

# **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>Insiemi di generatori</b>	<b>4</b>
<b>2</b>	<b>Automorfismi di <math>(\mathbb{Z}/p\mathbb{Z})^n</math></b>	<b>5</b>
<b>3</b>	<b>Gruppo diedrale</b>	<b>6</b>
3.1	Elementi del gruppo . . . . .	6
3.2	Sottogruppi . . . . .	7
3.3	Classi di coniugio . . . . .	10
3.4	Legge di gruppo e omomorfismi . . . . .	11
3.5	Automorfismi . . . . .	12
<b>4</b>	<b>Automorfismi di un prodotto diretto</b>	<b>14</b>
<b>5</b>	<b>Gruppo derivato</b>	<b>17</b>
<b>6</b>	<b>Azioni di gruppo</b>	<b>19</b>
6.1	Azioni transitive . . . . .	19
6.2	Teorema di Cauchy e Piccolo Teorema di Fermat . . . . .	21
6.3	Teorema di Poincaré . . . . .	23
<b>7</b>	<b>Gruppo simmetrico</b>	<b>25</b>
7.1	Sottogruppi abeliani massimali di $S_n$ . . . . .	25
7.2	Classi di coniugio in $\mathcal{A}_n$ . . . . .	28
7.3	Studio di $S_5$ . . . . .	29
7.4	Generatori di $S_n$ e $\mathcal{A}_n$ . . . . .	30

## Ringraziamenti

Diego Monaco, Niccolò Nannicini, Pietro Crovetto.

## §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 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  $\langle x_1, \dots, x_n \rangle = G$ .

## §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  $\tilde{\lambda}$  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 2.1

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  $\varphi(v_1)$ :  $\varphi(v_1)$  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

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

□

## §3 Gruppo diedrale

### §3.1 Elementi del gruppo

**Definizione 3.1.** Dato  $n \geq 2$  un naturale, consideriamo un poligono regolare di  $n$  vertici, definiamo il **gruppo diedrale** su  $n$  vertici  $D_n$  come l'insieme delle isometrie del piano che mandano i vertici in se stessi, cioè che fissano il poligono (per  $n = 2$  consideriamo le isometrie che mandano un segmento in se stesso).

**Osservazione 3.2 —**  $D_n$  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 3.3 —** 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 3.4.** Data  $r \in D_n$  una rotazione di ordine  $n$ , indichiamo con  $\mathcal{R}$  il **sottogruppo delle rotazioni**  $\langle r \rangle$ .

**Osservazione 3.5 —** 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 3.6 —** 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 3.7

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

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

*Dimostrazione.*

$$sr s^{-1} = r^{-1} \iff sr = r^{-1}s = (s^{-1}r)^{-1}$$

si conclude osservando che  $s^2 = 1$ , pertanto  $s^{-1} = s$  e

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

□

### Proposizione 3.8

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. Allora  $|D_n| = 2n$ . □

**Osservazione 3.9** — 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 3.10** — 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  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

## §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  $\langle \frac{n}{d} \rangle$ , con  $d \mid n$ .

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  $H/H \cap \mathcal{R} \cong \mathbb{Z}/2\mathbb{Z}$ , quindi  $|H \cap \mathcal{R}| = \frac{1}{2}|H|$ . Dato che  $H \cap \mathcal{R} \subseteq \mathcal{R}$ , 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 3.11

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

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

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

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

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  $m \in \mathbb{Z}$  abbiamo

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

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 3.12** — 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  $H$ .

**Osservazione 3.13** — 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 3.14 (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.

<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  $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$ .



*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 3.15

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  $\varphi_{g|B} \in \text{Aut}(B)$ . Dal momento che  $A$  è un sottogruppo caratteristico di  $B$  abbiamo che  $\varphi_{g|B}(A) = \varphi_g(A) = A$ , pertanto  $A \trianglelefteq G$ . □

### Corollario 3.16

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 2.15 abbiamo  $\langle r^k \rangle \trianglelefteq D_n$ . □

**Osservazione 3.17** —  $\mathcal{R}$  è caratteristico in  $D_n$  per  $n \geq 3$ . Infatti se  $\mathcal{R} = \langle r \rangle$ , necessariamente  $\text{ord}(r) = \text{ord}(\varphi(r))$ , 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  $|D_n| = 2n \geq 6$ . Questo non è vero per  $D_2$ , che contiene una rotazione e due simmetrie. Poiché  $\text{Aut}(D_2) \cong S_3$ , esiste un automorfismo che manda la rotazione in una riflessione, quindi che non fissa  $\mathcal{R}$ .

### Corollario 3.18

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  $H_{k,h} \trianglelefteq D_n$ .

□

Vediamo effettivamente quali sono i sottogruppi normali della forma  $\langle r^k, sr^h \rangle$ . Consideriamo gli automorfismi di coniugio

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

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 3.19** — 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.

### §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  $sr^h$  hanno ordine 2.

Consideriamo la classe di coniugio di  $r$ ,  $C_r = \{grg^{-1} \mid g \in D_n\}$ , fissato  $g \in D_n$  abbiamo due possibili valori per  $grg^{-1}$ :

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

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

cioè  $C_r = \{r, r^{-1}\}$ . In modo analogo si mostra che  $C_{r^k} = \{r^k, r^{-k}\}$  per ogni  $k \in \mathbb{Z}$ .

**Osservazione 3.20** — 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  $C_{r^m} = \{r^m\}$ , 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  $C_x = \{x\}$ ).

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

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

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

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

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

cioè  $C_{sr^k} = \{sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z}\}$ .

**Osservazione 3.21** — La classe di coniugio di  $sr^h$  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.

### §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  $b \in \{0, \dots, n-1\}$ ), 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  $\varphi \in \text{Hom}(D, G)$  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

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

Mostriamo che effettivamente queste condizioni sono anche sufficienti:

### Proposizione 3.22

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  $h_1, h_2, k_1, k_2 \in \mathbb{Z}$

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

□

**Osservazione 3.23** — Abbiamo visto che le condizioni  $D_n = \langle r, s \rangle$  con  $\text{ord}(r) = n$ ,  $\text{ord}(s) = 2$  e  $srs^{-1} = r^{-1}$  determinano in modo univoco la struttura astratta di  $D_n$ , racchiudiamo queste proprietà fondamentali nella scrittura

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

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

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

$$\langle x \rangle$$

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

e sono rispettivamente le presentazioni di  $\mathbb{Z}/n\mathbb{Z}$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (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).

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

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

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

## §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

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

con

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

Mostriamo che  $\iota$  è ben definita e che è 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

$$\ker(\varphi_1 \times \varphi_2) = \{(g_1, g_2) \in H \times K \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K)\} = \{(0, 0)\}$$

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

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

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  $e_{\text{Aut}(H)}$ ,  $e_{\text{Aut}(K)}$  abbiamo

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

### Proposizione 4.1

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 4.2

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 4.3

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.* Poniamo  $m = |H|$ ,  $n = |K|$ ,  $S = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^n = (e_H, e_K)\}$ , 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 4.4**

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

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



## §5 Gruppo derivato

**Definizione 5.1.** 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 5.2** —  $[x, y] = e$  se e solo se  $x$  e  $y$  commutano.

### Proposizione 5.3

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 5.4** — 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 5.5** — 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

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

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

### Esempio 5.6

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  $\{id\}$ ,  $\langle (1\ 2\ 3) \rangle$ ,  $S_3$ .

## §6 Azioni di gruppo

### §6.1 Azioni transitive

**Definizione 6.1.** 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 6.2

Dato  $G$  un gruppo finito e  $H \leq G$  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>3</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 6.3

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>3</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  $\text{Orb}(N) = C_N = \{gNg^{-1} \mid g \in G\}$ . Vale quindi la relazione  $|G| = |C_N| \cdot |N_G(N)|$ .

- (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  $h = gw g^{-1}$ . Allora

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

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 6.2](#) 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. □

#### Proposizione 6.4

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

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

indebolendo la condizione di appartenenza otteniamo l'inclusione

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

Poiché  $[G : \ker \psi] = [G : H] = p$  e  $G$  è un gruppo finito abbiamo che effettivamente  $\ker \psi = H$ , cioè  $H$  è normale in  $G$ . □

## §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 6.5 (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 6.6 (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:

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

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 6.7.** 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

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

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  $|\text{Im}\varphi|_H$  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 6.8** — 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 6.9.** 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 6.10

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  $[K : H \cap K] = 2$ .  $\square$

## §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 6.11 (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  $\psi$

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

indebolendo la condizione di appartenenza otteniamo l'inclusione

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

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



## §7 Gruppo simmetrico

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

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

**Definizione 7.1.** 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 7.2

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 6.3](#) 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  $\text{St}(i) = \{id_{S_n}\}$  per ogni  $i \in \{1, \dots, n\}$ . Fissato  $i \in \{1, \dots, n\}$ , abbiamo

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

in quanto  $G$  è transitivo. □

#### Lemma 7.3

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  $i \in \{1, \dots, k\}$ , 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.  $\square$

#### Lemma 7.4

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

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

$\square$

**Esercizio 7.5.** 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 7.2](#) abbiamo  $|G_i| = |\Omega_i|$  per ogni  $i \in \{1, \dots, k\}$ . Vale quindi la seguente disuguaglianza, data dall'iniettività 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 7.3](#) 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 7.3](#) 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 7.6** — Se  $a_1, \dots, a_k$  sono interi tali che

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

ragionando come nella dimostrazione del [Lemma 7.3](#) 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 7.7** — I sottogruppi di  $S_n$  di questo tipo sono tutti coniugati tra loro, infatti se

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

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

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 7.4](#) 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.

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

Fissato  $\sigma \in \mathcal{A}_n$ , indichiamo con  $C_{\mathcal{A}_n}(\sigma)$  la classe di coniugio ottenuta coniugando  $\sigma$  solo con elementi di  $\mathcal{A}_n$ , con  $C_{S_n}(\sigma)$  la classe ottenuta coniugando con tutti gli elementi di  $S_n$ . Vogliamo studiare come si relazionano  $C_{\mathcal{A}_n}(\sigma)$  e  $C_{S_n}(\sigma)$  al variare di  $\sigma \in \mathcal{A}_n$ .

Dato che  $|\mathcal{A}_n| = |C_{\mathcal{A}_n}(\sigma)| \cdot |Z_{\mathcal{A}_n}(\sigma)|$  e  $Z_{\mathcal{A}_n}(\sigma) = Z_{S_n}(\sigma) \cap \mathcal{A}_n$ , abbiamo

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

Poiché  $[S_n : \mathcal{A}_n] = 2$ , per la [Proposizione 6.10](#) 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

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

poiché  $C_{\mathcal{A}_n}(\sigma) \subseteq C_{S_n}(\sigma)$  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  $Z_{S_n}(\sigma) \subseteq \mathcal{A}_n$ ,

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

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

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

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

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

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

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

### §7.3 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	$\binom{5}{5} 4! = 4!$
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  $C_{\mathcal{A}_n}(id) = C_{S_n}(id) = \{id\}$ , 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

$$|Z_{S_5}(\sigma)| = \frac{|S_5|}{|C_{S_5}(\sigma)|} = \frac{5!}{4!} = 5$$

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

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

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

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

- $Z_{S_5}(\rho)$  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

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

## §7.4 Generatori di $S_n$ e $\mathcal{A}_n$

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

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

**Osservazione 7.8** — 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  $D_4$ , in effetti è proprio isomorfo a  $D_4$ , e quindi non genera  $S_4$ .