

# APPUNTI DI ALGEBRA

MANUEL DEODATO



# INDICE

<b>1</b>	<b>Teoria dei gruppi</b>	<b>3</b>
1.1	Il gruppo degli automorfismi	3
1.2	Azioni di gruppo	4
1.2.1	Azione di coniugio	6
1.2.2	Formula delle classi	7
1.3	I p-gruppi	8
1.4	Teoremi di Cauchy e Cayley	9
1.5	Commutatore e gruppo derivato	11
1.6	Gruppi diedrali	13
1.6.1	Sottogruppi di $D_n$	14
1.6.2	Centro, quozienti e automorfismi di $D_n$	17
1.7	Permutazioni	18
1.8	Gruppi di Sylow e prodotti diretti	23
1.9	Esercizi e complementi	26
1.9.1	Complementi di teoria	26
1.9.2	Esercizi	26

# 1 TEORIA DEI GRUPPI

## 1.1 Il gruppo degli automorfismi

**Lemma 1.0.1.** Siano  $H, G$  due gruppi ciclici; un omomorfismo  $\varphi : G \rightarrow H$  è univocamente determinato da come agisce su un generatore di  $G$ .

*Dimostrazione.* Sia  $g_0 \in G$  tale che  $\langle g_0 \rangle = G$  e sia  $\varphi(g_0) = \bar{h} \in H$ . Per  $g \in G$  generico, per cui  $g_0^k = g$  per qualche intero  $k$ , si ha:

$$\varphi(g) = \varphi(g_0^k) = \varphi(g_0)^k = \bar{h}^k$$

Cioè tutti gli elementi di  $\text{Im } \varphi$  sono esprimibili come potenze di  $\bar{h}$ . □

**Osservazione 1.1.** Non ogni scelta di  $\bar{h} \in H$  è ammissibile, ma bisogna rispettare l'ordine di  $g_0$ . Se  $g_0^n = e_G$ , allora  $e_H = \varphi(g_0^n) = \varphi(g_0)^n = \bar{h}^n$ . Questa condizione, impone che  $\text{ord}(\bar{h}) \mid \text{ord}(g_0)$ .

**Definizione 1.1 (Gruppo degli automorfismi).** Sia  $G$  un gruppo; si definisce il gruppo dei suoi automorfismi come

$$\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ è un isomorfismo di gruppi}\}$$

**Esempio 1.1.** Si calcola  $\text{Aut}(\mathbb{Z})$ .

*Svolgimento.* Il gruppo  $(\mathbb{Z}, +)$  è ciclico, quindi un omomorfismo è determinato in base a come agisce su un generatore. Prendendo, per esempio 1, si definisce  $q_a : \mathbb{Z} \rightarrow \mathbb{Z}$  tale che  $q_a(1) = a$ ; perché  $\langle q_a(1) \rangle = \mathbb{Z}^1$ , è necessario che  $a$  sia un generatore di  $\mathbb{Z}$ , perciò sono ammessi  $a = \pm 1$ . In questo caso,  $\text{Aut}(\mathbb{Z}) = \{\pm \text{Id}_{\mathbb{Z}}\} \cong (\mathbb{Z}/2\mathbb{Z}, +)$ . ■

**Teorema 1.1.**  $\text{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ .

*Dimostrazione.*  $(\mathbb{Z}/m\mathbb{Z}, +)$  è ciclico, quindi si stabilisce l'azione di  $f : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  su un generatore. Preso, allora,  $\bar{k} \in \mathbb{Z}/m\mathbb{Z}$  tale che  $\text{gcd}(k, m) = 1$  e scelto  $f(\bar{k}) = \bar{a}$ , si ha che  $\langle f(\bar{k}) \rangle = \langle \bar{a} \rangle = \mathbb{Z}/m\mathbb{Z} \iff \text{gcd}(a, m) = 1 \iff \bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$ . □

**Definizione 1.2 (Automorfismo interno).** Sia  $G$  un gruppo; si definisce  $\phi_g : G \rightarrow G$ ,  $\forall g \in G$ , come  $\phi_g(x) = gxg^{-1}$  ed è detto *automorfismo interno*. L'insieme di questi automorfismi, al variare di  $g \in G$ , forma il gruppo

$$\text{Int}(G) = \{\phi_g : G \rightarrow G \mid g \in G \text{ e } \phi_g \text{ automorfismo interno}\}$$

**Proposizione 1.1.** Sia  $G$  un gruppo; allora  $\text{Int}(G) \triangleleft \text{Aut}(G)$  e  $\text{Int}(G) \cong G/Z(G)$ .

---

<sup>1</sup>Richiesto dal fatto che  $q_a$  sia suriettivo.

*Dimostrazione.*  $\text{Int}(G)$  è un sottogruppo di  $\text{Aut}(G)$  perché  $\text{Id}(x) = exe^{-1} = x \Rightarrow \text{Id} \in \text{Int}(G)$ . Inoltre,  $\phi_g \circ \phi_h(x) = ghxh^{-1}g^{-1} = \phi_{gh}(x) \in \text{Int}(G)$  e  $\phi_{g^{-1}} \circ \phi_g(x) = x \Rightarrow \phi_g^{-1} = \phi_{g^{-1}} \in \text{Int}(G)$ .

È un sottogruppo normale perché  $\forall f \in \text{Aut}(G)$ , si ha

$$f \circ \phi_g \circ f^{-1}(x) = f(gf^{-1}(x)g^{-1}) = f(g)xf(g)^{-1} \in \text{Int}(G)$$

Per finire, si definisce  $\Phi : G \rightarrow \text{Int}(G)$ . Questo è un omomorfismo perché  $\Phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(g)\Phi(h)$ . È, inoltre, suriettivo perché ogni automorfismo interno è associato ad un elemento di  $G$ , cioè  $\forall \phi_g \in \text{Int}(G)$ ,  $\exists g \in G : \Phi(g) = \phi_g$ . Allora, la tesi deriva dal I teorema di omomorfismo, visto che  $\text{Ker } \Phi = Z(G)$ .  $\square$

**Osservazione 1.2.**  $H \triangleleft G \iff \phi_g(H) = H, \forall \phi_g \in \text{Int}(G)$ .

*Dimostrazione.* Per ogni elemento di  $\text{Int}(G)$ , si ha  $\phi_g(H) = H \iff gHg^{-1} = H \iff H \triangleleft G$ .  $\square$

**Definizione 1.3 (Sottogruppo caratteristico).** Sia  $G$  un gruppo e  $H < G$ . Si dice che  $H$  è *caratteristico* se è invariante per automorfismo, cioè  $\forall f \in \text{Aut}(G)$ ,  $f(H) = H$ .

**Corollario 1.1.1.** Sia  $G$  un gruppo; per la proposizione 1.1 e l'osservazione 1.2 se  $H$  è caratteristico, allora  $H \triangleleft G$ .

Il viceversa è falso, cioè normale  $\nRightarrow$  caratteristico; infatti, in  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , il sottogruppo  $\langle(1, 0)\rangle$  è normale, ma non caratteristico perché l'automorfismo che scambia le coordinate è tale per cui  $\langle(1, 0)\rangle \mapsto \langle(0, 1)\rangle \neq \langle(1, 0)\rangle$ .

## 1.2 Azioni di gruppo

**Definizione 1.4 (Azione).** Sia  $G$  un gruppo; un'azione di  $G$  su un insieme  $X$  è un omomorfismo

$$\gamma : \begin{array}{ccc} G & \longrightarrow & S(X) = \{f : X \rightarrow X \mid f \text{ biettiva}\} \\ g & \longmapsto & \psi_g : \psi_g(x) = g \cdot x \end{array}$$

Più concretamente, si definisce *azione* la mappa  $\gamma : G \times X \rightarrow X$  tale che

- (a).  $e \cdot x = x$ , per  $e \in G$  e  $x \in X$ ;
- (b).  $h \cdot (g \cdot x) = (hg) \cdot x$ , per  $g, h \in G$  e  $x \in X$ .

Si verifica che una mappa  $\gamma : G \times X \rightarrow X$ , con  $G$  gruppo e  $X$  insieme generico, che soddisfa le proprietà (a) e (b), è tale che  $\gamma(g)(x) = \psi_g(x)$  (cioè a  $g$  fissato) è biettiva.

*Dimostrazione.* Per l'iniettività, si ha  $\psi_g(x) = \psi_g(y) \iff g \cdot x = g \cdot y \iff x = y$ , visto che si può applicare l'azione inversa  $\gamma(g^{-1})$  ad entrambi i lati. Per la suriettività,

invece, si nota che  $\forall x \in X$ , si trova anche una  $y \in X : y = g^{-1} \cdot x$  dovuta all'azione di  $\gamma(g^{-1})$ , per cui  $\psi_g(y) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = x$ .  $\square$

**Esempio 1.2.** Sia  $G = \{z \in \mathbb{C}^* \mid |z| = 1\} \cong S^1$  la circonferenza unitaria e  $X = \mathbb{R}^2$ . Un'azione di  $G$  su  $X$  è una rotazione definita da  $\gamma(z) = R(\arg z)$ . Questa è un omomorfismo perché  $\gamma(zw) = R(\arg zw) = R(\arg z + \arg w) = R(\arg z)R(\arg w) = \gamma(z)\gamma(w)$ .

Un'azione  $\gamma$  di  $G$  su  $X$  definisce, proprio su  $X$ , una relazione di equivalenza definita da

$$x \sim_\gamma y \iff x = \psi_g(y) = g \cdot y, \text{ con } x, y \in X \quad (1.2.1)$$

La relazione di equivalenza è ben definita perché le  $\psi_g$  sono mappe biettive.

**Definizione 1.5 (Orbita).** Sia  $\gamma : G \rightarrow S(X)$  un'azione di  $G$  gruppo su  $X$ . Dato  $x \in X$ , la sua classe di equivalenza rispetto alla relazione  $\sim_\gamma$  è detta *orbita* ed è indicata con  $\text{Orb}(x) = \{g \cdot x \mid g \in G\}$ .

Ricordando che una relazione di equivalenza fornisce una partizione dell'insieme su cui è definita, si ha:

$$X = \bigsqcup_{x \in R} \text{Orb}(x) \quad (1.2.2)$$

con  $R$  insieme dei rappresentanti di tutte le orbite. Se, poi,  $X$  ha cardinalità finita, allora:

$$|X| = \sum_{x \in R} |\text{Orb}(x)| \quad (1.2.3)$$

**Definizione 1.6 (Stabilizzatore).** Sia  $\gamma : G \rightarrow S(X)$  un'azione di  $G$  su  $X$ ; allora per ogni  $x \in X$ , si definisce l'insieme

$$\text{Stab}(x) = \{g \in G \mid g \cdot x = x\} < G$$

**Lemma 1.1.1.** Sia  $G$  un gruppo che agisce su un insieme  $X$  e sia  $x \in X$  un suo elemento. Dati anche  $g \cdot x, h \cdot x \in \text{Orb}(x)$  tali che  $g \cdot x = h \cdot x$ , allora  $g$  e  $h$  appartengono alla stessa classe di  $G/\text{Stab}(x)$ .

*Dimostrazione.* Se  $g \cdot x, h \cdot x \in \text{Orb}(x)$  sono uguali, allora  $x = h^{-1}g \cdot x$ , cioè  $h^{-1}g \in G$  lascia invariato  $x$ , quindi è in  $\text{Stab}(x)$ . Da questo segue che  $h \text{Stab}(x) = hh^{-1}g \text{Stab}(x) = g \text{Stab}(x)$ .  $\square$

**Teorema 1.2 (Teorema di orbita-stabilizzatore).** Esiste una mappa biettiva  $\Gamma : \text{Orb}(x) \rightarrow G/\text{Stab}(x)$  tale che  $\Gamma(g \cdot x) = g \text{Stab}(x)$ .

*Dimostrazione.*  $\Gamma$  è iniettiva come diretta conseguenza del lemma 1.1.1 ed è suriettiva perché  $\forall g \text{ Stab}(x) \in G/\text{Stab}(x), \exists g \cdot x \in \text{Orb}(x)$  tale che  $\Gamma(g \cdot x) = g \text{Stab}(x)$ . Segue che  $|\text{Orb}(x)| = |G|/|\text{Stab}(x)|$ .  $\square$

**Osservazione 1.3.** Si osserva che, per il teorema di orbita-stabilizzatore, la cardinalità di un'orbita indica il numero di classi laterali dello stabilizzatore nel gruppo che compie l'azione, cioè il teorema di orbita-stabilizzatore si può riscrivere come  $|\text{Orb}(x)| = [G : \text{Stab}(x)] = |G/\text{Stab}(x)| = |G|/|\text{Stab}(x)|$ .

### 1.2.1 Azione di coniugio

Un caso notevole di azione è il coniugio: per  $X = G$ , si definisce  $\gamma : G \rightarrow \text{Int}(G) \subset S(G)$ . Le orbite indotte da questa azione sono dette *classi di coniugio* e si indicano con  $\text{cl}(x)$ , mentre lo stabilizzatore è detto *centralizzatore* e si indica con:

$$Z(x) = \{g \in G \mid g \cdot x = gxg^{-1} = x\} \quad (1.2.4)$$

Come conseguenza del teorema di orbita-stabilizzatore (1.2), si ha:

$$|G| = |\text{cl}(x)||Z(x)|, \quad \forall x \in G \quad (1.2.5)$$

**Proposizione 1.2.** Sia  $G$  un gruppo e  $\gamma$  l'azione di coniugio su di esso; allora

$$\bigcap_{x \in G} Z(x) = Z(G)$$

*Dimostrazione.* Si ha  $g \in Z(x), \forall x \iff gxg^{-1} = x, \forall x \in G \iff g \in Z(G)$ .  $\square$

**Osservazione 1.4 (Centro di un sottogruppo).** Sia  $G$  un gruppo e  $H < G$ ; allora il centro di  $H$  è definito come

$$\bigcap_{x \in H} Z(x) = Z(H)$$

Si considera, ora, l'azione di coniugio di un gruppo  $G$  su  $X = \{H \subseteq G \mid H < G\}$  e  $\gamma(g) = \psi_g$  tale che  $\psi_g(H) = gHg^{-1}$ . Questa è un'azione ed è ben definita.

*Dimostrazione.* Per dimostrare che è un'azione, si deve mostrare che la mappa  $g \mapsto \psi_g$  è un omomorfismo e che  $\psi_g : X \rightarrow X$  sia biettiva.

Si nota che  $g \mapsto \psi_g$  è un omomorfismo perché  $\psi_{g_1 g_2}(H) = g_1 g_2 H g_2^{-1} g_1^{-1} = \psi_{g_1} \circ \psi_{g_2}(H)$ , cioè  $g_1 g_2 \mapsto \psi_{g_1} \psi_{g_2}$ . Inoltre,  $\psi_g : X \rightarrow X$  è biettiva perché  $\exists \psi_g^{-1} = \psi_{g^{-1}} : \psi_{g^{-1}} \circ \psi_g(H) = H$ .

Per mostrare che è ben definita, si fa vedere che effettivamente  $\forall g, \psi_g$  mappa un sottogruppo di  $G$  in un altro sottogruppo, cioè che  $gHg^{-1} < G$ . Intanto,  $e \in gHg^{-1}$

perché  $H < G \Rightarrow e \in H \Rightarrow geg^{-1} = e$ ; poi,  $(ghg^{-1})(gh'g^{-1}) = gh'h'g^{-1} \in gHg^{-1}$  e  $h^{-1} \in H \Rightarrow \exists (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$  elemento inverso.  $\square$

Lo stabilizzatore di questa azione è detto *normalizzatore*, in quanto è definito come tutti elementi di  $G$  rispetto a cui  $H$  è normale:

$$N_G(H) = \text{Stab}(H) = \{g \in G \mid gHg^{-1} = H\} \quad (1.2.6)$$

Infine, l'orbita è l'insieme (classe di equivalenza) di tutti i coniugati di un sottogruppo di  $G$ :

$$\text{Orb}(H) = \{gHg^{-1} \mid g \in G\} \quad (1.2.7)$$

Per il teorema di orbita-stabilizzatore (1.2), si ha:

$$|G| = |N_G(H)| |\text{Orb}(H)| \quad (1.2.8)$$

da cui si ricava anche che  $H \triangleleft G \iff N_G(H) = G \iff \text{Orb}(H) = \{H\}$ .

### 1.2.2 Formula delle classi

Si ricorda che le orbite definite da un'azione di un gruppo  $G$  su un insieme  $X$  formano una partizione di  $X$  stesso, in quanto sono delle classi di equivalenza. Se  $|X| < \infty$ , si ha:

$$|X| = \sum_{x \in R} |\text{Orb}(x)| = \sum_{x \in R} \frac{|G|}{|\text{Stab}(x)|} = \sum_{x \in R'} 1 + \sum_{x \in R \setminus R'} \frac{|G|}{|\text{Stab}(x)|} \quad (1.2.9)$$

con  $R$  insieme dei rappresentanti delle orbite e  $R'$  insieme dei rappresentati delle orbite tali che  $\text{Orb}(x) = \{x\}$ , cioè degli elementi invarianti sotto l'azione di  $G$ .

**Teorema 1.3 (Formula delle classi).** Sia  $\gamma : G \rightarrow S(G)$  l'azione di coniugio di un gruppo  $G$  su un insieme  $X$ ; allora:

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

*Dimostrazione.* Segue per quanto appena detto e dall'osservazione che

$$R' = \{x \in R \mid \text{Orb}(x) = \{x\}\} = \{x \in R \mid gxg^{-1} = x\} = Z(G)$$

Visto che ogni orbita del genere contiene un solo elemento, i rappresentanti delle orbite sono esattamente tutti gli elementi di  $Z(G)$ , cioè un elemento  $x \in Z(G)$  non può essere contenuto in nessun'altra orbita, se non nel singoletto  $\{x\}$ . Perciò, la relazione in eq. 1.2.9, avendo  $X = G$ , conferma la tesi.  $\square$

### 1.3 I p-gruppi

**Definizione 1.7 (p-gruppo).** Sia  $p \in \mathbb{Z}$  un numero primo; allora si dice che  $G$  è  $p$ -gruppo se  $|G| = p^n$ , per qualche  $n \in \mathbb{N}$ .

**Proposizione 1.3.** Il centro di un  $p$ -gruppo è non-banale.

*Dimostrazione.* Per la formula delle classi, si ha:

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

Se  $|Z(G)| = p^n$ , la tesi è verificata, altrimenti  $\exists x \in R \setminus Z(G)$ , quindi tale che  $Z(x) \subsetneq G$ ; allora, per qualche intero  $k > 0$ , si ha  $|G|/|Z(x)| = p^k$ , da cui

$$|Z(G)| = p^n - \sum_{x \in R \setminus Z(G)} p^k \implies p \mid |Z(G)|$$

Visto che  $e \in Z(G)$ , deve risultare  $|Z(G)| \geq 1$ , da cui  $|Z(G)| = p^s$ , per qualche intero  $s > 1$ .  $\square$

**Lemma 1.3.1.** Vale  $G/Z(G)$  ciclico  $\iff G$  è abeliano.

*Dimostrazione.* Sia  $G/Z(G)$  ciclico e sia  $x_0Z(G)$  il suo generatore. Date due classi laterali distinte  $xZ(G), yZ(G) \in G/Z(G)$  e visto che  $x_0Z(G)$  genera, si avrà  $x_0^m Z(G) = xZ(G)$  e  $x_0^n Z(G) = yZ(G)$ , ossia, per  $z, w \in Z(G)$ ,  $x = x_0^m z$ ,  $y = x_0^n w$ . Allora:

$$xy = x_0^m z x_0^n w = x_0^m x_0^n z w = x_0^n w x_0^m z = yx$$

Essendo questo valido per  $x, y \in G$  generiche, si è dimostrata l'implicazione verso destra.

Per l'implicazione inversa, sia  $G$  abeliano; allora  $Z(G) = G$  e  $G/Z(G) = \{e\}$ , che è ovviamente ciclico.  $\square$

**Proposizione 1.4.** Un gruppo di ordine  $p^2$  è abeliano.

*Dimostrazione.* Sia  $G$  un  $p$ -gruppo tale che  $|G| = p^2$ . Per mostrare che è abeliano, si fa vedere che  $Z(G) = G$ , ossia  $|Z(G)| = p^2$ . Per la proposizione 1.3, si può avere solamente  $|Z(G)| = p$ , oppure  $|Z(G)| = p^2$ . Se, per assurdo, fosse  $|Z(G)| = p$ , allora  $|G|/|Z(G)| = p$ , quindi  $G/Z(G)$  avrebbe ordine primo e, quindi, sarebbe ciclico; per il lemma precedente (1.3.1), però, questo è assurdo perché risulterebbe anche abeliano al contempo, ma senza avere  $|Z(G)| = |G|$ . Quindi deve essere  $|Z(G)| = p^2 = |G| \implies Z(G) = G$ , da cui  $G$  è abeliano.  $\square$



## 1.4 Teoremi di Cauchy e Cayley

**Lemma 1.3.2 (Teorema di Cauchy abeliano).** Sia  $p$  un primo e  $G$  un gruppo abeliano finito; se  $p \mid |G|$ , allora  $\exists x \in G : \text{ord}(x) = p$ .

*Dimostrazione.* Sia  $|G| = pn$ ; si procede per induzione su  $n$ . Il passo base è ovvio: se  $|G| = p$ , allora è ciclico e, quindi, contiene un elemento di ordine  $p$ .

Per il passo induttivo, si suppone che la tesi sia vera per ogni  $m < n$  e si dimostra per  $n$ .

Sia, allora  $|G| = pn$ ; sia, poi  $y \in G$ ,  $y \neq e$  tale che  $\langle y \rangle = H < G$ : per Lagrange,  $|G| = |G/H||H|$ . Allora, se  $p \mid |G| \Rightarrow p \mid |H|$ , oppure  $p \mid |G/H|$ .

- Se  $p \mid |H|$ , allora può essere  $|G| = |H|$ , caso in cui  $G = \langle y \rangle$  sarebbe ciclico e, quindi, avrebbe un elemento di ordine  $p^1$ , oppure può essere  $|H| = pm < pn$ , caso in cui l'elemento di ordine  $p$  è presente per ipotesi induttiva.
- Se  $p \mid |G/H|$ , invece, allora  $|G/H| = pm' < pn$  perché  $H$  contiene almeno due elementi, cioè  $y$  ed  $e$ ; per ipotesi induttiva, allora, esiste  $zH \in G/H$  il cui ordine è  $p$ . Considerando la proiezione  $\pi_H : G \rightarrow G/H$  tale che  $x \mapsto xH$  e ricordando che è un omomorfismo, si ha che, per questo motivo,  $\text{ord}(zH) \mid \text{ord}(z) \Rightarrow \text{ord}(z) = pk$ ; se  $k = n$ , allora  $G$  è ciclico e  $z^n$  ha ordine  $p$ , altrimenti, se  $k < n$ , si ha la tesi per induzione.

□

**Teorema 1.4 (Teorema di Cauchy).** Sia  $p$  un numero primo e  $G$  un gruppo finito; se  $p \mid |G|$ , allora esiste  $x \in G : \text{ord}(x) = p$ .

*Dimostrazione.* Sia  $|G| = pn$ , con  $p$  primo e  $n \in \mathbb{N}$ ; si procede per induzione su  $n$ . Se  $n = 1$ ,  $|G| = p \Rightarrow G$  è ciclico, quindi  $\exists x \in G : \langle x \rangle = G$  e  $\text{ord}(x) = p$ .

Per il passo induttivo, si assume che la tesi sia valida per ogni  $m < n$  e si dimostra per  $n$ .

Si nota che se  $\exists H < G$  tale che  $p \mid |H|$ , allora  $|H| = pm$ ,  $m < n \Rightarrow \exists x \in H$  tale che  $\text{ord}(x) = p$  per ipotesi induttiva. Si assume, dunque, che non esista alcun sottogruppo di  $G$  il cui ordine sia divisibile per  $p$ . Per la formula delle classi

$$pn - \sum_{x \in G \setminus Z(G)} \frac{|G|}{|Z(x)|} = |Z(G)|$$

Ora, visto che  $Z(x) < G \Rightarrow p$  non divide  $|Z(x)|$ , quindi si ha la certezza che, essendo  $p \mid |G| = |Z(x)||G/Z(x)|$ ,  $p$  divide  $|G/Z(x)|$ . Allora  $p \mid |Z(G)|$ , per cui  $Z(G) = G$ ;

---

<sup>1</sup>In questo caso, l'elemento di ordine  $p$  sarebbe proprio  $y^{p^{n-1}} \in G$ ; infatti,  $(y^{p^{n-1}})^p = y^{p^n} = e$ , visto che  $|G| = p^n$ .

infatti, se così non fosse, sarebbe un sottogruppo proprio di  $G$  e  $p$  non lo potrebbe dividere, il che è assurdo.

Da questo, segue che  $G$  è abeliano, quindi la tesi segue dal teorema di Cauchy per gruppi abeliani (lemma 1.3.2).  $\square$

**Proposizione 1.5.** Siano  $H, K < G$ ; allora  $HK < G \iff HK = KH$  e  $|HK| = |H||K|/|H \cap K|$ .

*Dimostrazione.* Per la prima parte, è sufficiente osservare che per  $hk \in HK$ , l'elemento neutro  $(hk)^{-1} = k^{-1}h^{-1}$  sta in  $HK$  se e solo se  $HK = KH$ , e, allo stesso modo, il prodotto è chiuso cioè  $hkh'k' = hh''k''k' \in HK$  solamente se  $HK = KH$  così da poter trovare un elemento di  $HK$  che sia uguale a  $kh' \in KH$  che compare in tale prodotto.

La seconda parte, invece, si verifica considerando l'applicazione  $\gamma : H \times K \rightarrow HK$  tale che  $\gamma((h, k)) = hk$ , che è evidentemente suriettiva; inoltre, se  $s \in H \cap K$ , allora  $(hs, s^{-1}k) \in H \times K \Rightarrow \gamma((hs, s^{-1}k)) = hk$ , il che vuol dire che  $\forall hk \in HK$ , si trovano  $|H \cap K|$  coppie in  $H \times K$  che hanno immagine  $hk$ , da cui la tesi.  $\square$

#### Classificazione dei gruppi di ordine 6

Sia  $G$  un gruppo di ordine 6; per Cauchy, allora, esistono  $x, y \in G$  tali che  $\text{ord}(x) = 2$  e  $\text{ord}(y) = 3$ . Se  $G$  è abeliano, poi, si ha  $\text{ord}(xy) = 6^a$ , quindi  $G = \langle xy \rangle \cong \mathbb{Z}/6\mathbb{Z}$ . Se, invece,  $G$  non è abeliano, si considera il sottogruppo  $\langle x, y \rangle$  e si considera anche l'insieme  $\langle x \rangle \langle y \rangle$  che, in generale, non è un sottogruppo.

Applicando la proposizione precedente (1.5), si ha che  $|\langle x, y \rangle| = (3 \cdot 2)/1 = 6^b$ , da cui  $G = \langle x \rangle \langle y \rangle$ , con  $\langle x \rangle = \{e, x\}$  e  $\langle y \rangle = \{e, y, y^2\}$ , quindi  $G = \{e, x, y, xy, y^2, xy^2\}$ .

Per finire, si mostra che  $G \cong S_3$ . Per farlo, si definisce  $\phi : G \rightarrow S_3 = \{e, \tau, \rho, \tau\rho, \tau^2, \rho\tau^2\}$  tale che  $\phi(x) = \rho$  e  $\phi(y) = \tau$ , con  $\tau = (1, 2, 3)$  e  $\rho = (1, 2)$ . Questa mappa è suriettiva per costruzione, quindi è biettiva per questioni di cardinalità; inoltre, è un omomorfismo, da cui segue la tesi.

<sup>a</sup>Si dimostra per calcolo diretto; per esempio:  $(xy)^3 = xyxyxy = xxxyyy = x$ .

<sup>b</sup>L'intersezione è solo l'unità perché i due elementi hanno ordini diversi, quindi generano gruppi disgiunti.

**Teorema 1.5 (Teorema di Cayley).** Sia  $G$  un gruppo; allora  $G$  è isomorfo a un sottogruppo di  $S(G)$ . In particolare, se  $|G| = n$ , allora  $G$  è isomorfo a un sottogruppo di  $S_n$ .

*Dimostrazione.* Si definisce l'azione

$$\phi : \begin{array}{ccc} G & \longrightarrow & S(G) \\ g & \longmapsto & \gamma_g \end{array}, \quad \text{tale che } \gamma_g(x) = g \cdot x$$

Questa è ben definita perché  $\gamma : G \rightarrow G$  è biettiva, infatti  $\gamma_g(x) = \gamma_g(y) \iff g \cdot x = g \cdot y \iff x = y$  e  $\forall y \in G, \exists \gamma_g(g^{-1} \cdot y) = y$ , il che mostra che è rispettivamente

iniettiva e suriettiva. Inoltre,  $\phi$  è un omomorfismo (ovvio) ed è anche iniettiva perché  $\text{Ker } \phi = \{g \in G \mid \phi_g = \phi_e\} = \{g \in G \mid g \cdot x = x\} = \{e\}$ . Da questo, segue che  $S(G)$  contiene una copia isomorfa a  $G$ .  $\square$

## 1.5 Commutatore e gruppo derivato

**Definizione 1.8.** Sia  $G$  un gruppo e  $S \subset G$  un suo sottoinsieme; allora  $\langle S \rangle$  è il più piccolo sottogruppo di  $G$  contenente anche  $S$ .

**Proposizione 1.6.** Dato  $G$  un gruppo e  $S \subset G$  un suo sottoinsieme, vale la relazione

$$\langle S \rangle = \{s_1 s_2 \dots s_k \mid k \in \mathbb{N}, s_i \in S \cup S^{-1}\} = X$$

con  $S^{-1} = \{s^{-1} \mid s \in S\}$ .

*Dimostrazione.* Per definizione

$$\langle S \rangle = \bigcap_{\substack{H < G \\ S \subset H}} H$$

Questa scrittura è ben definita perché l'intersezione di gruppi è ancora un gruppo e, in questo modo, si ha il gruppo più piccolo contenente  $S$ ; se così non fosse, ne esisterebbe uno più piccolo ancora, che, però, farebbe parte dell'intersezione e sarebbe assurdo.

Ora, per quanto detto sopra,  $S$  è contenuto in tutti i gruppi la cui intersezione genera  $\langle S \rangle$ , quindi anche  $S^{-1}$  deve essere contenuto in tali sottogruppi di  $G$ . Segue che  $S, S^{-1} \subset H \Rightarrow X \subset H, \forall H < G$  e  $S \subset H$ , quindi  $X \subset \bigcap H = \langle S \rangle$ .

Allo stesso tempo,  $X$  è evidentemente un sottogruppo di  $G$  e contiene  $S$  per costruzione, quindi  $X \supset \langle S \rangle$ , da cui la tesi.  $\square$

**Definizione 1.9 (Commutatore).** Sia  $G$  un gruppo; dati  $g, h \in G$ , il loro *commutatore* è definito come

$$[g, h] = ghg^{-1}h^{-1}$$

**Definizione 1.10 (Gruppo derivato).** Dato un gruppo  $G$ , si definisce *gruppo dei commutatori*, o *derivato* di  $G$ , il gruppo

$$G' = \langle [g, h] \mid g, h \in G \rangle = [G : G]$$

Ora si caratterizza il gruppo derivato. Intanto, si ricorda che  $\langle S \rangle$  è abeliano  $\iff \forall s_1, s_2 \in S, s_1 s_2 = s_2 s_1$ ,  $\langle S \rangle$  è normale  $\iff \forall g \in G, \forall s \in S, gsg^{-1} \in \langle S \rangle$  e, infine,  $\langle S \rangle$  è caratteristico  $\iff \forall f \in \text{Aut}(G), \forall s \in S$  si ha  $f(s) \in S$ . Applicando queste alla definizione di commutatore, si ottiene la seguente.

**Proposizione 1.7 (Proprietà del derivato).** Sia  $G$  un gruppo e  $G'$  il suo derivato; allora:

- (a).  $G' = \{e\} \iff G$  è abeliano;
- (b).  $G' \triangleleft G$ ;
- (c).  $G'$  è caratteristico in  $G$ ;
- (d). dato  $H \triangleleft G$ , se  $G/H$  è abeliano, allora  $G' \subset H$ .

*Dimostrazione.* La (a) è immediata perché  $G' = \{e\} \iff \forall g_1, g_2 \in G, [g_1, g_2] = e$ , cioè  $g_1$  e  $g_2$  commutano, da cui  $G$  abeliano.

Per la (b),  $\forall x \in G, \forall g, h \in G$ , si ha

$$\begin{aligned} x[g, h]x^{-1} &= xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} \\ &= [xgx^{-1}, xhx^{-1}] \in G' \end{aligned}$$

Per la (c), si nota che  $\forall f \in \text{Aut}(G), \forall g, h \in G$ , si ha:

$$f([g, h]) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = [f(g), f(h)] \in G'$$

Infine, per la (d), se  $H \triangleleft G$  e  $G/H$  è abeliano, si ha  $\forall x, y \in G$

$$xHyH = yHxH \Rightarrow xyH = yxH \implies x^{-1}y^{-1}xy \in H \Rightarrow [x, y] \in H$$

da cui  $H \supset G'$ . □

**Corollario 1.5.1.** Sia  $G$  un gruppo e  $G'$  il suo derivato; allora  $G/G'$  è sempre abeliano ed è chiamato *abelianizzazione* di  $G$ , nel senso che è il più grande quoziente abeliano di  $G$ .

*Dimostrazione.* Si mostra che  $G/G'$  è sempre abeliano. Siano, quindi  $gG', hG' \in G/G'$  due classi laterali; allora si osserva che

$$(gG')(hG') = ghG' = hg[g^{-1}, h^{-1}]G' = hgG'$$

visto che  $g^{-1}h^{-1}gh = [g^{-1}, h^{-1}] \in G'$ . Allora, dalla proprietà (d) della precedente proposizione (1.7), si ha  $G' \subset H = G'$ , cioè in questo caso si ha l'inclusione nell'insieme più piccolo, ovvero proprio  $G'$ . Questo vuol dire che  $G/G'$  è il quoziente con più elementi che sia abeliano perché ottenuto tramite quoziente con  $G'$ , che è l'insieme più piccolo che soddisfa la proprietà<sup>1</sup>. □

---

<sup>1</sup>Per controposizione, se  $G' \not\subset H \implies G/H$  non abeliano.

## 1.6 Gruppi diedrali

**Definizione 1.11 (Gruppo diedrale).** Per  $n \in \mathbb{N}$ , si considera un  $n$ -agono regolare nel piano; l'insieme di tutte le isometrie del piano che mandano l' $n$ -agono in se stesso è indicato con  $D_n$  ed è noto col nome di *gruppo diedrale*.

**Proposizione 1.8.** Per  $n \in \mathbb{N}$ , il gruppo diedrale  $D_n$  ha cardinalità  $|D_n| = 2n$ .

*Dimostrazione.* Un'isometria è univocamente determinata dall'immagine di un vertice e di un lato adiacente al vertice stesso; allora, l'immagine può essere pari a  $n$  possibili vertici, con due, conseguenti, possibilità per il lato, da cui  $2n$  possibili isometrie.  $\square$

**Proposizione 1.9.** Sia  $\rho$  una rotazione che sottende un lato<sup>1</sup> e  $\sigma$  una simmetria (riflessione) dell' $n$ -agono regolare; allora  $\rho^n = e$ ,  $\sigma^2 = e$  e  $\sigma\rho\sigma = \rho^{-1}$ .

*Dimostrazione.* Visto che  $\rho$  manda un lato dell' $n$ -agono regolare nella posizione del successivo, impiegherà  $n$  iterazioni a far tornare il lato di partenza nella posizione originale; similmente, se  $\sigma$  è una riflessione, sarà sufficiente riapplicarla per far tornare l' $n$ -agono nella posizione originale.

Per l'ultima, si nota che, componendo una rotazione e una riflessione, si ottiene una riflessione; applicando la seconda proprietà, si ottiene  $\sigma\rho\sigma\rho = e \Rightarrow \sigma\rho\sigma = \rho^{-1}$ .  $\square$

**Osservazione 1.5.** Le isometrie del piano che agiscono su un  $n$ -agono, quindi gli elementi di  $D_n$ , si possono mettere in relazione con  $\text{GL}_2(\mathbb{R})$ , cioè possono essere rappresentate tramite matrici:

$$\rho \xrightarrow{\gamma} \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} = M_\rho \quad \sigma \xrightarrow{\gamma} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = M_\sigma \quad (1.6.1)$$

Si nota, inoltre, che indicando con  $\mathbb{D}_n$  il gruppo generato da queste matrici, allora la mappa  $\gamma : \langle \rho, \sigma \rangle \rightarrow \mathbb{D}_n$  e notare che questo è un omomorfismo di gruppi; infatti, la composizione di isometrie che fissano un punto, sono ancora isometrie che fissano lo stesso punto (in questo caso, l' $n$ -agono). Questo per dire che la mappa  $\rho^i \sigma^j \mapsto M_\rho^i M_\sigma^j$  è ben definita.

Si può, inoltre, verificare che  $M_\rho^n = \text{Id}$ ,  $M_\sigma^2 = \text{Id}$  e  $M_\sigma M_\rho M_\sigma = M_\rho^{-1}$ , per cui si conclude che  $\gamma$  è un omomorfismo.

Essendo  $\gamma$  un omomorfismo, si vede anche che  $\rho$  e  $\sigma$ , come elementi di  $D_n$ , non sono legati da alcuna relazione perché, altrimenti, lo sarebbero anche le loro matrici associate, cosa che sarebbe assurda.

**Proposizione 1.10.** Tutti gli elementi di  $D_n$  si scrivono come  $\sigma\rho^i$ , oppure  $\rho^i$ , con  $i \in \{0, \dots, n-1\}$ .

---

<sup>1</sup>Cioè che manda un lato nel successivo.

*Dimostrazione.* Sia  $g \in D_n$ ; allora  $g$  sarà una generica composizione di riflessioni e rotazioni del tipo  $g = \rho^{a_1} \sigma^{b_1} \dots \rho^{a_k} \sigma^{b_k}$ , dove  $a_i \in \mathbb{Z}$  e  $b_j \in \{0, 1\}$ . Usando le relazioni  $\sigma^2 = \rho^n = e$ , si riscalgano gli esponenti per scrivere  $g = \rho^{c_1} \sigma \dots \rho^{c_m} \sigma$ , dove si sono anche, eventualmente, uniti esponenti di rotazioni consecutive (quindi  $m \leq k$ ).

Usando  $\sigma^2 = e$  e assumendo  $c_1 \neq 0$ , si può scrivere

$$g = \rho^{c_1} \sigma \dots \rho^{c_m} \sigma = \sigma \sigma \rho^{c_1} \sigma \sigma \rho^{c_2} \dots \sigma \rho^{c_m} \sigma = \sigma \rho^{-c_1} \rho^{-c_2} \dots \rho^{-c_m} = \sigma \rho^{-d}$$

dove si è fatto uso della relazione  $\sigma \rho \sigma = \rho^{-1}$  e con  $d \equiv -\sum_{i=1}^m c_i \pmod{n}$ .

Se, invece,  $c_1 = 0$  (cioè la *parola* inizia con  $\sigma$ ), allora  $g = \rho^{-c_2} \dots \rho^{-c_m} = \rho^{d'}$ , con  $d' \equiv -\sum_{i=2}^m c_i \pmod{n}$ .  $\square$

Grazie alla precedente proposizione, è possibile definire  $\rho^{[i]} = \rho^i$ , con  $[i] \in \mathbb{Z}/n\mathbb{Z}$ , visto che  $\rho^n = e$ .

Inoltre, se  $\rho, \sigma \in D_n$ , allora  $\langle \rho, \sigma \rangle < D_n$ ; però, per quanto detto finora, si ha  $|\langle \rho, \sigma \rangle| = 2n$  perché  $\rho^n = e = \sigma^2$ , quindi, per ragioni di cardinalità, segue che  $D_n = \langle \rho, \sigma \rangle$ .

### 1.6.1 Sottogruppi di $D_n$

**Numero di elementi di ordine  $k$ .** Sia  $\rho$  una rotazione in  $D_n$ ; si considera  $\langle \rho \rangle \cong C_n < D_n$ <sup>1</sup>.

Essendo  $C_n$  ciclico, vi sono  $\phi(k)$  elementi di ordine  $k$ , se  $k \mid n$ . Oltre alle  $n$  rotazioni  $\rho^i$ , in  $D_n$  sono presenti anche le  $n$  riflessioni  $\sigma \rho^i$ ; osservando che  $\sigma \rho^i \sigma \rho^i = \rho^{-i} \rho^i = e$ , si conclude che se  $n$  è pari, vi sono  $n + 1$  elementi di ordine 2 (cioè le  $n$  riflessioni e  $\rho^{n/2}$ ), mentre se  $n$  è dispari, vi sono  $n$  elementi di ordine 2. Ricapitolando:

$$\# \{\text{elementi di ordine } k\} = \begin{cases} n + 1 & , \text{ se } k = 2 \text{ e } n \text{ pari} \\ n & , \text{ se } k = 2 \text{ e } n \text{ dispari} \\ \phi(k) & , \text{ se } k \mid n \\ 0 & , \text{ altrimenti} \end{cases} \quad (1.6.2)$$

visto che le  $n$  riflessioni sono tutte di ordine 2 e l'esistenza di  $\rho^{n/2}$  dipende dalla parità di  $n$ .

**I sottogruppi.** Nel punto precedente, si è notato che  $C_n$  è uno dei sottogruppi. Inoltre, i sottogruppi di  $C_n$  sono noti: ne esiste uno per ogni divisore dell'ordine del gruppo, cioè  $n$  in questo caso, per cui se  $H < D_n$  e  $H < C_n$ , allora  $H$  è l'unico sottogruppo di ordine  $|H|$ . Se, invece  $H < D_n$  e  $H \not< C_n$ , allora  $H$  contiene almeno una riflessione  $\tau$ .

**Proposizione 1.11.** Si ha  $(H \cap C_n) \sqcup (\tau H \cap C_n)$  ed esiste una mappa biettiva tra  $(H \cap C_n)$  e  $(\tau H \cap C_n)$ .

---

<sup>1</sup>Qui, con  $C_n$  si indica un generico gruppo ciclico di ordine  $n$ .

*Dimostrazione.* Si considera

$$\begin{array}{ccc} D_n & \xrightarrow{\gamma} & \text{GL}_2(\mathbb{R}) \xrightarrow{\det} \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z} \\ & \searrow \varphi & \nearrow \end{array}$$

dove  $\gamma$  è l'omomorfismo definito che a  $\rho$  e  $\sigma$  associa le relative matrici, mentre le matrici di  $\text{GL}_2(\mathbb{R})$  sono mappate a  $\{\pm 1\}$  tramite il determinante:  $\det M_\rho = 1$  e  $\det M_\sigma = -1$ . La mappa  $\phi = \gamma \circ \det$  è un omomorfismo suriettivo proprio per come è definita  $\gamma$  (cioè è un omomorfismo) e per il teorema di Binet per cui  $\det(M_\rho^i M_\sigma^j) = \det(M_\rho)^i \det(M_\sigma)^j = 1^i (-1)^j = 1 \iff j = 0$ .

Considerando, quindi,  $\varphi : D_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ , la sua restrizione  $\varphi_H$  con  $H < D_n$  e  $H \not\leq C_n$  è suriettiva e il suo kernel è  $H \cap C_n$ ; per il I teorema di omomorfismo, allora  $H/(H \cap C_n) \cong \mathbb{Z}/2\mathbb{Z}$ . Per il teorema di Lagrange, poi, si ha  $|H|/|H \cap C_n| = |\mathbb{Z}/2\mathbb{Z}|$ , per cui  $|H| = 2|H \cap C_n|$ .

Si nota che  $\tau H \cap C_n \not\subset H \cap C_n$  perché se  $h \in H$ , allora  $\det(M_\tau M_h) = \det M_\tau \det M_h = -1$ , per cui i due insiemi sono disgiunti; inoltre,  $\tau h_1 = \tau h_2 \Rightarrow h_1 = h_2$ , per cui  $|\tau H \cap C_n| = |H \cap C_n|$ . Considerando, allora

$$\psi : \begin{array}{ccc} H \cap C_n & \longrightarrow & \tau H \cap C_n \\ h & \longmapsto & \tau h \end{array}$$

questa è biettiva. Ora,  $H \cap C_n = \langle \rho^m \rangle = \{e, \rho^m, \rho^{2m}, \dots, \rho^{n-m}\}$ , con  $m \mid n$ ; se  $\tau = \sigma \rho^i$ , allora

$$\tau H \cap C_n = \{\sigma \rho^i, \sigma \rho^{i+m}, \dots, \sigma \rho^{i+n-m}\}$$

quindi, l'unione dei due restituisce tutto  $H$ . □

Segue che  $H$  è composto da  $m$  rotazioni e  $m$  simmetrie; in particolare  $H = \langle \rho^m, \tau \rangle \cong D_m$ , quindi, se  $m \mid n$ , si hanno dei sottogruppi della forma  $\mathbb{Z}/m\mathbb{Z}$  e  $D_m$ .

**Sottogruppi normali.** Per lo studio dei sottogruppi normali, si considerano le due seguenti proposizioni.

**Proposizione 1.12.** Sia  $G$  un gruppo e sia  $H < G$ ; se  $H$  ha indice 2 in  $G$ , allora  $H \triangleleft G$ .

*Dimostrazione.* Sia, quindi,  $G/H = \{H, \tau H\}$ , per qualche  $\tau \in G$ ; dato  $g \in G$ , allora, si ha  $g = h_1$ , oppure  $g = \tau h_2$ , con  $h_1, h_2 \in H$ . Sia, ora,  $hg \in Hg$  per  $g \in G \setminus H$ ; allora  $g = \tau h_3$ , oppure  $hg = \tau h_4 = \tau h_3 h_3^{-1} h_4 = gh_5$ , per cui  $Hg \subset gH$ . Inoltre,  $|Hg| = |gH|$ , quindi deve essere  $Hg = gH$  e, quindi,  $H \triangleleft G$ . □

**Proposizione 1.13.** Siano  $H \triangleleft G$  e  $K < H$ , con  $K$  caratteristico in  $H$ ; allora  $K \triangleleft G$ .

*Dimostrazione.* Si considera, per  $g \in G$ ,  $\phi_g : G \rightarrow G$  con  $\phi_g(x) = gxg^{-1}$ ; per definizione, si ha  $\phi_g(H) = H$ , quindi  $\phi_g|_H$  è un automorfismo, quindi  $\phi_g|_H(K) = K$ ,  $\forall g \in G \Rightarrow gKg^{-1} = K$ , pertanto  $K \triangleleft G$ .  $\square$

L'indice di  $C_n$  in  $D_n$  è 2, quindi  $C_n \triangleleft D_n$  per la prima proposizione. Visto che per  $G$  ciclico di ordine  $n$ , esiste un unico  $H$ , con  $|H| = m \mid n$ , allora ogni sottogruppo di un gruppo ciclico è caratteristico e, quindi, nel caso di  $D_n$ , ogni sottogruppo di  $\langle \rho \rangle \cong C_n$  è caratteristico. Per la seconda proposizione, questo significa che ogni sottogruppo di  $C_n$  è normale; se  $n$  è pari, allora  $\langle \rho^2 \rangle < C_n$  ha  $n/2$  elementi.

Considerando  $H < D_n$  e  $H \not\subset C_n$ , con  $H \cap C_n = \langle \rho^2 \rangle$ , si ha

$$H = \langle \rho^2 \rangle \sqcup \tau \langle \rho^2 \rangle$$

quindi  $[D_n : H] = 2$ , per cui  $H \triangleleft D_n$ .

Di sottogruppi di questa forma, se ne trovano due:  $\langle \rho^2, \sigma \rangle$  e  $\langle \rho^2, \sigma\rho \rangle$ , ma non si sa se siano tutti i sottogruppi normali, quindi si cerca di caratterizzarli meglio. Si sa che  $H \triangleleft G \iff gHg^{-1} = H$ ,  $\forall g \in G$ , quindi per ogni elemento di un sottogruppo normale, devono figurare anche tutti i suoi coniugati. Per la proposizione 1.10, per capire come sono fatti i coniugati di  $D_n$ , è sufficiente studiare quali siano quelli di  $\rho^i$  e  $\sigma\rho^i$ . Si nota che:

$$\rho^i \rho^i \rho^{-i} = \rho^i \quad \sigma \rho^i \rho^i \rho^{-i} \sigma = \sigma \rho^i \sigma = \rho^{-i}$$

quindi l'insieme dei coniugati di  $\rho^i$  è  $\{\rho^i, \rho^{-i}\}$ ; in particolare, se  $i \in \{0, n/2\}$ , tale insieme diventa  $\{e\}$ , oppure  $\{\rho^{n/2}\}$  rispettivamente. Poi, si nota che:

$$\rho^i \sigma \rho^j \rho^{-i} = \sigma \rho^{-i} \rho^j \rho^{-i} = \sigma \rho^{j-2i} \quad \sigma \rho^i \sigma \rho^j \rho^{-i} \sigma = \rho^{-i} \rho^j \rho^{-i} \sigma = \sigma \rho^{2i-j}$$

quindi se  $n$  è pari, allora  $\sigma \rho^s \sim \sigma \rho^t \iff \equiv t \pmod{2}$ , quindi le riflessioni di spezzano in due classi di coniugio; se  $n$  è dispari, invece, le riflessioni sono tutte coniugate.

Ricapitolando:

- se  $n$  è dispari e se un sottogruppo contiene una riflessione, allora le contiene tutte e tutte le riflessioni generano  $D_n$ , infatti  $\sigma$  è dato e  $\rho = \sigma \sigma \rho$ , quindi  $H \triangleleft D_n \Rightarrow H = D_n$ , mentre se non contiene alcuna riflessione, allora è un sottogruppo di  $C_n$ ;
- se  $n$  è pari, oltre ai sottogruppi di  $C_n$ , si considerano gli  $H \triangleleft D_n$  che sono tali che  $\sigma \rho^i \in H$ , per cui  $\sigma \rho^{i+2} \in H$  e  $\rho^2 \in H$ , pertanto, se  $H \neq D_n$ , devono essere della forma  $\langle \rho^2, \sigma \rangle$ , o  $\langle \rho^2, \sigma\rho \rangle$ .

**Sottogruppi caratteristici.** Usando quanto visto per i sottogruppi normali, si conclude che i possibili sottogruppi caratteristici sono i sottogruppi di  $C_n$  e  $\langle \rho^2, \sigma \rangle$  e  $\langle \rho^2, \sigma\rho \rangle$ . Mentre si sa già che i sottogruppi di  $C_n$  sono caratteristici, si osserva che, per gli altri due, la mappa  $\tau : D_n \rightarrow D_n$  tale che  $\tau(\rho) = \rho$  e  $\tau(\sigma) = \sigma\rho$  è un automorfismo che scambia  $\langle \rho^2, \sigma \rangle$  con  $\langle \rho^2, \sigma\rho \rangle$  e viceversa, quindi non sono caratteristici.



### 1.6.2 Centro, quozienti e automorfismi di $D_n$

**Il centro.** Si cercano tutti gli elementi  $\tau \in D_n$  tale che  $\forall \rho \in D_n, \rho\tau\rho^{-1} = \tau$ . Dal precedente studio dei coniugi nei sottogruppi normali, si conclude che  $Z(D_n) = \{e\}$  se  $n$  è dispari e  $Z(D_n) = \{e, \rho^{n/2}\} \cong \mathbb{Z}/2\mathbb{Z}$  se  $n$  è pari.

**Quozienti.** Si sa che i quozienti sono in corrispondenza biunivoca con i sottogruppi normali, il che vuol dire che esiste un quoziente per ciascun  $H \triangleleft G$ . A meno di un automorfismo, i quozienti si ottengono come segue. Per quanto visto precedentemente, i sottogruppi normali sono i sottogruppi di  $C_n$  e, se  $n$  è pari, anche quelli della forma  $\langle \rho^2, \sigma \rangle$  e  $\langle \rho^2, \sigma\rho \rangle$ . Sia,  $\langle \rho^m \rangle < C_n$ , con  $m \mid n$ , per cui  $|D_n/\langle \rho^m \rangle| = 2n/m$ .

**Proposizione 1.14.** Si ha  $D_n/\langle \rho^m \rangle \cong D_{n/m}$ .

*Dimostrazione.* Si considera

$$\begin{array}{ccc} D_n & \longrightarrow & D_{n/m} \\ \gamma: \quad \sigma & \longmapsto & \tau \\ & \rho & \longmapsto \epsilon \end{array}$$

dove  $D_n = \langle \sigma, \rho \mid \rho^n = \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} \rangle$  e  $D_{n/m} = \langle \tau, \epsilon \mid \epsilon^{n/m} = \tau^2 = e, \tau\epsilon\tau\epsilon^{-1} \rangle$ . Si nota che questo è suriettivo e il suo nucleo è  $\langle \rho^m \rangle$ , quindi si ha la tesi per il I teorema di omomorfismo.  $\square$

Nel caso di  $n$  pari, poi, vi sono gli altri due sottogruppi citati sopra, che hanno indice 2 e, quindi, i cui quozienti sono isomorfi a  $\mathbb{Z}/2\mathbb{Z}$ .

**Gli automorfismi.** Si studia  $\text{Aut}(D_n)$ . Per farlo, si cerca di calcolarne la cardinalità. Per definire un automorfismo in  $D_n$ , lo si definisce sui generatori, che si sanno essere  $\rho$  e  $\sigma$ . L'immagine di questi generatori deve essere un altro generatore: ad esempio, l'immagine di  $\rho$ , che ha ordine  $n$ , deve avere come immagine un elemento di ordine  $n$ ; questi sono della forma  $\rho^i$ , con  $\gcd(i, n) = 1$ , quindi ci sono  $\phi(n)$  possibili scelte. Poi,  $\sigma$  ha ordine 2 e deve avere, come immagine, un altro elemento di ordine 2 che, insieme al  $\rho^i$  scelto prima, generi  $D_n$ ; ci sono  $n$  riflessioni della forma  $\sigma\rho^j$ , quindi un totale di  $n$  scelte possibili. Si nota che se  $n$  è pari, anche  $\rho^{n/2}$  ha ordine 2, ma la coppia  $\rho^i, \rho^{n/2}$  non genera  $D_n$ .

Sia, allora

$$\begin{array}{ccc} D_n & \longrightarrow & D_n \\ \gamma: \quad \rho^h & \longmapsto & \rho^{ih} \\ & \sigma\rho^k & \longmapsto \sigma\rho^j\rho^{ik} \end{array}$$

con  $\gcd(i, n) = 1$  e  $j$  qualsiasi;  $\gamma$  è ben definita e

$$\gamma((\rho^s)(\sigma\rho^t)) = \gamma(\sigma\rho^{t-s}) = \sigma\rho^j\rho^{i(t-s)} = \sigma\rho^{-is}\rho^j\rho^{it} = \rho^{is}\sigma\rho^j\rho^{it} = \gamma(\rho^s)\gamma(\sigma\rho^t)$$

per cui è un omomorfismo. Inoltre, è biettiva per costruzione, quindi si ha  $|\text{Aut}(D_n)| = n\phi(n)$ ; da un punto di vista insiemistico, esiste una biezione tra  $\text{Aut}(D_n)$  e  $\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$ .

**Esercizio 1.1.** Studiare  $D_4$  (risultati a pagina 19) e  $D_6$ .

## 1.7 Permutazioni

**Definizione 1.12 (Permutazione).** Sia  $X$  un insieme; una mappa  $f : X \rightarrow X$  è detta *permutazione* se è biettiva. Le permutazioni formano un gruppo rispetto alla composizione tra funzioni ed è indicato con

$$S(X) = \{f : X \rightarrow X \mid f \text{ è biettiva}\}$$

Se  $X = \{1, \dots, n\}$ , allora il gruppo delle permutazioni si indica con  $S_n$  e  $|S_n| = n!$ .

Una permutazione di  $S_n$  può essere rappresentata tramite cicli, i quali sono disgiunti e, quindi, commutano fra loro.

Ogni  $k$ -ciclo (ciclo di lunghezza  $k$ ) ha  $k$  scritture diverse, tutte equivalenti fra loro, dovute alla possibilità di scegliere uno fra i  $k$  elementi del ciclo come primo elemento; dopo questa scelta, tutti gli altri sono univocamente determinati.

**Proposizione 1.15.** I cicli di una permutazione di  $S_n$  sono orbite degli elementi di  $X = \{1, \dots, n\}$  formate dall'azione indotta da tale permutazione.

*Dimostrazione.* Sia  $\sigma \in S_n$  e sia  $\langle \sigma \rangle$  il sottogruppo ciclico generato da  $\sigma$ . Si considera l'azione di  $\langle \sigma \rangle$  su  $X$  secondo la legge  $\sigma^k \cdot x = \sigma^k(x)$ ; l'orbita di ciascun elemento di  $X$  è della forma

$$\text{Orb}(x) = \left\{ \sigma^k(x) \mid k \in \mathbb{Z} \right\}$$

Si nota che  $|X| < \infty \Rightarrow |\text{Orb}(x)| < \infty, \forall x$ . Sia, poi,  $m \geq 1$  il più piccolo intero tale che  $\sigma^m(x) = x^1$ ; allora gli elementi

$$x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)$$

sono tutti distinti (per definizione di  $m$ ) e formano  $\text{Orb}(x)$ . Facendo agire  $\sigma$  su  $\text{Orb}(x) \subset X$ , si nota che

$$x \mapsto \sigma(x), \sigma(x) \mapsto \sigma^2(x), \dots, \sigma^{m-1}(x) \mapsto \sigma^m(x) = x$$

---

<sup>1</sup>Questo esiste per forza, altrimenti si avrebbero orbite di infiniti elementi a partire da un insieme finito.

L'azione di  $\sigma$  ristretta a  $\text{Orb}(x)$ , allora, si può vedere come la permutazione

$$\begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \cdots & \sigma^{m-1}(x) \end{pmatrix}$$

che è un  $m$ -ciclo. Se  $O_1, \dots, O_r$  sono le orbite non banali (cioè di lunghezza  $> 1$ ),  $\sigma$  agisce su ciascuna  $O_i$  come un  $m_i$ -ciclo, chiamato  $c_i$  per ogni orbita, con  $|O_i| = m_i$ , mentre su quelle banali agisce come l'identità. Visto che le orbite partizionano  $X$ , ciascun ciclo  $c_i$  è disgiunto dagli altri e la loro composizione restituisce proprio  $\sigma$ , visto che per definizione sono la restrizione di  $\sigma$  a partizioni di  $X$ .  $\square$

**Corollario 1.5.2.** Il gruppo  $S_n$  è generato dai cicli.

*Dimostrazione.* Il teorema precedente mostra come ciascuna permutazione  $\sigma \in S_n$  si possa scrivere come composizione di un numero finito di cicli disgiunti, pertanto combinando l'insieme di tutti i possibili cicli, si ottiene  $S_n$ .  $\square$

**Numero di  $k$ -cicli di  $S_n$ .** Si cerca quanti  $k$ -cicli, con  $k \leq n$ , sono contenuti in  $S_n$ . Visto che un ciclo è una sequenza di  $k$  numeri, il problema si riduce a trovare quanti  $k$  numeri possono essere estratti da un insieme di  $n$  numeri, che si sa essere dato da  $\binom{n}{k}$ . Queste, però, non sono tutte perché i  $k$  numeri si possono scambiare in  $k!$  modi diversi; allo stesso tempo, è possibile costruire  $k$   $k$ -cicli equivalenti, quindi il numero totale ammonta a  $\binom{n}{k} \frac{k!}{k} = \binom{n}{k} (k-1)!$ .

**Numero di permutazioni di  $S_{12}$  sono composizione di 2 3-cicli e 3 2-cicli disgiunti.**

Dal punto precedente, si sa che in  $S_{12}$  si trovano  $\binom{12}{3} \frac{3!}{3}$ ; fissato il primo 3-ciclo, restano  $12 - 3$  elementi liberi per gli altri cicli<sup>1</sup>, quindi, per il secondo 3-ciclo, si hanno  $\binom{9}{3} \frac{3!}{3}$  scelte possibili. Continuando così per tutti i cicli rimanenti, si ottengono

$$\binom{12}{3} \frac{3!}{3} \binom{9}{3} \frac{3!}{3} \binom{6}{3} \frac{2!}{2} \binom{4}{3} \frac{2!}{2} \binom{2}{3} \frac{2!}{2}$$

possibili permutazioni, dove si è modificata la formula per scegliere due 3-cicli e tre 2-cicli. Però se ne sono contati troppi: prendendo d'esempio i due 3-cicli, essendo disgiunti, questi possono commutare senza alterare la permutazione, però col conto precedente si sono considerati distinti. Per risolvere, si deve dividere per tutti i possibili modi di commutare i 3-cicli, cioè  $2!$  in questo caso. Lo stesso si deve fare per i tre 2-cicli, i cui modi di permutarle sono  $3!$ . Complessivamente, si hanno un totale di

$$\binom{12}{3} \frac{3!}{3} \binom{9}{3} \frac{3!}{3} \binom{6}{3} \frac{2!}{2} \binom{4}{3} \frac{2!}{2} \binom{2}{3} \frac{2!}{2} \frac{1}{3!2!}$$

possibili permutazioni.

---

<sup>1</sup>I tre scelti vanno rimossi affinché gli altri cicli siano disgiunti.

**Ordine di una permutazione di  $S_n$ .** Un  $k$ -ciclo ha ordine  $k$ ; infatti per  $\sigma = (a_1 \cdots a_k)$ , si ha

$$\sigma^s(a_i) = a_j \quad \text{con } j \equiv s + i \pmod{k} \text{ e } j < k$$

quindi  $\sigma^s(a_i) = a_{i+s} = a_i \iff s + i \equiv i \pmod{k} \iff s \equiv 0 \pmod{k}$ .

Se la permutazione è formata da  $\ell$  cicli disgiunti  $\sigma_i$ , invece, il suo ordine è

$$\text{ord}(\sigma) = \text{mcm}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_\ell))$$

perché è il più piccolo numero tale che ogni ciclo torni al punto di partenza. Si nota, infatti, che se  $m$  è tale che  $\sigma^m = e$ , allora

$$e = \sigma^m = \sigma_1^m \cdots \sigma_\ell^m \implies \sigma_i^m = e, \quad \forall i = 1, \dots, \ell$$

quindi  $\text{ord}(\sigma_i) \mid m$ ,  $\forall i$  e, quindi,  $m = \text{mcm}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_\ell))$ .

**Definizione 1.13 (Trasposizione).** Sia  $\tau \in S_n$ ; se  $\tau$  è della forma  $(a_i, a_j)$ , cioè è un 2-ciclo, allora si dice *trasposizione*.

**Proposizione 1.16.** Tutte le permutazioni di  $S_n$  si scrivono come composizione di trasposizioni.

*Dimostrazione.* Per il corollario 1.5.2, è sufficiente mostrare che vale per un  $k$ -ciclo generico. A questo proposito, si osserva che:

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

□

**Osservazione 1.6.** La decomposizione in trasposizioni non è unica: per esempio:

$$(12) = (12)(34)(34) = (12)(34)(35)(67)(34)(35)(67)$$

**Proposizione 1.17.** L'applicazione

$$\begin{aligned} S_n &\longrightarrow \{\pm 1\} = \mathbb{Z}^* \\ \text{sgn} : \sigma &\longmapsto \text{sgn } \sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

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

*Dimostrazione.* È un omomorfismo perché:

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

dove si è moltiplicato sopra e sotto per  $\tau(i) - \tau(j)$  e si sono separate le produttorie<sup>1</sup>.

Sia  $\sigma = (a, b)$  una trasposizione; allora

$$\operatorname{sgn} \sigma = \prod_{1 \leq i < j \leq n} \frac{t(i) - t(j)}{i - j}$$

Se  $\{i, j\} \cap \{a, b\} = \emptyset$ , allora

$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{i - j}{i - j} = 1$$

mentre se  $\{i, j\} \cap \{a, b\} = \{i, a\}$ , si trova

$$\begin{cases} \frac{\sigma(i) - \sigma(a)}{i - a} = \frac{i - b}{i - a} & , \text{ se } i < a \\ \frac{\sigma(a) - \sigma(i)}{a - i} = \frac{b - i}{a - i} = \frac{i - b}{i - a} & , \text{ se } a < i \end{cases}$$

Lo stesso vale per l'intersezione  $\{i, j\} \cap \{a, b\} = \{i, b\}$ :

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

I fattori delle due intersezioni non vuote si semplificano a 1, quindi rimane unicamente il caso in cui  $\{i, j\} \cap \{a, b\} = \{a, b\}$ ; assumendo senza perdita di generalità che  $a < b$ , si trova:

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

pertanto, nella produttoria, si ha un unico fattore pari a  $-1$ , il che implica che  $\operatorname{sgn} \sigma = -1$ .  $\square$

**Corollario 1.5.3.** La mappa  $\operatorname{sgn} \sigma$  restituisce la parità di trasposizioni presenti in  $\sigma$ , quando decomposta in prodotto di trasposizioni.

**Nucleo del segno.** Si nota che

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\} = A_n \quad (1.7.1)$$

ed è noto come *gruppo alterno*. Alcune sue caratteristiche sono:

- (a).  $A_n \triangleleft S_n$ ;
- (b).  $S_n/A_n \cong \{\pm 1\}$ .

---

<sup>1</sup>La prima produttoria restituisce il  $\operatorname{sgn} \sigma$  perché al massimo applicare prima  $\tau$  altera l'ordine dell'insieme, quindi non è garantito che  $\tau(i) < \tau(j)$  se  $i < j$ ; questo, però, non importa perché se  $\tau(i) > \tau(j)$ , allora l'espressione si può riscrivere come  $\frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}$ . Prendendo  $a = \tau(i)$  e  $b = \tau(j)$ , si potrebbe anche riscrivere la produttoria come  $\prod_{1 \leq a < b \leq n} \frac{\sigma(a) - \sigma(b)}{a - b}$ .

Visto che  $S_n/A_n \cong \{\pm 1\}$ , per il teorema di Lagrange, si ha:

$$2 = |S_n/A_n| = \frac{S_n}{A_n} \implies |A_n| = \frac{|S_n|}{|S_n/A_n|} = \frac{n!}{2}$$

**Teorema 1.6.** Due permutazioni di  $S_n$  sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli disgiunti.

*Dimostrazione.* Si divide la dimostrazione nelle due implicazioni.

- ( $\Rightarrow$ ) Siano  $\sigma, \tau \in S_n$ ; si considerano  $\sigma = (a_1, \dots, a_k)$  e  $\tau\sigma\tau^{-1}$ . Si nota che, se  $\tau(a_i) = b_i \Rightarrow \tau\sigma\tau^{-1}(b_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1}$ ; inoltre, se  $x \neq b_i$  per ogni  $i$ :

$$\tau^{-1}(x) \neq a_i \implies \tau\sigma\tau^{-1}(x) = \tau\sigma(\tau^{-1}(x)) = \tau\tau^{-1}(x) = x$$

pertanto il coniugato di un  $k$ -ciclo è ancora un  $k$ -ciclo. Se la permutazione è composizione di cicli disgiunti, invece, si può scrivere

$$\sigma = \sigma_1 \dots \sigma_k \implies \tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1} \dots \tau\sigma_k\tau^{-1}$$

quindi ci si può ricondurre al caso precedente.

- ( $\Leftarrow$ ) Siano  $\sigma = (a_1, \dots, a_k)$  e  $\rho = (b_1, \dots, b_k)$  due  $k$ -cicli; si può prendere, allora,  $\tau$  tale che  $\tau(a_i) = b_i$ , da cui  $\tau\sigma\tau^{-1} = \rho$ . Nel caso di più cicli disgiunti, si mappa ciclo con ciclo:

$$\begin{array}{ccc} \sigma = & (x_{11} \dots x_{1k_1}) & \cdots & (x_{r1} \dots x_{rk_r}) \\ & \downarrow & & \downarrow \\ \rho = & (y_{11} \dots y_{1k_1}) & \cdots & (y_{r1} \dots y_{rk_r}) \end{array}$$

con  $\tau(x_{ij}) = y_{ij}$ , quindi vale  $\tau\sigma\tau^{-1} = \rho$ .

□

Quanto al centralizzatore di  $\sigma \in S_n$ , si sa dal teorema orbita-stabilizzatore che

$$|Z(\sigma)| |\text{cl}(\sigma)| = n! \tag{1.7.2}$$

Per il teorema precedente, si sa calcolare  $|\text{cl}(\sigma)|$ , quindi è possibile ottenere  $|Z(\sigma)|$ .

**Esempio 1.3.** Sia  $\sigma = (1234)(56) \in S_{10}$ ; il numero possibile di permutazioni coniugate sono tutte quelle che si scrivono come un 4-ciclo e un 2-ciclo in  $S_{10}$ , numero ottenuto come

$$|\text{cl}(\sigma)| = \binom{10}{4} \frac{4!}{4} \binom{6}{2} = \frac{10!}{192} \implies |Z(\sigma)| = 192 = 4!8$$

Sia

$$H = \text{Sym}(7, 8, 9, 10) = \{h \in S_{10} \mid h(i) = i, \forall i \notin \{7, 8, 9, 10\}\} \cong S_4$$

e sia  $K = \langle (1234), (56) \rangle$ ; allora  $H, K < Z(\sigma)$ ,  $H \cap K = \{e\}$  e  $HK = Z(\sigma)$ , per cui

$$Z(\sigma) \cong H \times K \cong S_4 \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

*Dimostrazione.* Si ha  $H < Z(\sigma)$  perché ogni permutazione di  $H$  modifica solo l'insieme  $\{7, 8, 9, 10\}$ , quindi commuta con  $\sigma$ . Inoltre,  $H \cong S_4 \Rightarrow |H| = 4!$ .

Si ha  $K < Z(\sigma)$  perché ogni elemento di  $K$  è della forma  $(1234)^j(56)^k$ , quindi commuta sempre con  $\sigma$ . Visto che  $(1234)$  ha ordine 4 e  $(56)$  ha ordine 2 e i due cicli sono disgiunti, si ha  $|K| = 4 \cdot 2 = 8$ . Si nota, in particolare, che  $\langle (1234) \rangle \cong C_4 \cong \mathbb{Z}/4\mathbb{Z}$ , cioè è isomorfo a un gruppo ciclico di ordine 4; analogamente  $\langle (56) \rangle \cong C_2 \cong \mathbb{Z}/2\mathbb{Z}$ .

Evidentemente la loro intersezione è banale perché le permutazioni di  $H$  agiscono esclusivamente su  $\{7, 8, 9, 10\}$ , mentre quelle di  $K$  su  $\{1, 2, 3, 4, 5, 6\}$ , quindi deve essere  $H \cap K = \{e\}$ .

Visto che  $H, K < Z(\sigma)$  e  $|HK| = |H||K| = 192$  (essendo  $|H \cap K| = 1$ ), si ha  $HK = Z(\sigma)$ . Sempre perché  $H \cap K$  è banale, si ha  $HK \cong H \times K$ , da cui

$$Z(\sigma) \cong H \times K \cong S_4 \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

□

## 1.8 Gruppi di Sylow e prodotti diretti

**Definizione 1.14 (Gruppo di Sylow).** Sia  $G$  un gruppo finito con  $|G| = p^m n$ , con  $p$  primo e  $\gcd(p, n) = 1$ ; se  $H < G$  e  $|H| = p^m$ , allora  $H$  è detto  $p$ -Sylow di  $G$ .

**Esempio 1.4.** Si considera il gruppo diedrale  $D_7$ ; si ha  $|D_7| = 14 = 7 \cdot 2$ , con  $|\langle \rho \rangle| = 7$ ; allora  $\langle \rho \rangle$  è un 7-Sylow di  $D_7$  ed è unico. Tuttavia, i  $p$ -Sylow non sono unici; per esempio, i  $\langle \rho^i \sigma \rangle \subset D_7$  sono sette 2-Sylow.

**Lemma 1.6.1.** Siano  $H, K \triangleleft G$ , con  $H \cap K = \{e\}$ ; allora  $hk = kh$ ,  $\forall h \in H, \forall k \in K$ .

*Dimostrazione.* Si ha  $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ ; visto che  $K$  è normale, allora  $hkh^{-1} \in K$ , quindi  $hkh^{-1}k^{-1} \in K$ . Allo stesso tempo,  $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$  e, siccome anche  $H$  è normale, si ha  $kh^{-1}k^{-1} \Rightarrow hkh^{-1}k^{-1} \in H$ . Allora, visto che  $hkh^{-1}k^{-1} \in H \cap K$  e visto che  $H \cap K = \{e\}$  per assunzione, si ha  $hkh^{-1}k^{-1} = e \Rightarrow hk = kh$ . □

**Teorema 1.7.** Sia  $G$  un gruppo e siano  $H, K \triangleleft G$ ; se  $HK = G$  e  $H \cap K = \{e\}$ , allora  $G \cong H \times K$ .

*Dimostrazione.* Sia  $\phi : H \times K \rightarrow G$  tale che  $\phi((h, k)) = hk$ ; allora  $\phi$  è un omomorfismo per il lemma precedente (1.6.1), è iniettiva per la seconda ipotesi ed è suriettiva per la prima. □

**Corollario 1.7.1.** In un prodotto diretto, i fattori commutano fra loro.

**Osservazione 1.7.** Sia  $G = H \times K$ ; per il teorema precedente (1.7),  $Z(H \times K) \cong Z(H) \times Z(K)$ , visto che  $Z(H) \times \{e_K\}$  e  $\{e_H\} \times Z(K)$  sono sottogruppi normali di  $Z(H \times K)$ . Conseguentemente, ricordando la proposizione 1.1, si trova:

$$\text{Int}(H \times K) \cong (H \times K)/Z(H \times K) \cong H/Z(H) \times K/Z(K) \cong \text{Int}(H) \times \text{Int}(K)$$

dove il penultimo isomorfismo è ottenuto definendo

$$\gamma : \begin{array}{ccc} H \times K & \longrightarrow & H/Z(H) \times K/Z(K) \\ (h, k) & \longmapsto & (h + Z(H), k + Z(K)) \end{array}$$

e dal I teorema di omomorfismo.

**Teorema 1.8.** Sia

$$\phi : \begin{array}{ccc} \text{Aut}(H) \times \text{Aut}(K) & \longrightarrow & \text{Aut}(H \times K) \\ (f, g) & \longmapsto & \gamma = (f, g) \end{array}$$

Allora  $\phi$  è un omomorfismo iniettivo, mentre è suriettivo se e solo se  $H \times \{e_K\}$  e  $\{e_H\} \times K$  sono caratteristici in  $H \times K$ .

*Dimostrazione.* Intanto,  $\gamma$  è ben definita perché  $\forall (f, g) \in \text{Aut}(H) \times \text{Aut}(K)$ , si ha  $f(h) \in H$ ,  $\forall h \in H$  e  $g(k) \in K$ ,  $\forall k \in K$ , quindi  $\gamma((h, k)) = (f(h), g(k)) \in H \times K$ .

Poi,  $\phi$  è ben definita perché  $\gamma$  è un automorfismo; infatti è un omomorfismo:

$$\gamma((h, k)(h', k')) = (f(hh'), g(kk')) = (f(h)f(h'), g(k)g(k')) = \gamma((h, k))\gamma(h', k')$$

È anche iniettiva perché

$$\begin{aligned} \text{Ker } \gamma &= \{(h, k) \in H \times K \mid \gamma((h, k)) = (e_H, e_K)\} = \{(h, k) \in \text{Ker } f \times \text{Ker } g\} \\ &= \{(e_H, e_K)\} \end{aligned}$$

ed è suriettiva perché  $\forall (h, k) \in H \times K$ ,  $\exists!(h_0, k_0) \in H \times K : ((f(h_0), g(k_0)) = (h, k)$ , dove si è usato, in tutte le dimostrazioni, che sia  $f$  che  $g$  sono automorfismi. Segue che  $\gamma$  è effettivamente un automorfismo di  $H \times K$ .

Ora si verifica che  $\phi$  è un omomorfismo ed è sempre iniettivo; la prima vale perché

$$\phi((f, g)(\varphi, \psi)) = \phi(f \circ \varphi, g \circ \psi) = (f \circ \varphi, g \circ \psi) = (f, g) \circ (\varphi, \psi) = \phi((f, g)) \circ \phi((\varphi, \psi))$$

mentre è iniettivo perché  $\phi((f, g)) = \text{Id}_{H \times K} \iff f = \text{Id}_H \text{ e } g = \text{Id}_K$ .

Ora si dimostra che  $\phi$  è suriettivo se e solo se  $H \times \{e_K\}$  e  $\{e_H\} \times K$  sono caratteristici in  $H \times K$ .

- ( $\Leftarrow$ ) Si assume che  $H \times \{e_K\}$  e  $\{e_H\} \times K$  siano caratteristici in  $H \times K$  e si mostra che  $\phi$  è suriettivo. Per farlo, si considerano,  $\forall \gamma \in \text{Aut}(H \times K)$ , le mappe  $f : H \rightarrow H$



e  $g : K \rightarrow K$  tali che

$$f(h) = \pi_H \gamma(h, e_K) \quad g(k) = \pi_K \gamma(e_H, k)$$

e si dimostra che  $f \in \text{Aut}(H)$ ,  $g \in \text{Aut}(K)$  e  $\gamma = \phi(f, g)$ . Si nota che, sia  $f$  che  $g$  sono composizioni di due omomorfismi, quindi sono, a loro volta, omomorfismi; inoltre

$$\begin{aligned} \text{Ker } f &= \{h \in H \mid \pi_H \gamma(h, e_K) = e_H\} = \{h \in H \mid \pi_H(h', e_K) = e_H\} \\ &= \{h \in H \mid e_H = h' = \gamma(h)\} = \{e_H\} \end{aligned}$$

Lo stesso vale per  $g$ , quindi entrambe le mappe sono omomorfismi iniettivi. Usando il fatto che  $\gamma$  è suriettiva, si ha che  $\forall h' \in H, \exists h \in H : \gamma(h, e_K) = (h', e_K)$ , quindi  $f(h) = \pi_H \gamma(h, e_K) = \pi_H(h', e_K) = h'$  e lo stesso si può ripetere per  $g$  quindi  $f$  e  $g$  sono automorfismi. Per concludere, si nota che

$$\phi(f, g)((h, k)) = (\pi_H \gamma((h, e_K)), \pi_K \gamma((e_H, k))) = (h', k') = \gamma(h, k)$$

- $(\Rightarrow)$  Sia  $\phi$  anche suriettivo, quindi è un isomorfismo; si mostra che  $H \times \{e_K\}$  e  $\{e_H\} \times K$  sono caratteristici in  $H \times K$ .

Se  $\phi$  è suriettivo, significa che ogni automorfismo di  $\text{Aut}(H \times K)$  è della forma  $(f, g) : f \in \text{Aut}(H), g \in \text{Aut}(K)$ , ma allora, per  $\psi \in \text{Aut}(H \times K)$ , si ha:

$$\psi(H \times \{e_K\}) = f(H) \times \{e_K\} = H \times \{e_K\}$$

perché  $f$  è un automorfismo di  $H$  e  $\{e_K\} \xrightarrow{g} \{e_K\}$  perché  $g$  è un automorfismo di  $K$ .

□

**Proposizione 1.18.** Sia  $G = H \times K$ , con  $|H| = n$  e  $|K| = m$ ; se  $\text{gcd}(n, m) = 1$ , allora  $H$  e  $K$  sono caratteristici in  $G$ .

*Dimostrazione.* Sia  $f \in \text{Aut}(H \times K)$ , con  $f(h, e_K) = (h', k')$ ; visto che  $\text{ord}((h, e_K)) = \text{ord}(h) \mid n$ , deve essere  $\text{ord}((h', k')) = \text{mcm}(\text{ord}(h'), \text{ord}(k')) \mid n$ , visto che  $f$  è automorfismo e, in particolare  $\text{ord}(k') \mid n$ . Per ipotesi, deve essere  $\text{ord}(k') \mid m$ , ma, visto che  $\text{gcd}(n, m) = 1$ , deve essere  $k' = e_K$ , da cui  $f(H \times \{e_K\}) \subset H \times \{e_K\}$ . Lo stesso procedimento si può applicare a  $f(e_H, k)$ . □

## 1.9 Esercizi e complementi

### 1.9.1 Complementi di teoria

### 1.9.2 Esercizi

**Esercizio 1.2.** Studiare  $\text{Aut}(\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ .

*Svolgimento.* Si nota che  $\mathbb{Z}/20\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ , quindi:

$$\begin{aligned}\text{Aut}(\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) &\cong \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z}) \\ &\cong \text{Aut}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}\end{aligned}$$

dove si è usato che  $(\mathbb{Z}/5\mathbb{Z})^*$  è ciclico di ordine 4, quindi isomorfo a  $\mathbb{Z}/4\mathbb{Z}$ . Rimane da studiare  $\text{Aut}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ .

Il gruppo  $G_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  ha, come generatori,  $\langle (a, 0), (0, b) \rangle$ , con  $\text{ord}((a, 0)) = 4$  e  $\text{ord}((0, b)) = 2$ ; per studiare gli automorfismi di  $G_2$ , è necessario e sufficiente stabilire come si comportano su questi elementi, cioè imporre che vengano mandati in altri elementi di ordine 4 e 2 rispettivamente.

Concretamente, siano  $(1, 0)$  e  $(0, 1)$  i generatori di ordine 4 e 2 rispettivamente; il primo, allora, può essere mandato in un elemento di  $\{(1, 0), (3, 0), (1, 1), (3, 1)\}$ , mentre il secondo in un elemento di  $\{(0, 1), (2, 0), (2, 1)\}$ .

Ora, considerando  $u \in \{(1, 0), (3, 0), (1, 1), (3, 1)\}$ ,  $\langle u \rangle$  è un gruppo ciclico di ordine 4, pertanto contiene un elemento di ordine 2, che è proprio  $u^2$ ; evidentemente, il gruppo  $\langle u, u^2 \rangle \neq G_2$  perché ha ordine 4, quindi, fissato  $u$ , si deve rimuovere dalla lista degli elementi di ordine 2 quello corrispondente a  $u^2$ .

A questo punto, le possibili scelte sono 4 dall'insieme degli elementi di ordine 4 e 2 da quelli di ordine 2, per un totale di 8 automorfismi.

Si è dimostrato che  $|\text{Aut}(G_2)| = 8$ ; ora si mostra che  $\text{Aut}(G_2) \cong D_4$ . Per farlo, si cercano due elementi  $\alpha, \Gamma \in \text{Aut}(G_2)$  tali che  $\text{ord}(\Gamma) = 4$ ,  $\text{ord}(\alpha) = 2$  e  $\alpha\Gamma\alpha = \Gamma^{-1}$ . Si prendono  $\alpha((1, 0)) = (1, 0)$ ,  $\alpha(0, 1) = (2, 1)$  e  $\Gamma((0, 1)) = (2, 1)$  e  $\Gamma((1, 0)) = (1, 1)$ ; si osserva che:

$$\begin{aligned}\alpha((x, y)) &= \alpha(x(1, 0) + y(0, 1)) = x(1, 0) + y(2, 1) = (2y + x, y) \\ \Gamma((x, y)) &= \Gamma(x(1, 0) + y(0, 1)) = x(1, 1) + y(2, 1) = (2y + x, x + y)\end{aligned}$$

da cui si può verificare l'ordine di ciascun automorfismo e, conseguentemente, che  $\alpha\Gamma\alpha = \Gamma^{-1}$ . ■

**Esercizio 1.3.** Sia  $\rho = (1234)(56) \in S_{10}$ ; calcolare  $Z(\rho)$  e

$$N(\langle \rho \rangle) = \{ \tau \in S_{10} \mid \tau \rho \tau^{-1} \in \langle \rho \rangle \}$$

*Svolgimento.* Si nota, intanto, che  $|Z(\rho)| = |S_{10}|/|\text{cl}(\rho)| = 8 \cdot 4!$ . Si considerano, poi,  $H = \langle (1234), (56) \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  e  $K = S_{\{7,8,9,10\}} \cong S_4$ ; per il teorema 1.7, visto che questi due sottogruppi sono normali, con  $HK = Z(\rho)$  e hanno intersezione banale, si ha  $Z(\rho) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times S_4$ .

Per  $N(\langle \rho \rangle)$ , visto che  $\langle \rho \rangle = \{\text{Id}, \rho, \rho^2, \rho^{-1}\}$ , si ha

$$\begin{aligned} N(\langle \rho \rangle) &= \{\tau \in S_{10} \mid \tau\rho\tau^{-1} = \rho \text{ o } \tau\rho\tau^{-1} = \rho^{-1}\} \\ &= Z(\rho) \cup \{\tau \in S_{10} \mid \tau\rho\tau^{-1} = \rho^{-1}\} = Z(\rho) \times G_{-1} \end{aligned}$$

cioè è necessario che l'immagine sotto coniugio di un generatore, in questo caso  $\rho$ , sia ancora un generatore. Allora è sufficiente caratterizzare  $G_{-1}$ . Si nota che  $\rho^{-1} = \rho^3 = (56)(2341)$ , quindi una possibilità è  $\tau_0 = (24)$ , oppure  $\tau_1 = (1, 4)(2, 3)(5, 6)$ ; per trovarle tutte, si osserva che

$$\tau_1^{-1}\tau_0\rho\tau_0^{-1}\tau_1 = \tau_1^{-1}\rho^{-1}\tau_1 = \rho \implies \tau_1^{-1}\tau_0 \in Z(\rho) \iff \tau_0 \in \tau_1 Z(\rho)$$

perciò  $\tau \in G_{-1} \iff \tau \in \tau_0 Z(\rho)$ . Ne consegue che  $|N(\langle \rho \rangle)| = 2|Z(\rho)|$ ; in generale:

$$\begin{aligned} N_{S_n}(\langle \rho \rangle) &= \left\{ \tau \in S_n \mid \tau\rho\tau^{-1} = \rho^k, \text{ gcd}(\text{ord}(\rho), k) = 1 \right\} \\ \implies |N_{S_n}(\langle \rho \rangle)| &= |\{k \in \mathbb{Z} \mid \text{gcd}(k, \text{ord}(\rho)) = 1\}| |Z_{S_n}(\rho)| = \phi(\text{ord}(\rho)) |Z_{S_n}(\rho)| \end{aligned} \tag{1.9.1}$$

cioè è il centralizzatore per il numero di equazioni della forma  $\tau\rho\tau^{-1} = \rho^k$ . ■

**Osservazione 1.8.** Si nota che il coniugio non cambia la forma della permutazione, quindi l'equazione  $\tau\rho\tau^{-1} = \rho^k$  ha soluzione se e solo se  $k$  è coprimo con  $\text{ord}(\rho)$ .