

# **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

Anno Accademico 2022-23

## Indice

<b>1</b>	<b>Gruppi</b>	<b>4</b>
1.1	Insiemi di generatori	4
1.2	Automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$	5
1.3	Gruppo diedrale	6
1.3.1	Elementi del gruppo	6
1.3.2	Sottogruppi	8
1.3.3	Classi di coniugio	11
1.3.4	Legge di gruppo e omomorfismi	11
1.3.5	Automorfismi	13
1.4	Automorfismi di un prodotto diretto	15
1.5	Gruppo derivato	18
1.6	Azioni di gruppo	20
1.6.1	Azioni transitive	20
1.6.2	Teorema di Cauchy e Piccolo Teorema di Fermat	22
1.6.3	Teorema di Poincaré	24
1.7	Gruppo simmetrico	26
1.7.1	Generatori di $S_n$	26
1.7.2	Sottogruppi abeliani massimali di $S_n$	26
1.7.3	Classi di coniugio in $\mathcal{A}_n$	29
1.7.4	Studio di $S_5$	30
1.7.5	Sottogruppi normali di $\mathcal{A}_n$	32
1.7.6	Sottogruppi normali di $S_n$	34
1.7.7	Sottogruppi isomorfi a $S_{n-1}$	35
1.7.8	Costruzione di un automorfismo esterno di $S_6$	37
1.8	Prodotti semidiretti	38
1.8.1	Descrizione di $S_4$ come prodotto semidiretto	38
1.8.2	Automorfismi di $D_n$	39
1.8.3	Prodotti semidiretti isomorfi	40
1.9	Classificazione dei gruppi semplici di ordine al più 100	44
1.10	Studio di $SL_2(\mathbb{F}_3)$	48

## Ringraziamenti

Diego Monaco, Niccolò Nannicini, Pietro Crovetto, Leonardo Alfani, Daniele Lapadula, Francesco Sorce.

## §1 Gruppi

### §1.1 Insiemi di generatori

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

$$\langle x_1, \dots, x_n \rangle = \bigcap_{\substack{H \leq G \\ \{x_1, \dots, x_n\} \subseteq H}} H$$

**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  $x_1, \dots, x_n$ . Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi  $x_1, \dots, x_n$ .

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

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

#### Proposizione 1.3

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

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

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

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

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

## §1.2 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 definire una struttura di spazio vettoriale, quindi un prodotto per scalari

$$\cdot : \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n : (\bar{\lambda}, v) \longmapsto \bar{\lambda}v$$

con  $\bar{\lambda}v = \underbrace{v + \dots + v}_{\bar{\lambda} \text{ volte}}$  e  $\bar{\lambda}$  un qualsiasi rappresentante di  $\bar{\lambda}$ . Tale prodotto è ben definito, infatti se  $\lambda, \lambda' \in \mathbb{Z}$  sono tali che  $\bar{\lambda} = \bar{\lambda}'$ , cioè esiste  $k \in \mathbb{Z}$  tale che  $\lambda = \lambda' + kp$ , allora

$$\bar{\lambda}'v = \underbrace{v + \dots + v}_{\lambda' \text{ volte}} = \underbrace{v + \dots + v}_{\lambda + kp \text{ volte}} = \underbrace{v + \dots + v}_{\lambda \text{ volte}}$$

in quanto  $\underbrace{v + \dots + v}_{kp \text{ volte}} = 0$ . Si verifica che  $((\mathbb{Z}/p\mathbb{Z})^n, +, \cdot)$  è effettivamente uno spazio vettoriale sul campo  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  (dove  $\cdot$  è il prodotto per scalari appena definito). Per come abbiamo definito il prodotto per scalari, abbiamo che per ogni  $\varphi \in \text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$  vale  $\varphi(\lambda v) = \lambda \varphi(v)$  per ogni  $\lambda \in \mathbb{F}_p$ , pertanto

$$\text{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL((\mathbb{F}_p)^n) = \{\varphi : (\mathbb{F}_p)^n \longrightarrow (\mathbb{F}_p)^n \mid \varphi \text{ isomorfismo di spazi vettoriali}\}$$

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

### Proposizione 1.5

Dato  $p$  un primo, allora

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

*Dimostrazione.* Osserviamo che un elemento di  $\text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$  deve necessariamente mandare una base di  $(\mathbb{Z}/p\mathbb{Z})^n$  in un'altra base, e si determina univocamente in questo modo. Sia  $\{v_1, \dots, v_n\}$  una base di  $(\mathbb{Z}/p\mathbb{Z})^n$  e  $\varphi \in \text{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ , consideriamo  $\varphi(v_1)$ :  $\varphi(1)$  può assumere qualsiasi valore non nullo, pertanto abbiamo  $(p^n - 1)$  possibilità per l'immagine del primo vettore. Per quanto riguarda  $v_2$ ,  $\varphi(v_2)$  può assumere qualsiasi valore non nullo che non sia multiplo di  $\varphi(v_1)$ , che sono  $p^n - p$ , analogamente  $\varphi(v_3)$  può assumere qualsiasi valore non nullo che non sia combinazione lineare di  $v_1$  e  $v_2$ , che sono  $p^n - p^2$ , e così via. Reiteriamo questo ragionamento fino a  $\varphi(v_n)$ , che può essere scelto in  $p^n - p^{n-1}$  modi, da cui

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

□

## §1.3 Gruppo diedrale

### §1.3.1 Elementi del gruppo

**Definizione 1.6.** Dato  $n \geq 2$  un numero naturale consideriamo un poligono regolare di  $n$  vertici centrato nell'origine del piano  $\mathbb{R}^2$ , chiamiamo **gruppo diedrale** su  $n$  vertici l'insieme  $D_n$  delle isometrie di  $\mathbb{R}^2$  che fissano il poligono, cioè che mandano i vertici in se stessi (per  $n = 2$  consideriamo le isometrie che mandano un segmento in se stesso).

**Osservazione 1.7** —  $D_n$  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, che è anch'essa un'isometria.

**Osservazione 1.8** — Una rotazione di angolo  $\frac{2\pi}{n}$  è un elemento di  $D_n$ , così come una simmetria rispetto a un asse.

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. Notiamo che  $\text{ord}(r) = n$  e  $\text{ord}(s) = 2$  (per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario).

**Definizione 1.9.** Data  $r \in D_n$  una rotazione di ordine  $n$ , indichiamo con  $\mathcal{R}$  il **sottogruppo delle rotazioni**  $\langle r \rangle$ .

**Osservazione 1.10** — Il sottogruppo  $\mathcal{R}$  contiene tutte le rotazioni di  $D_n$ , infatti se  $r'$  è una rotazione di angolo  $\frac{2k\pi}{n}$ ,  $k \in \mathbb{Z}$ , allora  $r^k = r'$  in quanto anche  $r^k$  è una rotazione di angolo  $\frac{2k\pi}{n}$ .

Per determinare come sono fatti gli elementi di  $D_n$ , 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  $D_n$  è generato da  $r$  e  $s$ .

**Osservazione 1.11** — Gli elementi della forma  $r^k$  e  $sr^h$  sono distinti per ogni  $h, k \in \mathbb{Z}$ . Infatti sappiamo dall'algebra lineare che il determinante di una simmetria è  $-1$  e che il determinante di una rotazione è  $1$ , per la moltiplicatività del determinante quindi  $\det(r^k) = (\det r)^k = 1$  e  $\det(sr^h) = (\det s)(\det r)^h = -1$ , da cui  $r^k \neq sr^h$ .

#### Lemma 1.12

Per ogni rotazione  $r \in D_n$  e per ogni simmetria  $s \in D_n$  vale

$$sr s^{-1} = r^{-1}$$

*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

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

svolgendo esplicitamente il prodotto quindi

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

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

### Proposizione 1.13

Se  $n \geq 3$  allora  $|D_n| = 2n$ .

*Dimostrazione.* Indicando con  $1, \dots, n$  gli  $n$  vertici di un poligono regolare di  $n$  lati, notiamo che un elemento  $g \in D_n$  è univocamente determinato da  $g(1), \dots, g(n)$ . In particolare, fissato  $g(1)$ , per il quale abbiamo  $n$  possibili scelte, abbiamo al massimo due valori per  $g(2)$ , cioè  $g(2) \in \{g(1) + 1, g(1) - 1\}$  (a meno di sommare  $n$  se uno dei due elementi è negativo). Poiché  $g(1)$  e  $g(2)$  individuano due vettori nel piano non allineati, cioè linearmente indipendenti, ne costituiscono una base: fissati i valori di  $g(1)$  e  $g(2)$  abbiamo quindi determinato ogni elemento di  $D_n$  in modo unico e, poiché possiamo farlo in al più  $2n$  modi,  $|D_n| \leq 2n$ . Ricordiamo adesso che  $D_n$  contiene gli elementi della forma  $r^k, sr^h$  al variare di  $h, k \in \mathbb{Z}$ , mostriamo che questi sono infatti  $2n$ . Gli elementi  $r^k$  appartengono al gruppo ciclico  $\mathcal{R}$  di ordine  $n$ , pertanto sono  $n$  elementi distinti, inoltre

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

pertanto anche questi sono  $n$  elementi distinti. Poiché gli insiemi  $\mathcal{R}$  e  $\{sr^h \mid h \in \mathbb{Z}\}$  sono disgiunti (Osservazione 1.11) abbiamo  $|D_n| = 2n$ .  $\square$

**Osservazione 1.14** — Abbiamo mostrato che effettivamente  $D_n = \langle r, s \rangle$ , quindi i suoi elementi sono tutti della forma  $r^k, sr^h$  al variare di  $h, k \in \mathbb{Z}$ .

**Osservazione 1.15** — Il risultato è valido anche per  $D_2$ , ma con motivazioni diverse. Se consideriamo un segmento nel piano  $\mathbb{R}^2$  giacente sulla retta  $y = 0$ , le isometrie che possiamo applicare sono l'identità, la rotazione di angolo  $\pi$ , la simmetria lungo la retta  $y = 0$  e la simmetria lungo l'asse passante per il suo punto medio.  $D_2$  contiene quindi quattro elementi, l'identità e tre elementi di ordine 2, pertanto è isomorfo a  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

### §1.3.2 Sottogruppi

Consideriamo un sottogruppo  $H \leq D_n$ , distinguiamo due possibilità:  $H \subseteq \mathcal{R}$  oppure  $H \not\subseteq \mathcal{R}$ . Nel primo caso abbiamo che  $|H| \mid n$ , ed è l'unico sottogruppo di  $\mathcal{R}$  con questa proprietà in quanto  $\mathcal{R}$  è ciclico, in particolare  $H$  è ciclico della forma  $\langle r^{\frac{n}{d}} \rangle$ , con  $\mathcal{R} = \langle r \rangle$  e  $d \mid n$ .

Studiamo quindi il caso  $H \not\subseteq \mathcal{R}$ : notiamo che  $\mathcal{R} \trianglelefteq D_n$  in quanto  $[D_n : \mathcal{R}] = 2$ , pertanto  $D_n/\mathcal{R}$  è un gruppo con l'operazione indotta da  $D_n$  e risulta essere isomorfo a  $\mathbb{Z}/2\mathbb{Z}$ .

Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : D_n \longrightarrow D_n/\mathcal{R} : g \mapsto g\mathcal{R}$$

poiché  $H \not\subseteq \mathcal{R}$  abbiamo che esiste  $h \in H$  tale che  $h \notin \mathcal{R}$ , pertanto  $\pi_{\mathcal{R}}(h) \neq \mathcal{R}$  e in particolare  $\pi_{\mathcal{R}}(H) \not\subseteq \{\mathcal{R}\}$ . Dato che i sottogruppi di  $D_n/\mathcal{R}$  sono solo  $\{\mathcal{R}\}$  e  $D_n/\mathcal{R}$  abbiamo  $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$ . Osserviamo inoltre che  $\ker \pi_{\mathcal{R}|_H} = \ker \pi_{\mathcal{R}} \cap H = \mathcal{R} \cap H$ , per il Primo Teorema di Omomorfismo allora  $\frac{H}{H \cap \mathcal{R}} \cong \mathbb{Z}/2\mathbb{Z}$ , quindi  $|H \cap \mathcal{R}| = \frac{1}{2}|H|$ . Dato che  $\mathcal{R} \cap H \subseteq \mathcal{R}$ , esiste  $k \in \mathbb{Z}$  tale che  $H \cap \mathcal{R} = \langle r^k \rangle$  in particolare  $\langle r^k \rangle$  e  $\langle sr^h \rangle$ ,  $h \in \mathbb{Z}$ , sono contenuti in  $H$ .

#### Proposizione 1.16

Dati  $H \leq D_n$  un sottogruppo tale che  $H \not\subseteq \mathcal{R}$ , se  $r$  è un generatore di  $\mathcal{R}$  tale che  $H \cap \mathcal{R} = \langle r^k \rangle$  e  $s$  è una simmetria allora

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

*Dimostrazione.* Per quanto visto sopra vale  $|\langle r^k \rangle| = \frac{1}{2}|H|$ , inoltre  $\text{ord}(sr^h) = 2$ :

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

pertanto  $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$ . Da questo ricaviamo  $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$ , infatti per ogni  $m \in \mathbb{Z}$

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

cioè  $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$  e quindi  $\langle r^k \rangle \cdot \langle sr^h \rangle$  è un sottogruppo di  $D_n$ <sup>1</sup>. Poiché  $\langle r^k \rangle$  e  $\langle sr^h \rangle$  sono contenuti in  $H$  abbiamo che  $\langle r^k \rangle \cdot \langle sr^h \rangle \subseteq H$ , inoltre

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

in quanto  $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$ <sup>2</sup>, pertanto i due sottogruppi coincidono.  $\square$

**Osservazione 1.17** — 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  $sr^h$ , in particolare gli elementi di  $H$ .

<sup>1</sup>Dati  $K, N$  sottogruppi di un gruppo  $G$ , se vale almeno una delle inclusioni  $K \subseteq N_G(N)$ ,  $N \subseteq N_G(K)$  allora  $HK = KH$ , quindi  $HK$  è un sottogruppo di  $G$ .

<sup>2</sup>Se  $H, K$  sono sottogruppi finiti di un gruppo  $G$  e  $HK \leq G$  allora vale  $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$ .



**Osservazione 1.18** — 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, simmetricamente  $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$  in quanto  $sr^{h+k} = (sr^h)r^k$  è un elemento del primo gruppo.

**Teorema 1.19** (Classificazione dei sottogruppi di  $D_n$ )

I sottogruppi di  $D_n$  sono della forma

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

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

*Dimostrazione.* Abbiamo già visto che i sottogruppi di  $D_n$  sono di questo tipo, mostriamo quindi che sono tutti distinti. A meno di cambiare  $k$ , possiamo supporre  $\mathcal{R} = \langle r \rangle$ , cioè  $\text{ord}(r) = n$ . Consideriamo  $H, K \leq D_n$  due sottogruppi, abbiamo tre casi:

- se  $H = \langle r^k \rangle$  e  $K = \langle r^m \rangle$ ,  $m \in \mathbb{Z}$ , allora  $H = K \iff k = m$  in quanto entrambi sottogruppi di  $\mathcal{R}$ , pertanto esiste un unico sottogruppo della forma  $\langle r^k \rangle$  per  $k \mid n$ ;
- se  $H = \langle r^k \rangle$  e  $K = \langle r^m, sr^h \rangle$ ,  $m \mid n$ , allora  $H \neq K$  in quanto  $H$  è ciclico e  $K$  no;
- se  $H = \langle r^k, sr^h \rangle$  e  $K = \langle r^m, sr^l \rangle$ , con  $m \mid n$  e  $0 \leq l < m$ , considerando le intersezioni  $H \cap \mathcal{R} = \langle r^k \rangle$  e  $K \cap \mathcal{R} = \langle r^m \rangle$  abbiamo

$$H \cap \mathcal{R} = K \cap \mathcal{R} \iff \langle r^k \rangle = \langle r^m \rangle \iff k = m$$

Inoltre, se  $sr^h \in \langle r^m, sr^l \rangle = \langle r^m \rangle \cdot \langle sr^l \rangle$ , allora esiste  $t \in \mathbb{Z}$  tale che

$$sr^h = (r^m)^t sr^l \iff sr^h = s^2 r^{mt} sr^l \iff r^h = r^{-mt+l} \iff h \equiv l - mt \pmod{n}$$

da cui ricaviamo  $h \equiv l \pmod{m}$  in quanto  $m \mid n$ . Ma allora  $h = l$  dato che  $0 \leq h < k$  e  $0 \leq l < m$ .

□

**Lemma 1.20**

Dati un gruppo  $G$  e  $A, B$  due sottogruppi tali che  $A \leq B \leq G$ , 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  $\varphi_{g|B} \in \text{Aut}(B)$ <sup>3</sup>. Dal momento che  $A$  è un sottogruppo caratteristico di  $B$  abbiamo che  $\varphi_{g|B}(A) = \varphi_g(A) = A$ , pertanto  $A \trianglelefteq G$ . □

<sup>3</sup>Notiamo che  $\varphi_{g|B}$  in generale non è un coniugio di  $B$ , poiché  $g$  non appartiene necessariamente a  $B$ .

### Corollario 1.21

Ogni sottogruppo di  $\mathcal{R}$  è normale in  $D_n$ .

*Dimostrazione.* Siano  $\langle r^k \rangle$  un sottogruppo di  $\mathcal{R}$  e  $\varphi \in \text{Aut}(\mathcal{R})$ , allora  $\varphi(\langle r^k \rangle) = \langle r^k \rangle$  in quanto  $\varphi$  preserva l'ordine del sottogruppo e  $\langle r^k \rangle$  è l'unico sottogruppo di  $\mathcal{R}$  di tale ordine ( $\mathcal{R}$  è ciclico), pertanto  $\langle r^k \rangle$  è caratteristico in  $\mathcal{R}$ . Poiché  $\mathcal{R}$  è un sottogruppo normale di  $D_n$ , per il [Lemma 1.20](#) abbiamo  $\langle r^k \rangle \trianglelefteq D_n$ .  $\square$

**Osservazione 1.22** —  $\mathcal{R} = \langle r \rangle$  è caratteristico in  $D_n$  per  $n \geq 3$ . Infatti per ogni  $\varphi \in \text{Aut}(D_n)$  allora  $\text{ord}(r) = \text{ord}(\varphi(r))$ , da cui  $|\langle \varphi(r) \rangle| = n$ . Se fosse  $\varphi(r) \notin \mathcal{R}$  avremmo  $\text{ord}(\varphi(r)) = 2$ , quindi  $|\langle \varphi(r) \rangle| = n = 2$ , che è assurdo in quanto  $|D_n| \geq 6$ . Questo non è vero per  $D_2$ , che contiene una rotazione e due simmetrie: poiché  $\text{Aut}(D_2) \cong S_3$  esiste un  $\psi \in \text{Aut}(D_2)$  che manda la rotazione in una riflessione.

### Corollario 1.23

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

*Dimostrazione.*

- Se  $H_{k,h} \trianglelefteq D_n$  allora  $N_{D_n}(H_{k,h}) = D_n$ , in particolare  $r, s \in N_{D_n}(H_{k,h})$ ;
- se  $r, s \in N_{D_n}(H_{k,h})$ , poiché il normalizzatore è un sottogruppo di  $D_n$  abbiamo che  $D_n = \langle r, s \rangle \subseteq N_{D_n}(H_{k,h})$ , pertanto  $H_{k,h} \trianglelefteq D_n$ .

$\square$

Vediamo quali sono i sottogruppi normali della forma  $\langle r^k, sr^h \rangle$ , consideriamo i coniugi

$$\varphi_s : D_n \longrightarrow D_n : x \longmapsto sxs^{-1} \quad \varphi_r : D_n \longrightarrow D_n : x \longmapsto rxr^{-1}$$

e sia  $x_1^{\pm 1} \dots x_m^{\pm 1} \in H_{k,h} = \langle r^k, sr^h \rangle$ , allora

$$\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots \varphi_s(x_m)^{\pm 1} \in \langle srs, r^h s^{-1} \rangle = \langle sr^k s, r^h s^{-1} \rangle = \langle r^k, sr^{-h} \rangle$$

$$\varphi_r(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_r(x_1)^{\pm 1} \dots \varphi_r(x_m)^{\pm 1} \in \langle r^k, rsr^{h-1} \rangle = \langle r^k, sr^{h-2} \rangle$$

Pertanto  $H_{k,h} \trianglelefteq D_n$  se e solo se  $\langle r^k, sr^{h-2} \rangle = \langle r^k, sr^{-h} \rangle = \langle r^k, sr^h \rangle$ , se e solo se  $h \equiv h-2 \pmod{k}$ , cioè  $k \in \{1, 2\}$ .

- Se  $k = 1$  allora  $H_{k,h} = \langle r, s \rangle = D_n$ ;
- se  $k = 2$  (e  $n$  pari) allora  $H_{k,h} = \langle r^2, sr \rangle$  oppure  $H_{k,h} = \langle r^2, s \rangle$ .

**Osservazione 1.24** — Il secondo caso si presenta solo se  $n$  è pari, questo corrisponde 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. In un poligono con un numero dispari di lati gli assi di simmetria sono tutti passanti per i lati.

### §1.3.3 Classi di coniugio

Abbiamo visto che possiamo scrivere ogni elemento di  $D_n$  nella forma  $s^h r^k$ , dove  $s$  è una simmetria e  $r$  è una rotazione che genera  $\mathcal{R}$ , con  $h \in \{0, 1\}$  e  $k \in \{0, \dots, n-1\}$  in quanto  $\text{ord}(s) = 2$  e  $\text{ord}(r) = n$ . Inoltre tutti gli elementi della forma  $s r^k$  hanno ordine 2.

Consideriamo la classe di coniugio di  $r$ ,  $\mathcal{C}\ell(r) = \{g r g^{-1} \mid g \in D_n\}$ , fissato  $g \in D_n$  abbiamo due possibili valori per  $g r g^{-1}$ :

- se  $g \in \mathcal{R}$  allora  $g$  è una potenza di  $r$ , pertanto i due elementi commutano e si ha  $g r g^{-1} = r$ ;
- se  $g \notin \mathcal{R}$  allora  $g = s r^h$  con  $h \in \mathbb{Z}$ , quindi

$$(s r^h) r (s r^h)^{-1} = (s r^h) r (s r^h) = s r^{h+1} s r^h = s^2 r^{-1-h} r^h = r^{-1}$$

cioè  $\mathcal{C}\ell(r) = \{r, r^{-1}\}$ . In modo analogo si mostra che  $\mathcal{C}\ell(r^k) = \{r^k, r^{-k}\}$  per ogni  $k \in \mathbb{Z}$ .

**Osservazione 1.25** — Se  $n$  è pari, scriviamo  $n = 2m$  e consideriamo la classe di coniugio di  $r^m$ . Poiché  $r^m \neq e$  e  $r^{2m} = (r^m)^2 = e$  abbiamo che  $\text{ord}(r^m) = 2$ , cioè  $(r^m)^{-1} = r^m$ . Allora  $\mathcal{C}\ell(r^m) = \{r^m\}$ , pertanto abbiamo trovato un elemento del centro di  $D_n$  (infatti se  $G$  è un gruppo e  $x \in G$ , allora  $x \in Z(G)$  se e solo se  $\mathcal{C}\ell(x) = \{x\}$ ).

Consideriamo adesso la classe di coniugio di  $s r^h$ ,  $\mathcal{C}\ell(s r^h) = \{g (s r^h) g^{-1} \mid g \in D_n\}$ , fissato  $g \in D_n$  abbiamo due possibili valori per  $g (s r^h) g^{-1}$ :

- se  $g \in \mathcal{R}$  allora  $g = r^k$  con  $k \in \mathbb{Z}$ , pertanto

$$r^k (s r^h) r^{-k} = s r^{-k} r^h r^{-k} = s r^{h-2k}$$

- se  $g \notin \mathcal{R}$  allora  $g = s r^k$  con  $k \in \mathbb{Z}$ , pertanto

$$(s r^k) (s r^h) (s r^k)^{-1} = (s r^k) (s r^h) (s r^k) = s r^{2k-h}$$

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

**Osservazione 1.26** — La classe di coniugio di  $s r^h$  contiene tutte le simmetrie in cui l'esponente di  $r$  ha la stessa parità di  $h$ . Se  $n$  è dispari tutte le simmetrie appartengono alla stessa classe, mentre se  $n$  è pari abbiamo due classi distinte: quella delle simmetrie rispetto agli assi passanti per i vertici opposti e quella delle simmetrie rispetto agli assi passanti per i lati.

### §1.3.4 Legge di gruppo e omomorfismi

Se  $g$  è un elemento di  $D_n$  possiamo scrivere  $g$  in modo unico come  $s^a r^b$  con  $a \in \{0, 1\}$  e  $b \in \{0, \dots, n-1\}$ , utilizziamo questa proprietà per esplicitare la legge di gruppo di  $D_n$ . Fissati  $g_1, g_2 \in D_n$ , scriviamo  $g_1 = s^{a_1} r^{b_1}$  e  $g_2 = s^{a_2} r^{b_2}$  con  $a_1, a_2 \in \{0, 1\}$  e  $b \in \{0, \dots, n-1\}$ ,

$$g_1 g_2 = (s^{a_1} r^{b_1}) (s^{a_2} r^{b_2}) = s^{a_1} s^{a_2} (s^{a_2} r^{b_1} s^{-a_2}) r^{b_2} = s^{a_1} s^{a_2} \varphi_{s^{a_2}}(r^{b_1}) r^{b_2}$$

dove  $\varphi_{s^{a_2}}$  è l'automorfismo di coniugio per  $s^{a_2}$  (ricordiamo che  $s^{a_2} = s^{-a_2}$ ). Poiché  $\varphi_{s^{a_2}}$  è un omomorfismo e  $\varphi_x \circ \varphi_y = \varphi_{xy}$  per ogni  $x, y \in G$ , abbiamo  $(\varphi_{s^{a_2}}(r^{b_1})) = (\varphi_s^{a_2}(r))^{b_1}$ , quindi

$$g_1 g_2 = s^{a_1} s^{a_2} (\varphi_s^{a_2}(r))^{b_1} r^{b_2} = s^{a_1+a_2} r^{(-1)^{a_2} b_1 + b_2}$$

Per l'unicità della scrittura che stiamo usando (scegliendo  $a \in \{0, 1\}$  e  $b \in \{0, \dots, n-1\}$ )<sup>4</sup> possiamo identificare ogni elemento  $g = s^a r^b \in D_n$  con la coppia  $(a, b)$ , la legge di gruppo è quindi tale che

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

Usiamo il risultato appena ottenuto per descrivere gli omomorfismi da  $D_n$  in un qualsiasi gruppo  $G$ . Poiché ogni elemento  $g \in D_n$  si scrive come  $s^a r^b$ , con  $a, b \in \mathbb{Z}$ , un omomorfismo  $\varphi \in \text{Hom}(D_n, G)$  è univocamente determinato da  $\varphi(r)$  e  $\varphi(s)$ : infatti

$$\varphi(g) = \varphi(s^a r^b) = \varphi(s)^a \varphi(r)^b$$

Poniamo  $x = \varphi(s)$ ,  $y = \varphi(r)$ , necessariamente  $\text{ord}(x) \mid 2$  e  $\text{ord}(y) \mid n$ , cioè  $x^2 = e_G$  e  $y^n = e_G$ , inoltre

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

Mostriamo che effettivamente queste condizioni sono anche sufficienti:

### Proposizione 1.27

Dati un gruppo  $G$  e un'applicazione

$$\varphi : D_n \longrightarrow G : s^a r^b \longmapsto x^a y^b$$

dove  $x = \varphi(s)$  e  $y = \varphi(r)$ , 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  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$  abbiamo

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

dove  $\varphi_g$  è l'automorfismo di coniugio per  $g \in G$ . Allora abbiamo che  $\varphi$  è un omomorfismo, infatti per ogni  $h_1, h_2, k_1, k_2 \in \mathbb{Z}$

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

□

<sup>4</sup>Ricordiamo che  $\varphi_s^m = \underbrace{\varphi_s \circ \dots \circ \varphi_s}_{m \text{ volte}}$  in quanto l'operazione del gruppo degli automorfismi è la composizione di funzioni.

**Osservazione 1.28** — Abbiamo visto che le condizioni  $D_n = \langle r, s \rangle$  con  $\text{ord}(r) = n$ ,  $\text{ord}(s) = 2$  e  $sr s^{-1} = r^{-1}$  determinano in modo univoco la struttura astratta di  $D_n$ , racchiudiamo queste proprietà fondamentali nella scrittura

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

Tale scrittura si chiama **presentazione di un gruppo** e ne determina in modo univoco la classe di isomorfismo. Senza scendere troppo nei dettagli, nella presentazione indichiamo un insieme di generatori minimale e il minor numero di proprietà che i generatori devono rispettare affinché il gruppo abbia la struttura desiderata. Altri esempi di presentazioni sono

$$\langle x \mid x^n = e \rangle$$

$$\langle x \rangle$$

$$\langle x, y \mid x^2 = y^2 = e, xy = yx \rangle$$

rispettivamente dei gruppi  $\mathbb{Z}/n\mathbb{Z}$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (notiamo che  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  e  $D_2$  hanno la stessa presentazione, e questo ha senso in quanto i due gruppi sono isomorfi).

### §1.3.5 Automorfismi

Studiamo separatamente gli automorfismi di  $D_n$  per  $n \geq 3$  e di  $D_2$ .

Per  $n \geq 3$  consideriamo  $\varphi \in \text{Aut}(D_n)$ , 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:

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

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

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  $0 \leq h < n$ . Verifichiamo che  $\varphi$  è un omomorfismo, per la caratterizzazione che abbiamo dato sopra è sufficiente verificare che  $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)^{-1}$ :

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

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

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

da cui  $\text{Im}\varphi = D_n$ . 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  $|\text{Aut}(D_n)| = n\phi(n)$ .

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

$$\text{Aut}(D_2) \cong \text{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3$$

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

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

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  $GL_2(\mathbb{F}_2) \cong S_3$ . 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.

## §1.4 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  $\text{Aut}(H) \times \text{Aut}(K)$  in  $\text{Aut}(H \times K)$  data dall'omomorfismo

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

con

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

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

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

$$\begin{aligned} (\varphi_1 \times \varphi_2)((g_1, g_2)(h_1, h_2)) &= (\varphi_1(g_1 h_1), \varphi_2(g_2 h_2)) = (\varphi_1(g_1) \varphi_1(h_1), \varphi_2(g_2) \varphi_2(h_2)) = \\ &= (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(h_1), \varphi_2(h_2)) = ((\varphi_1 \times \varphi_2)(g_1, g_2))((\varphi_1 \times \varphi_2)(h_1, h_2)) \end{aligned}$$

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

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

$$\begin{aligned} \iota((\varphi_1, \varphi_2)(\psi_1, \psi_2))(g_1, g_2) &= \iota(\varphi_1 \psi_1, \varphi_2 \psi_2)(g_1, g_2) = (\varphi_1 \psi_1 \times \varphi_2 \psi_2)(g_1, g_2) = \\ &= (\varphi_1(\psi_1(g_1)), \varphi_2(\psi_2(g_2))) = (\varphi_1 \times \varphi_2)(\psi_1(g_1), \psi_2(g_2)) = \\ &= ((\varphi_1 \times \varphi_2)(\psi_1 \times \psi_2))(g_1, g_2) = (\iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2))(g_1, g_2) \end{aligned}$$

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

$$\begin{aligned} \ker \iota &= \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid \iota(\varphi_1, \varphi_2) = \text{id}_{\text{Aut}(H \times K)}\} = \\ &= \{(\varphi_1, \varphi_2) \in \text{Aut}(H) \times \text{Aut}(K) \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K) \forall (g_1, g_2) \in H \times K\} \end{aligned}$$

Poiché gli unici elementi  $\varphi_1 \in \text{Aut}(H)$ ,  $\varphi_2 \in \text{Aut}(K)$  tali che  $\varphi_1(H) = \{e_H\}$  e  $\varphi_2(K) = \{e_K\}$  sono rispettivamente  $\text{id}_{\text{Aut}(H)}$ ,  $\text{id}_{\text{Aut}(K)}$  abbiamo

$$\ker \iota = \{(\text{id}_{\text{Aut}(H)}, \text{id}_{\text{Aut}(K)})\} = \{\text{id}_{\text{Aut}(H \times K)}\}$$

### Proposizione 1.29

Dati due gruppi finiti  $H, K$ ,  $\text{Aut}(H) \times \text{Aut}(K) \cong \text{Aut}(H \times K)$  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  $\text{Aut}(H) \times \text{Aut}(K)$  in  $\text{Aut}(H \times K)$  definita come sopra, se  $\iota$  è surgettiva allora ogni elemento di  $\text{Aut}(H \times K)$  può essere scritto come  $\varphi_1 \times \varphi_2$  con  $\varphi_1 \in \text{Aut}(H)$  e  $\varphi_2 \in \text{Aut}(K)$ . 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  $\varphi \in \text{Aut}(H \times K)$  poniamo  $\varphi_1 \in \text{Aut}(H)$  tale che  $\varphi(g_1, e_K) = (\varphi_1(g_1), e_K)$  e  $\varphi_2 \in \text{Aut}(K)$  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  $\text{Aut}(H) \times \text{Aut}(K)$  e  $\text{Aut}(H \times K)$ .  $\square$

### Esempio 1.30

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  $\text{Aut}(\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/n\mathbb{Z})$  dentro a  $\text{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ , 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 1.31

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  $\text{ord}(g_1, g_2) \mid n$  allora  $\text{ord}(g_1) \mid n$  e  $\text{ord}(g_2) \mid n$ , ma  $\text{ord}(g_2) \mid m$  per il Teorema di Lagrange, quindi



$\text{ord}(g_2) = 1$  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.  $\square$

**Corollario 1.32**

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

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

## §1.5 Gruppo derivato

**Definizione 1.33.** 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 1.34** —  $[x, y] = e$  se e solo se  $x$  e  $y$  commutano.

### Proposizione 1.35

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  $\varphi \in \text{Hom}(G, A)$ , allora  $G' \subseteq \ker \varphi$ .

*Dimostrazione.* Mostriamo le affermazioni singolarmente:

- (1) consideriamo  $\varphi \in \text{Aut}(G)$ , 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

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

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 1.36** — 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 1.37** — Dato  $A$  un gruppo abeliano, il Primo Teorema di Omomorfismo produce una bigezione naturale tra  $\text{Hom}(G, A)$  e  $\text{Hom}(G/G', A)$ . Consideriamo infatti  $\varphi \in \text{Hom}(G, A)$ ,  $\pi_{G'} : G \rightarrow G/G'$  la proiezione al quoziente e  $\bar{\varphi} : G/G' \rightarrow A$ , il Teorema fornisce un'unico omomorfismo  $\bar{\varphi} : G/G' \rightarrow A$  che

rende commutativo il diagramma

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & A \\
 \pi_{G'} \downarrow & \circlearrowleft & \nearrow \bar{\varphi} \\
 G/G' & & 
 \end{array}$$

Viceversa, dato un omomorfismo  $\bar{\varphi} : G/G' \rightarrow A$  otteniamo un'unico omomorfismo  $\varphi : G \rightarrow A$  con la composizione  $\bar{\varphi} \circ \pi_{G'}$ .

### Esempio 1.38

Consideriamo il gruppo  $S_3$ , chiaramente  $(S_3)' \neq \{id\}$  in quanto  $S_3/\langle id \rangle \cong S_3$  che non è abeliano, pertanto abbiamo due possibilità:  $(S_3)' = S_3$  oppure  $(S_3)' = \langle (1\ 2\ 3) \rangle$ <sup>a</sup>. D'altra parte  $S_3/\langle (1\ 2\ 3) \rangle$  è isomorfo a  $\mathbb{Z}/2\mathbb{Z}$ , che è abeliano, pertanto  $(S_3)'$  è contenuto in  $\langle (1\ 2\ 3) \rangle$ , da cui necessariamente  $(S_3)' = \langle (1\ 2\ 3) \rangle$ . Più in generale vedremo che  $(S_n)' = \mathcal{A}_n$ , dove  $\mathcal{A}_n$  è il sottogruppo di  $S_n$  delle permutazioni pari (sappiamo già che  $(S_n)' \subseteq \mathcal{A}_n$  in quanto  $S_n/\mathcal{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ ).

<sup>a</sup>Gli unici sottogruppi normali di  $S_3$  sono  $\{id\}$ ,  $\langle (1\ 2\ 3) \rangle$ ,  $S_3$ .

## §1.6 Azioni di gruppo

### §1.6.1 Azioni transitive

**Definizione 1.39.** Siano  $G$  un gruppo e  $X$  un insieme, un'azione

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

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

#### Lemma 1.40

Dato  $G$  un gruppo finito e  $H \subsetneq G$  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  $[G : N_G(H)] = \frac{|G|}{|N_G(H)|}$  elementi distinti<sup>5</sup>. 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  $G \neq K$ .  $\square$

#### Proposizione 1.41

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

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

è un'azione transitiva valgono i seguenti fatti:

- (1) per ogni  $x, y \in X$  esiste  $g \in G$  tale che  $g \text{St}(x)g^{-1} = \text{St}(y)$ ;
- (2) se  $|X| \geq 2$  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:

<sup>5</sup>Infatti, se  $X = \{N \mid N \leq G\}$  e  $\varphi$  è l'azione di coniugio su  $X$ , per ogni  $N \in X$  abbiamo  $\text{St}(N) = N_G(N)$  e  $\text{Orb}(N) = \mathcal{C}\ell(N) = \{gNg^{-1} \mid g \in G\}$ . 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

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

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  $|X| \geq 2$ . 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 1.42** — 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 1.43

Dato  $G$  un gruppo finito e  $H \leq G$  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  $G/H$

$$\psi : G \longrightarrow S(G/H) : g \longmapsto \psi_g$$

con

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

Poiché l'immagine di  $\psi$  è un sottogruppo di  $S(G/H)$ , che è isomorfo a  $S_p$ , abbiamo che  $|\operatorname{Im} \psi| \mid p!$ , inoltre  $|\operatorname{Im} \psi| = \frac{|G|}{|\ker \psi|}$  come conseguenza del Primo Teorema di Omo-morfismo. Pertanto  $|\operatorname{Im} \psi| \mid (p!, |G|) = p$ , in quanto  $p$  è il più piccolo primo che divide

$|G|$ , quindi  $|\text{Im}\psi| \in \{1, p\}$ . D'altra parte osserviamo che  $\psi$  è un'azione transitiva, infatti per ogni  $g_1, g_2 \in G$  abbiamo  $\psi_{g_2g_1^{-1}}(g_1H) = g_2g_1^{-1}g_1H = g_2H$ , pertanto non è possibile  $\text{Im}\psi = \{id\}$ , da cui  $|\text{Im}\psi| = p$  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  $G$ .  $\square$

### §1.6.2 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 1.44 (Teorema di Cauchy)

Dato un gruppo  $G$  e un numero primo  $p$ , se  $p \mid |G|$  allora esiste  $g \in G$  tale che  $\text{ord}(g) = p$ .

#### Teorema 1.45 (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

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

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:

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

con

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

Fissato  $x \in X$ , poiché la cardinalità di  $\text{Orb}(x)$  divide l'ordine di  $\mathbb{Z}/p\mathbb{Z}$  abbiamo che  $|\text{Orb}(x)| \in \{1, p\}$ , in particolare le orbite di cardinalità 1 sono date dalle  $p$ -uple della forma  $(g, \dots, g)$  con  $g^p = e$ . Poniamo  $S = \{g \in G \mid \text{ord}(g) = p\}$  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

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

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 1.46.** 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  $\text{ord}(h) = 5$  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

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

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

$$\text{id}_H : H \longrightarrow H : h \longmapsto h$$

Poiché  $H \cong \mathbb{Z}/5\mathbb{Z}$ , abbiamo  $\text{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$ , d'altra parte  $|\text{Im} \varphi|$  divide  $(|G|, |H|) = 1$ , pertanto  $|\text{Im} \varphi| = 1$  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  $\text{ord}(hk) = \text{ord}(h) \text{ord}(k) = 15$  in quanto i due elementi hanno ordine coprimi. 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  $\text{ord}(h) \mid |Z_G(k)|$  e  $\text{ord}(k) \mid |Z_G(k)|$ , 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 1.47** — In generale dati  $x, y \in G$ , se  $x$  e  $y$  commutano allora  $\text{ord}(xy) = [\text{ord}(x), \text{ord}(y)]$  anche se  $G$  non è un gruppo abeliano.

**Esercizio 1.48.** 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  $G$

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

con

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

Fissato un isomorfismo  $\psi : S(G) \longrightarrow S_{2d}$  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

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

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  $[G : \ker(\pi_{\mathcal{A}_{2d}} \circ \varphi)] \leq 2$ . 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  $\text{ord}(\varphi(g)) = \text{ord}(g) = 2$ , 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  $[G : \varphi^{-1}(\mathcal{A}_{2d})] = 2$ ,  $\square$

Possiamo generalizzare il ragionamento appena usato nel seguente risultato

#### Proposizione 1.49

Dato un gruppo  $G$  e  $H \leq G$  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  $K \not\subseteq H$  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  $[K : H \cap K] = 2$ .  $\square$

### §1.6.3 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 1.50 (Teorema di Poincaré)

Dato un gruppo  $G$  finito e  $H \leq G$  un suo sottogruppo, se  $[G : H] = n$  allora esiste un sottogruppo normale  $N \triangleleft G$  tale che:

- (1)  $N \leq H \leq G$ ;
- (2)  $n \mid [G : N] \mid n!$ .



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

$$\psi : G \longrightarrow S(G/H) : g \longmapsto \psi_g$$

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  $\ker \psi \leq H$ ;

(2) poiché  $\ker \psi \leq H$  abbiamo  $[G : H] \mid [G : \ker \psi]$ , cioè  $n \mid [G : \ker \psi]$ . Dal Primo Teorema di Omomorfismo abbiamo che  $G/\ker \psi \cong \text{Im} \psi$ , che è un sottogruppo di  $S(G/H) \cong S_n$ , 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.  $\square$

**Osservazione 1.51** — In particolare, se  $G$  ha un sottogruppo di indice  $n$  e  $n! < |G|$  allora  $G$  ammette sottogruppi normali non banali.

## §1.7 Gruppo simmetrico

### §1.7.1 Generatori di $S_n$

Esibiamo alcuni insiemi di generatori per  $S_n$ :

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

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

- $\{(i\ i+1) \mid i \in \{1, \dots, n-1\}\}$ , infatti per ogni  $j$  abbiamo

$$(1\ j) = (j-1\ j)(1\ j-1)(j-1\ j)$$

- $\{(1\ 2), (1\ 2 \dots n)\}$ , infatti per ogni  $i$  abbiamo

$$(i\ i+1) = (1 \dots n)^{i-1}(1\ 2)(1 \dots n)^{1-i}$$

**Osservazione 1.52** — Non è vero in generale che una trasposizione e un  $n$ -ciclo generano  $S_n$ , consideriamo ad esempio  $\langle \sigma, \rho \rangle \leq S_4$  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  $\rho \in N_{S_4}(\sigma)$ , pertanto  $\langle \sigma, \rho \rangle = \langle \sigma \rangle \langle \rho \rangle$  e  $|\langle \sigma, \rho \rangle| = 8$ , pertanto è isomorfo a  $D_4$ .

### §1.7.2 Sottogruppi abeliani massimali di $S_n$

Vogliamo studiare i sottogruppi abeliani di  $S_n$ , caratterizzando in particolare i suoi sottogruppi abeliani massimali.

**Definizione 1.53.** Un sottogruppo  $G \leq S_n$  si dice **transitivo** se l'azione

$$\varphi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$

indotta da  $G$  su  $\{1, \dots, n\}$  è transitiva, cioè se per ogni  $i, j \in \{1, \dots, n\}$  esiste  $\sigma \in G$  tale che  $\sigma(i) = j$ .

#### Lemma 1.54

Dato  $G$  un sottogruppo abeliano di  $S_n$ , se  $G$  è transitivo allora  $|G| = n$ .

*Dimostrazione.* Consideriamo l'azione di  $G$  su  $\{1, \dots, n\}$

$$\psi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$

poiché  $G$  è transitivo, per la [Proposizione 1.41](#) gli stabilizzatori degli elementi di  $\{1, \dots, n\}$  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  $\text{St}(i) = \text{St}(j)$  per ogni  $i, j \in \{1, \dots, n\}$ . Osserviamo infine che

$$\bigcap_{i=1}^n \text{St}(i) = \{id_{S_n}\}$$

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

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

in quanto  $G$  è transitivo. □

### Lemma 1.55

Se  $a_1, \dots, a_k$  sono interi positivi tali che  $\sum_{i=1}^k a_i = 3m$ , con  $m \geq k$  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  $i \in \{1, \dots, k\}$ .

*Dimostrazione.* Senza perdita di generalità, a meno di aumentare  $k$  possiamo supporre  $a_i \in \{1, 2, 3\}$  per ogni  $i \in \{1, \dots, k\}$ , 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  $a_i \leq 3$  per ogni  $i \in \{1, \dots, n\}$ , 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  $i \in \{1, \dots, k\}$  in quanto possiamo supporre  $a_i \in \{1, 2, 3\}$  senza perdita di generalità. □

### Lemma 1.56

Dati  $\sigma, \tau \in S_n$ , se  $\sigma = (x_1 \dots x_k)$  è un  $k$ -ciclo allora

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

*Dimostrazione.*

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

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

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

□

**Esercizio 1.57.** Posto  $n = 3m$ , mostrare che la massima cardinalità di un sottogruppo abeliano di  $S_n$  è  $3^m$  e caratterizzare la sua classe di isomorfismo.

*Soluzione.* Per prima cosa, osserviamo che  $S_n$  contiene sottogruppi abeliani di cardinalità  $3m$ , ad esempio

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

è un sottogruppo abeliano di  $S_n$  di cardinalità  $3^m$ , essendo isomorfo a

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

Sia  $G$  un sottogruppo abeliano di  $S_n$  di ordine massimo, data

$$\psi : G \longrightarrow S_n : \sigma \longmapsto \sigma$$

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

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

che è iniettivo in quanto

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

per ogni  $i \in \{1, \dots, k\}$ , che è equivalente a  $\sigma = id_{S_n}$  dato che le orbite ricoprono  $\{1, \dots, n\}$ , da cui  $\ker \varphi = \{id_{S_n}\}$ . 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 7.3](#) abbiamo  $|G_i| = |\Omega_i|$  per ogni  $i \in \{1, \dots, k\}$ . Vale quindi la seguente disuguaglianza, data dall'injectività di  $\varphi$

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

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  $S_n$  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  $i \in \{1, \dots, k\}$ . Abbiamo quindi che  $\varphi$  è un isomorfismo e che  $G_1 \times \dots \times G_k$  è isomorfo a  $(\mathbb{Z}/3\mathbb{Z})^k$ , pertanto  $G$  è isomorfo a  $(\mathbb{Z}/3\mathbb{Z})^k$ .  $\square$

**Osservazione 1.58** — Se  $a_1, \dots, a_k$  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

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

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

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

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

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

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  $\Omega_1, \dots, \Omega_k$  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  $S_n$  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  $S_4$ , chiamato **gruppo di Klein** o **Klein 4-group**. Pertanto un sottogruppo abeliano di ordine massimo deve avere una di queste due forme.

**Osservazione 1.59** — I sottogruppi di  $S_n$  di questo tipo sono tutti coniugati tra loro, infatti se

$$G = \langle (x_1 \ x_2 \ x_3) \rangle \cdot \dots \cdot \langle (x_{n-2} \ x_{n-1} \ x_n) \rangle$$

$$G' = \langle (y_1 \ y_2 \ y_3) \rangle \cdot \dots \cdot \langle (y_{n-2} \ y_{n-1} \ y_n) \rangle$$

sono due sottogruppi abeliani di  $S_n$  di ordine massimo (per semplicità supponiamo  $n = 3m$ , gli altri due casi si studiano in modo analogo) consideriamo  $\sigma \in S_n$  tale che  $\sigma(y_i) = x_i$  per ogni  $i \in \{1, \dots, n\}$ , 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  $i \in \{1, \dots, n-2\}$ , pertanto  $G$  e  $G'$  sono coniugati.

### §1.7.3 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  $\mathcal{C}\ell_{S_n}(\sigma)$ . Poiché valgono  $|\mathcal{A}_n| = |\mathcal{C}\ell_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n}(\sigma)|$  e  $Z_{\mathcal{A}_n}(\sigma) = Z_{S_n}(\sigma) \cap \mathcal{A}_n$ , abbiamo

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

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

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

Nel primo caso otteniamo

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

poiché  $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$  abbiamo che le due classi coincidono. In particolare questo succede se  $Z_{S_n}(\sigma) \not\subseteq \mathcal{A}_n$ .

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

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

Più precisamente, abbiamo  $\mathcal{C}\ell_{S_n}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})$  per ogni  $\tau$  permutazione dispari. Infatti  $\mathcal{C}\ell_{\mathcal{A}_n}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1}) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$  (i coniugati di  $\tau\sigma\tau^{-1}$  sono anche coniugati di  $\sigma$ ), d'altra parte per ogni  $\rho \in S_n$  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:

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

Tuttavia se fosse  $|\mathcal{C}\ell_{\mathcal{A}_n}(\tau\sigma\tau^{-1})| = |\mathcal{C}\ell_{S_n}(\tau\sigma\tau^{-1})|$  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

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

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

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

#### §1.7.4 Studio di $S_5$

Consideriamo gli elementi di  $S_5$   $\sigma = (1\ 2\ 3\ 4\ 5)$ ,  $\tau = (2\ 5)(3\ 4)$ , 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  $\langle \tau \rangle \subseteq N_{S_5}(\langle \sigma \rangle)$ , 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  $\mathcal{C}\ell_{\mathcal{A}_n}(id) = \mathcal{C}\ell_{S_n}(id) = \{id\}$ , studiamo quindi le classi di  $\sigma, \tau, \rho$  fissate come sopra.

- $Z_{S_5}(\sigma) = \langle (a_1 \ a_2 \ a_3 \ a_4 \ a_5) \rangle$ , infatti

$$|Z_{S_5}(\sigma)| = \frac{|S_5|}{|\mathcal{C}\ell_{S_5}(\sigma)|} = \frac{5!}{4!} = 5$$

Allora  $Z_{S_5}(\sigma)$  contiene solo permutazioni pari, fissata  $\psi$  una permutazione dispari la sua classe di coniugio in  $S_5$  si scrive come

$$\mathcal{C}\ell_{S_5}(\sigma) = \mathcal{C}\ell_{\mathcal{A}_5}(\sigma) \cup \mathcal{C}\ell_{\mathcal{A}_5}(\psi\sigma\psi^{-1})$$

- $Z_{S_5}(\tau)$  non è contenuto in  $\mathcal{A}_5$ , infatti una trasposizione  $\psi$  disgiunta da  $\tau$  è una permutazione dispari che appartiene al centralizzatore. Pertanto

$$\mathcal{C}\ell_{S_5}(\tau) = \mathcal{C}\ell_{\mathcal{A}_5}(\tau)$$

- $Z_{S_5}(\rho)$  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

$$\mathcal{C}\ell_{S_5}(\rho) = \mathcal{C}\ell_{\mathcal{A}_5}(\rho)$$

### §1.7.5 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 1.60.** Un gruppo non banale  $G$  si dice **semplice** se i suoi unici sottogruppi normali sono  $\{e\}$  e  $G$ .

#### Proposizione 1.61

$\mathcal{A}_5$  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.  $\square$

#### Lemma 1.62

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  $(\text{ord}(g), [G : N]) = 1$ , consideriamo la proiezione

$$\pi_N : G \longrightarrow G/N (x \longmapsto xN)$$

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

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 1.63

$\mathcal{A}_n$  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

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

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  $\text{St}(i) = H_i$  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  $l_1 \leq l_2 \leq \dots \leq l_k$ , allora i suoi cicli hanno tutti la stessa lunghezza, cioè  $l_i = l_j$  per ogni  $i \neq j$ . Infatti, posto  $r = \min\{l_i \mid 1 \leq i \leq k\} = l_1$ , abbiamo

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

da cui  $\sigma^{l_1} = id$  in quanto ha almeno un punto fisso e quindi  $l_1 = l_2 = \dots = l_k$ . Fissata  $\sigma \in N$  possiamo quindi scrivere  $\sigma = \sigma_1 \dots \sigma_k$ , dove  $\sigma_i$  sono  $l$ -cicli disgiunti con  $l = \frac{n+1}{k}$ . Supponiamo per assurdo  $N \cap H_i \neq \{id\}$ , 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  $ord(\sigma_i) = l > 2$  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  $N \cap H_i = \{id\}$ , cioè  $\mathcal{A}_{n+1}$  è un gruppo semplice. □

### Corollario 1.64

L'insieme  $X = \{\sigma \in S_n \mid \sigma \text{ è un 5-ciclo}\}$  genera  $\mathcal{A}_n$  per  $n \geq 5$ .

*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  $\{id\}$ . □

### §1.7.6 Sottogruppi normali di $S_n$

#### Lemma 1.65

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

*Dimostrazione.* Sia  $\sigma \in Z(S_n) \setminus \{id\}$ , 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  $Z(S_n) = \{id\}$ .  $\square$

### Proposizione 1.66

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

*Dimostrazione.* Sia  $N$  un sottogruppo normale di  $S_n$ , 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  $\mathcal{A}_n \leq N$ : per il Teorema di Corrispondenza i sottogruppi di  $S_n$  contenenti  $\mathcal{A}_n$  sono in bigezione con i sottogruppi di  $S_n/\mathcal{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $N = \mathcal{A}_n$  oppure  $N = S_n$ ;
- se  $K = \{id\}$ , poiché  $[S_n : \mathcal{A}_n] = 2$  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  $S_n$  su  $N$

$$\varphi : N_{S_n}(N) \longrightarrow \text{Aut}(N) : g \longmapsto \varphi_g$$

dove  $\varphi_g$  è la mappa

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

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

$$\psi : \frac{N_{S_n}(N)}{Z_{S_n}(N)} \hookrightarrow \text{Aut}(N)$$

Poiché  $|N| = 2$  abbiamo  $N \cong \mathbb{Z}/2\mathbb{Z}$ , pertanto  $\text{Aut}(N) = \{id\}$ . Dato che  $N_{S_n}(N) = S_n$  per la normalità di  $N$  questo implica che sia  $Z_{S_n}(N) = S_n$ , cioè che  $N \subseteq Z(S_n)$ , ma questo è assurdo in quanto  $Z(S_n) = \{id\}$ .  $\square$

**Osservazione 1.67** — 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, ed è vero anche per  $n = 4$  anche se con una dimostrazione diversa. Infatti un sottogruppo  $H$  di indice 2 di  $S_n$  contiene necessariamente il commutatore, in quanto  $S_n/H \cong \mathbb{Z}/2\mathbb{Z}$ , d'altra parte il commutatore di  $S_n$  è  $\mathcal{A}_n$ , pertanto  $H = \mathcal{A}_n$ .

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

6

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

<sup>6</sup>Non sono sicuro di essere stato chiarissimo in questa sezione, se ci sono dei passi che ritenete poco comprensibili fatemelo sapere :)

**Proposizione 1.68**

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

*Dimostrazione.* Consideriamo l'azione di moltiplicazione a sinistra di  $S_n$  sull'insieme quoziente  $S_n/H$ :

$$\varphi : S_n \longrightarrow S(S_n/H) \cong S_n$$

tale azione è transitiva in quanto per ogni  $\sigma, \rho \in S_n$  vale

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

in particolare  $\ker \varphi \neq S_n$ . Poiché  $\ker \varphi \trianglelefteq S_n$  allora il nucleo di  $\varphi$  è banale oppure è  $\mathcal{A}_n$ . D'altra parte se fosse  $\ker \varphi = \mathcal{A}_n$  avremmo  $|\operatorname{Im} \varphi| = 2$ , pertanto l'orbita di ogni elemento di  $S_n/H$  contiene al più due elementi, ma questo è assurdo in quanto per la transitività di  $\varphi$  si ha  $\operatorname{Orb}(\rho H) = S_n/H$  per ogni  $\rho \in S_n$ , 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

$$\operatorname{St}(H) = \{\sigma \in S_n \mid \sigma H = H\} = \{\sigma \in H\} = H$$

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

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 1.69**

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

$$\varphi : S_n \longrightarrow \operatorname{Aut}(S_n) : \sigma \longmapsto \varphi_\sigma$$

**Osservazione 1.70** — In particolare gli automorfismo di  $S_n$  sono tutti interni nei casi  $n \notin \{2, 6\}$ , cioè sono coniugi per elementi di  $S_n$

Con le stesse notazioni di sopra chiamiamo  $\varphi'$  l'isomorfismo tra  $S(S_n/H)$  e  $S_n$ , componendo  $\varphi'$  con  $\varphi$  otteniamo un isomorfismo

$$\psi : S_n \longrightarrow S_n$$

che, per  $n \notin \{2, 6\}$ , è il coniugio per un elemento di  $S_n$ . Abbiamo quindi che  $\psi(H)$  è lo stabilizzatore di un elemento per l'azione naturale di  $S_n$  su  $\{1, \dots, n\}$ , ma allora anche  $H$  è uno stabilizzatore per tale azione in quanto coniugato a  $\psi(H)$ <sup>7</sup>. Pertanto i sottogruppi di  $S_n$  isomorfi a  $S_{n-1}$  sono tra loro coniugati e ognuno è lo stabilizzatore di un elemento per l'azione naturale di  $S_n$  su  $\{1, \dots, n\}$ .

<sup>7</sup>Notiamo che l'azione naturale di  $S_n$  su  $\{1, \dots, n\}$  è transitiva, pertanto gli stabilizzatori sono tra loro coniugati.

**§1.7.8 Costruzione di un automorfismo esterno di  $S_6$** 

Abbiamo visto che i casi  $n = 2$  e  $n = 6$  sono gli unici per cui non vale che  $S_n \cong \text{Aut}(S_n)$ . Per  $n = 2$  il motivo è semplice, infatti essendo  $S_2$  isomorfo a  $\mathbb{Z}/2\mathbb{Z}$  il suo gruppo di automorfismi è banale, per  $n = 6$  invece abbiamo che gli automorfismi di  $S_6$  non sono tutti elementi di  $\text{Inn}(S_6)$ , vogliamo quindi esibire un automorfismo di  $S_6$  che non sia interno.

Iniziamo osservando che  $S_5$  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,  $S_5$  ne contiene esattamente

$$\frac{1}{\phi(5)} \binom{5}{4} 3! = 6$$

Posto  $X = \{P_1, \dots, P_6\}$  l'insieme dei 5-Sylow di  $S_5$ , consideriamo l'azione di coniugio di  $S_5$  su  $X$

$$\varphi : S_5 \longrightarrow S(X) \cong S_6$$

dove l'isomorfismo tra  $S(X)$  e  $S_6$  è dato dall'associare  $P_i$  a  $i$ , poniamo  $\Phi$  la composizione di  $\varphi$  con tale isomorfismo, notiamo che  $\Phi$  è un'immersione di  $S_5$  in  $S_6$ . L'azione  $\varphi$  è transitiva in quanto i 5-Sylow di  $S_5$  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  $|\text{Im} \varphi| = 2$ , pertanto l'orbita di ogni elemento ha cardinalità 2, che è assurdo in quanto  $\text{Orb}(P_i) = X$  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  $S_5$  sull'insieme  $\{1, \dots, 6\}$ , notiamo quindi che  $\text{Im} \Phi$  non può essere lo stabilizzatore di un elemento di  $\{1, \dots, 6\}$  per l'azione naturale di  $S_6$  su tale insieme. Infatti se lo fosse esisterebbe  $k \in \{1, \dots, n\}$  tale che  $\Phi(\sigma)(i) = i$  per ogni  $\sigma \in S_5$ , ma questo è assurdo in quanto per la [Proposizione 1.41](#)  $S_5$  contiene una permutazione che agisce su  $\{1, \dots, 6\}$  senza punti fissi.

Abbiamo che  $H = \text{Im} \Phi$  è un sottogruppo di  $S_6$  di indice 6 e possiamo considerare l'azione transitiva e iniettiva di moltiplicazione a sinistra di  $S_6$  su  $S_6/H$

$$\alpha : S_6 \longrightarrow S(S_6/H) \cong S_6$$

chiamiamo  $\psi : S_6 \longrightarrow S_6$  l'isomorfismo risultante dalla composizione di  $\alpha$  con l'isomorfismo tra  $S(S_6/H)$  e  $S_6$ . Sia  $i \in \{1, \dots, 6\}$  l'elemento associato alla classe  $H$ , abbiamo visto nella dimostrazione della [Proposizione 1.67](#) che  $\psi(H) = \text{St}(i)$  per l'azione naturale di  $S_6$  sull'insieme  $\{1, \dots, 6\}$ . Concludiamo osservando che se  $\psi$  fosse un automorfismo interno di  $S_6$ , allora anche  $\psi^{-1}$  sarebbe un automorfismo interno, cioè  $\psi^{-1}$  sarebbe il coniugio per un qualche  $\sigma \in S_6$  fissato, da cui

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

che è assurdo in quanto  $H$  non può essere uno stabilizzatore per tale azione, pertanto  $\psi \notin \text{Inn}(S_6)$ .

## §1.8 Prodotti semidiretti

### §1.8.1 Descrizione di $S_4$ come prodotto semidiretto

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

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

dove  $(a \ b)$  è una trasposizione di  $S_n$ , vogliamo però dare una decomposizione di  $S_4$  più specifica.

Consideriamo il sottogruppo di Klein  $V_4 = \{id, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$  e  $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$  lo stabilizzatore di 4 secondo l'azione naturale di  $S_4$  su  $\{1, 2, 3, 4\}$ , osserviamo che  $V_4$  è normale in  $S_4$  in quanto unione delle classi di coniugio di ogni suo elemento<sup>8</sup> e che  $H$  è isomorfo a  $S_3$  (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  $V_4 H = S_4$  in quanto i due insiemi hanno la stessa cardinalità. Possiamo quindi scrivere

$$S_4 \cong V_4 \rtimes H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi} S_3$$

con

$$\varphi : S_3 \longrightarrow \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Specifichiamo come agisce la mappa  $\varphi$ <sup>9</sup>: consideriamo gli isomorfismi

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

$$\beta : H \longrightarrow S_3 : \sigma \longmapsto \sigma|_{\{1,2,3\}}$$

le immagini di  $\varphi$  in  $\text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$  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  $V_4$ :

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

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

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

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

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

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

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

<sup>8</sup>Le classe di coniugio in  $S_4$  di  $(1 \ 2)(3 \ 4)$  è  $\{(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$ .

<sup>9</sup>Se descriviamo  $S_4$  come prodotto semidiretto di due sottogruppi questo non è necessario, in quanto tale mappa è sempre il coniugio.

### §1.8.2 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 nulla ed è chiuso per composizione). Notiamo che un elemento di  $G$  è univocamente determinato dalla coppia  $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ <sup>10</sup>, pertanto  $G$  contiene  $n\phi(n)$  elementi. In realtà possiamo essere più precisi:

#### Proposizione 1.71

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  $g \in H$  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  $(b, a) \in \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ , la composizione in  $G$  produce la seguente operazione sulle coppie:

$$(b_1, a_1)(b_2, a_2) = (b_1 + a_1b_2, a_1 + a_2)$$

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

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

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

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

<sup>10</sup>Consideriamo qua solo l'insieme prodotto cartesiano, non la struttura di gruppo data dal prodotto diretto.

**Proposizione 1.72**

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

*Dimostrazione.* Siano  $r, s \in D_n$  tali che  $\text{ord}(r) = n$ ,  $\text{ord}(s) = 2$ ,  $D_n = \langle r, s \rangle$ , consideriamo  $\varphi \in \text{Aut}(D_n)$ . 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

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

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

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

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

**§1.8.3 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

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

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 mutlipli 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  $GL_3(\mathbb{R})$

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

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

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

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 1.73

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

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

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

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

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

$$(g, g)(n, e)(g^{-1}, g^{-1}) = (gng^{-1}, e) = (n, e) \quad \forall g \in G, \forall n \in N$$

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

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

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

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

**Proposizione 1.74** (Criterio di isomorfismo tra prodotti semidiretti)

Siano  $H, N$  due gruppi e  $\varphi : H \longrightarrow \text{Aut}(N)$  un omomorfismo. Dato  $f \in \text{Aut}(H)$  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 1.75**

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

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

Posto  $f_k \in \text{Aut}(\mathbb{Z}/q\mathbb{Z})$  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 1.65](#).

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

**Proposizione 1.76**

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

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

con

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

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  $\mathcal{G}_1 \triangleleft X_1$  e  $\mathcal{G}_2 \triangleleft X_2$ ), mentre  $f(\mathcal{H}_1)$  è un  $q$ -Sylow di  $X_2$  coniugato a  $\mathcal{H}_2$ . In particolare esiste  $\psi \in \text{Inn}(X_2)$  tale che

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

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

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

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

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

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

## §1.9 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;
- $A_5$  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, che 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 8 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  $N \triangleleft G$  tale che  $N \subseteq P_2$  e  $[G : N] \mid 3!$ , 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

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

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  $X$

$$\varphi : G \longrightarrow S(X) \cong S_4$$

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  $S(X) \cong S_4$ . 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

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

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 esser 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  $G/P_2$

$$\varphi : G \longrightarrow S(G/P_2) \cong S_5$$

Poiché  $|G| \nmid |S_5|$  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 1.77

$\mathcal{A}_5$  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  $X$

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

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

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

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

$$\text{St}(5) = \{\sigma \in \mathcal{A}_5 \mid \sigma(5) = 5\} \cong \mathcal{A}_4^{11}$$

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  $n_2 = 5$ .  $\square$

<sup>11</sup>Qua stiamo considerando l'azione naturale di  $\mathcal{A}_5$  sull'insieme  $\{1, 2, 3, 4, 5\}$ .

**Proposizione 1.78**

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

*Dimostrazione.* Dalle condizioni

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

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  $X$

$$\varphi : G \longrightarrow S(X) \cong S_3$$

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  $|G| > |S_3|$ ;

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

$$\varphi : G \longrightarrow S(X) \cong S_5$$

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  $H \leq S_5$  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  $\mathbb{Z}/2\mathbb{Z}$ <sup>12</sup>. 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  $S_2$  2-Sylow distinti di  $G$  tali che  $H = S_1 \cap S_2 \cong \mathbb{Z}/2\mathbb{Z}$ , consideriamo il normalizzatore  $N_G(H)$ . Osserviamo che  $S_1$  e  $S_2$  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 proprio di ordine al più  $3!$ , che è assurdo. Abbiamo quindi  $|N_G(H)| = 12$ , consideriamo l'azione di moltiplicazione a sinistra di  $G$  sull'insieme quoziente  $G/H$

$$\varphi : G \longrightarrow S(G/H) \cong S_5$$

<sup>12</sup>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.

□

**§1.10 Studio di  $SL_2(\mathbb{F}_3)$** 

Consideriamo il gruppo  $GL_2(\mathbb{F}_3)$ , ricordiamo che il determinante è un omomorfismo di gruppi surgettivo

$$\det : GL_2(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^*$$

e che il suo nucleo è il gruppo  $SL_2(\mathbb{F}_3) = \{M \in GL_2(\mathbb{F}_3) \mid \det M = 1\}$ , che è quindi un sottogruppo normale di  $GL_2(\mathbb{F}_3)$ . Inoltre, poiché  $\mathbb{F}_3^* \cong \mathbb{Z}/2\mathbb{Z}$  abbiamo che  $SL_2(\mathbb{F}_3)$  ha indice 2 in  $GL_2(\mathbb{F}_3)$ , pertanto  $|SL_2(\mathbb{F}_3)| = 24$  in quanto  $|GL_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$ .

Consideriamo quindi il gruppo  $S = SL_2(\mathbb{F}_3)$ , 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

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

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 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  $X$

$$\Phi : S \longrightarrow S(X) \cong S_4$$

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  $\text{Im} \Phi \cong S/Z(S)$ , che ha cardinalità 12. D'altra parte  $A_4$  è l'unico sottogruppo di  $S_4$  con 12 elementi, pertanto  $S/Z(S) \cong A_4$ , 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  $A_4$ , e tale bigezione preserva l'indice e la normalità dei sottogruppi. Poiché  $V_4$  è l'unico 2-Sylow di  $S_4$  abbiamo che  $S$  contiene un unico 2-Sylow di indice 3, cioè di cardinalità 8, chiamiamo  $J$  tale sottogruppo.  $J$  contiene le matrici

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{13}$$

entrambe di ordine 4, inoltre

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

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  $Z(S) \subseteq S'^{14}$ . Inoltre  $Z(S) \neq S'$  in quanto il quoziente è isomorfo a  $A_4$ , pertanto  $S'$  ha ordine 4 oppure 8, cioè  $[S : S'] \in \{3, 6\}$ . Consideriamo l'omomorfismo surgettivo

$$\varphi : S \longrightarrow A_4$$

dato dalla composizione della proiezione su  $S/Z(S)$  con l'isomorfismo tra il quoziente e  $A_4$ , per il Teorema di Corrispondenza  $\varphi(S')$  è un sottogruppo normale di  $A_4$  con  $[A_4 : \varphi(S')] = [S : S']$ . D'altra parte un sottogruppo di indice 6 di  $A_4$  è della forma  $\{id, (a \ b)(c \ d)\}$  con  $(a \ b)$  e  $(c \ d)$  trasposizioni disgiunte, che non è normale in  $A_4$ , pertanto  $\varphi(S')$  ha indice 3 e quindi  $S'$  ha ordine 8, da cui  $S' = J$ .

<sup>13</sup>Il determinante di questa matrice è  $-2$ , che è uguale a 1 in  $\mathbb{F}_3$

<sup>14</sup>Infatti l'unico elemento di ordine 2 di  $S$  è  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ .