = \{id\}$ oppure $\ker\varphi = \mathcal{A}_5$. D'altra parte se fosse $\ker\varphi = \mathcal{A}_5$ si avrebbe che $|\mathrm{Im}\varphi| = 2$, pertanto l'orbita di ogni elemento ha cardinalità 2, che è assurdo in quanto $\operatorname{Orb}(P_i) = X$ per ogni $P_i \in X$ per transitività di $\varphi$, quindi l'azione è iniettiva.
La transitività di $\varphi$ implica che $\Phi$ sia un'azione transitiva di $\mathcal{S}_5$ sull'insieme $\{1, \ldots, 6\}$, notiamo quindi che $\mathrm{Im}\Phi$ non può essere lo stabilizzatore di un elemento di $\{1, \ldots, 6\}$ per l'azione naturale di $\mathcal{S}_6$ su tale insieme. Infatti se lo fosse esisterebbe $k \in \{1, \ldots, n\}$ tale che $\Phi(\sigma)(i) = i$ per ogni $\sigma \in \mathcal{S}_5$, ma questo è assurdo in quanto per la Proposizione 1.41 $\mathcal{S}_5$ contiene una permutazione che agisce su $\{1, \ldots, 6\}$ senza punti fissi.
Abbiamo che $H = \mathrm{Im}\Phi$ è un sottogruppo di $\mathcal{S}_6$ di indice 6 e possiamo considerare l'azione transitiva e iniettiva di moltiplicazione a sinistra di $\mathcal{S}_6$ su ${\mathcal{S}_6}/{H}$

$$\alpha : \mathcal{S}_6 \longrightarrow \mathcal{S}\left({\mathcal{S}_6}/{H}\right) \cong \mathcal{S}_6$$

chiamiamo $\psi : \mathcal{S}_6 \longrightarrow \mathcal{S}_6$ l'isomorfismo risultante dalla composizione di $\alpha$ con l'isomorfismo tra $\mathcal{S}\left({\mathcal{S}_6}/{H}\right)$ e $\mathcal{S}_6$. Sia $i \in \{1, \ldots, 6\}$ l'elemento associato alla classe $H$, abbiamo visto nella dimostrazione della Proposizione 1.68 che $\psi(H) = \operatorname{St}(i)$ per l'azione naturale di $\mathcal{S}_6$ sull'insieme $\{1, \ldots, 6\}$. Concludiamo osservando che se $\psi$ fosse un automorfismo interno di $\mathcal{S}_6$, allora anche $\psi^{-1}$ sarebbe un automorfismo interno, cioè $\psi^{-1}$ sarebbe il coniugio per un qualche $\sigma \in \mathcal{S}_6$ fissato, da cui

$$H = \psi^{-1}(\operatorname{St}(i)) = \sigma \operatorname{St}(i)\sigma^{-1} = \operatorname{St}(\sigma(i))$$

che è assurdo in quanto $H$ non può essere uno stabilizzatore per tale azione, pertanto $\psi \notin \operatorname{Inn}(\mathcal{S}_6)$.

[10]Notiamo che l'azione naturale di $\mathcal{S}_n$ su $\{1, \ldots, n\}$ è transitiva, pertanto gli stabilizzatori sono tra loro coniugati.

## §1.9 Prodotti semidiretti

### §1.9.1 Descrizione di $\mathcal{S}_4$ come prodotto semidiretto

Per ogni $n \geq 2$ vale in generale la relazione

$$\mathcal{S}_n \cong \mathcal{A}_n \rtimes \langle (a\ b) \rangle$$

dove $(a\ b)$ è una trasposizione di $\mathcal{S}_n$, vogliamo però dare una decomposizione di $\mathcal{S}_4$ più specifica.
Consideriamo il sottogruppo di Klein $V_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ e $H = \{\sigma \in \mathcal{S}_4 \mid \sigma(4) = 4\}$ lo stabilizzatore di 4 secondo l'azione naturale di $\mathcal{S}_4$ su $\{1, 2, 3, 4\}$, osserviamo che $V_4$ è normale in $\mathcal{S}_4$ in quanto unione delle classi di coniugio di ogni suo elemento[11] e che $H$ è isomorfo a $\mathcal{S}_3$ (in effetti gli elementi di $H$ sono tutte e sole le permutazioni di 3 elementi). Dato che l'unica permutazione di $V_4$ che fissa 4 è l'identità abbiamo $V_4 \cap H = \{id\}$, inoltre $V_4 H = \mathcal{S}_4$ in quanto i due insiemi hanno la stessa cardinalità. Possiamo quindi scrivere

$$\mathcal{S}_4 \cong V_4 \rtimes H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathcal{S}_3$$

con

$$\varphi : \mathcal{S}_3 \longrightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Specifichiamo come agisce la mappa $\varphi$[12]: consideriamo gli isomorfismi

$$\alpha : V_4 \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : (1\ 2)(3\ 4) \longmapsto (1, 0), (1\ 3)(2\ 4) \longmapsto (0, 1)$$

$$\beta : H \longrightarrow \mathcal{S}_3 : \sigma \longmapsto \sigma_{|\{1,2,3\}}$$

le immagini di $\varphi$ in $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ corrispondono tramite $\alpha$ e $\beta$ ai coniugi su $V_4$ per elementi di $H$. Vediamo quindi come i generatori $(1\ 2\ 3)$, $(1\ 2)$ di $H$ agiscono per coniugio sui generatori $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ di $V_4$:

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

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

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

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

Pertanto $\varphi((1\ 2\ 3)) = f$ e $\varphi((1\ 2)) = g$, dove $f$ e $g$ sono gli automorfismi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tali che

$$f : (1, 0) \longmapsto (1, 1), (0, 1) \longmapsto (1, 0)$$

$$g : (1, 0) \longmapsto (1, 0), (0, 1) \longmapsto (1, 1)$$

[11]La classe di coniugio in $\mathcal{S}_4$ di $(1\ 2)(3\ 4)$ è $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.
[12]Se descriviamo $\mathcal{S}_4$ come prodotto semidiretto di due sottogruppi questo non è necessario, in quanto tale mappa è sempre il coniugio.

### §1.9.2 Automorfismi di $D_n$

Consideriamo il gruppo

$$G = \{f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \mid \exists a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z} \text{ per cui } f(x) = ax + b \ \forall x \in \mathbb{Z}/n\mathbb{Z}\}$$

delle sostituzioni lineari in $\mathbb{Z}/n\mathbb{Z}$, effettivamente $G$ è un gruppo con l'operazione di composizione. Infatti fissati $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$ e $f \in G$ tali che $f(x) = ax + b$, abbiamo che $f^{-1}$ è tale che $f^{-1}(x) = a^{-1}(x - b)$ (chiaramente $G$ contiene l'applicazione identità ed è chiuso per composizione). Notiamo che un elemento di $G$ è univocamente determinato dalla coppia $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$[13], pertanto $G$ contiene $n\phi(n)$ elementi. In realtà possiamo essere più precisi:

**Proposizione 1.76**

Il gruppo $G$ definito come sopra è isomorfo a un prodotto semidiretto

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

*Dimostrazione.* Consideriamo i sottogruppi di $G$

$$N = \{f \in G \mid f(x) = x + b,\ b \in \mathbb{Z}/n\mathbb{Z}\}$$
$$H = \{f \in G \mid f(x) = ax,\ a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

osserviamo che $N$ e $H$ sono naturalmente isomorfi a $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$ rispettivamente e che $N \cap H = \{id\}$, pertanto $NH = G$ in quanto

$$|NH| = \frac{|N| \cdot |H|}{|N \cap |H|} = |N| \cdot |H| = n\phi(n) = |G|$$

Mostriamo quindi che $N$ è un sottogruppo normale di $G$: fissati $f \in N$ e $g \in G$ tali che $f(x) = x + t$ e $g(x) = ax + b$, con $b, t \in \mathbb{Z}/n\mathbb{Z}$ e $a \in (\mathbb{Z}/n\mathbb{Z})^*$, abbiamo

$$(g^{-1} \circ f \circ g)(x) = (g^{-1} \circ f)(ax + b) = g^{-1}(ax + b + t) = x + a^{-1}t$$

pertanto $g^{-1} \circ f \circ g \in N$, cioè $N \trianglelefteq G$. Possiamo quindi decomporre $G$ come prodotto semidiretto:

$$G \cong N \rtimes H$$

poiché $N \cong \mathbb{Z}/n\mathbb{Z}$ e $H \cong (\mathbb{Z}/n\mathbb{Z})^*$ abbiamo che $G$ è isomorfo a un prodotto semidiretto

$$\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^*$$

□

Rappresentiamo gli elementi di $G$ tramite le coppie $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ (come insieme, non come gruppo), la composizione in $G$ produce la seguente operazione sulle coppie:

$$(b_1, a_1)(b_2, a_2) = (b_1 + a_1 b_2, a_1 a_2)$$

pertanto l'omomorfismo che definisce il prodotto semidiretto $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^*$ a cui è isomorfo $G$ è

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) : a \longmapsto \varphi_a$$

dove $\varphi_a$ è l'omomorfismo di moltiplicazione per $a$

$$\varphi_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} : x \longmapsto ax$$

[13] Consideriamo qua solo l'insieme prodotto cartesiano, non la struttura di gruppo data dal prodotto diretto.

**Proposizione 1.77**
Il gruppo $G$ delle sostituzioni lineari in $\mathbb{Z}/n\mathbb{Z}$ è isomorfo a $\mathrm{Aut}(D_n)$ per $n \geq 3$.

*Dimostrazione.* Siano $r, s \in D_n$ tali che $\mathrm{ord}(r) = n$, $\mathrm{ord}(s) = 2$, $D_n = \langle r, s\rangle$, consideriamo $\varphi \in Aut(D_n)$. Poiché $\langle r\rangle \cong \mathbb{Z}/n\mathbb{Z}$ è un sottogruppo caratteristico di $D_n$ abbiamo che esistono unici $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$ tali che

$$\varphi(r) = r^a \qquad \varphi(s) = sr^b$$

Consideriamo $\varphi_1$, $\varphi_2 \in \mathrm{Aut}(D_n)$ tali che

$$\varphi_i(r) = r^{a_i} \qquad \varphi_i(s) = sr^{b_i}$$

con $a_i \in (\mathbb{Z}/n\mathbb{Z})^*$, $b_i \in \mathbb{Z}/n\mathbb{Z}$ per $i \in \{1, 2\}$, componendo $\varphi_1$ con $\varphi_2$ otteniamo

$$\varphi_1(\varphi_2(r)) = \varphi_1(r^{a_2}) = r^{a_1 a_2}$$

$$\varphi_1(\varphi_2(s)) = \varphi_1(sr^{b_2}) = sr^{b_1 + a_1 b_2}$$

Pertanto $\mathrm{Aut}(D_n)$ è isomorfo a un quoziente di $G$ in quanto i suoi elementi rispettano la stessa legge di gruppo, d'altra parte $|\,\mathrm{Aut}(D_n)| = |G|$, pertanto i due gruppi sono proprio isomorfi. □

### §1.9.3 Prodotti semidiretti isomorfi

Dati due gruppi, può succedere che il loro prodotto diretto sia isomorfo a un loro prodotto semidiretto non banale.
Consideriamo il gruppo $GL_3(\mathbb{R})$ e $N = SL_3(\mathbb{R}) = \{M \in GL_3(\mathbb{R}) \mid \det M = 1\}$, $N$ è un sottogruppo normale di $GL_3(\mathbb{R})$ in quanto è il nucleo dell'omomorfismo

$$\det : GL_3(\mathbb{R}) \longrightarrow \mathbb{R}^*$$

mostriamo che $GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \times \mathbb{R}^*$. Consideriamo il sottogruppo

$$H = \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \,\middle|\, \lambda \in \mathbb{R}^* \right\}$$

isomorfo a $\mathbb{R}^*$, abbiamo che:

- $N \cap H = \{Id\}$ in quanto $M = \lambda Id \in N \cap H$ è tale che $\det M = \lambda^3 = 1$, cioè $\lambda = 1$ e quindi $M = Id$;
- $H$ è un sottogruppo normale di $GL_3(\mathbb{R})$, in quanto tutti i suoi elementi sono multipli scalari della matrice identità e quindi commutano con gli elementi di $GL_3(\mathbb{R})$;
- $GL_3(\mathbb{R}) = NH$, infatti per ogni $M \in GL_3(\mathbb{R})$ possiamo scrivere $M = S(\lambda Id)$, dove $\lambda = (\det M)^{\frac{1}{3}}$ e $S = (\det M)^{-\frac{1}{3}} M \in N$.

Possiamo quindi scrivere

$$GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \times H \cong SL_3(\mathbb{R}) \times \mathbb{R}^*$$

Consideriamo adesso il sottogruppo di $GL_3(\mathbb{R})$

$$K = \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R}^* \right\}$$

anch'esso isomorfo a $\mathbb{R}^*$. Ragionando in modo analogo abbiamo $N \cap H = \{Id\}$, inoltre $GL_3(\mathbb{R}) = NK$ in quanto per ogni $M \in GL_3(\mathbb{R})$ possiamo scrivere $M = (MA^{-1})A$ con

$$A = \begin{pmatrix} \det M & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in K, \quad MA^{-1} \in N$$

Possiamo quindi scrivere

$$GL_3(\mathbb{R}) \cong SL_3(\mathbb{R}) \rtimes K$$

Notiamo che l'azione di coniugio di $K$ su $SL_3(\mathbb{R})$ non è banale, in quanto

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \lambda \neq 0, 1$$

quindi il prodotto non è diretto.

È in realtà relativamente semplice costruire prodotti diretti e prodotti semidiretti isomorfi a partire da un gruppo non abeliano, diamo l'esempio di una possibile procedura nella seguente dimostrazione.

**Proposizione 1.78**

Dato un gruppo $G$ non abeliano, esiste un omomorfismo

$$\varphi : G \longrightarrow \mathrm{Aut}(G)$$

non banale tale che $G \times G \cong G \rtimes_\varphi G$.

*Dimostrazione.* Consideriamo i sottogruppi $N = G \times \{e\}$, $H = \{(g, g) \mid g \in G\}$, notiamo che $N$ è un sottogruppo normale di $G \times G$. Inoltre $N \cap H = \{e, e\}$ e $NH = G \times G$, in quanto per ogni elemento $(g_1, g_2) \in G \times G$ abbiamo

$$(g_1, g_2) = (g_1 g_2^{-1}, e)(g_2, g_2)$$

con $(g_1 g_2^{-1}, e) \in N$ e $(g_2, g_2) \in H$, pertanto possiamo scrivere $G \times G = N \rtimes_\varphi H$, dove $\varphi$ è un omomorfismo

$$\varphi : H \longrightarrow \mathrm{Aut}(N)$$

Tale $\varphi$ è banale se e solo se $\varphi(h) = id$ per ogni $h \in H$, se e solo se $hnh^{-1} = n$ per ogni $h \in H$, per ogni $n \in N$. Questo è equivalente a richiedere

$$(g, g)(h, e)(g^{-1}, g^{-1}) = (ghg^{-1}, e) = (h, e) \; \forall g, h \in G$$

cioè $g \in Z(G)$ per ogni $g \in G$, ma questo è assurdo in quanto $G$ non è abeliano, pertanto $\varphi$ non è l'omomorfismo banale. Poiché $N \cong H \cong G$ abbiamo quindi

$$G \times G \cong G \rtimes_{\varphi'} G$$

dove

$$\varphi' : G \longrightarrow \mathrm{Aut}(G)$$

è l'omomorfismo non banale corrispondente a $\varphi$. $\square$

Vediamo adesso un criterio che stabilisce una condizione sufficiente affinché i prodotti semidiretti di due gruppi siano isomorfi.

**Proposizione 1.79** (Criterio di isomorfismo tra prodotti semidiretti)
Siano $H, N$ due gruppi e $\varphi : H \longrightarrow \mathrm{Aut}(N)$ un omomorfismo. Dato $f \in \mathrm{Aut}(H)$ allora $N \rtimes_\varphi H \cong N \rtimes_{\varphi \circ f} H$.

*Dimostrazione.* Consideriamo l'applicazione

$$\psi : N \rtimes_\varphi H \longrightarrow N \rtimes_{\varphi \circ f} H : (n, h) \longmapsto (n, f^{-1}(h))$$

$\psi$ è una bigezione tra i due insiemi in quanto $f$ è bigettiva, mostriamo che è anche un omomorfismo di gruppi. Per ogni $(n_1, h_1)$, $(n_2, h_2) \in N \rtimes_\varphi H$ abbiamo

$$\begin{aligned}\psi((n_1, h_1)(n_2, h_2)) &= \psi(n_1 \cdot \varphi(h_1)(n_2), h_1 h_2) = \\ &= (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1 h_2)) = (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1) f^{-1}(h_2))\end{aligned}$$

d'altra parte

$$\begin{aligned}&\psi(n_1, h_1)\psi(n_2, h_2) = (n_1, f^{-1}(h_1))(n_2, f^{-1}(h_2)) = \\ &= (n_1 \cdot (\varphi \circ f)(f^{-1}(h_1))(n_2), f^{-1}(h_1) f^{-1}(h_2)) = (n_1 \cdot \varphi(h_1)(n_2), f^{-1}(h_1) f^{-1}(h_2))\end{aligned}$$

cioè $\psi$ è un omomorfismo, quindi i due gruppi sono isomorfi. □

**Esempio 1.80**
Abbiamo visto che i prodotti semidiretti della forma $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ con $p$, $q$ primi tali che $q \mid p-1$ si suddividono in esattamente due classi di isomorfismo, utilizziamo il risultato appena mostrato per verificare che tutti i prodotti semidiretti non banali sono tra loro isomorfi. Consideriamo un omomorfismo

$$\varphi_a : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z} : 1 \longmapsto a$$

con $\mathrm{ord}(a) = q$ (poiché $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ questo è equivalente a fissare un omomorfismo tra $\mathbb{Z}/q\mathbb{Z}$ e $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$), possiamo scrivere

$$a = k\frac{p-1}{q} \quad k \in \{1, \dots, q-1\}$$

Posto $f_k \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ tale che

$$f_k : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} : x \longmapsto kx$$

con $(k, q) = 1$, possiamo scrivere $\varphi_a = \varphi_{\frac{p-1}{q}} \circ f_k$. Allora i prodotti semidiretti non banali $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_a} \mathbb{Z}/q\mathbb{Z}$ sono tutti isomorfi a tra loro per la Proposizione 1.74.

Vediamo adesso un criterio che fornisce una condizione sufficiente affinché due prodotti semidiretti di $p$-gruppi non siano isomorfi.

**Proposizione 1.81**

Siano $p$, $q$ due primi distinti, $G$ un $p$-gruppo e $H$ un $q$-gruppo, consideriamo i prodotti semidiretti

$$X_1 = G \rtimes_{\varphi_1} H \qquad X_2 = G \rtimes_{\varphi_2} H$$

con

$$\varphi_1, \varphi_2 : H \longrightarrow \mathrm{Aut}(G)$$

Se $\ker \varphi_1$ e $\ker \varphi_2$ non sono isomorfi allora $X_1$ e $X_2$ non sono isomorfi.

*Dimostrazione.* Dimostriamo la contronominale, cioè che se $X_1$ e $X_2$ sono isomorfi allora $\ker \varphi_1 \cong \ker \varphi_2$.
Sia $f : X_1 \longrightarrow X_2$ un isomorfismo, poniamo $\mathcal{G}_1 = G \rtimes_{\varphi_1} \{e_H\}$, $\mathcal{G}_2 = G \rtimes_{\varphi_2} \{e_H\}$, $\mathcal{H}_1 = \{e_G\} \rtimes_{\varphi_1} H$, $\mathcal{H}_2 = \{e_G\} \rtimes_{\varphi_2} H$. Osserviamo che $f(\mathcal{G}_1) = \mathcal{G}_2$ in quanto $\mathcal{G}_1$ è l'unico $p$-Sylow di $X_1$ e $\mathcal{G}_2$ è l'unico $p$-Sylow di $X_2$ (infatti $\mathcal{G}_1 \trianglelefteq X_1$ e $\mathcal{G}_2 \trianglelefteq X_2$), mentre $f(\mathcal{H}_1)$ è un $q$-Sylow di $X_2$ coniugato a $\mathcal{H}_2$. In particolare esiste $\psi \in \mathrm{Inn}(X_2)$ tale che

$$(\psi \circ f)(\mathcal{G}_1) = \mathcal{G}_2 \qquad (\psi \circ f)(\mathcal{H}_1) = \mathcal{H}_2$$

pertanto, a meno di coniugio, possiamo supporre $f(\mathcal{G}_1) = \mathcal{G}_2$ e $f(\mathcal{H}_1) = \mathcal{H}_2$. Caratterizziamo i nuclei di $\varphi_1$, $\varphi_2$ in termini di centralizzatori, in particolare scriviamo

$$\begin{aligned} Z_{\mathcal{H}_1}(\mathcal{G}_1) &= \{(e_G, h) \in \mathcal{H}_1 \mid (e_G, h)(g, e_H)(e_G, h)^{-1} = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid (\varphi_1(h)(g), h)(e_G, h^{-1}) = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid (\varphi_1(h)(g), e_H) = (g, e_H)\ \forall g \in G\} = \\ &= \{(e_G, h) \in \mathcal{H}_1 \mid \varphi_1(h) = id\} = \{e_G\} \rtimes_{\varphi_1} \ker \varphi_1 \end{aligned}$$

e ragionando in modo analogo

$$Z_{\mathcal{H}_2}(\mathcal{G}_2) = \{e_G\} \rtimes_{\varphi_2} \ker \varphi_2$$

Poniamo $\chi = \psi \circ f$, chiaramente $\chi : X_1 \longrightarrow X_2$ è un isomorfismo e $\chi(\mathcal{G}_1) = \mathcal{G}_2$, $\chi(\mathcal{H}_1) = \mathcal{H}_2$ per quanto detto sopra, pertanto

$$\begin{aligned} \{e_G\} \rtimes_{\varphi_2} \ker \varphi_2 &= Z_{\mathcal{H}_2}(\mathcal{G}_2) = Z_{\chi(\mathcal{H}_1)}(\chi(\mathcal{G}_1)) = \\ &= \{\chi(h_1) \mid h_1 \in \mathcal{H}_1, \chi(h_1)\chi(g_1) = \chi(g_1)\chi(h_1)\ \forall g_1 \in \mathcal{G}_1\} = \\ &= \{\chi(h_1) \mid h_1 \in \mathcal{H}_1, \chi(h_1 g_1) = \chi(g_1 h_1)\ \forall g_1 \in \mathcal{G}_1\} = \\ &= \{\chi(h_1) \mid h_1 \in Z_{\mathcal{H}_1}(\mathcal{G}_1)\} = \chi(\{e_G\} \rtimes_{\varphi_1} \ker \varphi_1) \end{aligned}$$

In particolare quindi $\chi$ induce un isomorfismo tra $\ker \varphi_2$ e $\ker \varphi_1$. $\square$

## §1.10 Classificazione dei gruppi semplici di ordine al più 100

In questa sezione vogliamo determinare quali sono i sottogruppi semplici di ordine minore o uguale a 100. Facciamo prima una serie di osservazioni che ci permetterà di ridurre lo studio a pochi casi interessanti.

- Gli unici gruppi abeliani semplici sono i gruppi $\mathbb{Z}/p\mathbb{Z}$ con $p$ primo, in quanto i loro sottogruppi sono solo quelli banali e tutti i sottogruppi di un gruppo abeliano sono normali;
- i gruppi $G$ di ordine $p^k$ con $p$ primo e $k > 1$ non sono semplici in quanto hanno centro non banale e il centro è un sottogruppo caratteristico, in particolare normale (alternativamente, dal Teorema di Sylow abbiamo che $G$ contiene un sottogruppo proprio di ordine $p^{k-1}$, che è normale in quanto il suo indice è $p$, il più piccolo primo che divide $|G|$);
- i gruppi di ordine $2d$ con $d$ dispari non sono semplici in quanto contengono un sottogruppo di indice 2, che è normale e non banale, per l'Esercizio 1.48;
- i gruppi di ordine $pq$ con $q > p$ primi non sono semplici, in quanto possiamo scriverli come prodotto semidiretto dei loro sottogruppi di Sylow, pertanto almeno uno di questi è normale e non banale;
- $\mathcal{A}_5$ è un gruppo semplice di ordine 60.

Ci riduciamo quindi a studiare i gruppi di ordine 56, 60, 72, 80, 96.

$|G| = 56 = 2^3 \cdot 7$: poiché $n_7 \equiv 1 \pmod 7$ e $n_7 \mid 56$ abbiamo $n_7 \in \{1, 8\}$. Se $n_7 = 1$ allora $G$ contiene un unico 7-Sylow, chè è quindi un sottogruppo proprio normale di $G$. Se $n_7 = 8$ allora $G$ contiene $6 \cdot 8 = 48$ elementi di ordine 7 (dato che i 7-Sylow di $G$ sono isomorfi a $\mathbb{Z}/7\mathbb{Z}$) pertanto i restanti 7 elementi non banali devono essere contenuti in un unico 2-Sylow, che è quindi normale. In entrambi i casi $G$ non è semplice.

$|G| = 96 = 2^5 \cdot 3$: sia $P_2$ un 2-Sylow di $G$, poiché $[G : P_2] = 3$ per il Teorema 1.50 esiste un sottogruppo $N \lhd G$ tale che $N \subseteq P_2$ e $3 \mid [G : N] \mid 3!$, da cui $N \neq G$ e $N \neq \{e\}$ in quanto $[G : \{e\}] = |G|$. Pertanto $G$ non è semplice.

$|G| = 72 = 2^3 \cdot 3^2$: dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 72 \end{cases} \qquad \begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 72 \end{cases}$$

otteniamo $n_2 \in \{1, 3, 9\}$ e $n_3 \in \{1, 4\}$, distinguiamo quindi due casi.

- Se $n_3 = 1$ allora $G$ contiene un unico 3-Sylow, che è quindi un sottogruppo normale non banale di $G$, cioè $G$ non è semplice;
- se $n_3 = 4$, siano $Q_1$, $Q_2$, $Q_3$, $Q_4$ i 3-Sylow di $G$ e $X = \{Q_1, Q_2, Q_3, Q_4\}$, consideriamo l'azione di coniugio di $G$ su $X$

  $$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_4$$

  poiché i 3-Sylow di $G$ sono tutti coniugati tale azione è transitiva. Mostriamo che $\ker \varphi$ è un sottogruppo di $G$ non banale. Se $\ker \varphi = \{e\}$ allora $\varphi$ sarebbe un omomorfismo iniettivo, che è assurdo in quanto l'ordine di $G$ non divide l'ordine di $\mathcal{S}(X) \cong \mathcal{S}_4$. D'altra parte se fosse $\ker\varphi = G$ allora $\varphi$ sarebbe l'azione banale, che è assurdo in quanto $\varphi$ è transitiva e $|X| > 1$ (alternativamente, se $\varphi$ fosse l'azione banale allora i 3-Sylow di $G$ sarebbero tutti normali). Pertanto $\ker\varphi$ è un sottogruppo normale non banale di $G$, cioè $G$ non è semplice.

$|G| = 80 = 2^4 \cdot 5$: dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 80 \end{cases} \qquad \begin{cases} n_5 \equiv 1 \pmod 5 \\ n_5 \mid 80 \end{cases}$$

otteniamo $n_2 \in \{1, 5\}$ e $n_5 \in \{1, 16\}$, distinguiamo quindi due casi.

- Se $n_5 = 1$ allora $G$ contiene un unico 5-Sylow, che è quindi un sottogruppo normale non banale di $G$, cioè $G$ non è semplice;
- se $n_5 = 16$ allora $G$ contiene $4 \cdot 16 = 64$ elementi di ordine 5 (dato che i 5-Sylow di $G$ sono isomorfi a $\mathbb{Z}/5\mathbb{Z}$), pertanto i restanti 15 elementi devono essere contenuti in un unico 2-Sylow, che è quindi normale. Allora $G$ non è semplice.
  Alternativamente, consideriamo $P_2$ un 2-Sylow e l'azione di moltiplicazione a sinistra di $G$ sull'insieme quoziente ${}^{G}\!/\!{}_{P_2}$
  $$\varphi : G \longrightarrow \mathcal{S}\left({}^{G}\!/\!{}_{P_2}\right) \cong \mathcal{S}_5$$
  Poiché $|G| \nmid |\mathcal{S}_5|$ abbiamo $\ker\varphi \neq \{e\}$, d'altra parte $\ker\varphi \neq G$ in quanto $\varphi$ è un'azione transitiva (per ogni $x, y \in G$ vale $\varphi(xy^{-1})(yP_2) = xy^{-1}yP_2 = xP_2$). Quindi $\ker\varphi$ è un sottogruppo normale di $G$ non banale, cioè $G$ non è semplice.

Rimangono da studiare i gruppi di ordine 60, vogliamo dimostrare che $\mathcal{A}_5$ è l'unico sottogruppo semplice di tale ordine (a meno di isomorfismo).

**Lemma 1.82**
$\mathcal{A}_5$ contiene esattamente 5 2-Sylow.

*Dimostrazione.* Sia $X$ l'insieme dei 2-Sylow di $\mathcal{A}_5$, consideriamo l'azione di coniugio di $\mathcal{A}_5$ su $X$
$$\varphi : \mathcal{A}_5 \longrightarrow \mathcal{S}(X)$$
poiché i 2-Sylow di $\mathcal{A}_5$ sono tutti coniugati e $\mathcal{A}_5$ è semplice tale azione è transitiva, in particolare $X$ è composto da un'unica orbita. Fissato $P$ un 2-Sylow abbiamo

$$n_2 = |\operatorname{Orb}(P)| = \frac{|\mathcal{A}_5|}{|N_{\mathcal{A}_5}(P)|}$$

Scegliamo $P = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ una copia di $V_4$ in $\mathcal{A}_5$, il normalizzatore di $P$ in $\mathcal{A}_5$ contiene necessariamente il sottogruppo

$$\operatorname{St}(5) = \{\sigma \in \mathcal{A}_5 \mid \sigma(5) = 5\} \cong \mathcal{A}_4$$ [14]

in quanto $V_4$ è un sottogruppo normale di $\mathcal{A}_4$, quindi $|N_{\mathcal{A}_5}(P)| \in \{12, 60\}$. D'altra parte $|N_{\mathcal{A}_5}(P)| \neq 60$, altrimenti $\mathcal{A}_5$ conterrebbe un unico 2-Sylow, che sarebbe quindi un sottogruppo normale non banale, che è assurdo in quanto $\mathcal{A}_5$ è semplice. Allora $|N_{\mathcal{A}_5}(P)| = 12$, cioè $n_2 = 5$. □

[14] Qua stiamo considerando l'azione naturale di $\mathcal{A}_5$ sull'insieme $\{1, 2, 3, 4, 5\}$.

**Proposizione 1.83**
Se $G$ è un gruppo semplice di ordine 60 allora è isomorfo a $\mathcal{A}_5$.

*Dimostrazione.* Dalle condizioni

$$\begin{cases} n_2 \equiv 1 \pmod 2 \\ n_2 \mid 60 \end{cases} \qquad \begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 60 \end{cases} \qquad \begin{cases} n_5 \equiv 1 \pmod 5 \\ n_5 \mid 60 \end{cases}$$

otteniamo $n_2 \in \{1, 3, 5, 15\}$, $n_3 = \{1, 4, 10\}$, $n_5 = \{1, 6\}$. Poiché $G$ è semplice, $n_2$, $n_3$ e $n_5$ sono tutti diversi da 1, altrimenti $G$ conterrebbe un sottogruppo caratteristico, quindi normale, non banale. Distinguiamo tre casi:

- supponiamo per assurdo $n_2 = 3$, posto $X$ l'insieme dei 2-Sylow di $G$ consideriamo l'azione di coniugio di $G$ su $X$

$$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_3$$

  poiché i 2-Sylow sono tutti coniugati e $G$ è semplice tale azione è transitiva, pertanto $\ker \varphi \neq G$. Allora $\ker \varphi = \{e\}$ in quanto $\ker \varphi \triangleleft G$, ma questo è assurdo dato che $|G| > |\mathcal{S}_3|$;

- supponiamo $n_2 = 5$, posto $X$ l'insieme dei 2-Sylow di $G$ consideriamo l'azione di coniugio di $G$ su $X$

$$\varphi : G \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_5$$

  argomentando come sopra si ha che tale azione è transitiva, pertanto $\ker \varphi \neq G$. Allora $\ker \varphi = \{e\}$ in quanto $\ker \varphi \triangleleft G$, cioè $\varphi$ è un omomorfismo iniettivo e $G$ è isomorfo a un sottogruppo $H \leqslant \mathcal{S}_5$ di indice 2. Consideriamo l'intersezione $H \cap \mathcal{A}_5$, per la Proposizione 1.49 allora $[\mathcal{A}_5 : H \cap \mathcal{A}_5] \in \{1, 2\}$. D'altra parte se fosse 2 allora $H \cap \mathcal{A}_5$ sarebbe un sottogruppo normale di $\mathcal{A}_5$ non banale, che è assurdo, pertanto l'indice di $H$ è 1, cioè $H = \mathcal{A}_5$. Quindi $G$ è isomorfo a $\mathcal{A}_5$;

- supponiamo per assurdo $n_2 = 15$, notiamo che due 2-Sylow distinti di $G$ si intersecano banalmente o in un sottogruppo isomorfo a $\mathbb{Z}/2\mathbb{Z}$[15]. Se tutti i 2-Sylow di $G$ si intersecassero banalmente allora la loro unione conterrebbe $1 + 3 \cdot 15 = 46$ elementi, poiché l'unione dei 5-Sylow di $G$ contribuisce con $4 \cdot 6 = 24$ elementi di ordine 5, ma allora $G$ non conterrebbe elementi di ordine 3, che è assurdo. Siano quindi $S_1$ e $\mathcal{S}_2$ 2-Sylow distinti di $G$ tali che $H = S_1 \cap \mathcal{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$, consideriamo il normalizzatore $N_G(H)$. Osserviamo che $S_1$ e $\mathcal{S}_2$ sono sottogruppi di $N_G(H)$ in quanto, essendo abeliani, $H$ è un sottogruppo normale di entrambi, pertanto $|N_G(H)| > 4$. D'altra parte poiché tale ordine deve dividere 60 abbiamo $|N_G(H)| \in \{12, 20\}$, infatti se fosse uguale a 60 $H$ sarebbe un sottogruppo normale non banale di $G$, che non è possibile in quanto $G$ è semplice. Inoltre $|N_G(H)| \neq 20$ in quanto si avrebbe $[G : N_G(H)] = 3$, allora per il Teorema 1.50 $G$ conterrebbe un sottogruppo normale non banale di indice al più 3!, che è assurdo. Abbiamo quindi $|N_G(H)| = 12$, consideriamo l'azione di moltiplicazione a sinistra di $G$ sull'insieme quoziente ${}^{G}\!/_{N_G(H)}$

$$\varphi : G \longrightarrow \mathcal{S}\left({}^{G}\!/_{N_G(H)}\right) \cong \mathcal{S}_5$$

[15] Questo perché la massima potenza di 2 che divide 60 è 4, pertanto un 2-Sylow di $G$ è isomorfo a $\mathbb{Z}/4\mathbb{Z}$ oppure a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

argomentando come sopra si ha che tale azione è transitiva, pertanto $\ker\varphi \neq G$. Allora $\ker\varphi = \{e\}$ in quanto $\ker\varphi \triangleleft G$, cioè $\varphi$ è un omomorfismo iniettivo e si mostra come sopra che $G \cong \mathcal{A}_5$, ma questo è assurdo in quanto $\mathcal{A}_5$ contiene 5 2-Sylow.

□

## §1.11 Studio di $\mathrm{SL}_2(\mathbb{F}_3)$

Consideriamo il gruppo $\mathrm{GL}_2(\mathbb{F}_3)$, ricordiamo che il determinante è un omomorfismo di gruppi surgettivo

$$\det : \mathrm{GL}_2(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^*$$

e che il suo nucleo è il gruppo $\mathrm{SL}_2(\mathbb{F}_3) = \{M \in \mathrm{GL}_2(\mathbb{F}_3) \mid \det M = 1\}$, che è quindi un sottogruppo normale di $\mathrm{GL}_2(\mathbb{F}_3)$. Inoltre, poiché $\mathbb{F}_3^* \cong \mathbb{Z}/2\mathbb{Z}$ abbiamo che $\mathrm{SL}_2(\mathbb{F}_3)$ ha indice 2 in $\mathrm{GL}_2(\mathbb{F}_3)$, pertanto $|\mathrm{SL}_2(\mathbb{F}_3)| = 24$ in quanto $|\mathrm{GL}_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$.

Consideriamo quindi il gruppo $S = \mathrm{SL}_2(\mathbb{F}_3)$, dalle condizioni

$$\begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 24 \end{cases}$$

otteniamo $n_3 \in \{1, 4\}$, notiamo però che $S$ non può contenere un unico 3-Sylow in quanto questi sono isomorfi a $\mathbb{Z}/3\mathbb{Z}$ e le matrici

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

hanno ordine 3 e i gruppi che generano sono distinti. In particolare $S$ contiene almeno 2 3-Sylow, pertanto ne contiene esattamente 4. Calcoliamo il centro di $S$ imponendo la commutazione sulle matrici appena esibite. Dall'equazione

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

otteniamo

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

da cui $c = 0$ e $a = d$. In modo analogo dall'equazione

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

otteniamo

$$\begin{pmatrix} a & b \\ a & a+b \end{pmatrix} = \begin{pmatrix} a+b & b \\ a & a \end{pmatrix}$$

da cui $b = 0$, pertanto un generico elemento del centro è della forma $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ d'altra parte il suo determinante deve essere uguale a 1, quindi $Z(S) = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$. Utilizziamo questo fatto per determinare la classe di isomorfismo del normalizzatore di un 3-Sylow di $S$.
Fissiamo $P$ un 3-Sylow, poiché $n_3 = [S : N_S(P)]$ abbiamo

$$|N_S(P)| = \frac{|S|}{n_3} = 6$$

inoltre $Z(S)$ e $P$ sono sottogruppi di $N_S(P)$. Notiamo che $N_S(P)$ contiene un elemento di ordine 3 e un elemento di ordine 2 che commutano, ad esempio il generatore di $P$ e il generatore di $Z(S)$, pertanto contiene un elemento di ordine 6, il loro prodotto, da cui $N_S(P) = PZ(S) \cong \mathbb{Z}/6\mathbb{Z}$.

Posto $X$ l'insieme dei 3-Sylow di $S$, consideriamo l'azione transitiva di coniugio di $S$ su $X$

$$\Phi : S \longrightarrow \mathcal{S}(X) \cong \mathcal{S}_4$$

il nucleo di $\Phi$ è

$$\begin{aligned}\ker\Phi = \{g \in S \mid gPg^{-1} = P\ \forall P \in X\} = \\ = \{g \in S \mid g \in N_S(P)\ \forall P \in X\} = \\ = \bigcap_{P\in X} N_S(P) = \bigcap_{P \in X} PZ(S) = Z(S)\end{aligned}$$

dove l'ultima uguaglianza è giustificata dal fatto che i 3-Sylow di $S$ si intersecano banalmente. Per il Primo Teorema di Omomorfismo otteniamo che $\mathrm{Im}\Phi \cong S/Z(S)$, che ha cardinalità 12. D'altra parte $\mathrm{A}_4$ è l'unico sottogruppo di $\mathcal{S}_4$ con 12 elementi, pertanto $S/Z(S) \cong \mathcal{A}_4$, sfruttiamo questo fatto per studiare i 2-Sylow di $S$. Per il Teorema di Corrispondenza i sottogruppi di $S$ contenenti $Z(S)$ sono in bigezione con i sottogruppi di $\mathcal{A}_4$, e tale bigezione preserva l'indice e la normalità dei sottogruppi. Poiché $V_4$ è l'unico 2-Sylow di $\mathcal{A}_4$ abbiamo che $S$ contiene un unico 2-Sylow di indice 3, cioè di cardinalità 8, chiamiamo $J$ tale sottogruppo. $J$ contiene le matrici

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ [16]

entrambe di ordine 4, inoltre

$$ij = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$ji = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

pertanto $ij = -ji$. Quindi $J$ è un gruppo di ordine 8 che contiene due elementi di ordine 4 che anticommutano, in particolare ha la seguente presentazione

$$J = \langle i, j \mid i^4 = j^4 = 1, i^2 = -1, ij = -ji\rangle$$

quindi è isomorfo a $Q_8$. Osserviamo che il sottogruppo derivato $S'$ è contenuto in $J$ in quanto il quoziente $S/J$ è abeliano (in particolare è isomorfo a $\mathbb{Z}/3\mathbb{Z}$), mostriamo che effettivamente vale l'uguaglianza. Sicuramente $S'$ non è il sottogruppo formato dalla sola identità in quanto $S$ non è abeliano, inoltre $S'$ deve necessariamente contenere un elemento di ordine 2 in quanto sottogruppo non banale di $J$, quindi $Z(S) \subseteq S'$[17]. Inoltre $Z(S) \neq S'$ in quanto il quoziente è isomorfo a $\mathcal{A}_4$, pertanto $S'$ ha ordine 4 oppure 8, cioè $[S : S'] \in \{3, 6\}$. Consideriamo l'omomorfismo surgettivo

$$\varphi : S \longrightarrow \mathcal{A}_4$$

dato dalla composizione della proiezione su $S/Z(S)$ con l'isomorfismo tra il quoziente e $\mathcal{A}_4$, per il Teorema di Corrispondenza $\varphi(S')$ è un sottogruppo normale di $\mathcal{A}_4$ con $[\mathcal{A}_4 : \varphi(S')] = [S : S']$. D'altra parte un sottogruppo di indice 6 di $\mathcal{A}_4$ è della forma $\{id, (a\ b)(c\ d)\}$ con $(a\ b)$ e $(c\ d)$ trasposizioni disgiunte, che non è normale in $\mathcal{A}_4$, pertanto $\varphi(S')$ ha indice 3 e quindi $S'$ ha ordine 8, da cui $S' = J$.

[16] Il determinante di questa matrice è $-2$, che è uguale a 1 in $\mathbb{F}_3$

[17] Infatti l'unico elemento di ordine 2 di $S$ è $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

# §2 Anelli

A meno di ulteriori specificazioni, gli anelli che tratteremo saranno sempre anelli commutativi con identità.

## §2.1 Interpolazione polinomiale via TCR

Mostriamo il seguente enunciato di interpolazione utilizzando il Teorema Cinese del Resto.

**Proposizione 2.1**

Siano $a_1, \ldots, a_n \in \mathbb{Q}$ valori distinti e $b_1, \ldots, b_n \in \mathbb{Q}$, allora esiste un unico polinomio $p(x) \in \mathbb{Q}[x]$ di grado al più $n-1$ tale che $p(a_i) = b_i$ per ogni $i \in \{1, \ldots, n\}$.

*Dimostrazione.* Posto $I_i = (x - a_i)$ per $i \in \{1, \ldots, n\}$, osserviamo che $I_i + I_j = \mathbb{Q}[x]$ per $i \neq j$, infatti $a_i - a_j \in I_i + I_j$, che è un elemento invertibile di $\mathbb{Q}[x]$. Per il Teorema Cinese del Resto abbiamo quindi

$$\frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \cong \mathbb{Q}[x]/I_1 \times \ldots \times \mathbb{Q}[x]/I_n$$

tramite l'isomorfismo

$$\Phi : \frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \longrightarrow \mathbb{Q}[x]/I_1 \times \ldots \times \mathbb{Q}[x]/I_n : \overline{p(x)} \longmapsto (p(x) + I_1, \ldots, p(x) + I_n)$$

abbiamo inoltre che $\mathbb{Q}[x]/I_i \cong \mathbb{Q}$ per ogni $i \in \{1, \ldots, n\}$ tramite l'isomorfismo

$$\Psi : \mathbb{Q}[x]/I_i \longrightarrow \mathbb{Q} : p(x) + I_i \longmapsto p(a_i)$$

La composizione di questi due risulta in un isomorfismo

$$\Psi \circ \Phi : \frac{\mathbb{Q}[x]}{I_1 \ldots I_n} \longrightarrow \mathbb{Q}^n : \overline{p(x)} \longmapsto (p(a_1), \ldots, p(a_n))$$

in particolare per ogni $n$-upla di razionali $(b_1, \ldots, b_n)$ esiste un unico[18] polinomio $p \in \mathbb{Q}[x]$ con $\deg p \leq n-1$ tale che $p(a_i) = b_i$ per ogni $i \in \{1, \ldots, n\}$. □

**Osservazione 2.2** — Con la dimostrazione data l'enunciato è vero su ogni campo con almeno $n$ elementi distinti. Più in generale è vero in ogni anello con almeno $n$ elementi distinti a patto di scegliere $a_1, \ldots, a_n$ tali che $a_i - a_j$ sia invertibile per ogni $i \neq j$.

[18] L'unicità deriva dal fatto che gli elementi di $\dfrac{\mathbb{Q}[x]}{I_1 \ldots I_n}$ possono essere rappresentati in modo unico da polinomi a coefficienti razionali di grado al più $n-1$.

## §2.2 Localizzazione di $\mathbb{Z}$ rispetto a un ideale primo

Sia $P = (p)$ un ideale primo non nullo di $\mathbb{Z}$, consideriamo $S = \mathbb{Z} \setminus P$. $S$ è una parte moltiplicativa di $\mathbb{Z}$, infatti

- $0 \notin S$ in quanto $0 \in P$;
- $1 \in S$ in quanto $1 \notin P$;
- per ogni $x, y \in S$ vale $xy \in S$, infatti se $x, y \notin P$ allora $xy \notin P$ poiché $P$ è un ideale primo.

Per quanto già visto, sappiamo che $S^{-1}\mathbb{Z}$ è un anello contenente un unico ideale massimale, detto anche **anello locale**. Più precisamente, tale ideale è $S^{-1}\mathbb{Z} \setminus (S^{-1}\mathbb{Z})^*$ e il gruppo degli elementi invertibili è

$$(S^{-1}\mathbb{Z})^* = \left\{ \frac{a}{s} \;\middle|\; a, s \in S \right\}$$

Inoltre, gli ideali di $S^{-1}\mathbb{Z}$ sono tutti della forma $S^{-1}(m)$ con $(m) \subseteq \mathbb{Z}$ un ideale, e vale

$$S^{-1}(m) = \left\{ \frac{mk}{s} \;\middle|\; k \in \mathbb{Z}, s \in S \right\} = \left\{ m\frac{k}{s} \;\middle|\; \frac{k}{s} \in S^{-1}\mathbb{Z} \right\} = (m)S^{-1}\mathbb{Z}$$

Vediamo un esempio esplicito per $P = (2)$, descrivendo esplicitamente gli ideali di $S^{-1}\mathbb{Z}$.

$$S^{-1}\mathbb{Z} = \left\{ \frac{m}{s} \;\middle|\; s \text{ dispari} \right\}$$

Per prima cosa osserviamo che la corrispondenza tra gli ideali di $\mathbb{Z}$ e quelli di $S^{-1}\mathbb{Z}$ non è biunivoca, ma solo surgettiva. Infatti alcuni ideali di $\mathbb{Z}$ diventano uguali quando localizziamo l'anello rispetto a $S$, in particolare

$$S^{-1}(m) = S^{-1}(n) \iff \exists u \in (S^{-1}\mathbb{Z})^* \text{ tale che } m = un \iff u = \frac{m}{n} \in (S^{-1}\mathbb{Z})^*$$

dove l'ultima uguaglianza è giustificata dal fatto che $S^{-1}\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, pertanto esiste $\dfrac{m}{n}$ come numero razionale ed è l'unico valore per cui l'equazione è verificata. D'altra parte abbiamo

$$(S^{-1}\mathbb{Z})^* = \left\{ \frac{m}{s} \;\middle|\; m, s \in S \right\} = \left\{ \frac{m}{n} \;\middle|\; m, n \text{ entrambi dispari} \right\}$$

pertanto $S^{-1}(m) = S^{-1}(n)$ se e solo se la massima potenza di due che divide $m$ e $n$ è la stessa[19]. Gli ideali di $S^{-1}\mathbb{Z}$ sono quindi tutti e soli quelli della forma $S^{-1}(2^k)$. Consideriamo la bigezione

$$\{\text{Ideali primi di } S^{-1}\mathbb{Z}\} \longleftrightarrow \{\text{Ideali primi } P \subseteq \mathbb{Z} \mid P \cap S = \emptyset\}$$

poiché gli unici ideali primi di $\mathbb{Z}$ che non intersecano $S = \mathbb{Z} \setminus (2)$ sono $(0)$ e $(2)$, abbiamo che gli unici ideali primi di $S^{-1}\mathbb{Z}$ sono $(0)$ e $S^{-1}(2)$.

[19] In tal caso infatti il razionale $\frac{m}{n}$, se ridotto ai minimi termini, ha numeratore e denominatore entrambi dispari, quindi è un'unità dell'anello.

## §2.3 Ideali massimali e primi di $\mathbb{Z}[x]$

**Lemma 2.3**

Se $A \subseteq R$ sono due anelli e $P \subseteq R$ è un ideale primo di $R$ allora $P \cap A$ è un ideale primo di $A$.

*Dimostrazione.* $P \cap A$ è un ideale di $A$ in quanto controimmagine di $P$ tramite l'omomorfismo di anelli

$$\varphi : A \hookrightarrow R : a \longmapsto a$$

Poiché $P$ è un ideale primo di $R$, per ogni $a, b \in A$ tali che $ab \in P \cap A$ si ha $a \in P$ oppure $b \in P$, cioè $a \in P \cap A$ oppure $b \in P \cap A$, quindi $P \cap A$ è un ideale primo di $A$. $\square$

Consideriamo $P \subseteq \mathbb{Z}[x]$ un ideale primo, studiamo l'intersezione $P \cap \mathbb{Z}$. Questo è un ideale primo di $\mathbb{Z}$ per il Lemma 2.3, pertanto $P \cap \mathbb{Z} = (0)$ oppure esiste un primo $p \in \mathbb{Z}$ tale che $P \cap \mathbb{Z} = (p)$. Se non è l'ideale nullo allora $(p)\mathbb{Z}[x]$ è un ideale contenuto in $P$, per il Teorema di Corrispondenza gli ideali primi di $\mathbb{Z}[x]$ contenenti $(p)\mathbb{Z}[x]$ sono in bigezione con gli ideali primi del quoziente ${\mathbb{Z}[x]}\big/{(p)\mathbb{Z}[x]} \cong \mathbb{F}_p[x]$ e vale la stessa cosa per gli ideali massimali. Poiché $\mathbb{F}_p[x]$ è un dominio a ideali principali, i suoi ideali primi sono $(\overline{0})$ e quelli generati da un polinomio irriducibile, in particolare tutti i suoi ideali primi non nulli sono anche massimali. Pertanto se $\overline{f(x)} \in \mathbb{F}_p[x]$ è un polinomio irriducibile allora $(\overline{f(x)})$ è un ideale primo di $\mathbb{F}_p[x]$ e quindi $(p, f(x))$ è un ideale primo e massimale di $\mathbb{Z}[x]$. Abbiamo quindi che l'insieme degli ideali massimali di $\mathbb{Z}[x]$ contenenti $p$ è

$$\mathcal{M}_p = \{(p, f(x)) \mid \overline{f(x)} \text{ è irriducibile in } \mathbb{F}_p[x]\}$$

mentre l'insieme degli ideali primi di $\mathbb{Z}[x]$ contenenti $p$ è

$$\mathcal{P}_p = \mathcal{M}_p \cup \{(p)\mathbb{Z}[x]\}$$

Supponiamo adesso che $P$ sia un ideale primo di $\mathbb{Z}[x]$ tale che $P \cap \mathbb{Z} = (0)$. $S = \mathbb{Z} \setminus \{0\}$ è una parte moltiplicativa di $\mathbb{Z}$ e l'ipotesi appena data su $P$ può essere espressa come $P \cap S = \emptyset$. Consideriamo la bigezione

$$\{\text{Ideali primi di } S^{-1}\mathbb{Z}[x]\} \longleftrightarrow \{\text{Ideali primi } P \subseteq \mathbb{Z}[x] \mid P \cap S = \emptyset\} : \mathfrak{P} \longmapsto \mathfrak{P} \cap \mathbb{Z}[x]$$

poiché $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$ abbiamo che $P$ corrisponde a un unico ideale primo di $\mathbb{Q}[x]$. Essendo $\mathbb{Q}[x]$ un dominio a ideali principali, questi sono l'ideale nullo e gli ideali generati da polinomi irriducibili. Se $f(x) \in \mathbb{Q}[x]$ è un polinomio irriducibile il cui ideale corrisponde a $P$ allora, posto $m$ il minimo comune denominatore dei suoi coefficienti, abbiamo che $P = (f(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Q}[x] \cap \mathbb{Z}[x] = (mf(x))\mathbb{Z}[x]$. In particolare $P$ è generato da un polinomio irriducibile. Gli ideali primi di $\mathbb{Z}[x]$ possono quindi avere la seguente forma:

- $(0)$;
- $(p)\mathbb{Z}[x]$ con $p \in \mathbb{Z}$ primo;
- $(p, f(x))$ con $p \in \mathbb{Z}$ primo e $\overline{f(x)}$ irriducibile in $\mathbb{F}_p[x]$;
- $(f(x))$ con $f(x)$ irriducibile in $\mathbb{Z}[x]$.

Mostriamo che gli ideali primi di quest'ultimo tipo non sono massimali.
Siano $f(x) \in \mathbb{Z}[x]$ un polinomio irriducibile, non costante, $a \in \mathbb{Z}$ tale che $f(a) \notin \{-1, 0, 1\}$, $p \in \mathbb{Z}$ un primo che divide $f(a)$ e consideriamo le applicazioni

$$\varphi : \mathbb{Z}[x] \longrightarrow {}^{\mathbb{Z}[x]}\!\big/_{(p)\mathbb{Z}[x]} : g(x) \longmapsto \overline{g(x)}$$

$$\psi : {}^{\mathbb{Z}[x]}\!\big/_{(p)\mathbb{Z}[x]} \longrightarrow \mathbb{F}_p : \overline{g(x)} \longmapsto g(a)$$

Osserviamo che $(\psi \circ \varphi)(f(x)) = f(a) \equiv 0 \pmod p$ e che $(\psi \circ \varphi)(p) = p \equiv 0 \pmod p$, pertanto $p, f(x) \in \ker \psi \circ \varphi$ e quindi $(p, f(x)) \subseteq \ker(\psi \circ \varphi) \neq \mathbb{Z}[x]$. Abbiamo quindi $(f(x)) \subseteq (p, f(x))$, se $(f(x))$ fosse massimale allora conterrebbe $p$, che è assurdo in quanto $\deg f \geq 1$.

Poiché gli ideali di questo tipo non sono massimali, gli ideali massimali di $\mathbb{Z}[x]$ sono tutti e soli quelli della forma

$$(p, f(x)) \text{ con } \overline{f(x)} \text{ irriducibile in } \mathbb{F}_p[x]$$

## §2.4 Criterio di Eisenstein

Conosciamo il Criterio di Eisenstein per verificare che un polinomio a coefficienti interi è irriducibile in $\mathbb{Z}[x]$. Lo stesso risultato vale in generale in ogni anello UFD con praticamente la stessa dimostrazione, che ricordiamo.

**Proposizione 2.4** (Criterio di Eisenstein)

Siano $A$ un UFD, $p \in A$ un elemento primo e $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio a coefficienti in $A$ se sono verificate le ipotesi

- $p \nmid a_n$;
- $p \mid a_i$ per $i \in \{0, \ldots, n-1\}$;
- $p^2 \nmid a_0$;

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

## §2.5 Domini a ideali principali

**Proposizione 2.5**
Sia $A$ un PID, ogni ideale primo diverso da $(0)$ di $A$ è un ideale massimale

*Dimostrazione.* Sia $P = (p)$ un ideale primo non nullo, supponiamo per assurdo che esista un ideale $M$ tale che

$$P \subsetneq M \subsetneq A$$

Poiché $A$ è un dominio a ideali principali, esiste $x \in A$ tale che $M = (x)$, quindi $x \mid p$ dato che $P \subsetneq M$. Poiché $P$ è un ideale primo si ha che $p \in A$ è un elemento primo, quindi irriducibile. Sia $q \in A$ tale che $p = xq$, dato che $x \notin A^*$ abbiamo che $q \in A^*$, cioè $(x) = (p)$, che è assurdo. □

**Corollario 2.6**
Siano $A$ un PID e $B$ un dominio di integrità e $\varphi : A \longrightarrow B$ un omomorfismo di anelli surgettivo, allora $\varphi$ è un isomorfismo oppure $B$ è un campo.

*Dimostrazione.* Notiamo che $\ker \varphi$ è un ideale primo di $A$ in quanto $A/_{\ker \varphi} \cong B$ è un dominion di integrità. Se $\ker \varphi = (0)$, allora $\varphi$ è un isomorfismo di anelli. Altrimenti $\ker \varphi$ è un ideale massimale, pertanto $A/_{\ker \varphi} \cong B$ è un campo. □

**Corollario 2.7**
Se $C$ è un anello tale che $C[x]$ è un PID, allora $C$ è un campo.

*Dimostrazione.* Dall'inclusione $C \subseteq C[x]$ abbiamo che $C$ è un dominio di integrità. L'ideale $(x)$ è quindi primo in $C[x]$ in quanto $C[x]/_{(x)} \cong C$ è un dominio, quindi è massimale dato che $C[x]$ è un PID. Pertanto $C$ è un campo. □

## §2.6 Operazioni tra ideali

Ricordiamo che in un anello commutativo con identità $A$, sono ben definite le seguenti operazioni su due ideali $I, J$ e danno luogo a un terzo ideale (possibilmente uguale a uno dei due):

- $I \cap J = \{k \in A \mid k \in I, k \in J\}$;
- $I + J = (I, J) = \{i + j \mid i \in I, j \in J\}$;
- $IJ = (\{ij \mid i \in I, j \in J\})$;
- $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} \text{ per cui } x^n \in I\}$;
- $(I : J) = \{x \in A \mid xJ \subseteq I\}$.

**Proposizione 2.8**

Dati $A$ un anello commutativo con identità, $I, J \subseteq A$ due ideali, allora

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

*Dimostrazione.* Poiché vale l'inclusione $IJ \subseteq I \cap J$ abbiamo che $\sqrt{IJ} \subseteq \sqrt{I \cap J}$. Viceversa, se $a \in \sqrt{I \cap J}$ allora esiste $n \in \mathbb{N}$ tale che $a^n \in I \cap J$, allora abbiamo

$$a^{2n} = \underbrace{a^n}_{\in I} \cdot \underbrace{a^n}_{\in J} \in IJ$$

da cui $\sqrt{I \cap J} \subseteq \sqrt{IJ}$ e quindi l'uguaglianza.
Consideriamo adesso $b \in \sqrt{I} \cap \sqrt{J}$, allora esistono $m, n \in \mathbb{N}$ tali che $b^m \in I$ e $b^n \in J$, da cui

$$b^{m+n} = \underbrace{b^m}_{\in I} \cdot \underbrace{b^n}_{\in J} \in I \cap J$$

Pertanto $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$. Viceversa, Se $c \in \sqrt{I \cap J}$ allora esiste $n \in \mathbb{N}$ tale che $c^n \in I \cap J$, in particolare $c^n \in I$ e $c^n \in J$, quindi $c \in \sqrt{I} \cap \sqrt{J}$, da cui l'uguaglianza. □

**Proposizione 2.9**

Dato $A$ un anello commutativo con identità, allora

$$\sqrt{(0)} = \bigcap_{\substack{P \subseteq A \\ P \text{ ideale primo}}} P$$

*Dimostrazione.* Sia $X$ l'intersezione di tutti gli ideali primi di $A$. Se $x \in \sqrt{(0)}$ allora esiste $n \in \mathbb{N}$ tale che $x^n = 0$, procediamo per induzione su $n$. Se $n = 1$ allora $x = 0$, quindi $x$ è contenuto in tutti gli ideali di $A$, in particolare in quelli primi. Se $n > 1$, supponiamo che se $x^{n-1} \in X$ allora $x \in X$. Per ogni ideale primo $P$, poiché $x^n = 0$ si ha che $x^n$ è contenuto nella loro intersezione, da cui almeno uno tra $x$ e $x^{n-1}$ è un elemento di $X$. Se $x^{n-1} \in X$ allora $x \in X$ per ipotesi induttiva, pertanto $\sqrt{(0)} \subseteq X$. Viceversa, mostriamo che se $x \notin \sqrt{(0)}$ allora esiste un ideale primo $P$ tale che $x \notin P$. Consideriamo l'insieme

$$\mathcal{F} = \{I \subseteq A \mid I \text{ ideale}, x^n \notin I \ \forall n \in \mathbb{N}\}$$

notiamo che $\mathcal{F}$ è non vuoto in quanto contiene l'ideale nullo. Posta $\mathscr{C} = \{I_i\}$ una catena di ideali tali che $I_i \subseteq I_{i+1}$, sia

$$\mathcal{I} = \bigcup I_i$$

Per costruzione $\mathcal{I}$ è un maggiorante per $\mathscr{C}$ in quanto ogni $I_i$ è contenuto in $\mathcal{I}$, inoltre $\mathcal{I}$ è un ideale di $A$ dato che $I_i \subseteq I_{i+1}$. L'ideale $\mathcal{I}$ è un elemento di $\mathcal{F}$, infatti se le potenze di $x$ non sono elementi degli ideali di $\mathcal{F}$, a maggior ragione non sono contenute in $\mathcal{I}$. Pertanto ogni catena $\mathscr{C}$ di $\mathcal{F}$ ammette un maggiorante in $\mathscr{C}$, pertanto per il Lemma di Zorn esiste un ideale $M$ massimale in $\mathcal{F}$. Mostriamo che $M$ è un ideale primo di $A$. Siano $a, b \in A$ tali che $ab \in M$, supponiamo per assurdo $a \notin M$ e $b \notin M$, allora $M$ è contenuto strettamente negli ideali $(M, a), (M, b)$. Poiché $M$ è massimale in $\mathcal{F}$, esistono $h, k \in \mathbb{N}$ tali che $x^k \in (M, a)$ e $x^h \in (M, b)$, da cui

$$x^{h+k} \in (M, a)(M, b) \subseteq M$$

che è assurdo in quanto $M$ è un elemento di $\mathcal{F}$. Pertanto $M$ è un ideale primo di $A$ che non contiene nessuna potenza di $x$, da cui segue la tesi. □

**Corollario 2.10**

Dati $A$ un anello commutativo con identità e $I \subseteq A$ un ideale, allora

$$\sqrt{I} = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P$$

*Dimostrazione.* Consideriamo l'omomorfismo di proiezione

$$\pi : A \longrightarrow A/I$$

osserviamo che $\sqrt{I} = \pi^{-1}(\sqrt{(0)})$, dove $\sqrt{(0)}$ è il radicale di 0 in $A/I$. Per la Proposizione 2.9 abbiamo

$$\sqrt{I} = \pi^{-1}(\sqrt{(0)}) = \pi^{-1}\left( \bigcap_{\substack{P \subseteq A/I \\ P \text{ ideale primo}}} P \right) = \bigcap_{\substack{P \supseteq I \\ P \subseteq A \text{ ideale primo}}} P$$

□

Grazie a questo risultato, possiamo classificare gli elementi invertibili degli anelli di polinomi.

**Proposizione 2.11**

Se $A$ è un anello commutativo con identità allora

$$A[x]^* = \left\{ p(x) = \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_0 \in A^*, a_i \in \sqrt{0}\ \forall i \in \{1, \dots, n\} \right\}$$

*Dimostrazione.* Sia $X$ l'insieme definito come sopra. Consideriamo $p(x) = \sum_{i=0}^{n} a_i x^i$ un elemento di $X$, poiché $a_0 \in A^*$ possiamo scrivere

$$a_0^{-1} p(x) = 1 + \sum_{i=1}^{n} a_i' x^i \qquad a_i' = \frac{a_i}{a_0} \ \forall i \in \{1, \dots, n\}$$

poniamo $t = -\sum_{i=1}^{n} a_i' x^i$. Notiamo che $t$ è nilpotente in quanto tutti i coefficienti $a_i'$ sono nilpotenti e l'insieme dei nilpotenti è un ideale. Fissiamo $m \in \mathbb{N}$ tale che $t^m = 0$, dalla fattorizzazione

$$1 - t^m = (1 - t) \left( \sum_{i=0}^{m-1} t^i \right)$$

otteniamo

$$1 = a_0^{-1} p(x) \left( \sum_{i=0}^{m-1} t^i \right)$$

in particolare $p(x) \in A[x]^*$ e quindi $X \subseteq A[x]^*$.
Viceversa, siano $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ un elemento di $A[x]^*$ e $g(x) = f(x)^{-1}$, allora $f(x)g(x) = 1$. Notiamo che $\alpha_0 \in A^*$, infatti valutando i due polinomi in 0 abbiamo

$$f(0)g(0) = a_0 g(0) = 1$$

Sia $P \subsetneq A$ un ideale primo, $P[x]$ è un ideale primo di $A[x]$, riduciamo l'espressione $f(x)g(x)$ modulo $P[x]$ tramite l'omomorfismo di proiezione

$$\pi : A[x] \longrightarrow {}^{A}\!/_{P}[x] \cong {}^{A[x]}\!/_{P[x]}$$

Abbiamo $\pi(f(x))\pi(g(x)) = \pi(1)$, cioè $\pi(f(x))$ è invertibile in ${}^{A}\!/_{P}[x]$, da cui otteniamo $\pi(f(x)) \in ({}^{A}\!/_{P})^*$ in quanto ${}^{A}\!/_{P}$ è un dominio di integrità. Allora abbiamo $a_i \in P$ per ogni $i \in \{1, \dots, n\}$, in particolare tali coefficienti sono contenuti nell'intersezione di tutti gli ideali primi di $A$ per l'arbitrarietà di $P$, sono quindi nilpotenti per la Proposizione 2.9. Vale quindi l'inclusione $A[x]^* \subseteq X$, da cui l'uguaglianza. □

**Proposizione 2.12**

Siano $A$ un anello commutativo con identità e $I, J, K \subseteq A$ ideali. Valgono i seguenti fatti:

(1) se $I + J + K = A$ allora $I^n + J^n + K^n = A$ per ogni $n \geq 1$;

(2) se $I + J = J + K = I + K = A$ allora $IJ + JK + IK = A$.

*Dimostrazione.* Mostriamo i due fatti separatamente:

(1) poiché $I + J + K = A$ esistono $i \in I, j \in J, k \in K$ tali che $i + j + k = 1$. Consideriamo la potenza

$$(i + j + k)^N = \sum_{x+y+z=N} \binom{N}{x, y, z} i^x j^y k^z \text{[20]}$$

[20] Ricordiamo che $\binom{N}{x, y, z} = \frac{N!}{x!\, y!\, z!}$.

Se $N \geq 3n$ osserviamo che $\max x, y, z \geq n$ per ogni $x, y, z \in \mathbb{N}$ tali che $x+y+z = N$, pertanto scegliendo $N$ in questo modo abbiamo che $(i + j + k)^N = 1$ è un elemento di $I^n + J^n + K^n$, quindi l'ideale coincide con $A$;

(2) dalle ipotesi esistono $i_1, i_2 \in I, j_1, j_2 \in J, k_1, k_2 \in K$ tali che

$$i_1 + j_1 = 1 \qquad j_2 + k_1 = 1 \qquad i_2 + k_2 = 1$$

Per la proprietà di assorbimento degli ideali $IJ, JK, IK$, svolgendo i calcoli si ha

$$1 = (i_1 + j_1)(j_2 + k_1)(i_2 + k_2) \in IJ + JK + IK$$

$\square$

## §2.7 Interi di Gauss

Consideriamo l'anello degli Interi di Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, abbiamo visto che $\mathbb{Z}[i]$ è un dominio euclideo e la sua funzione grado è

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N} : a + ib \longmapsto a^2 + b^2$$

che chiamiamo **norma**. Notiamo che questa norma è il quadrato dell'usuale norma complessa, pertanto è una funzione moltiplicativa.

### §2.7.1 Elementi primi

**Lemma 2.13**

Il gruppo degli elementi invertibili di $\mathbb{Z}[i]$ è $\{1, -1, i, -i\}$.

*Dimostrazione.* Chiaramente $\{1, -1, i, -i\} \subseteq \mathbb{Z}[i]^*$, mostriamo quindi l'altra inclusione. Sia $a + ib \in \mathbb{Z}[i]^*$, allora esistono $c, d \in \mathbb{Z}$ tali che $(a + ib)(c + id) = 1$, passando alle norme otteniamo l'equazione

$$(a^2 + b^2)(c^2 + d^2) = 1$$

da cui ricaviamo $a^2 + b^2 = c^2 + d^2 = 1$, quindi $a + bi \in \{1, -1, i, -i\}$. □

**Lemma 2.14**

Dato $p \in \mathbb{Z}$ un primo, se $p \equiv 3 \pmod 4$ allora $p$ è irriducibile in $\mathbb{Z}[i]$.

*Dimostrazione.* Supponiamo per assurdo che $p$ non sia irriducibile in $\mathbb{Z}[i]$, scriviamo quindi la fattorizzazione

$$p = (a + ib)(c + id)$$

con entrambi i fattori non invertibili, passando alle norme otteniamo l'equazione

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

Poiché gli elementi invertibili di $\mathbb{Z}[i]$ coincidono con gli elementi di norma 1, abbiamo $a^2 + b^2 = c^2 + d^2 = p$. Quindi

$$a^2 + b^2 = p \equiv 3 \pmod 4$$

ma questo è assurdo in quanto gli unici quadrati in $\mathbb{Z}/4\mathbb{Z}$ sono 0 e 1. □

**Lemma 2.15**

Dato $a + ib \in \mathbb{Z}[i]$, se $N(a + ib)$ è primo in $\mathbb{Z}$ allora $a + ib$ è irriducibile in $\mathbb{Z}[i]$.

*Dimostrazione.* Fattorizziamo $a + ib$ come

$$a + ib = (c + id)(e + if)$$

passando alle norme otteniamo l'equazione

$$a^2 + b^2 = (c^2 + d^2)(e^2 + f^2)$$

Dato che $a^2 + b^2$ è primo in $\mathbb{Z}$ (quindi irriducibile in $\mathbb{Z}$) abbiamo che almeno uno dei due fattori ha norma 1, cioè è invertibile e quindi $a + ib$ è irriducibile in $\mathbb{Z}[i]$. □

**Lemma 2.16**
Valgono i seguenti fatti:

(1) $1+i$ è irriducibile in $\mathbb{Z}[i]$;

(2) $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$;

(3) $\dfrac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{F}_2$;

*Dimostrazione.* Mostriamo i tre fatti separatamente:

(1) poiché $N(1+i) = 2$, per il Lemma 2.14 abbiamo che $1+i$ è irriducibile in $\mathbb{Z}[i]$;

(2) Notiamo che $2 = -i(1+i)^2 = i(1-i)^2$, pertanto

$$(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = (1-i)^2\mathbb{Z}[i]$$

(3) Consideriamo l'isomorfismo

$$\varphi : \mathbb{Z}[i] \longrightarrow \frac{\mathbb{Z}[x]}{(x^2+1)} : a+bi \longmapsto \overline{a+bx}$$

tramite $\varphi$ abbiamo

$$\frac{\mathbb{Z}[i]}{(1+i)} \cong \frac{\mathbb{Z}[x]}{(x^2+1, 1+x)}$$

Notiamo che 2 è un elemento dell'ideale $(x^2+1, 1+x)$, in quanto possiamo scrivere

$$2 = x^2+1 - x(x+1) + x + 1$$

Pertanto

$$\frac{\mathbb{Z}[i]}{(i+1)} \cong \frac{\mathbb{Z}[x]}{(2, 1+x)} \cong \frac{\mathbb{Z}[x]/(2)}{(2, 1+x)/(2)} \cong \frac{\mathbb{F}_2[x]}{(1+x)} \cong \mathbb{F}_2$$

□

**Lemma 2.17**
Sia $p \in \mathbb{Z}$ un primo, se $p \equiv 1 \pmod 4$ allora $p = (a+bi)(a-bi)$ con $a+bi, a-bi \in \mathbb{Z}[i]$ primi e non associati.

*Dimostrazione.* Poiché $p \equiv 1 \pmod 4$ esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \pmod p$, da cui $p \mid x^2+1$. Fattorizziamo $x^2+1$ in $\mathbb{Z}[i]$ come

$$x^2+1 = (x+i)(x-i)$$

notiamo che $p \nmid x+i$ e $p \nmid x-i$, pertanto $p$ non è primo in $\mathbb{Z}[i]$. In particolare possiamo scrivere

$$p = (a+bi)(c+di)$$

con $a+bi, c+di \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$. Passando alle norme abbiamo

$$p^2 = (a^2+b^2)(c^2+d^2)$$

da cui $a^2 + b^2 = c^2 + d^2 = p$ in quanto nessuno dei due fattori è invertibile. Abbiamo quindi

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

notiamo che $a + bi$ e $a - bi$ sono primi in $\mathbb{Z}[i]$ in quanto la loro norma è un primo di $\mathbb{Z}$. Supponiamo per assurdo che esista $u \in \mathbb{Z}[i]^*$ tale che $a + bi = u(a - bi)$, distinguiamo i vari casi:

- se $u = 1$ allora $a + bi = a - bi$, da cui $b = 0$ e quindi $p = a^2$, che è assurdo in quanto $p$ è irriducibile in $\mathbb{Z}$;
- se $u = -1$ allora $a + bi = -a + bi$, da cui $a = 0$ e quindi $p = b^2$, che è assurdo in quanto $p$ è irriducibile in $\mathbb{Z}$;
- se $u = i$ allora $a + bi = ai + b$, da cui $a = b$ e quindi $p = 2a^2$, che è assurdo in quanto $p$ è dispari;
- se $u = -i$ allora $a + bi = -ai - b$, da cui $a = -b$ e quindi $p = 2a^2$, che è assurdo in quanto $p$ è dispari.

Pertanto $a + bi$ e $a - bi$ sono primi di $\mathbb{Z}[i]$ non associati. □

**Proposizione 2.18**

Gli elementi primi di $\mathbb{Z}[i]$ sono, a meno di associati, tutti e soli gli elementi della forma

- $1 + i$;
- i primi $p$ di $\mathbb{Z}$ tali che $p \equiv 3 \pmod 4$;
- $a + bi, a - bi \in \mathbb{Z}[i]$ tali che $a^2 + b^2 = p$ è un primo di $\mathbb{Z}$ con $p \equiv 1 \pmod 4$.

*Dimostrazione.* Per quanto visto nei lemmi precedenti sappiamo che gli elementi della forma descritta sopra sono tutti primi di $\mathbb{Z}[i]$, vediamo che effettivamente non ne esistono altri.
Sia $a + bi \in \mathbb{Z}[i]$ un primo, fattorizziamo in primi di $\mathbb{Z}$ la norma di $a + bi$

$$a^2 + b^2 = \prod_{j=1}^{k} p_j^{e_j}$$

Poiché $a + bi \mid a^2 + b^2$ in $\mathbb{Z}[i]$, poiché primo si ha che esiste $j_0 \in \{1, \ldots, k\}$ tale che $a + bi \mid p_{j_0}$, distinguiamo tre casi:

- se $p_{j_0} \equiv 3 \pmod 4$ allora $p_{j_0}$ è irriducibile in $\mathbb{Z}[i]$, pertanto $a + bi$ è associato a $p_{j_0}$;
- se $p_{j_0} \equiv 1 \pmod 4$ allora si fattorizza in $\mathbb{Z}[i]$ come
$$p_{j_0} = (c + di)(c - di)$$
con $c + di, c - di$ primi, quindi irriducibili, di $\mathbb{Z}[i]$ non associati, pertanto $a + bi$ è associato a uno dei due;
- se $p_{j_0} = 2$ allora $a + bi \mid -i(1 + i)^2$. Poiché $a + bi$ non è invertibile si ha $a + bi \mid 1 + i$, cioè $a + bi$ è associato a $1 + i$.

□

### §2.7.2 Quozienti di $\mathbb{Z}[i]$

Abbiamo visto che $\dfrac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{F}_2$, vogliamo determinare le classi di isomorfismo degli altri quozienti di $\mathbb{Z}[i]$ per ideali primi. Osserviamo che tali quozienti sono campi, infatti in un PID tutti gli ideali primi non nulli sono ideali massimali, pertanto il quoziente per un ideale primo produce un campo. In alternativa possiamo notare che tali quozienti sono dei domini finiti, quindi dei campi.

**Proposizione 2.19**

Sia $p \in \mathbb{Z}$ un primo dispari:

(1) se $p \equiv 3 \pmod 4$ allora ${}^{\mathbb{Z}[i]}\big/_{(p)} \cong \mathbb{F}_{p^2}$;

(2) se $p \equiv 1 \pmod 4$ e $p = (a+bi)(a-bi)$ è la sua fattorizzazione in primi di $\mathbb{Z}[i]$ allora $\dfrac{\mathbb{Z}[i]}{(a+bi)} \cong \mathbb{F}_p$.

*Dimostrazione.* Mostriamo i due fatti separatamente:

(1) possiamo identificare in modo univoco gli elementi di ${}^{\mathbb{Z}[i]}\big/_{(p)}$ con i resti della divisione per $p$, cioè con l'insieme

$$\{a + bi \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1\}$$

che contiene $p^2$ elementi. Poiché il quoziente è un campo di cardinalità $p^2$ si ha

$${}^{\mathbb{Z}[i]}\big/_{(p)} \cong \mathbb{F}_{p^2}$$

(2) poiché $p$ è un elemento dell'ideale $(a+bi)$, per il Secondo Teorema di Omomorfismo abbiamo

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \frac{{}^{\mathbb{Z}[i]}\big/_{(p)}}{{}^{(a+bi)}\big/_{(p)}}$$

Consideriamo solo la struttura di gruppo additivo, il quoziente ${}^{\mathbb{Z}[i]}\big/_{(p)}$ è isomorfo, come gruppo, all'insieme dei resti

$$\{a + bi \mid 0 \leq a \leq p-1, 0 \leq b \leq p-1\}$$

che è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Osserviamo che il quoziente ${}^{(a+bi)}\big/_{(p)}$ ha cardinalità 1, $p$, oppure $p^2$ in quanto, come gruppo, è isomorfo a un sottogruppo di $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Questa non può essere 1 in quanto altrimenti si avrebbe l'identità

$$(a+bi) = ((a+bi)(a-bi))$$

che non è vera in quanto $a+bi$ e $a-bi$ non sono associati. D'altra parte se fosse $p^2$ allora avremmo

$$\frac{{}^{\mathbb{Z}[i]}\big/_{(p)}}{{}^{(a+bi)}\big/_{(p)}} = \{\overline{0}\}$$

che sarebbe assurdo in quanto $a+bi$ non è invertibile. Pertanto abbiamo l'isomorfismo di gruppi

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \frac{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}{\mathbb{Z}/p\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z}$$

Pertanto il quoziente è un anello di cardinalità $p$, da cui necessariamente

$$\frac{\mathbb{Z}[i]}{(a+bi)} \cong \mathbb{F}_p$$

□

**Osservazione 2.20** — Se $p \equiv 1 \pmod 4$, gli anelli $\mathbb{Z}[i]/(p)$ e $\mathbb{F}_p \times \mathbb{F}_p$ sono isomorfi tramite un isomorfismo diverso da quello visto nella dimostrazione. Fattorizziamo in primi $p = (a+bi)(a-bi)$, poiché $\mathbb{Z}[i]$ è un PID gli ideali $(a+bi), (a-bi)$ sono massimali, quindi $(a+bi)+(a-bi) = \mathbb{Z}[i]$. Per il Teorema Cinese del Resto allora

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[i]}{(a+bi)(a-bi)} \cong \frac{\mathbb{Z}[i]}{(a+bi)} \times \frac{\mathbb{Z}[i]}{(a-bi)} \cong \mathbb{F}_p \times \mathbb{F}_p$$

**Osservazione 2.21** — Abbiamo mostrato anche che la cardinalità del quoziente $\mathbb{Z}[i]/(\alpha)$ con $\alpha$ un primo di $\mathbb{Z}[i]$ è uguale a $N(\alpha)$.

**Lemma 2.22**

Siano $A$ un PID e $I \subseteq A$ un ideale. Se il quoziente $A/I$ è finito allora vale

$$\left|A/I^n\right| = \left|A/I\right|^n \text{ [a]}$$

[a] Con $I^n$ intendiamo il prodotto dell'ideale $I$ con se stesso ripetuto $n$ volte.

*Dimostrazione.* Sia $I = (p)$, mostriamo la tesi per induzione su $n$. Consideriamo l'omomorfismo di anelli

$$\varphi : A \longrightarrow A : a \longmapsto ap$$

e la proiezione al quoziente

$$\pi : A \longrightarrow A/I^2 : a \longmapsto a + I^2$$

Il nucleo della loro composizione è

$$\ker \pi \circ \varphi = \{a \in A \mid pa \in I^2 = (p^2)\} = \{a \in A \mid a = pb, b \in A\} = I$$

e l'immagine è

$$\pi(\varphi(A)) = \pi(pA) = \pi(I) = I/I^2$$

Per il Primo Teorema di Omomorfismo allora

$$A/I \cong I/I^2$$

pertanto

$$A/I \cong \frac{A/I^2}{I/I^2}$$

da cui ricaviamo

$$\left|A/I\right| = \left|\frac{A/I^2}{I/I^2}\right| = \left|\frac{A/I^2}{A/I}\right| = \frac{\left|A/I^2\right|}{\left|A/I\right|}$$

Quindi abbiamo la tesi per $n = 2$:

$$\left|A/I^2\right| = \left|A/I\right|^2$$

Per $n > 2$, supponiamo che la tesi sia valida per $n - 1$. Consideriamo gli omomorfismi

$$\varphi : A \longrightarrow A : a \longmapsto p^{n-1}a$$

$$\pi : A \longrightarrow A/I^n : a \longmapsto a + I^n$$

Il nucleo e l'immagine della loro composizione sono

$$\ker \pi \circ \varphi = \{a \in A \mid p^{n-1}a \in I^n = (p^n)\} = I$$

$$\pi(\varphi(A)) = \pi(p^{n-1}A) = \pi(I^{n-1}) = I^{n-1}/I^n$$

Pertanto abbiamo l'isomorfismo

$$A/I \cong I^{n-1}/I^n$$

da cui, come sopra,

$$\left|A/I\right| = \frac{\left|A/I^n\right|}{\left|A/I^{n-1}\right|} = \frac{\left|A/I^n\right|}{\left|A/I\right|^{n-1}}$$

Da cui la tesi. □

Consideriamo adesso il quoziente di $\mathbb{Z}[i]$ per un generico ideale $I = (z)$, fattorizziamo $z$ in primi di $\mathbb{Z}[i]$:

$$z = u(1+i)^e \prod_{j=1}^{r} (a_j + b_j i)^{e_j} \prod_{h=1}^{s} p_h^{l_h} \qquad u \in \mathbb{Z}[i]^*$$

Gli ideali $(1+i)^e, (a_j + b_j i)^{e_j}, (p^{e_h})$ sono generati da elementi a due a due coprimi, quindi per il Teorema Cinese del Resto

$$\mathbb{Z}[i]/I \cong \frac{\mathbb{Z}[i]}{(1+i)^e} \times \prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j + b_j i)^{e_j}} \times \prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{l_h}}$$

La cardinalità di questo quoziente è $N(z)$, infatti applicando il Lemma 2.21 abbiamo

$$\begin{aligned}
\left|{}^{\mathbb{Z}[i]}\!/_{I}\right| &= \left|\frac{\mathbb{Z}[i]}{(1+i)^e}\right| \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_j i)^{e_j}}\right| \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)^{e_h}}\right| = \\
&= \left|\frac{\mathbb{Z}[i]}{(1+i)}\right|^e \cdot \left|\prod_{j=1}^{r} \frac{\mathbb{Z}[i]}{(a_j+b_j i)}\right|^{e_j} \cdot \left|\prod_{h=1}^{s} \frac{\mathbb{Z}[i]}{(p)}\right|^{e_h} = \\
&= N(1+i)^e \prod_{j=1}^{r} N(a_j+b_j i)^{e_j} \prod_{h=1}^{s} N(p_h)^{e_h} = \\
&= N\left(u(1+i)^e \prod_{j=1}^{r} (a_j+b_j i)^{e_j} \prod_{h=1}^{s} p_h^{e_h}\right) = N(z)
\end{aligned}$$

## §2.8 Esempio di dominio non euclideo

Consideriamo l'anello $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, vogliamo mostrare che non è un dominio euclideo.

**Proposizione 2.23**

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\frac{1+\sqrt{-19}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

*Dimostrazione.* Sia $\alpha = \frac{1+\sqrt{-19}}{2}$, il polinomio minimo di $\alpha$ su $\mathbb{Q}$ è $\mu(x) = x^2 - x + 5$. Consideriamo l'omomorfismo di valutazione

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C} : p(x) \longmapsto p(\alpha) \qquad \mathrm{Im}\varphi = \mathbb{Z}[\alpha]$$

poiché $\varphi$ è la restrizione dell'usuale omomorfismo di valutazione su $\mathbb{Q}[x]$, che è un PID, abbiamo

$$\ker\varphi = \mathbb{Z}[x] \cap \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\} = \mathbb{Z}[x] \cap (x^2 - x + 5)\mathbb{Q}[x] = (x^2 - x + 5)\mathbb{Z}[x]$$

dove l'ultima uguaglianza è giustificata dal fatto che $\mu(x)$ è un polinomio a coefficienti interi primitivo e per il Lemma di Gauss. Pertanto per il Primo Teorema di Omomorfismo abbiamo

$$\{a + b\alpha \mid a, b \in \mathbb{Z}\} = \frac{\mathbb{Z}[x]}{(x^2 - x + 5)} \cong \mathrm{Im}\varphi = \mathbb{Z}[\alpha]$$

□

**Osservazione 2.24** — Il risultato appena visto non è un fatto ovvio. Consideriamo $\beta = \frac{1+\sqrt{3}}{2}$, il suo polinomio minimo su $\mathbb{Q}$ è $\mu(x) = x^2 - x - \frac{1}{2}$. Ragionando in modo analogo a quanto fatto sopra, il nucleo della valutazione in $\beta$ è

$$\mathbb{Z}[x] \cap \left(x^2 - x - \frac{1}{2}\right)\mathbb{Q}[x] = (2x^2 - 2x - 1)\mathbb{Z}[x]$$

E $\frac{\mathbb{Z}[x]}{(2x^2 - x - 1)} \cong \mathbb{Z}[\beta]$. D'altra parte

$$\mathbb{Z}[\beta] \neq \{a + b\beta \mid a, b \in \mathbb{Z}\}$$

in quanto il quoziente $\frac{\mathbb{Z}[x]}{(2x^2 - x - 1)}$ contiene delle classi di resto della forma $\overline{x^k}$ per ogni $k \in \mathbb{N}$, in quanto $x^k$ e $2x^2 - x - 1$ sono coprimi in $\mathbb{Z}[x]$. Notiamo che il risultato di sopra non è valido in questo caso in quanto il polinomio minimo di $\beta$ non ha coefficienti interi.

Mostriamo che $A$ non è un domino euclideo. Sia $\omega = \frac{1+\sqrt{-19}}{2}$, consideriamo l'applicazione

$$N : A \longrightarrow \mathbb{N} : a + b\omega \longmapsto (a + b\omega)(a + b\overline{\omega}) = a^2 + 5b^2 + ab$$

$N$ è la restrizione all'anello $A$ dell'usuale norma su $\mathbb{C}$, pertanto è moltiplicativa. Osserviamo inoltre che se $u \in A^*$ si ha $N(u) = 1$, infatti se $v \in A$ è tale che $uv = 1$ allora $N(uv) = N(u)N(v) = 1$ da cui $N(u) = N(v) = 1$ necessariamente. D'altra parte l'equazione

$$a^2 + ab + 5b^2 = \left(a + \frac{1}{2}b\right)^2 + \frac{19}{4}b^2 = 1$$

ha soluzione se e solo se $a = \pm 1$ e $b = 0$, pertanto $A^* = \{-1, 1\}$.

Supponiamo per assurdo che $A$ sia un dominio euclideo, cioè che esista un'applicazione

$$\mathcal{N} : A \setminus \{0\} \longrightarrow \mathbb{N}$$

che rispetta gli assiomi di norma euclidea, ricordiamo che gli elementi invertibili di $A^*$ sono gli elementi di norma $\mathcal{N}$ minima. Consideriamo l'insieme $X = \{\mathcal{N}(x) \mid x \in A \setminus A^*\}$, poiché $X$ è un sottoinsieme non vuoto di $\mathbb{N}$ esiste un elemento minimo $m \in X$, sia $x \in A \setminus A^*$ tale che $\mathcal{N}(x) = m$. Per definizione di dominio euclideo, per ogni $a \in A$ esistono $q, r \in A$ tali che $a = qx + r$, con $r = 0$ oppure $\mathcal{N}(r) < \mathcal{N}(x)$. Se $r \neq 0$ allora $r \in A^*$ per minimalità di $\mathcal{N}(x)$, pertanto l'insieme dei possibili resti della divisione per $x$ è $\{0, 1, -1\}$. Abbiamo quindi che l'insieme $\{0, 1, -1\}$ è un insieme di rappresentanti, possibilmente con ripetizioni, per gli elementi del quoziente ${}^{A}\!/_{(x)}$, che è quindi isomorfo a $\mathbb{F}_2$ oppure $\mathbb{F}_3$.
Il polinomio $\mu(x) = x^2 - x + 5$ ha come soluzioni in $A$ $\omega$ e $\overline{\omega}$, pertanto è riducibile in $A[x]$. Da questo si ricava che le classi di $\omega$ e $\overline{\omega}$ nel quoziente ${}^{A}\!/_{(x)}$ sono le radici della classe del polinomio $\mu(x)$, che è assurdo in quanto $\mu(x)$ è irriducibile in $\mathbb{F}_2[x]$ e in $\mathbb{F}_3[x]$. Pertanto $A$ non è un dominio euclideo.

# §3 Campi

## §3.1 Estensioni normali

Ricordiamo che un'estensione di campi algebrica ${}^{L}\!/_{K}$ si dice **normale** se per ogni immersione $\varphi : L \hookrightarrow \overline{K}$ tale che $\varphi_{|K} = id_K$ vale $\varphi(L) = L$. Diciamo che l'estensione è **separabile** se il polinomio minimo su $K$ di ogni elemento di $K$ ha radici distinte nel suo campo di spezzamento. Diciamo anche che un polinomio è separabile su $K$ se le sue radici in $\overline{K}$ sono tutte distinte. Chiamiamo **estensione di Galois finita** un'estensione di campi finita che sia normale e separabile. I campi che considereremo saranno sempre **campi perfetti**, cioè tutte le estensioni saranno separabili.

**Esempio 3.1**

${}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}}$ non è un'estensione normale di $\mathbb{Q}$. Infatti, poiché il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $\mu(x) = x^3 - 2$, esistono 3 immersioni $\varphi_i : \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbb{Q}}$ tali che $\varphi_{i|K} = id_K$, $i \in \{0, 1, 2\}$. Poiché il campo $\mathbb{Q}$ è fissato da $\varphi_i$, è sufficiente studiare l'immagine delle radici di $\mu(x)$ tramite le immersioni: le possibili immagini di $\sqrt[3]{2}$ sono $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$. Poiché i tre campi $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\zeta_3), \mathbb{Q}(\sqrt[3]{2}\zeta_3^2)$ sono diversi, l'estensione non è normale.

**Esempio 3.2**

${}^{\mathbb{Q}(\sqrt{2})}\!/_{\mathbb{Q}}$ è un'estensione normale di $\mathbb{Q}$. Infatti, poiché il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2 - 2$, abbiamo due immersioni $\varphi_1, \varphi_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ che fissano $\mathbb{Q}$ tali che $\varphi_1(\sqrt{2}) = \sqrt{2}$, $\varphi_2(\sqrt{2}) = -\sqrt{2}$. Pertanto le immagini di $\mathbb{Q}(\sqrt{2})$ tramite le immersioni sono

$$\varphi_1(\mathbb{Q}(\sqrt{2})) = \{\varphi_1(a + b\sqrt{2}) \mid a, b \in \mathbb{Q}\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
$$\varphi_2(\mathbb{Q}(\sqrt{2})) = \{\varphi_2(a + b\sqrt{2}) \mid a, b \in \mathbb{Q}\} = \{a - b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

che sono uguali, quindi l'estensione è normale.

Se un'estensione ${}^{L}\!/_{K}$ è normale possiamo definire il **Gruppo di Galois** di ${}^{L}\!/_{K}$ come il gruppo delle immersioni $\varphi : L \hookrightarrow \overline{K}$ che fissano $K$. Questo coincide con il gruppo degli automorfismi di $L$ che fissano $K$, e il suo ordine è pari al grado dell'estensione.

**Osservazione 3.3** — Un'estensione quadratica è sempre un'estensione normale. Infatti se $K$ è un campo (perfetto) e $\alpha \in \overline{K}$ è tale che $\sqrt{\alpha} \notin K$, allora $K(\alpha)$ è il campo di spezzamento del polinomio $x^2 - \alpha$. Quindi ${}^{K(\alpha)}\!/_{K}$ è normale e $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/2\mathbb{Z}$.

Diamo qualche esempio di calcolo del gruppo di Galois di un'estensione.

**Esempio 3.4**

Sia $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ verifichiamo che ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale e calcoliamo $\mathrm{Gal}(L/\mathbb{Q})$. ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale in quanto $L$ è il campo di spezzamento del polinomio $(x^2-2)(x^2-3)$ su $\mathbb{Q}$, pertanto è ben definito il gruppo di Galois dell'estensione, che ha ordine 4 in quanto $[L : \mathbb{Q}] = 4$. Siano $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ una $\mathbb{Q}$-base di $L$ come spazio vettoriale e $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$, poiché $\varphi$ è in particolare un'applicazione lineare è sufficiente determinare la sua immagine sulla base. Abbiamo quindi

$$\varphi(\sqrt{2}) = \pm\sqrt{2}$$
$$\varphi(\sqrt{3}) = \pm\sqrt{3}$$
$$\varphi(\sqrt{6}) = \varphi(\sqrt{2})\varphi(\sqrt{3})$$

in particolare abbiamo al più 4 omomorfismi. D'altra parte $\mathrm{Gal}(L/\mathbb{Q})$ contiene esattamente 4 elementi, quindi questi sono tutti e soli gli automorfismi del campo $L$ che fissano $\mathbb{Q}$. Si verifica che questi omomorfismi, ad eccezione dell'identità, hanno ordine 2, pertanto $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Esempio 3.5**

Sia $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ il campo di spezzamento del polinomio $x^3 - 2$ su $\mathbb{Q}$, ${}^{L}\!/_{\mathbb{Q}}$ è un'estensione normale di $\mathbb{Q}$ e $[L : \mathbb{Q}] = 6$. Esplicitando le radici del polinomio $x^3 - 2$, abbiamo $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$. Sappiamo dalla teoria che $\mathrm{Gal}(L/\mathbb{Q})$ si immerge in $\mathcal{S}_3$, poiché sono entrambi gruppi finiti della stessa cardinalità si ha quindi $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathcal{S}_3$.

**Definizione 3.6.** Dato $p$ un numero primo, l'applicazione

$$\Phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n} : x \longmapsto x^p$$

si dice **automorfismo di Frobenius**

L'automorfismo di Frobenius è effettivamente un automorfismo, poiché $\mathbb{F}_{p^n}$ è un campo finito è sufficiente mostrare che è un omomorfismo iniettivo:

- per ogni $x, y \in \mathbb{F}_{p^n}$
$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$
$$\Phi(x+y) = (x+y)^p \stackrel{[21]}{=} x^p + y^p = \Phi(x) + \Phi(y)$$
pertanto $\Phi$ è un omomorfismo:

- sia $x \in \ker \Phi$, allora
$$\Phi(x) = x^p = 0 \iff x = 0$$
in quanto il polinomio $t^p$ ha 0 come unica radice in $\mathbb{F}_{p^n}$, pertanto $\Phi$ è iniettivo.

**Teorema 3.7**

Per ogni primo $p$, l'estensione ${}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p}$ è normale e $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

[21] Per il Lemma del Binomio Ingenuo.

*Dimostrazione.* L'estensione ${}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_p}$ è normale in quanto $\mathbb{F}_{p^n}$ è, per costruzione, il campo di spezzamento del polinomio $t^{p^n} - t$ su $\mathbb{F}_p$, e il grado di tale estensione è $n$. Osserviamo che l'automorfismo di Frobenius $\Phi$ è un elemento di $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, infatti per ogni $x \in \mathbb{F}_p$ vale $\Phi(x) = x^p = x$ per il Piccolo Teorema di Fermat. L'ordine di $\Phi$ è $n$, infatti

$$\Phi^k = id_{\mathbb{F}_{p^n}} \iff x^{p^k} = x \ \forall x \in \mathbb{F}_{p^n}$$

e l'equazione è verificata se e solo se il polinomio $t^{p^k} - t$ ha almeno $p^n$ radici, cioè se $k \geq n$. D'altra parte l'ordine di $\Phi$ deve dividere $n$, pertanto $\operatorname{ord}\Phi = n$. Quindi $\Phi$ è un generatore di $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, che è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. □

## §3.2 Estensioni ciclotomiche

**Lemma 3.8**

Dato $K$ un campo, il polinomio $x^n - 1$ è separabile su $K$ se e solo se $\operatorname{char} K \nmid n$.

*Dimostrazione.* Per il Criterio della Derivata il polinomio $x^n - 1$ ha radici multiple in $\overline{K}$ se e solo se $(x^n - 1, nx^{n-1}) \neq 1$. Se $\operatorname{char} K = 0$ allora $\mathbb{Q} \subseteq K$ e le radici di $x^n - 1$ sono le $n$ radici complesse dell'unità, che sono tutte distinte. Se $\operatorname{char} K = p$, $p$ primo, allora $(x^n - 1, nx^{n-1}) \neq 1$ se e solo se $p \mid n$, in quanto in quel caso si ha $nx^{n-1} = 0$. □

**Teorema 3.9**

Sia $\zeta_n \in \mathbb{C}$ una radice primitiva $n$-esima dell'unità, allora l'estensione ${}^{\mathbb{Q}(\zeta_n)}\!/_{\mathbb{Q}}$ è normale e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$.

*Dimostrazione.* Poiché $\zeta_n$ è una radice primitiva dell'unità, l'insieme delle sue potenze coincide con l'insieme delle radici del polinomio $x^n - 1$[22], pertanto ${}^{\mathbb{Q}(\zeta_n)}\!/_{\mathbb{Q}}$ è normale in quanto $\mathbb{Q}(\zeta_n)$ è il campo di spezzamento di $x^n - 1$ su $\mathbb{Q}$. Per comodità suddividiamo la dimostrazione in passi:

- mostriamo che $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$. Un'immersione $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ è univocamente determinata dall'immagine di $\zeta_n$, inoltre $\psi(\zeta_n)$ è un elemento dell'insieme $\{\zeta_n^k \mid k = 0, \ldots, n-1\}$ in quanto è radice di $x^n - 1$. Supponiamo per assurdo che $\psi(\zeta_n) = \zeta_n^k$ con $d = (k, n) \neq 1$, allora

$$\psi(\zeta_n^{\frac{n}{d}}) = \psi(\zeta_n)^{\frac{n}{d}} = \zeta^{k\frac{n}{d}} = \zeta^{\frac{k}{d}n} = 1$$

da cui $\zeta_n^{\frac{n}{d}} = 1$ in quanto $\psi$ è iniettiva, quindi ha nucleo banale. Questo è assurdo dato che $\operatorname{ord}\zeta_n = n$. Pertanto $\psi(\zeta_n) \in \{\zeta_n^k \mid k < n, \ (n,k) = 1\}$, quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$;

- siano $p$ un primo che non divide $n$, $f(x)$ e $g(x)$ i polinomi minimi su $\mathbb{Q}$ rispettivamente di $\zeta_n$ e $\zeta_n^p$, osserviamo che $f(x) \mid g(x^p)$ in quanto $g(\zeta_n^p) = 0$;

[22]Ricordiamo che l'insieme delle radici complesse di $x^n - 1$ è un gruppo isomorfo a $\mathbb{Z}/n\mathbb{Z}$, i cui generatori sono le radici primitive.

- supponiamo per assurdo $f(x) \neq g(x)$, allora $f(x)$ e $g(x)$ sono coprimi in $\mathbb{Q}[x]$ ed entrambi dividono $x^n - 1$, pertanto $f(x)g(x) \mid x^n - 1$. Per il Lemma di Gauss esistono $q(x), r(x) \in \mathbb{Z}[x]$ tali che

$$f(x)g(x)q(x) = x^n - 1 \qquad f(x)r(x) = g(x^p)$$

  Riducendo modulo $p$ abbiamo

$$g(x)^p = g(x^p) = f(x)r(x)$$

  in $\mathbb{F}_p[x]$. Pertanto se $\alpha \in \overline{\mathbb{F}_p}$ è una radice di $f(x)$ allora è anche una radice di $g(x)$. Pertanto $\alpha$ è una radice almeno doppia di $x^n - 1 \in \mathbb{F}_p[x]$, che è assurdo in quanto $x^n - 1$ è separabile su $\mathbb{F}_p$ per il Lemma 3.8. Pertanto $f(x) = g(x)$;

- abbiamo quindi che $\zeta_n$ e $\zeta_n^p$ hanno lo stesso polinomio minimo su $\mathbb{Q}$. Ripetendo lo stesso ragionamento con qualsiasi altro primo $q$ che non divide $n$ otteniamo che $\zeta_n$ e $\zeta_n^q$ hanno lo stesso polinomio minimo su $\mathbb{Q}$, quindi questo è valido in generale per $\zeta_n$ e $\zeta_n^k$ con $(n, k) = 1$. In particolare $\zeta_n^k$ è radice di $f(x)$ per ogni $k < n$ con $(n, k) = 1$, pertanto $\deg f \geq \phi(n)$;

- poiché $\deg f = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$ abbiamo che effettivamente $\deg f = \phi(n)$, quindi $\# \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$. Gli elementi di $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sono tutti e soli della forma

$$\psi_k : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}} : \zeta_n \longmapsto \zeta_n^k$$

  con $k < n$ e $(n, k) = 1$, inoltre $\psi_k \circ \psi_h = \psi_{kh} = \psi_{hk}$ in quanto

$$\psi_k(\psi_h(\zeta_n)) = \psi_k(\zeta_n^h) = \psi_k(\zeta_n)^h = \zeta_n^{hk} = \zeta_n^{kh} = \psi_h(\zeta_n^k) = \psi_h(\psi_k(\zeta_n))$$

  abbiamo quindi un isomorfismo

$$\Psi : \mathbb{Z}/n\mathbb{Z}^* \longmapsto \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : k \longmapsto \psi_k$$

□

**Definizione 3.10** (Polinomio ciclotomico)**.** Data $\zeta_n \in \mathbb{C}$ una radice primitiva $n$-esima dell'unità, chiamiamo ***n*-esimo polinomio ciclotomico** il polinomio minimo $\Phi_n(x)$ di $\zeta_n$ su $\mathbb{Q}$.

**Osservazione 3.11** — Poiché gli elementi di $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sono

$$\psi_k : \mathbb{Q}(\zeta_n) \longrightarrow \overline{\mathbb{Q}} : \zeta_n \longmapsto \zeta_n^k$$

per $0 \leq k \leq n$, $(k, n) = 1$, possiamo scrivere $\Phi_n(x)$ come

$$\Phi_n(x) = \prod_{\substack{0 \leq k \leq n \\ (k,n)=1}} (x - \zeta_n^k)$$

Notiamo che le radici di $\Phi_n(x)$ sono tutte e sole le radici primitive $n$-esime dell'unità e che $\deg \Phi_n = \phi(n)$.

**Proposizione 3.12**

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

*Dimostrazione.* Sia $f(x) = \prod_{d|n} \Phi_d(x)$, notiamo che:

- sia $\alpha$ una radice di $x^n - 1$, allora esiste un intero $d$ che divide $n$ tale che $\alpha^d = 1$, pertanto $\alpha$ è una radice primitiva $d$-esima. In particolare ogni radice di $x^n - 1$ è una radice di $f(x)$, cioè $x^n - 1 \mid f(x)$;
- sia $\alpha$ una radice di $f(x)$, allora $\alpha$ è una radice primitiva $d$-esima dell'unità con $d \mid n$, in particolare$\alpha^d = 1$ e quinci $\alpha^n = 1$. Allora $\alpha$ è una radice $n$-esima dell'unità, cioè $f(x) \mid x^n - 1$;
- dai due punti precedenti si deduce che esiste $\lambda \in \mathbb{Q}^*$ tale che $x^n - 1 = \lambda f(x)$, d'altra parte entrambi i polinomi sono monici, quindi $x^n - 1 = f(x)$.

□

**Leonardo Migliorini** (l.migliorini@studenti.unipi.it)
**Gabriel Antonio Videtta** (g.videtta1@studenti.unipi.it)
**Università di Pisa** (Anno Accademico 2022-23)

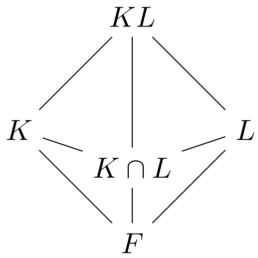

## §3.3 Gruppo di Galois del traslato e del composto

**Proposizione 3.13**
Siano $K/F$ un'estensione di Galois finita e $L/F$ un'estensione finita, allora

(1) $KL/L$ è un'estensione di Galois;

(2) $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$.

*Dimostrazione.* Consideriamo il seguente diagramma di campi, mostriamo i due enunciati separatamente




(1) poiché $K/F$ è un'estensione di Galois finita possiamo scrivere $K$ come $F(\alpha_1, \ldots, \alpha_n)$, dove $\alpha_1, \ldots, \alpha_n \in \overline{K}$ sono le radici di un certo polinomio $p(x) \in F[x]$. Allora abbiamo che $KL = L(\alpha_1, \ldots, \alpha_n)$ è il campo di spezzamento di $p(x)$ su $L$, pertanto $KL/L$ è un'estensione di Galois;

(2) l'estensione $K/K \cap L$ è di Galois, in quanto lo è $K/F$. Consideriamo la mappa di restrizione
$$\Phi : \mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/K \cap L) : \varphi \longmapsto \varphi_{|K}$$
questa è ben definita in quanto ogni immersione $KL \hookrightarrow \overline{F}$ che fissa $L$ fissa anche $K \cap L$. Chiaramente $\Phi$ è un omomorfismo di gruppi, mostriamo che in realtà è un isomorfismo. $\Phi(\varphi) = id$ se e solo se $\varphi_{|K} = id$, ma questo è possibile se e solo se $\varphi = id$ in quanto se $\varphi$ è la mappa identità su $K$ e su $L$ allora lo è anche sul composto $KL$, pertanto $\Phi$ è iniettivo. Mostriamo adesso che è anche surgettivo. Sia $H = \mathrm{Im}\Phi$, il sottocampo di $K$ fissato da $H$ è
$$K^H = \{x \in K \mid \psi(x) = x \ \forall \psi \in H\}$$
Poiché $H$ contiene le restrizioni a $K$ degli elementi di $\mathrm{Gal}(KL/L)$, si ha
$$\begin{aligned} K^H &= \{x \in K \mid \psi(x) = x \ \forall \psi \in \mathrm{Gal}(KL/L)\} = \\ &= K \cap \{x \in KL \mid \psi(x) = x \ \forall \psi \in \mathrm{Gal}(KL/L)\} = \\ &= K \cap (KL)^{\mathrm{Gal}(KL/L)} = K \cap L \end{aligned}$$
pertanto $H = \mathrm{Gal}(K/K \cap L)$ per il Teorema di Corrispondenza di Galois. Quindi $\Phi$ è surgettivo, di conseguenza è un isomorfismo tra $\mathrm{Gal}(KL/L)$ e $\mathrm{Gal}(K/K \cap L)$.

$\square$

**Corollario 3.14**

Siano ${}^{K}\!/_{F}$ un'estensione di Galois finita e ${}^{L}\!/_{F}$ un'estensione finita, se $K \cap L = F$ allora $[KL : F] = [K : F][L : F]$.

*Dimostrazione.* Consideriamo il seguente diagramma di campi

$$\begin{tikzcd}
& KL \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

per il Teorema delle Torri abbiamo $[KL : F] = [KL : L][L : F]$. Poiché $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L) = \mathrm{Gal}(K/F)$ per la Proposizione 3.13, in particolare $[KL : L] = [K : F]$, quindi $[KL : F] = [K : F][L : F]$. □

**Proposizione 3.15**

Siano ${}^{K_1}\!/_{F}$, ${}^{K_2}\!/_{F}$ estensioni di Galois finite, allora ${}^{K_1K_2}\!/_{F}$ è un'estensione di Galois. Inoltre:

(1) esiste un'immersione $\Phi : \mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$;

(2) $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ se e solo se $K_1 \cap K_2 = F$.

*Dimostrazione.* Poiché ${}^{K_1}\!/_{F}$ e ${}^{K_2}\!/_{F}$ sono estensioni normali, esistono $p_1(x), p_2(x) \in F[x]$ tali che $K_1$ e $K_2$ sono rispettivamente i campi di spezzamento di $p_1(x)$ e $p_2(x)$ su $F$. Allora il composto $K_1K_2$ è il campo di spezzamento del polinomio $p_1(x)p_2(x)$ su $F$, quindi ${}^{K_1K_2}\!/_{F}$ è un'estensione di Galois.

(1) Consideriamo la mappa

$$\Phi : \mathrm{Gal}(K_1K_2/F) \longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) : \varphi \longmapsto (\varphi_{|K_1}, \varphi_{|K_2})$$

chiaramente $\Phi$ è un omomorfismo di gruppi, mostriamo quindi che il suo nucleo è banale. $\Phi(\varphi) = (id_{K_1}, id_{K_2})$ se e solo se $\varphi_{|K_1} = id_{K_1}$ e $\varphi_{|K_2} = id_{K_2}$, ma allora $\varphi$ è l'identità anche sul composto $K_1K_2$, pertanto $\Phi$ è iniettivo;

(2) poiché i gruppi in questione sono finiti, è sufficiente mostrare che hanno la stessa cardinalità per concludere che sono isomorfi. Per il Teorema delle Torri abbiamo $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$, d'altra parte $[K_1K_2 : K_1] = [K_2 : K_1 \cap K_2]$ per la Proposizione 3.13. Pertanto $|\,\mathrm{Gal}(K_1K_2/F)| = |\,\mathrm{Gal}(K_1/F)| \cdot |\,\mathrm{Gal}(K_2/F)|$ se e solo se $[K_2 : K_1 \cap K_2][K_1 : F] = [K_1 : F][K_2 : F]$, cioè se e solo se $[K_2 : K_1 \cap K_2] = [K_2 : F]$, ovvero $K_1 \cap K_2 = F$.

□

## §3.4 Gruppo di Galois di un polinomio di grado 3

Consideriamo un polinomio $f(x)$ di grado 3 che non sia completamente fattorizzabile in $\mathbb{Q}[x]$, cioè che ha campo di spezzamento $K$ su $\mathbb{Q}$ diverso da $\mathbb{Q}$. Dalla teoria sappiamo che 3 divide l'ordine di $\mathrm{Gal}(K/\mathbb{Q})$ e che questo è isomorfo a un sottogruppo di $\mathcal{S}_3$, pertanto $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_3$ oppure $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Vediamo che entrambi i casi sono possibili con due esempi.
Consideriamo il polinomio $f(x) = x^3 - 2$, le sue radici in $\overline{\mathbb{Q}}$ sono $\alpha_0 = \sqrt[3]{2}$, $\alpha_1 = \sqrt[3]{2}\zeta_3$, $\alpha_2 = \sqrt[3]{2}\zeta_3^2$, dove $\zeta_3$ è una radice primitiva terza di 1. In particolare, il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Infatti $\sqrt[3]{2} = \alpha_0$ e $\zeta_3 = \frac{\alpha_1}{\alpha_0}$, quindi $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$, d'altra parte $\alpha_i = \sqrt[3]{(2)}\zeta_3^i$ per $i = 0, 1, 2$, pertanto si ha anche l'altra inclusione, da cui l'uguaglianza. Consideriamo il diagramma di campi

$$
\begin{tikzcd}
 & K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

l'estensione ${}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}}$ ha grado 3 in quanto il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$, mentre l'estensione ${}^{\mathbb{Q}(\zeta_3)}\!/_{\mathbb{Q}}$ ha grado 2 in quanto il polinomio minimo di $\zeta_3$ su $\mathbb{Q}$ è $x^2 + x + 1$. Dato che i gradi sono coprimi, l'estensione ${}^{K}\!/_{\mathbb{Q}}$ ha grado 6, di conseguenza $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathcal{S}_3$.

Adesso vogliamo determinare un polinomio il cui gruppo di Galois sia isomorfo a $\mathbb{Z}3$. Consideriamo l'estensione ${}^{\mathbb{Q}(\zeta_7)}\!/_{\mathbb{Q}}$, dove $\zeta_7$ è una radice primitiva settima di 1, per il Teorema 3.9 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}^* \cong \mathbb{Z}/6\mathbb{Z}$. Vale il seguente risultato.

**Proposizione 3.16**

Sia $\zeta_n \in \overline{\mathbb{Q}}$ una radice primitiva $n$-esima di 1 per $n \geq 3$, allora $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$.

*Dimostrazione.* Sia $\alpha = \zeta_n + \zeta_n^{-1}$, poiché $\overline{\zeta_n} = \zeta_n^{-1}$ si ha $\overline{\alpha} = \overline{\zeta_n + \zeta_n^{-1}} = \zeta_n + \zeta_n^{-1} = \alpha$, cioè $\alpha \in \mathbb{R}$ e quindi $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Il polinomio $x^2 - \alpha x + 1$ è a coefficienti reali e si annulla in $\zeta_n$, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] \leq 2$. D'altra parte $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\zeta_n) \cap \mathbb{R}$, quindi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n) \cap \mathbb{R}] = 2$. □

**Osservazione 3.17** — In realtà vale che $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Infatti il polinomio $x^2 - \alpha x + 1$, con le notazioni di sopra, è un polinomio a coefficienti in $\mathbb{Q}(\alpha)$ che si annulla in $\zeta_n$, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] \leq 2$. D'altra parte $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\alpha)$, pertanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$ e quindi $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$.

Abbiamo quindi che la sottoestensione $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ ha grado 3 su $\mathbb{Q}$, mostriamo quindi che è una sua estensione normale. Posto $\alpha = \zeta_7 + \zeta_7^{-1}$, le immersioni di $\mathbb{Q}(\alpha) \longrightarrow \overline{\mathbb{Q}}$ sono le restrizioni a $\mathbb{Q}(\alpha)$ degli elementi di $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, pertanto sono univocamente determinate dalle assegnazioni

$$\zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7 + \zeta_7^{-1} \qquad \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2} \qquad \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^3 + \zeta_7^{-3}$$

Il polinomio minimo di $\alpha$ su $\mathbb{Q}$ è quindi

$$\mu_\alpha(x) = (x - (\zeta_7 + \zeta_7^{-1}))(x - (\zeta_7^2 + \zeta_7^{-2}))(x - (\zeta_7^3 + \zeta_7^{-3})) = x^3 + x^2 - 2x - 1$$

Notiamo che $\zeta_7^2 + \zeta_7^{-2}$ e $\zeta_7^3 + \zeta_7^{-3}$ sono elementi di $\mathbb{Q}(\alpha)$, in quanto

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 2$$

$$\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1})$$

pertanto ${}^{\mathbb{Q}(\alpha)}\!\big/_{\mathbb{Q}}$ è un'estensione normale di grado 3 in quanto campo di spezzamento di $\mu_\alpha(x)$ su $\mathbb{Q}$, quindi il suo gruppo di Galois è isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

## §3.5 Possibili gruppi di Galois

Vogliamo vedere quali gruppi finiti si possono realizzare come gruppi di Galois di un'estensione di campi.

**Lemma 3.18**

Dato $p$ un primo, $S_p$ è generato da un $p$-ciclo e da una trasposizione.

*Dimostrazione.* Per motivi di notazione, consideriamo $S_p$ come l'insieme delle permutazioni dell'insieme $\{0, 1, \ldots, p-1\}$, che pensiamo come $\mathbb{F}_p$. Siano $\sigma = (0\ 1\ \ldots\ p-1)$ un $p$-ciclo e $\tau = (a\ b)$ una trasposizione, poiché $\sigma^k \tau \sigma^{-k} = (a+k\ b+k)$ ed esiste $h \in \mathbb{F}_p$ tale che $a + h = 0$, possiamo supporre $\tau = (0\ \alpha)$ senza perdita di generalità. Notiamo che gli elementi $\sigma^k \tau \sigma^{-k}$ sono tutti della forma $(k\ \alpha + k)$, in particolare $\langle \sigma, \tau \rangle$ contiene le permutazioni $(k\alpha\ (k+1)\alpha)$ al variare di $k \in \mathbb{F}_p$. Possiamo quindi costruire in modo iterativo le permutazioni $(0\ k\alpha)$, ad esempio

$$(0\ \alpha)(\alpha\ 2\alpha)(0\ \alpha) = (0\ 2\alpha)$$

$$(0\ 2\alpha)(2\alpha\ 3\alpha)(0\ 2\alpha) = (0\ 3\alpha)$$
$$(0\ 3\alpha)(3\alpha\ 4\alpha)(0\ 3\alpha) = (0\ 4\alpha)$$

e così via. Poiché $\mathbb{F}_p$ è un campo e $\alpha \neq 0$ (altrimenti $\tau$ non sarebbe una trasposizione) esiste $h \in \mathbb{F}_p$ tale che $h\alpha = 1$, pertanto $(0\ 1) \in \langle \sigma, \tau \rangle$. Poiché $\langle (0\ 1), \sigma \rangle = S_p$ si ha la tesi. □

**Lemma 3.19**

Dati $p$ un primo e $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado $p$, se $f(x)$ ha esattamente $p-2$ radici reali e 2 radici non reali e $K$ è il suo campo di spezzamento su $\mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.

*Dimostrazione.* Poiché $\deg f = p$ esiste un omomorfismo iniettivo

$$\Phi : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_p$$

inoltre $p \mid [K : \mathbb{Q}]$ in quanto $f(x)$ è irriducibile su $\mathbb{Q}$, pertanto $\Phi(\mathrm{Gal}(K/\mathbb{Q}))$ contiene un $p$-ciclo. Notiamo che contiene anche una trasposizione, che corrisponde alla restrizione del coniugio complesso in $\mathrm{Gal}(K/\mathbb{Q})$. Allora $\Phi(\mathrm{Gal}(K/\mathbb{Q})) = S_p$ per il Lemma 3.18, cioè $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$. □

**Lemma 3.20** (Lemma di Artin)

[a] Dato $K$ un campo e $G$ un sottogruppo finito di $\mathrm{Aut}(K)$, allora ${}^{K}\!/_{K^G}$ è un'estensione di Galois finita e $\mathrm{Gal}(K/K^G) = G$.

[a] La dimostrazione è da revisionare nella parte della dimostrazione della finitezza dell'estensione.

*Dimostrazione.* Consideriamo un'immersione $\varphi : K \longrightarrow \overline{K}$ tale che $\varphi_{|K^G} = id_{K^G}$, per definizione di $K^G$ si ha che $\varphi \in G$. In particolare $G$ è l'insieme delle immersioni di $K$ in $\overline{K}$ che fissano $K^G$, pertanto $[K : K^G] = |G|$, cioè ${}^{K}\!/_{K^G}$ è un'estensione finita.

Per il Teorema dell'Elemento Primitivo esiste $\alpha \in K$ tale che $K = K^G(\alpha)$, posto $\mu(x) \in K^G[x]$ il polinomio minimo di $\alpha$ su $K^G$ sia $L$ il campo di spezzamento di $\mu(x)$ su $K^G$, vale l'inclusione $K \subseteq L$ in quanto $K = K^G(\alpha)$. Consideriamo il polinomio

$$f(x) = \prod_{g \in G} (x - g(\alpha)) \in K[x]$$

In realtà si ha $f(x) \in K^G[x]$, in quanto per ogni $h \in G$ vale

$$h(f(x)) = \prod_{g \in G} (x - (hg)(\alpha)) = f(x)$$

in quanto la composizione per $h$ induce una bigezione tra gli elementi di $G$, quindi un riordinamento del prodotto. Poiché $f(\alpha) = 0$ si ha che $\mu(x) \mid f(x)$, pertanto le radici di $\mu(x)$ sono tutte della forma $g(\alpha)$ per opportuni $g \in G$. Allora le radici di $\mu(x)$ sono tutti elementi di $K$, pertanto $L = K$ e quindi ${}^{K}\!/\!_{K^G}$ è un'estensione di Galois. Sia $H = \mathrm{Gal}(K/K^G)$, allora

$$K^H = K^{\mathrm{Gal}(K/K^G)} = K^G$$

da cui $H = G$ per il Teorema di Corrispondenza di Galois. $\square$

**Proposizione 3.21**

Ogni gruppo finito $G$ si realizza come gruppo di Galois di un'estensione di campi.

*Dimostrazione.* Sia $|G| = n$ e $p \geq n$ un primo, si hanno le immersioni

$$G \hookrightarrow \mathcal{S}_n \hookrightarrow S_p$$

Consideriamo $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado $p$ avente esattamente $p - 2$ radici reali e 2 radici non reali e sia $K$ il suo campo di spezzamento su $\mathbb{Q}$. Per il Lemma 3.19 vale $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$, per il Lemma di Artin allora ${}^{K}\!/\!_{K^G}$ è un'estensione di Galois finita e il suo gruppo di Galois è isomorfo a $G$. $\square$

**Leonardo Migliorini** (l.migliorini@studenti.unipi.it)
**Gabriel Antonio Videtta** (g.videtta1@studenti.unipi.it)
**Università di Pisa** (Anno Accademico 2022-23)


## §3.6 Estensioni quadratiche di $\mathbb{Q}$

**Teorema 3.22**

Siano $p_1, \dots, p_n \in \mathbb{Z}$ primi distinti, poniamo $K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. ${K_n}/{\mathbb{Q}}$ è un'estensione di Galois e $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$.

*Dimostrazione.* Mostriamo la tesi per induzione su $n \geq 1$. Per $n = 1$ si ha $K_1 = \mathbb{Q}(\sqrt{p_1})$, che è un'estensione di Galois di $\mathbb{Q}$ in quanto di grado 2, e il suo gruppo di Galois è isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Per $n > 1$, supponiamo che l'estensione ${K_n}/{\mathbb{Q}}$ sia di Galois e che $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$, mostriamo la tesi per $n+1$. Consideriamo il seguente diagramma di campi

$$\begin{tikzcd}
& K_{n+1} \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
K_n \arrow[dr, dash] & & \mathbb{Q}(\sqrt{p_{n+1}}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

l'estensione ${K_{n+1}}/{\mathbb{Q}}$ è di Galois in quanto composto di due estensioni di Galois su $\mathbb{Q}$. Notiamo che si ha la tesi nel caso in cui $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$, e che se questo non si verifica allora $\mathbb{Q}(\sqrt{p_{n+1}}) \subseteq K_n$. Per il Teorema di Corrispondenza di Galois le sottoestensioni di $K_n$ di grado due su $\mathbb{Q}$ sono tante quanti i sottogruppi di indice due di $(\mathbb{Z}/2\mathbb{Z})^n$, che a loro volta sono tanti quanti gli iperpiani di $(\mathbb{F}_2)^n$[23], che sono $2^n - 1$. Consideriamo le sottoestensioni quadratiche $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n}})$ con $\varepsilon_i \in \{0, 1\}$ non tutti nulli, se queste sono due a due distinte allora sono tutte e sole le sottoestensioni quadratiche di $K_n$, in quanto sono $2^n - 1$. In effetti, le estensioni $\mathbb{Q}(\sqrt{p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n}})$ e $\mathbb{Q}(\sqrt{p_1^{\delta_1} \dots p_n^{\delta_n}})$, con $\varepsilon_i, \delta_i \in \{0, 1\}$ non tutti nulli, coincidono se e solo se $(p_1^{\varepsilon_1} \dots p_n^{\varepsilon_n})(p_1^{\delta_1} \dots p_n^{\delta_n})$ è un quadrato in $\mathbb{Q}$, quindi in $\mathbb{Z}$. Questo è equivalente a richiedere $\varepsilon_i + \delta_i \equiv 0 \pmod 2$ per ogni $i$, ovvero $\varepsilon_i = \delta_i$ per ogni $i$. Abbiamo quindi determinato tutte e sole le sottoestensioni di $K_n$ quadratiche su $\mathbb{Q}$. Notiamo quindi che $\mathbb{Q}(\sqrt{p_{n+1}}) \not\subseteq K_n$ in quanto $p_{n+1}$ non è un quadrato in $\mathbb{Q}$ essendo irriducibile in $\mathbb{Z}$, quindi per la Proposizione 3.15 si ha $\mathrm{Gal}(K_{n+1}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^{n+1}$. $\square$

**Osservazione 3.23** — Otteniamo come corollario che $\mathbb{Q}$ ammette infinite estensioni quadratiche.

**Osservazione 3.24** — Un elemento primitivo per l'estensione ${K_n}/{\mathbb{Q}}$ è dato da $\alpha = \sum_{i=1}^{n} \sqrt{p_i}$. Consideriamo infatti le immersioni $\mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$ che fissano $\mathbb{Q}$, poiché $\mathbb{Q}(\alpha) \subseteq K_n$ queste si estendono a immersioni $K_n \hookrightarrow \overline{\mathbb{Q}}$, che sono gli elementi di $\mathrm{Gal}(K_n/\mathbb{Q})$. In particolare, se $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ si ha $\sigma(\alpha) = \sum_{i=1}^{n} a_i \sqrt{p_i}$, con

[23] Stiamo qua considerando la struttura di spazio vettoriale di $(\mathbb{F}_2)^n$.

$a_i \in \{1, -1\}$. Le immagini di $\alpha$ tramite gli elementi di $\mathrm{Gal}(K_n/\mathbb{Q})$ sono quindi tutte distinte in quanto $\sqrt{p_1}, \ldots, \sqrt{p_n}$ sono elementi di una base di $K_n$ su $\mathbb{Q}$, pertanto la scrittura di $\sigma(\alpha)$ come combinazione lineare di tali elementi è unica al variare di $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$. In particolare $\alpha$ ha $2^n$ immagini distinte, pertanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ e quindi $\mathbb{Q}(\alpha) = K_n$.

## §3.7 Gruppo di Galois di un polinomio biquadratico

**Teorema 3.25**

Siano $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ un polinomio irriducibile, definiamo $\Delta = a^2 - 4b$. Posto $K$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ si ha:

(1) se $\sqrt{b} \notin \mathbb{Q}$ e $\sqrt{b\Delta} \notin \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$;

(2) se $\sqrt{b} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(3) se $\sqrt{b\Delta} \in \mathbb{Q}$ allora $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$;

*Dimostrazione.* Sostituendo $t = x^2$ e risolvendo l'equazione $t^2 + at + b$ ricaviamo le radici di $f(x)$ in $\overline{\mathbb{Q}}$

$$x_1 = \sqrt{\frac{-a+\sqrt{\Delta}}{2}} \qquad x_2 = -\sqrt{\frac{-a+\sqrt{\Delta}}{2}} \qquad x_3 = \sqrt{\frac{-a-\sqrt{\Delta}}{2}} \qquad x_4 = -\sqrt{\frac{-a-\sqrt{\Delta}}{2}}$$

quindi $K = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_3)$. Per ogni $i \in \{1, 2, 3, 4\}$ osserviamo che $\mathbb{Q}(x_i^2) = \mathbb{Q}(\sqrt{\Delta})$, consideriamo quindi il seguente diagramma di campi

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(x_1) \arrow[dr, no head] & & \mathbb{Q}(x_3) \arrow[dl, no head] \\
 & \mathbb{Q}(\sqrt{\Delta}) \arrow[d, no head] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Poiché $f(x)$ è irriducibile su $\mathbb{Q}[x]$ si ha $\sqrt{\Delta} \notin \mathbb{Q}$, pertanto $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$. Per il Teorema delle Torri allora il grado di $\mathbb{Q}(x_1)$ e di $\mathbb{Q}(x_3)$ su $\mathbb{Q}(\sqrt{\Delta})$ è uguale a 2, quindi $[K : \mathbb{Q}] \in 4, 8$. In particolare $[K : \mathbb{Q}] = 4$ se e solo se $\mathbb{Q}(x_1) = \mathbb{Q}(x_3)$, cioè se e solo se $x_1^2 x_3^2$ è un quadrato in $\mathbb{Q}(\sqrt{\Delta})$, cioè $x_1 x_3 \in \mathbb{Q}(\sqrt{\Delta})$.

$$x_1 x_3 = \sqrt{\frac{-a+\sqrt{\Delta}}{2} \cdot \frac{-a-\sqrt{\Delta}}{2}} = \sqrt{\frac{a^2 - \Delta}{4}} = \sqrt{b}$$

quindi $\mathbb{Q}(x_1) = \mathbb{Q}(x_3)$ se e solo se $\sqrt{b} \in \mathbb{Q}(\Delta)$, cioè se e solo se $\sqrt{b} \in \mathbb{Q}$ oppure $\sqrt{b\Delta} \in \mathbb{Q}$. Distinguiamo tre casi:

(1) se $\sqrt{b} \notin \mathbb{Q}$ e $\sqrt{b\Delta} \notin \mathbb{Q}$ allora $[K : \mathbb{Q}] = 8$. Allora $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ in quanto $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo a un sottogruppo di $\mathcal{S}_4$ e i 2-Sylow di $\mathcal{S}_4$ sono isomorfi a $D_4$;

(2) se $\sqrt{b} \in \mathbb{Q}$ (e di conseguenza $\sqrt{b\Delta} \notin \mathbb{Q}$) allora $K = \mathbb{Q}(x_1)$, quindi $[K : \mathbb{Q}] = 4$ e $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oppure a $\mathbb{Z}/4\mathbb{Z}$. Siano $\varphi_i \in \mathrm{Gal}(K/\mathbb{Q})$ per $i \in \{1, 2, 3, 4\}$ gli omomorfismi determinati dalle seguenti assegnazioni

$$\varphi_1 : x_1 \longmapsto x_1 \qquad \varphi_2 : x_1 \longmapsto x_2 \qquad \varphi_3 : x_1 \longmapsto x_3 \qquad \varphi_4 : x_1 \longmapsto x_4$$

poiché $x_2 = -x_1$ abbiamo che $\varphi_2^2 = \varphi_1 = id$, cioè $\varphi_2$ ha ordine 2. Sfruttando la relazione $x_1 x_3 = \sqrt{b}$ abbiamo

$$\varphi_3^2(x_1) = \varphi_3(x_3) = \varphi_3\left(\frac{\sqrt{b}}{x_1}\right) = \frac{\varphi_3(\sqrt{b})}{\varphi_3(x_1)}[24] = \frac{\sqrt{b}}{x_3} = x_1$$

pertanto anche $\varphi_3$ ha ordine 2. Allora $\mathrm{Gal}(K/\mathbb{Q})$ non è ciclico, quindi è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(3) se $\sqrt{b\Delta} \in \mathbb{Q}$ (e di conseguenza $\sqrt{b} \notin \mathbb{Q}$) scriviamo $b = \Delta q^2$, con $q \in \mathbb{Q}$. Ragionando allo stesso modo e con le stesse notazioni si ha che $\varphi_2$ ha ordine 2 e

$$\varphi_3^2(x_1) = \varphi_3(x_3) = \varphi_3\left(\frac{\sqrt{b}}{x_1}\right) = \frac{\varphi_3(\sqrt{\Delta}q)}{\varphi_3(x_1)} = q\frac{\varphi_3(\sqrt{\Delta})}{x_3}$$

Poiché $\sqrt{\Delta} = 2x_1^2 + a$ si ha $\varphi_3(\sqrt{\Delta}) = 2x_3^2 + a = -\sqrt{\Delta}$, pertanto

$$\varphi_3^2(x_1) = -q\frac{\sqrt{\Delta}}{x_3} = -\frac{\sqrt{b}}{x_3} = -x_1$$

quindi $\varphi_3$ ha ordine 4. Allora $\mathrm{Gal}(K/\mathbb{Q})$ è ciclico, in particolare è isomorfo a $\mathbb{Z}/4\mathbb{Z}$.

□

[24] L'uguaglianza è data dal fatto che $\sqrt{b}$ è un elemento di $\mathbb{Q}$, pertanto è fissato da tutti gli elementi di $\mathrm{Gal}(K/\mathbb{Q})$.

## §3.8 Contare le sottoestensioni quadratiche di un campo

Consideriamo un'estensione di Galois finita ${}^{F}\!/_{K}$, sia $G = \mathrm{Gal}(F/K)$, le sottoestensioni di $F$ di grado due su $K$ sono in corrispondenza con i sottogruppi di $G$ di indice 2. Osserviamo che un sottogruppo $H \leqslant G$ di indice 2 contiene il sottogruppo

$$\mathscr{G} = \langle g^2 \mid g \in G \rangle$$ [25]

Infatti se consideriamo il quoziente ${}^{G}\!/_{H} \cong \mathbb{Z}/2\mathbb{Z}$, per ogni $g \in G$ si ha

$$(gH)^2 = g^2 H = H$$

da cui $g^2 \in H$ e quindi anche $\mathscr{G} \leqslant H$. Per il Teorema di Corrispondenza tra sottogruppi abbiamo una bigezione

$$\{H \leqslant G \mid [G : H] = 2\} \longleftrightarrow \left\{\mathcal{H} \leqslant {}^{G}\!/_{\mathscr{G}} \;\middle|\; \left[{}^{G}\!/_{\mathscr{G}} : \mathcal{H}\right] = 2\right\}$$

Gli elementi di ${}^{G}\!/_{\mathscr{G}}$ hanno ordine al più 2. Questo implica che sia un gruppo abeliano, infatti per ogni $a, b \in {}^{G}\!/_{\mathscr{G}}$ si ha

$$aba^{-1}b^{-1} = abab = (ab)^2 = e$$

pertanto $ab = ba$. Essendo un gruppo finito per il Teorema di Struttura dei Gruppi Abeliani Finiti si ha ${}^{G}\!/_{\mathscr{G}} \cong (\mathbb{Z}/2\mathbb{Z})^k$, dove $k$ è un parametro che dipende da $G$. Il numero di sottogruppi di indice 2 di $(\mathbb{Z}/2\mathbb{Z})^k$ è uguale al numero di iperpiani dello spazio vettoriale $(\mathbb{F}_2)^k$, quindi $2^k - 1$, e questo è il numero di sottoestensioni di $F$ quadratiche su $K$.

**Esempio 3.26**
Sia $F = \mathbb{Q}(i, \zeta_3, \sqrt[3]{3})$, si verifica che il gruppo di Galois dell'estensione ${}^{F}\!/_{\mathbb{Q}}$ è isomorfo a $G = \mathcal{S}_3 \times \mathbb{Z}/2\mathbb{Z}$. Il sottogruppo $\langle g^2 \mid g \in G \rangle$ è isomorfo al sottogruppo $\mathscr{G} = \mathcal{A}_3 \times \{0\}$, pertanto ${}^{G}\!/_{\mathscr{G}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, che contiene tre sottogruppi di indice 2. Quindi $F$ contiene tre sottoestensioni quadratiche su $\mathbb{Q}$, che sono $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$.

**Osservazione 3.27** — Possiamo ripetere la costruzione di sopra per cercare i sottogruppi normali di indice $k$, in quanto questi contengono il sottogruppo $\langle g^k \mid g \in G \rangle$, ma la caratterizzazione del quoziente è più complicata in generale.

[25] Stiamo usando la notazione moltiplicativa. In notazione additiva allora $\mathscr{G} = \langle 2g \mid g \in G \rangle$.

## §3.9 Radici dell'unità

Consideriamo un'estensione di Galois finita ${}^{K}\!/_{\mathbb{Q}}$ con gruppo di Galois $G$, sia $\zeta_n$ una radice primitiva $n$-esima dell'unità, vogliamo capire come determinare se $\zeta_n$ è contenuta in $F$ al variare di $n \in \mathbb{N}$.

$$\begin{tikzcd}[column sep=small]
K \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
& F = K \cap \mathbb{Q}(\zeta_n) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Il gruppo $\mathrm{Gal}(F/\mathbb{Q})$ è un sottogruppo di $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, che è isomorfo a $\mathbb{Z}/n\mathbb{Z}^*$ per il Teorema 3.9, in particolare $\mathrm{Gal}(F/\mathbb{Q})$ è un gruppo abeliano e ${}^{F}\!/_{\mathbb{Q}}$ è un'estensione normale in quanto tutte le sottoestensioni di $\mathbb{Q}(\zeta_n)$ sono normali. D'altra parte $\mathrm{Gal}(F/\mathbb{Q})$ è isomorfo a un quoziente ${}^{G}\!/_{H}$, con $H \trianglelefteq G$, in particolare $H$ deve contenere il sottogruppo derivato $G'$ in quanto il quoziente è abeliano (Proposizione 1.35).

**Esempio 3.28**

Per $n \geq 3$, sia $f(x) \in \mathbb{Q}[x]$ che il gruppo di Galois del suo campo di spezzamento $K$ su $\mathbb{Q}$ è isomorfo a $\mathcal{S}_n$, consideriamo i sottogruppi normali $H$ di $\mathcal{S}_n$ che contengono $\mathcal{S}_n'$. Poiché $\mathcal{S}_n' = \mathcal{A}_n$ tali sottogruppi sono solo $\mathcal{A}_n$ e $\mathcal{S}_n$. Se $H = \mathcal{S}_n$ allora $\mathbb{Q}(\zeta_n) \cap K = \mathbb{Q}$ in quanto ${}^{\mathrm{Gal}(K/\mathbb{Q})}\!/_{H}$ è il gruppo banale, quindi le uniche radici dell'unità contenute in $K$ sono $1$ e $-1$ (che sono rispettivamente $\zeta_1$ e $\zeta_2$). Se $H = \mathcal{A}_n$ allora $[\mathbb{Q}(\zeta_n) \cap K : \mathbb{Q}] = 2$. Poiché una sottoestensione di $\mathbb{Q}(\zeta_n)$ è della forma $\mathbb{Q}(\zeta_d)$ con $d \mid n$, abbiamo che $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = 2$. I possibili $d$ sono quindi da determinare tra le soluzioni dell'equazione $\phi(m) = 2$, cioè $d \in 3, 4, 6$. In particolare le uniche radici dell'unità non banali che possono essere contenute in $K$ sono $\zeta_3$, $\zeta_4$ e $\zeta_6$, e quali di queste sono effettivamente elementi del campo dipende dalle radici del polinomio $f(x)$.

Consideriamo adesso le estensioni ciclotomiche $\mathbb{Q}(\zeta_p)$ con $p$ primo, vogliamo determinare quando una sottoestensione quadratica di $\mathbb{Q}(\zeta_p)$ è reale oppure no. Il gruppo di Galois dell'estensione è isomorfo a $\mathbb{Z}/p\mathbb{Z}^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, che è un gruppo ciclico, quindi $\mathbb{Q}(\zeta_n)$ contiene un'unica sottoestensione quadratica su $\mathbb{Q}$. Osserviamo che l'insieme dei quadrati di $\mathbb{Z}/p\mathbb{Z}^*$ è un sottogruppo di indice 2, in quanto la mappa

$$\varphi : \mathbb{Z}/p\mathbb{Z}^* \longrightarrow \mathbb{Z}/p\mathbb{Z}^* : x \longmapsto x^2$$

è un omomorfismo di gruppi, essendo $\mathbb{Z}/p\mathbb{Z}^*$ abeliano, e il suo nucleo è $\{1, -1\}$, pertanto $|\mathrm{Im}\varphi| = \dfrac{p-1}{2}$. Siano $K = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$, $F_2$ l'unica sottoestensione quadratica di $\mathbb{Q}(\zeta_p)$, $K$ è il campo fissato dal coniugio complesso, pertanto corrisponde al sottogruppo $\langle -1 \rangle \leqslant \mathbb{Z}/p\mathbb{Z}^*$, mentre $F_2$ corrisponde al sottogruppo dei quadrati di $\mathbb{Z}/p\mathbb{Z}^*$. Allora $F_2 \subseteq K$ se e solo se $-1$ è un quadrato in $\mathbb{Z}/p\mathbb{Z}^*$, cioè se e solo se $p \equiv 1 \pmod 4$.

Più in generale vale il seguente teorema, di cui non diamo la dimostrazione.

**Teorema 3.29**

Dato $p$ un primo dispari, l'unica sottoestensione di $\mathbb{Q}(\zeta_p)$ quadratica su $\mathbb{Q}$ è

(1) $\mathbb{Q}(\sqrt{p})$ se $p \equiv 1 \pmod 4$;

(2) $\mathbb{Q}(\sqrt{-p})$ se $p \equiv 3 \pmod 4$.

## §3.10 Il discriminante polinomiale

In questa sezione si illustra il *discriminante polinomiale* e le sue principali applicazioni nella teoria di Galois.

**Definizione 3.30.** Sia $p \in K[x]$. Se $\deg p = n$ e $\alpha_1$, ..., $\alpha_n \in \overline{K}$ sono le radici di $p$, si definisce il **discriminante polinomiale** $\operatorname{disc} p$ in modo tale che:

$$\operatorname{disc} p = \operatorname{disc} p(x) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K[\alpha_1, \ldots, \alpha_n]$$

Si verifica facilmente che $p$ ha radici multiple se e solo se $\operatorname{disc} p = 0$. Inoltre, l'annullamento di $\operatorname{disc} p$ è indipendente dal coefficiente di testa $a_n$ del polinomio, dal momento che polinomi associati condividono le stesse radici[26]. Altrettanto semplicemente si verifica che $\operatorname{disc} p$ è un polinomio simmetrico negli $\alpha_i$, ovverosia una qualsiasi permutazione degli $\alpha_i$ in $p$ restituisce ancora $p$.

Si osserva facilmente che $\operatorname{disc} p$ è invariante per traslazioni. Infatti, se si considera $p(x+a)$ con $a \in K$, le radici di $p(x+a)$ sono $\alpha_1 - a$, ..., $\alpha_n - a$. Pertanto vale che:

$$\operatorname{disc} p(x+a) = \prod_{i<j} (\alpha_i - a - \alpha_j + a)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \operatorname{disc} p(x)$$

**Esempio 3.31** (disc $p$ per polinomi di grado 2)
Sia $p(x) = ax^2 + bx + c$ con $a \neq 0$. Se $\alpha_1$ e $\alpha_2$ sono le radici di $p$ in $\overline{K}$, allora vale che:

$$\operatorname{disc} p(x) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = \frac{b^2}{a^2} - 4\frac{c}{a} = \frac{\Delta}{a^2}$$

dove si è utilizzato il fatto per cui $\alpha_1 + \alpha_2 = -\frac{b}{a}$, $\alpha_1\alpha_2 = \frac{c}{a}$ e dove $\Delta$ indica l'usuale delta delle equazioni di secondo grado.

**Osservazione 3.32** (Utilizzo della matrice di Vandermonde) — Un'espressione di $\operatorname{disc} p$ può anche essere calcolata attraverso le matrici di Vandermonde. Infatti, se $M$ è la matrice di Vandermonde di $\alpha_1$, ..., $\alpha_n$ radici di $p$, vale che:

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

e quindi:

$$\det(M) = \prod_{i<j} (\alpha_i - \alpha_j)$$

[26] In generale, compare sempre un termine $a_n^{2n-2}$ al denominatore di $\operatorname{disc} p(x)$. Pertanto, in letteratura si definisce $\operatorname{disc} p(x)$ anche come il prodotto tra $a_n^{2n-2}$ e il discriminante qui definito. In tal caso, il discriminante di un polinomio di secondo grado è esattamente $\Delta$.

Pertanto vale che:

$$\det(M^2) = \det(MM^T) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \operatorname{disc} p(x)$$

**Osservazione 3.33 —** Sia $p \in K[x]$ di grado $n$ e siano $\alpha_1, \ldots, \alpha_n$ le sue radici. Se allora $\sigma \in S(\{\alpha_1, \ldots, \alpha_n\})$, vale che:

$$\prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{i<j} \frac{\sigma(\alpha_i) - \sigma(\alpha_j)}{\alpha_i - \alpha_j} \prod_{i<j}(\alpha_i - \alpha_j) = \operatorname{sgn}(\sigma) \prod_{i<j}(\alpha_i - \alpha_j)$$

Pertanto, se $L = K(\alpha_1, \ldots, \alpha_n)$ è un campo di spezzamento di $p$ su $K$ e ogni fattore irriducibile di $p$ è separabile, elevando al quadrato, vale che:

$$\sigma(\operatorname{disc} p) = \operatorname{disc} p \qquad \forall \sigma \in \operatorname{Gal}\left({}^{L}\!/_{K}\right)$$

e quindi[a] $\operatorname{disc} p \in L^G = K$.

[a] In generale, $\operatorname{disc} p$ appartiene sempre a $K$. Infatti $\operatorname{disc} p$ è un polinomio simmetrico negli $\alpha_i$, e in quanto tale, per il Teorema fondamentale dei polinomi simmetrici, può scriversi come elemento di $K[e_1, \ldots, e_n]$, dove:

$$e_0 = 1, \qquad e_i = \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq n} \alpha_{j_1} \cdots \alpha_{j_i} \quad \forall\, 1 \leq i \leq n$$

Pertanto, poiché per le formule di Viète vale che $a_i = (-1)^{n-i} a_n e_{n-i} \in K$, e dunque $e_i \in K$, $\operatorname{disc} p$, essendo combinazione dei vari $e_i$, è sempre un elemento di $K$.

L'utilità del discriminante polinomiale per la teoria di Galois è sancita dalla seguente proposizione:

**Proposizione 3.34**

Sia $p$ un polinomio irriducibile e separabile di grado $n$. Allora, se $L$ è il suo campo di spezzamento su $K$, $\operatorname{Gal}\left({}^{L}\!/_{K}\right) \hookrightarrow \mathcal{A}_n$ se e solo se $\operatorname{disc} p$ è un quadrato[a] in $K$.

[a] Questa proposizione è ancora vera utilizzando il discriminante moltiplicato per $a^{2n-2}$, e quindi vale ancora per la definizione alternativa di discriminante.

*Dimostrazione.* Sia $G := \operatorname{Gal}\left({}^{L}\!/_{K}\right)$. Allora $G \hookrightarrow \mathcal{A}_n$ se e solo se $\operatorname{sgn}(\sigma) = 1$ $\forall \sigma \in G$. Siano $\alpha_1, \ldots, \alpha_n$ le radici di $p$ in $\overline{K}$. Allora vale la seguente identità:

$$\sigma\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \operatorname{sgn}(\sigma) \prod_{i<j}(\alpha_i - \alpha_j)$$

dove si è utilizzata la precedente osservazione. Poiché gli elementi fissati da tutte le $\sigma \in G$ sono esattamente gli elementi di $K$, se $G \hookrightarrow \mathcal{A}_n$, $\operatorname{sgn}(\sigma)$ è sempre uguale ad 1, e quindi $\left(\prod_{i<j}(a_i - a_j)\right) \in K$. In tal caso $\operatorname{disc} p$ è un quadrato in $K$, essendo $\left(\prod_{i<j}(a_i - a_j)\right)$ una sua radice quadrata. Analogamente, se $\operatorname{disc} p$ è un quadrato in $K$, $x^2 - \operatorname{disc} p$ ammette una soluzione in $K$, e quindi deve scomporsi linearmente. Pertanto anche $\left(\prod_{i<j}(a_i - a_j)\right)$ deve appartenere a $K$, e quindi $\sigma$ deve fissarlo. Affinché $\sigma$ lo fissi deve dunque valere $\operatorname{sgn}(\sigma) = 1$, da cui la tesi. $\square$

**Osservazione 3.35** ($\operatorname{disc} p$ per polinomi *depressi* di grado 3) — Sia $p(x) = x^3 + px + q$. Si calcola il suo discriminante polinomiale in termini di $p$ e $q$. Siano $\alpha_1$, $\alpha_2$ e $\alpha_3$ le radici di $p(x)$. Allora per le osservazioni precedenti vale che:

$$\operatorname{disc} p(x) = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix} = \det \begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}$$

dove[a] $s_p := \alpha_1^p + \alpha_2^p + \alpha_3^p$.

Chiaramente $s_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$, dal momento che il coefficiente[b] di $x^2$ è nullo. Si calcola ora $s_2$:

$$s_2 = s_1^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) = s_1^2 - 2p = -2p$$

dove $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = e_2(\alpha_1, \alpha_2, \alpha_3) = p$ per le formule di Viète. Si calcola $s_3$:

$$s_3 = s_1^3 - 3\alpha_1^2(\alpha_2 + \alpha_3) - 3\alpha_2^2(\alpha_1 + \alpha_3) - 3\alpha_3^2(\alpha_1 + \alpha_2) - 6\alpha_1\alpha_2\alpha_3$$

Sempre per le formule di Viète, vale che $\alpha_1\alpha_2\alpha_3 = -q$, e quindi:

$$s_3 = s_1^3 - 3\alpha_1^2(s_1 - \alpha_1) - 3\alpha_2^2(s_1 - \alpha_2) - 3\alpha_3^2(s_1 - \alpha_3) + 6q$$

da cui, ricordando che $s_1 = 0$, si ricava che:

$$s_3 = 3s_3 + 6q \implies s_3 = -3q$$

Si calcola infine $s_4$:

$$s_4 = s_1^4 - 4(\alpha_1^3(s_1 - \alpha_1) + \alpha_2^3(s_1 - \alpha_2) + \alpha_3^3(s_1 - \alpha_3)) - 12\alpha_1\alpha_2\alpha_3 s_1 - 6(\alpha_1^2\alpha_2^2 + \alpha_2^2\alpha_3^2 + \alpha_3^2\alpha_1^2)$$

Ricordando che $s_1 = 0$, vale allora che:

$$s_4 = 4s_4 - 3(\alpha_1^2(s_2 - \alpha_1^2) + \alpha_2^2(s_2 - \alpha_2^2) + \alpha_3^2(s_2 - \alpha_3^2))$$

da cui:

$$-3s_4 = -3(s_2^2 - s_4) \implies s_4 = \frac{s_2^2}{2} = 2p^2$$

Pertanto si può ora concludere che:

$$\operatorname{disc} p(x) = \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = 3 \begin{vmatrix} -2p & -3q \\ -3q & 2p^2 \end{vmatrix} - 2p \begin{vmatrix} 0 & -2p \\ -2p & -3q \end{vmatrix}$$

e quindi che:

$$\operatorname{disc} p(x) = 3(-4p^3 - 9q^2) - 2p(-4p^2) = -12p^3 - 27q^2 + 8p^3 = \boxed{-4p^3 - 27q^2}$$

[a] In realtà esistono delle relazioni esplicite per il termine $s_p$, dette formule di Newton-Girard, che dunque permettono di estendere i calcoli a gradi più alti con più efficienza.

[b] Se si sta considerando un polinomio non depresso, ossia per il quale tale coefficiente è non nullo, si può applicare la trasformazione di Tschirnhaus, ossia si può considerare $p\left(x - \frac{a_{n-1}}{n\, a_n}\right)$. Infatti, come visto prima, il discriminante è invariante per traslazione.

**Esempio 3.36** (Gruppo di Galois di un polinomio cubico, irriducibile e separabile)
Sia $p(x) = x^3 + px + q \in K[x]$ irriducibile e separabile. Sia $L$ un campo di spezzamento di $p$ su $K$. Dalla teoria di Galois sappiamo che $3 \mid [L : K] \mid 3! = 6$. Poiché $G = \mathrm{Gal}\left({}^{L}\!/\!_{K}\right)$ si immerge in $\mathcal{S}_3$ agendo sulle radici di $p(x)$, $G$ è isomorfo a $\mathcal{A}_3$ o a $\mathcal{S}_3$.

Per la proposizione precedente, $G$ è isomorfo a $\mathcal{A}_3$ se e solo se $\operatorname{disc} p(x) = -4p^3 - 27q^2$ è un quadrato in $K$, e quindi:

$$G \cong \begin{cases} \mathcal{A}_3 & \text{se } -4p^3 - 27q^2 \text{ è quadrato in } K \\ \mathcal{S}_3 & \text{altrimenti} \end{cases}$$

## §3.11 Risoluzione delle equazioni di terzo grado

Si illustra adesso il metodo risolutivo delle equazioni di terzo grado, tramite la cosiddetta **formula di Cardano-Tartaglia-Del Ferro**.

Innanzitutto, si assume che $\varphi(x)$ sia un polinomio *depresso* di terzo grado della forma $x^3 + px + q$. Se invece tale polinomio non è depresso (ossia se il coefficiente di $x^2$ non è nullo) ed è della forma $ax^3 + bx^2 + cx + d$ con $b \neq 0$, è sufficiente sostituire $x = y - \frac{b}{3a}$ per ottenere un polinomio di tale tipo[27].

Sia $x = u + v$. Allora $\varphi(u + v) = u^3 + v^3 + 3u^2v + 3uv^2 + p(u + v) + q = (u^3 + v^3 + q) + (3uv + p)(u + v)$. Si impone allora il seguente sistema di equazioni:

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \implies u^3v^3 = -\frac{p^3}{27} \end{cases}$$

Infatti, se il precedente sistema ammette soluzione, $\varphi(x) = \varphi(u + v)$ si annulla e $u + v$ è soluzione.

Dal momento che abbiamo sia la somma che il prodotto di $u^3$ e $v^3$, è possibile ricavare queste due quantità risolvendo l'equazione di secondo grado associata:

$$0 = y^2 - (u^3 + v^3)y + u^3v^3 = y^2 + qy - \frac{p^3}{27}$$

Una volta ottenuti sia $u^3$ che $v^3$, prendendone la radice cubica, si otterrà dunque una radice di $\varphi(x)$. In particolare varrà che:

$$y_{1,2} = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

e quindi:

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Le altre due soluzioni di $\varphi(x)$ si possono poi computare facilmente riducendosi a considerare il polinomio di secondo grado $\varphi(x)/(x - \alpha)$, dove $\alpha$ è la soluzione ottenuta.

[27]Questa è ancora la cosiddetta trasformazione di Tschirnhaus.

## §3.12 Teorema fondamentale dell'algebra

**Teorema 3.37** (Teorema fondamentale dell'algebra)
$\mathbb{C}$ è algebricamente chiuso, ovvero ogni polinomio non costante in $\mathbb{C}[x]$ ammette almeno una radice in $\mathbb{C}$.

*Dimostrazione.* Dato $p(x) \in \mathbb{C}[x]$, non costante, vogliamo dimostrare che $\exists \alpha \in \mathbb{C}$ tale che $p(\alpha) = 0$; detto:

$$q(x) := p(x) \cdot \overline{p(x)} \in \mathbb{R}[x]$$

dove $\overline{p(x)}$ è il polinomio coniugato di $p(x)$[28] e $q(x) \in \mathbb{R}[x]$ in quanto ad esempio:

$$\overline{q(x)} = \overline{p(x)} \cdot \overline{\overline{p(x)}} = \overline{p(x)} \cdot p(x)$$

quindi coincide con il suo coniugato e dunque sta in $\mathbb{R}[x]$[29]. A questo punto è sufficiente far vedere che $q(x)$ ha una radice complessa, in quanto, se $q(\alpha) = 0$, o $p(\alpha) = 0$ e quindi abbiamo la tesi, oppure $\overline{p(\alpha)} = 0 \iff \overline{\overline{p(\alpha)}} = 0$ che è equivalente al dire che $\exists \overline{\alpha} \in \mathbb{C}$ tale che $p(\overline{\alpha}) = 0$ e quindi di nuovo la tesi (sostanzialmente se il coniugato si annulla, allora anche il polinomio iniziale deve annullarsi). Possiamo quindi considerare $q(x) \in \mathbb{R}[x]$ e chiamare $K$ il campo di spezzamento di $q(x)$ su $\mathbb{R}$, sia $G = \operatorname{Gal}\left({}^{K}\!/_{\mathbb{R}}\right)$ e $P_2 < G$ un 2-Sylow di $G$, abbiamo il diagramma:

$$\begin{tikzcd}
K \arrow[dd, dash] \arrow[dr, dash, "|P_2|"] & \\
& K^{P_2} = \mathbb{R}(\beta) \arrow[dl, dash, "d"] \\
\mathbb{R} &
\end{tikzcd}$$

con $d = [K^{P_2} : \mathbb{R}]$ dispari in quanto $d = \dfrac{|G|}{|P_2|}$ e per definizione $|P_2|$ è la massima potenza di 2 che divide $|G|$[30], inoltre per il Teorema dell'elemento primitivo, essendo ${}^{K^{P_2}}\!/_{\mathbb{R}}$ un'estensione finita è generata da un singolo elemento $\beta \in K$, possiamo quindi concludere che il polinomio minimo di $\beta$ su $K$, $\mu_\beta(x)$ ha grado dispari. Poiché $\mu_\beta(x) \in \mathbb{R}[x]$ e $\mu_\beta(x)$ è un polinomio di grado dispari, vale il Teorema di esistenza degli zeri, dunque $\mu_\beta(x)$ ha almeno una radice in $\mathbb{R}$, ma per definizione di polinomio minimo $\mu_\beta(x)$ è irriducibile su $\mathbb{R}$, dunque l'unica possibilità è che $d = \deg \mu_\beta(x) = 1$[31], pertanto il gruppo di Galois dell'estensione ${}^{K}\!/_{\mathbb{R}}$ non può contenere sottoestensioni di grado dispari, quindi $[K : \mathbb{R}] = 2^n$, $n \in \mathbb{N}$. Essendo $G$ un $p$-gruppo, sappiamo dalla teoria che esiste una catena del tipo:

$$\{e\} = G_n \trianglelefteq \ldots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$$

in cui l'indice di ogni sottogruppo normale nel successivo è esattamente $p$ (quindi 2 in questo caso), ciò si riflette per Corrispondenza di Galois in una catena di sottoestensioni

[28] Il polinomio che si ottiene da $p(x)$ scambiando i suoi coefficienti con i loro complessi coniugati.
[29] La stessa cosa si poteva giustificare anche dai coefficienti.
[30] Nel caso in cui il 2-Sylow fosse banale avremmo che $K = \mathbb{R}$ e quindi non stiamo veramente estendendo il campo.
[31] Il fatto che gli unici polinomi irriducibili in $\mathbb{R}[x]$ siano di grado 1 o 2 è una conseguenza del Teorema fondamentale dell'algebra, quindi in questo caso non stiamo usando quel risultato.

di $K/\mathbb{R}$ del tipo:

$$\begin{array}{c} K = K^{G_n} \\ {\scriptstyle 2}\Big| \\ K^{G_{n-1}} \\ {\scriptstyle 2}\Big| \\ \vdots \\ {\scriptstyle 2}\Big| \\ K^{G_2} = \mathbb{C}(\sqrt{\gamma_2}) \\ {\scriptstyle 2}\Big| \\ K^{G_1} = \mathbb{R}(\sqrt{\gamma_1}) \\ {\scriptstyle 2}\Big| \\ \mathbb{R} \end{array}$$

dove $K^{G_1} = \mathbb{R}(\sqrt{\gamma_1})$ in quanto ogni estensione di grado 2 (in caratteristica diversa da 2) si ottiene estraendo una radice quadrata, inoltre se $\gamma_1 > 0$, allora $K^{G_1} = \mathbb{R}$, ma questo non è possibile perché di grado 2, quindi $\gamma_1 < 0$, ed in questo caso $K^{G_1} = \mathbb{C}$ poiché $\mathbb{R}(\sqrt{\gamma_1}) = \mathbb{R}(\sqrt{-1}) \iff (-1) \cdot \gamma_1 > 0$ è un quadrato in $\mathbb{R}$, ed essendo il prodotto positivo è sempre vero, dunque $K^{G_1} = \mathbb{C}$. Infine, si osserva che ancora una volta $K^{G_2}$, avendo grado 2, si ottiene estraendo una radice quadrata da $K^{G_1} = \mathbb{C}$, ma in $\mathbb{C}$ ogni elemento è un quadrato, quindi $\mathbb{C}$ non si può estendere ulteriormente, dunque $K = \mathbb{C}$, pertanto i polinomi a coefficienti reali hanno tutte le loro radici in $\mathbb{C}$ e per quanto detto all'inizio ciò significa che tutti i polinomi in $\mathbb{C}[x]$ hanno tutte le loro radici in $\mathbb{C}$, che quindi è algebricamente chiuso. $\square$