

# ALGEBRA I

ANDREA GALLESE

OCTOBER 16, 2017

## G Teoria dei Gruppi

### G.1 Automorfismi e Azioni

**Teorema G.1.** Se  $G$  è un gruppo,  $(\text{Aut}(G), \circ)$  è un gruppo.

**Esempi.**

1.  $\text{Aut}(\mathbb{Z}) \cong \{\pm id\} \cong \mathbb{Z}_2$
2.  $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$
3.  $\text{Aut}(\mathbb{Q}) \cong \mathbb{Q}^\times$
4.  $\text{Aut}(\mathbb{R}) \cong ?$

**Definizione G.2** (Gruppo degli automorfismi interni). Sia  $\text{Int}(G) = \{\varphi_g \mid g \in G\}$  l'insieme di tutti gli automorfismi interni, i.e. degli automorfismi di coniugio:

$$\varphi_g(x) = gxg^{-1} \quad \forall x \in G$$

*Osservazione.* è immediato osservare che  $\text{Int}(G) \triangleleft \text{Aut}(G)$ .

**Teorema G.3.**

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

*Proof.* La funzione

$$\begin{aligned} \Phi: G &\rightarrow \text{Int}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

è un omomorfismo con kernel  $Z(G)$ . La tesi segue dal Primo Teorema di Omomorfismo. ♣

*Osservazione.*

$$H \triangleleft G \Leftrightarrow \varphi_g(H) = H \quad \forall \varphi_g \in \text{Int}(G)$$

**Definizione G.4** (Sottogruppo caratteristico). Un sottogruppo  $H < G$  si dice caratteristico se è invariante per tutto  $\text{Aut}(G)$ , i.e.

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

*Osservazione.* Un sottogruppo caratteristico è anche normale, ma non è vero il viceversa: basta considerare  $\langle(0, 1)\rangle \triangleleft \mathbb{Z}_2 \times \mathbb{Z}_2$

**Definizione G.5** (Azione). Si dice azione di un gruppo  $G$  su un insieme  $X$  un omomorfismo  $\varphi$  tale che

$$\begin{aligned} \varphi: G &\rightarrow \mathcal{S}(X) \\ g &\mapsto \phi_g(x) = g \cdot x. \end{aligned}$$

**Esempio.** Siano  $G = \{z \in \mathbb{C} \mid |z| = 1\}$  e  $X = \mathbb{R}^2$ . E sia  $\phi$  l'azione:

$$\begin{aligned} \varphi: G &\rightarrow \mathcal{S}(\mathbb{R}^2) \\ z &\mapsto \mathcal{R}(O, \arg z) \end{aligned}$$

*Osservazione.* Un'azione induce naturalmente una relazione di equivalenza su  $X$ :  $x \sim y \Leftrightarrow \exists g \in G$  t.c.  $g \cdot x = y$ . Viene quindi spontaneo prendere in considerazione gli elementi della partizione così ottenuta.

**Definizione G.6** (Orbita). Si dice orbita di un elemento  $x \in X$  l'insieme di tutti gli elementi che posso essere raggiunti da  $x$  tramite l'azione:

$$\text{Orb}(x) = \{g \cdot x \mid \forall g \in G\}$$

*Osservazione.* Detto  $R$  un insieme di rappresentanti delle varie orbite, per il partizionamento prima considerato:

$$X = \bigcup_{x \in R} \text{Orb}(x) \Rightarrow |X| = \sum_{x \in R} |\text{Orb}(x)|$$

**Definizione G.7** (Stabilizzatore). Si dice stabilizzatore di un elemento  $x \in X$  l'insieme di tutti gli elementi di  $G$  che agiscono in modo banale su  $x$ :

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

*Osservazione.* è immediato osservare che  $\text{Stab}(x) < G$ , ma non necessariamente normale.

**Teorema G.8.**

$$|G| = |\text{Orb}(x)| |\text{Stab}(x)|$$

*Proof.* La funzione  $f$  così definita

$$\begin{aligned} f: \{g\text{Stab}(x) \mid g \in G\} &\rightarrow \{\text{Orb}(x) \mid x \in X\} \\ g\text{Stab}(x) &\mapsto g \cdot x \end{aligned}$$

è biunivoca, infatti:

$$\begin{aligned} g \cdot x = h \cdot x &\Leftrightarrow \varphi_g(x) = \varphi_h(x) \\ &\Leftrightarrow \varphi_h^{-1} \varphi_g(x) = x \\ &\Leftrightarrow \varphi_{h^{-1}g}(x) = x \\ &\Leftrightarrow h^{-1}g \cdot x = x \\ &\Leftrightarrow h^{-1}g \in \text{Stab}(x) \\ &\Leftrightarrow g \in h\text{Stab}(x) \\ &\Leftrightarrow g\text{Stab}(x) = h\text{Stab}(x) \end{aligned}$$

♣

*Osservazione.* Dall'osservazione precedente

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

**Esempi.**

1.  $[G = C, X = \mathbb{R}^2]$  e l'azione dell'ultimo esempio. Questa sposta ruota ogni punto attorno all'origine, pertanto le orbite sono circonferenze centrate nell'origine e gli stabilizzatori sono tutti banali, tranne quello dell'origine che coincide con  $G$ .

2.  $[G = \mathbb{R}, X = \mathbb{R}^2]$  e l'azione che trasforma  $r \in \mathbb{R}$  nella traslazione orizzontale di lunghezza  $r$ . Le orbite sono le rette parallele alla traslazione e gli stabilizzatori sono tutti banali.
3.  $[G, X = G]$  e l'azione sia la mappa che manda un elemento  $g$  nel coniugio per questo  $\varphi_g(x) = gxg^{-1}$ . L'orbita di un elemento contiene tutti i coniugati di questo ed è detta *classe di coniugio* di  $x$  ( $\mathcal{C}_x$ ). Lo stabilizzatore di  $x$  contiene tutti e soli gli elementi tali che

$xg = gx$ , ovvero il sottogruppo di tutti gli elementi che commutano con  $x$ , è detto *centralizzatore* di  $x$  ( $Z_G(x)$ ).

4.  $[G, X = \{H \mid H < G\}]$  e l'azione di coniugio. Le orbite non sono particolarmente interessanti, mentre lo stabilizzatore di un sottogruppo è detto *Normalizzatore* di  $H$ ,  $N(H)$  ed è il più grande sottogruppo di  $G$  in cui  $H$  è normale.

*Osservazione.*  $H \triangleleft G \Leftrightarrow N(H) = G$

## G.2 Formula delle Classi e Cauchy

**Teorema G.9** (Formula delle Classi). *Per ogni gruppo finito vale*

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

*Proof.* Riprendiamo la partizione di  $X$  in orbite, ma separando quelle banali da quelle non

$$|X| = \sum_{\substack{x \in R \\ \text{Orb}(x) = \{x\}}} 1 + \sum_{\substack{x \in R \\ \text{Orb}(x) \neq \{x\}}} \frac{|G|}{|Stab(x)|}$$

Osserviamo cosa succede nel caso dell'azione di coniugio da un gruppo in se (l'esempio 3 della lezione precedente). L'orbita di  $x$  è banale se e solo se  $g x g^{-1} = x$ ,  $\forall g \in G$ , ovvero nel caso in cui  $x$  commuti con tutti gli elementi di  $G$  (stia nel centro). Dunque la formula di sopra si riscrive come desiderato. ♣

**Definizione G.10** ( $p$ -gruppo). Si dice  $p$ -gruppo un gruppo finito  $G$  di ordine potenza di un primo  $p$ :  $|G| = p^n$ .

**Esempi.**

1. **Un  $p$ -gruppo  $G$  ha centro non banale.** Tutti i centralizzatori degli elementi di  $R'$  hanno dimensione  $p^k$  per un intero  $0 \leq k < n$ , dunque

$$p \mid \frac{|G|}{|Z_G(x)|} \forall x \in R'$$

pertanto, per la formula delle classi,

$$p \mid |G| - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = |Z(G)|$$

che quindi, contenendo  $e$ , deve avere almeno  $p$  elementi.

2. **I gruppi di ordine  $p^2$  sono abeliani.** Il centro di  $G$  avrà, per quanto appena dimostrato, ordine  $p$  o  $p^2$ . Nel secondo caso abbiamo finito. Nel primo

$$|G/Z(G)| = p$$

dunque il quoziente è ciclico. Presi due elementi qualunque  $x, y \in G$  possiamo esprimerli come  $x = g^h a$  e  $y = g^k b$ , dove  $g$  è il generatore del quoziente e  $a, b \in Z(G)$ . Allora, sfruttando la commutatività degli elementi del centro

$$xy = (a)(g^k b) = g^{h+k} ab = g^{k+h} ba = (g^k b)(g^h a) = yx$$

ricaviamo la commutativa per tutti gli elementi del gruppo.

3. Una possibile dimostrazione del Teorema di Cauchy:

**Teorema G.11** (di Cauchy). *Per ogni fattore primo  $p$  di  $|G|$  esiste un elemento  $g$  di  $G$  di ordine  $p$ .*

*Dimostrazione Classica.* Sia  $|G| = pm$ , procediamo per induzione su  $n$ .

Se  $n = 1$ ,  $G$  è ciclico, quindi ha un generatore di ordine  $p$ . Supponiamo ora che tutti i gruppi di ordine  $kp$   $\forall k < m$  abbiano un elemento di ordine  $p$ . Se  $|G| = pm$  ci sono due casi:

1. Esiste un sottogruppo proprio  $H$  di ordine multiplo di  $p$ , da cui ricadiamo nell'ipotesi induttiva.
2. Se nessun sottogruppo di  $G$  ha ordine divisibile per  $p$ , allora

$$p \mid \frac{|G|}{|Z_G(x)|} \forall x \in R'$$

perché i  $Z_G(x) < G$ . Per la formula delle classi

$$p \mid |G| - \sum_{x \in R'} \frac{|G|}{|Z_G(x)|} = |Z(G)|$$

ma abbiamo supposto che i sottogruppi propri non abbiano ordine multiplo di  $p$ , dunque il centro deve coincidere con l'intero gruppo, che risulta pertanto commutativo. ♣

*Dimostrazione Magica.* Sia

$$X = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_n = 1\}$$

questo insieme ha esattamente  $|G|^{p-1}$  elementi, infatti scelti i primi  $(p-1)$  l'ultimo è univocamente determinato come il suo unico inverso. Se una  $p$ -upla non è composta da un solo elemento ripetuto, allora possiamo ciclare i suoi termini per ottenere altre  $(p-1)$   $p$ -uple in  $X$ . Dunque, detto  $n$  il numero di  $g$  tali che  $g^p = 1$

$$p \mid |G|^{p-1} - n \Rightarrow p \mid n$$

e poiché  $e^p = e$  ci sono almeno  $p$  elementi di ordine  $p$ . ♣

*Osservazione.* Cosa riusciamo a dire su un possibile teorema inverso a quello di Lagrange?

1. per Gruppi Abelian?
  - (a) elementi di ordine divisore? no, basti guardare  $\mathbb{Z}_2 \times \mathbb{Z}_2$
  - (b) sottogruppi di ordine divisore? sì! esercizio.
2. per Gruppi non Abelian?
  - (a) a maggior ragione no
  - (b) no

**Esercizio.** Classificare i gruppi  $G$  di ordine 6.

Per Cauchy esistono  $x, y \in G$  di ordine, rispettivamente, 2 e 3.

- Se  $G$  è abeliano,  $\text{ord}(xy) = 6$ , quindi  $G$  è ciclico e pertanto isomorfo a  $\mathbb{Z}_6$ .
- Se non lo è, costruiamo un isomorfismo esplicito...

**Teorema G.12** (Caylay). *Possiamo immergere ogni gruppo  $G$  in  $S(G)$ .*

*Proof.* Esibiamo un'azione fedele (ovvero, iniettiva):

$$\begin{aligned} \Phi: G &\rightarrow S(G) \\ g &\mapsto \varphi_g(x) = gx \end{aligned}$$

è ora sufficiente verificare che  $\Phi$  è ben definito ( $\varphi_g$  è una bigezione) e iniettivo. ♣

**Definizione G.13** (Sottogruppo generato). Sia  $S \subset G$  un sottoinsieme su  $G$ , chiamiamo il più sottogruppo contenente  $S$  sottogruppo generato da  $S$  ( $\langle S \rangle$ ).

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$$

**Teorema G.14** (Caratterizzazione dei sottogruppi generati).

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

*Proof.* Chiamiamo  $X$  il magico insieme nel RHS. Chiaramente  $S \subseteq X$  e pertanto  $X$ , che è facile verificare essere un gruppo, è parte della famiglia sotto intersezione:  $X \subseteq \bigcap \mathcal{F}$ . Inoltre se  $S \subseteq H < G$  sicuramente in  $H$  compaiono tutte le  $k$ -uple di  $X$  e quindi  $X < H$  per ogni sottogruppo di  $\mathcal{F}$ . Dunque  $X \subseteq \bigcap \mathcal{F}$ . ♣

**Esempi.**

1.  $\langle S \rangle$  è abeliano se e solo se tutti gli elementi di  $S$  commutano fra loro.
2.  $\langle S \rangle$  è normale se e solo se ogni elemento di  $S$  rimane in  $\langle S \rangle$  per coniugio.
3.  $\langle S \rangle$  è caratteristico se e solo se ogni elemento di  $S$  viene mandato in  $\langle S \rangle$  da ogni automorfismo di  $G$ .
4.  $G' = \langle ghg^{-1}h^{-1} \mid g, h \in G \rangle$  è detto *Gruppo dei Commutatori o Gruppo Derivato di  $G$* . Questo gruppo gode di alcune proprietà fondamentali
  - (a)  $G' = \{e\} \Leftrightarrow G$  abeliano.
  - (b)  $G'$  è caratteristico e pertanto normale in  $G$ .

- (c) **Dato  $H \triangleleft G$ , il quoziente  $G/H$  è abeliano se e solo se  $G' \leq H$ .**

*Proof.* La verifica delle proprietà (a) e (b) è banale. Rimane l'ultima (c):

$$\begin{aligned}
 G/H \text{ abeliano} &\Leftrightarrow xHyH = yHxH && \forall x, y \in G \\
 &\Leftrightarrow xyH = yxH && \forall x, y \in G \\
 &\Leftrightarrow x^{-1}y^{-1}xy \in H && \forall x, y \in G \\
 &\Leftrightarrow g' \in H && \forall g' \in G'
 \end{aligned}$$



**Definizione G.15.**  $G/G'$  è detto l'abelianizzato di  $G$ , perché è sempre abeliano!

### G.3 Gruppi Diedrali $D_n$

**Definizione G.16** (Gruppo Diedrale). Sia  $D_n$  il gruppo delle isometrie dell' $n$ -agono regolare.

**Teorema G.17** (Caratterizzazione di  $D_n$ ). Si ha

$$D_n = \langle \rho, \sigma \mid \rho^n = e, \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} \rangle$$

*Proof.* Tutti gli elementi sopra definiti possiamo ridurli a un elemento della forma  $\rho^k$  o  $\sigma\rho^k$  per un qualche  $0 \leq k < n$ . Questo perché così sono fatti i generatori e ogni operazione permessa (composizione e inversione) si riducono a questa forma attraverso le leggi a disposizione. Inoltre possiamo immergere  $D_n$  in un sottogruppo di  $\mathbf{O}_2(\mathbb{R})$  di ordine  $2n$  attraverso un omomorfismo suriettivo:

$$\begin{aligned} \Phi: D_n &\rightarrow \mathbf{O}_2(\mathbb{R}) \\ \sigma &\mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ \rho &\mapsto \begin{pmatrix} \cos \frac{2\pi}{n} & \sin \frac{2\pi}{n} \\ -\sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \end{aligned}$$

Pertanto ognuno dei rappresentati sopra individua un'effettiva trasformazione distinta. ♣

*Osservazione.* Conosciamo già un gruppo diedrale:  $D_3 \cong S_3$ .

*Osservazione.* Il sottogruppo  $C_n$  delle rotazioni, generato da  $\rho$ , è ovviamente ciclico e, avendo indice 2, è anche normale in  $D_n$ .

$$\langle \rho \rangle = C_n \triangleleft D_n$$

**Teorema G.18** (Ordine degli elementi di  $D_n$ ). Sappiamo che

- tutte le simmetrie hanno ordine 2.
- ci sono  $\varphi(m)$  rotazioni di ordine  $m$ , per ogni  $m \mid n$ .

*Proof.* La seconda parte è immediata conseguenza della ciclicità del sottogruppo delle rotazioni. L'ordine delle riflessioni possiamo calcolarlo esplicitamente notando che  $(\sigma\rho^k)(\sigma\rho^k) = (\sigma\rho^k\sigma)\rho^k = \rho^{-k}\rho^k = e$  grazie alla terza proprietà imposta nella caratterizzazione. ♣

**Teorema G.19** (Sottogruppi di  $D_n$ ). I sottogruppi  $H < D_n$  rientrano in una di queste due categorie:

- $H < C_n$ : di cui ne abbiamo esattamente uno per ogni ordine divisore di  $n$ .

- $H = (H \cap C_n) \sqcup \tau(H \cap C_n)$ : di cui ce ne sono  $d$  di ordine  $\frac{2n}{d}$  per ogni  $d \mid n$ .

*Proof.* Se  $H < C_n$  il risultato viene da Aritmetica. Se  $H \not< C_n$ ,  $H$  contiene almeno una rotazione  $\tau = \sigma\rho^i$ . Consideriamo l'omomorfismo  $f$  che fa commutare il diagramma

$$\begin{array}{ccc} D_n & \xrightarrow{\Phi} & \mathbf{O}_2(\mathbb{R}) \\ & \searrow f & \downarrow \det \\ & & \{\pm 1\} \cong \mathbb{Z}_2 \end{array}$$

Notiamo che  $\ker f = C_n \triangleleft D_n$  e osserviamo cosa succede quando restringiamo l'omomorfismo trovato ad  $H$

$$\begin{array}{ccc} H & \xrightarrow{f|_H} & f(H) \\ id \downarrow & & \downarrow id \\ D_n & \xrightarrow{f} & \mathbb{Z}_2 \end{array}$$

Abbiamo così scomposto il nostro sottogruppo come desiderato, poiché conosciamo il  $\ker$  della trasformazione

$$H = f^{-1}(0) \sqcup f^{-1}(1) = (H \cap C_n) \sqcup \tau(H \cap C_n)$$

Poiché  $(H \cap C_n) < C_n$  possiamo vederlo come il sottogruppo generato da una potenza della rotazione elementare

$$H \cap C_n = \langle \rho^d : d \mid n \rangle$$

Il suo unico laterale sarà allora composto dagli  $d$  elementi della forma

$$\begin{aligned} \tau(H \cap C_n) &= \{\tau\rho^d, \tau\rho^{2d}, \dots, \tau\rho^{n-m}\} \\ &= \{\sigma\rho^{d+i}, \sigma\rho^{2d+i}, \dots, \sigma\rho^{n-m+i}\} \end{aligned}$$

che è facile convincersi dipendere solamente dalla classe di  $i$  mod  $m$ . ♣

**Esercizi.**

1. Quali sottogruppi di  $D_n$  sono normali?
2. Quali sottogruppi di  $D_n$  sono caratteristici?
3. Quali sono i quozienti di  $D_n$ ?
4. (\*) Chi è  $\text{Aut}(D_n)$ ?

## G.4 Gruppi di Permutazioni $\mathcal{S}_n$

**Definizione G.20** (Gruppi di Permutazioni). Dato un insieme  $X$ , chiamiamo

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

con l'operazione di composizione, il gruppo delle permutazioni di  $X$ . Se l'insieme è finito  $|X| = n$ , allora

$$\mathcal{S}(X) \cong \mathcal{S}(\{1, 2, \dots, n\})$$

lo chiamiamo  $\mathcal{S}_n$ .

**Teorema G.21.** Ogni permutazione  $\sigma \in \mathcal{S}_n$  si scrive in modo unico come prodotto di cicli disgiunti.

*Osservazione.* Cicli disgiunti commutano.

**Teorema G.22.**  $\mathcal{S}_n$  è generato dai suoi cicli.

**Esercizi.**

1. Quanti  $k$ -cicli ci sono in  $\mathcal{S}_n$ ?
2. Come conto gli elementi con una composizione fissata in un  $\mathcal{S}_n$  dato? Per esempio, come calcolo le permutazioni del tipo  $3 + 3 + 2 + 2 + 2$  in  $\mathcal{S}_{10}$ ?
3. L'ordine di  $\sigma$  è il minimo comune multiplo delle lunghezze dei suoi  $k$ -cicli.

**Teorema G.23.**  $\mathcal{S}_n$  è generato dalle sue trasposizioni.

*Osservazione.* La decomposizione in trasposizioni non è unica. Ma la parità dei numeri di trasposizioni lo è:

**Teorema G.24.** La parità del numero di trasposizioni della scomposizione di una qualunque permutazione  $\sigma \in \mathcal{S}_n$  non dipende dalla scomposizione.

*Proof.* Consideriamo

$$\begin{aligned} \text{sgn} : \mathcal{S}_n &\rightarrow \mathbb{Z}^\times = \{\pm 1\} \\ \sigma &\mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

questo è un omomorfismo di gruppi. Infatti:

1. è ben definito, ovvero  $|\text{sgn}(\sigma)| = 1$ : tutte le differenze che compaiono a denominatore compaiono anche a numeratore, poiché  $\sigma$  è una permutazione, magari con ordine o segno, differente.

2. Si comporta bene con la composizione

$$\begin{aligned} \text{sgn}(\sigma \circ \tau) &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{i < j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \text{sgn}(\sigma) \cdot \text{sgn}(\tau) \end{aligned}$$

Infine, tutte le trasposizioni hanno segno negativo. ♣

**Definizione G.25** (Gruppo Alternato). Chiamiamo  $A_n$  o gruppo alternato il sottogruppo delle permutazioni pari

$$\ker(\text{sgn}) = A_n \triangleleft \mathcal{S}_n$$

**Teorema G.26.** Due permutazioni  $\sigma, \tau \in \mathcal{S}_n$  sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli.

*Proof.*  $\Rightarrow$ . Ci basta dimostrare che dato un ciclo  $\sigma = (a_1 \dots a_k)$  e una permutazione tale che  $\tau(a_i) = b_i$ . Allora le immagini del ciclo vengono mandati nel loro "successore"

$$\tau\sigma\tau^{-1}(b_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1}$$

mentre le non immagini di alcun  $a_i$ , con controimmagini invarianti per  $\sigma$ , rimangono fisse

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

pertanto

$$\tau\sigma\tau^{-1} = (b_1 \dots b_k)$$

$\Leftarrow$ . Se vogliamo mandare il ciclo  $(a_1 \dots a_k)$  in  $(b_1 \dots b_k)$  ci basta coniugare per la stessa permutazione di prima:  $\tau(a_i) = b_i$ . Possiamo poi costruire il coniugio moltiplicando tra loro tutte le  $\tau$  relative ai vari cicli. ♣

*Osservazione.* Notiamo che il centralizzatore di  $\sigma$  coincide con lo stabilizzatore dell'azione di coniugio di  $\mathcal{S}_n$  in se. Dunque

$$|Z(\sigma)| = \frac{n!}{|\mathcal{C}(\sigma)|}$$

**Esercizio.** Data una permutazione  $\sigma$  trovare  $N(\langle \sigma \rangle)$

## G.5 Prodotti diretti

A un certo punto vorremo arrivare a dimostrare il seguente risultato, che ora enunciamo un po' a caso.

**Teorema G.27** (di Struttura dei gruppi abeliani finitamente generati). *Possiamo scrivere ogni gruppo abeliano finitamente generato  $G$ , in modo unico, come prodotto diretto di gruppi ciclici nel modo seguente*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

dove  $n_1, \dots, n_k$  sono interi tali che  $n_1 \mid n_2 \mid \cdots \mid n_k$ .

**Definizione G.28.** Chiamiamo  $p$ -sylo ogni  $p$ -sottogruppo di ordine massimo. Ovvero  $H < G$ , dove  $|G| = p^m n$  con  $(m, n) = 1$  e  $|H| = p^m$ .

**Teorema G.29.** *Sia  $G$  un gruppo e  $H, K \triangleleft G$  due sottogruppi normali. Se*

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

allora  $G \cong H \times K$ .

*Proof.* Mostriamo innanzitutto che  $hkh^{-1}k^{-1}$  appartiene ad entrambi i sottogruppi, infatti:

$$H \ni h(kh^{-1}k^{-1}) = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1} \in K$$

dunque, per la seconda ipotesi,

$$hkh^{-1}k^{-1} = e$$

quindi gli elementi di un sottogruppo commutano con quelli dell'altro  $hk = kh$ .

Consideriamo ora l'isomorfismo

$$\begin{aligned} \Phi: H \times K &\rightarrow G \\ (h, g) &\mapsto hg \end{aligned}$$

e verifichiamo che

1. è ben definito.
2. è un omomorfismo: infatti

$$\Phi(hh', kk') = hh'kk' = hkh'k' = \Phi(h, k)\Phi(h', k')$$

3. è suriettivo per la prima ipotesi.
4. è iniettivo per la seconda, infatti

$$\ker \Phi = \{(h, k) \mid hk = e\} = \{(e, e)\}$$



*Osservazione.* Nel prodotto diretto i fattori commutano.

**Proprietà di  $G = H \times K$ .**

1.  $Z(G) = Z(H) \times Z(K)$ .
2.  $\text{Int}(G) \cong \text{Int}(H) \times \text{Int}(K)$ .
3.  $\text{Aut}(H) \times \text{Aut}(K) < \text{Aut}(G)$ .

**Teorema G.30.** *Si ha  $\text{Aut}(H) \times \text{Aut}(K) < \text{Aut}(H \times K)$  e sono isomorfi se e solo se  $H$  e  $K$  sono caratteristici.*

*Proof.* Consideriamo l'omomorfismo

$$\begin{aligned} \Phi: \text{Aut}(H) \times \text{Aut}(K) &\rightarrow \text{Aut}(H \times K) \\ (f, g) &\mapsto \varphi_{fg}: (h, k) \mapsto (f(h), g(k)) \end{aligned}$$

e verifichiamo che

- è bene definito, ovvero  $\varphi$  è un automorfismo. Immediata conseguenza del fatto che  $f$  e  $g$  sono a loro volta automorfismi.
- è un omomorfismo.

$$\begin{aligned} \Phi(ff', gg') &= (f(f'(h)), g(g'(k))) \\ &= \varphi_{fg}(\varphi_{f'g'}(h, k)) \\ &= \Phi(f, g)\Phi(f', g') \end{aligned}$$

- è iniettivo.

$$\ker \Phi = \{(id, id)\}$$

altrimenti c'è almeno un elemento di uno dei due gruppi che non va in se stesso.

- è suriettivo se e solo se  $H \times \{e_K\}$  e  $\{e_H\} \times K$  sono caratteristici in  $H \times K$ .

$\Rightarrow$ . Se  $\Phi$  è suriettivo, allora tutti gli automorfismi di  $H \times K$  sono della forma di cui sopra e pertanto  $\varphi_{fg}$  agisce sugli elementi di  $H$  come  $\varphi_{fg|H} = f \in \text{Aut}(H)$ .

$\Leftarrow$ . Viceversa, supponiamo  $H$  e  $K$  caratteristici, preso un automorfismo  $\varphi \in \text{Aut}(H \times K)$  consideriamo le sue restrizioni ai due sottogruppi caratteristici.

$$f = \Pi_H(\varphi|_{H \times \{e_K\}}) \quad g = \Pi_K(\varphi|_{\{e_H\} \times K})$$

Notiamo che  $f \in \text{Aut}(H)$ .

- $f$  è iniettiva. Se  $f(h) = f(h')$  allora

$$\Pi_H(\varphi(h, e_K)) = \Pi_H(\varphi(h', e_K))$$

poiché  $H \times \{e_K\}$  è caratteristico

$$\varphi(h, e_K) = (a, e_K) \quad \varphi(h', e_K) = (b, e_K)$$

ma necessariamente  $a = f(h)$  e  $b = f(h')$ , pertanto

$$\varphi(a, e_K) = (f(h), e_K) = (f(h'), e_K) = \varphi(b, e_K)$$

e, visto che  $\varphi$  è iniettivo,  $h = h'$ .

- $f$  è suriettiva. Fissiamo un qualunque  $h \in H$ . Essendo  $H \times \{e_K\}$  caratteristico, necessariamente la controimmagine di  $(h, e_K)$  è un suo elemento

$$\varphi^{-1}(h, e_K) = (h', e_K)$$

dunque

$$f(h') = \Pi_H(\varphi(h', e_K)) = \Pi_H(h, e_K) = h$$

Infine osserviamo che  $\Phi(f, g) = \varphi$ . Infatti

$$\begin{aligned} \varphi_{fg}(h, k) &= (f(h), g(k)) \\ &= (\Pi_H(\varphi(h, e_K)), \Pi_K(\varphi(e_H, k))) \\ &= (\Pi_H(\varphi(h, k)), \Pi_K(\varphi(h, k))) \\ &= \varphi(h, k) \end{aligned}$$

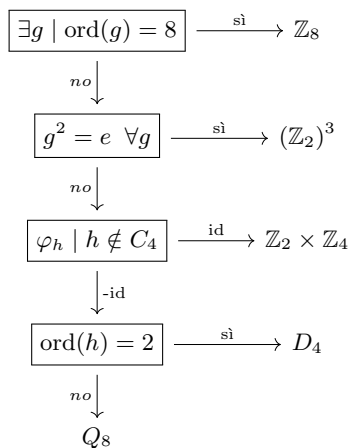
dove la terza uguaglianza segue da

$$\begin{aligned} \Pi_H(\varphi(h, e_K)) &= \Pi_H(\varphi(h, e_K)) \Pi_H(\varphi(e_H, k)) \\ &= \Pi_H(\varphi(h, e_K)\varphi(e_H, k)) \\ &= \Pi_H(\varphi(h, k)) \end{aligned}$$



**Esercizio.** Trovare  $\text{Aut}(\mathbb{Z}_{20} \times \mathbb{Z}_2)$ .

## G.6 Classificazione dei Gruppi di ordine 8



Prendiamo un gruppo  $G$  di ordine 8.

- Se esiste un elemento di ordine 8 il gruppo è ciclico e pertanto isomorfo a  $\mathbb{Z}_8$ .
- Se  $G$  ha solo elementi di ordine 2, allora è isomorfo a  $(\mathbb{Z}_2)^3$ . Mostriamo un risultato appena più generale.

**Teorema G.31.** *Se  $|G|$  ha solo elementi di ordine due ed è finito, allora  $G \cong (\mathbb{Z}_2)^n$ .*

*Proof.* Osserviamo che  $a^2b^2 = e = (ab)^2 = abab$  e, moltiplicando per  $a$  a sinistra e per  $b$  a destra, otteniamo  $ab = ba$  per ogni  $a, b \in G$ . Pertanto  $G$  è abeliano. Possiamo ora procedere per induzione sulla dimensione di  $G$ . Se  $|G| = 2$  il risultato è chiaro. Supponiamo ora che sia vero per tutti i gruppi di ordine  $< 2^n$  e supponiamo  $2^n \leq |G| < 2^{n+1}$ . Quando prendiamo un insieme minimale di  $h < n$  generatori  $\langle g_1, \dots, g_h \rangle$  di un sottogruppo di  $H < G$ , questo sarà isomorfo a  $(\mathbb{Z}_2)^h$  per ipotesi induttiva. Prendiamo un elemento  $g \notin H$ , abbiamo che  $H$  e  $\langle g \rangle \cong \mathbb{Z}_2$  sono sottoinsiemi normali e con intersezione banale, pertanto il sottoinsieme

$$\langle g, g_1, \dots, g_h \rangle \cong H \times \langle g \rangle \cong (\mathbb{Z}_2)^h \times \mathbb{Z}_2 \cong (\mathbb{Z}_2)^{h+1}$$

per il teorema di struttura G.29. Così facendo possiamo continuare ad aggiungere elementi fino a saturare il gruppo e raggiungere la tesi. ♣

Sia ora  $g \in G$  l'elemento di ordine 4 richiesto e  $C_4 = \langle g \rangle$ . Sia  $h \notin C_4$  e consideriamo l'azione di coniugio di  $h$  su  $C_4$

$$\begin{aligned}
 \phi_g: C_4 &\rightarrow C_4 \\
 x &\mapsto h x h^{-1}
 \end{aligned}$$

ben definita perché  $C_4$ , avendo indice 2, è normale in  $G$ . Poiché  $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$ , abbiamo solo due possibilità:

$$\varphi_g = id^{\pm 1}$$

- $[\varphi_g = id, \text{ord}(h) = 2]$ . Dunque gli elementi di  $C_4$  commutano con  $h$ , l'intersezione tra  $C_4$  e  $\langle h \rangle$  è banale e il loro prodotto genera  $G$  per ragioni di cardinalità, pertanto

$$G \cong \langle h \rangle \times C_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

- $[\varphi_g = id, \text{ord}(h) = 4]$ . Possiamo considerare  $h^2$  e ricondurci al caso precedente.
- $[\varphi_g = id^{-1}, \text{ord}(h) = 2]$ . Abbiamo che  $hgh = g^{-1}$ , quindi per la nostra caratterizzazione dei gruppi diedrali

$$G \cong D_4$$

- $[\varphi_g = id^{-1}, \text{ord}(h) = 4]$ . Anche  $\text{ord}(gh) = 4$ . Infatti

$$e = ghgh = ghgh^{-1}hh = hh \neq e$$

Dunque abbiamo trovato l'ordine di tutti gli elementi, possiamo costruire un'isomorfismo esplicito con  $Q_8$ .

**Definizione G.32** (Quaternioni). Sia  $Q_8$  l'insieme  $\{\pm 1, \pm i, \pm j, \pm k\}$  con l'operazione che soddisfa

$$i^2 = j^2 = k^2 = ijk = -1$$



## G.7 Lemmi vari

**Teorema G.33.** *Siano  $G$  un gruppo finito e  $H$  un sottogruppo che ha come ordine il più piccolo primo  $p$  che divide  $G$ , allora  $H \triangleleft G$ .*

*Proof.* Consideriamo l'azione di  $G$  sull'insieme  $X$  dei laterali di  $H$  per moltiplicazione a sinistra

$$\begin{aligned}\Phi: G &\rightarrow \mathcal{S}_p \\ g &\mapsto \Pi_g : xH \mapsto gxH\end{aligned}$$

Osserviamo che

$$\begin{aligned}g \in \text{Stab}(xH) &\Leftrightarrow gxH = xH \\ &\Leftrightarrow x^{-1}gx \in H \\ &\Leftrightarrow g \in xHx^{-1}\end{aligned}$$

dunque  $\text{Stab}(xH) = xHx^{-1}$  è il sottogruppo coniugato di  $H$  rispetto ad  $x$ . Possiamo ora riscrivere il nucleo come

$$\ker \Phi = \bigcap_{x \in G} xHx^{-1} < H$$

e osservare che, per il Primo Teorema di Omomorfismo

$$\Phi' : G/\ker \Phi \rightarrow \mathcal{S}_p$$

è iniettivo e pertanto

$$\left| G/\ker \Phi \right| \mid |\mathcal{S}_p| = p!$$

ma  $p$  era il più piccolo primo a dividere  $|G|$ , quindi non potendo  $\ker \Phi$  coincidere con tutto il gruppo, dovrà essere proprio  $H$ . Il che conclude la dimostrazione. ♣

*Osservazione.* Sia  $G$  un gruppo abeliano. Sia

$$\begin{aligned}\psi_n: G &\rightarrow G \\ x &\mapsto x^n\end{aligned}$$

preso un qualunque automorfismo  $\varphi \in \text{Aut}(G)$  il seguente diagramma è commutativo

$$\begin{array}{ccc} G & \xrightarrow{\psi_n} & G \\ \varphi \downarrow & & \downarrow \varphi \\ G & \xrightarrow{\psi_n} & G \end{array}$$

quindi  $\ker \psi_n$  e  $\psi_n(G)$  sono caratteristici in  $G$ .

**Esercizi.**

1. Trova  $\text{Aut}(\mathbb{Z} \times \mathbb{Z}_n)$ .
2. Trova  $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4)$ .
3. Trova  $\text{Aut}(Q_8 \times D_4)$ .
4. Sia  $G$  un gruppo abeliano finito. Se  $H \triangleleft G$  è ciclico e lo è anche il loro quoziente, allora anche  $G$  è ciclico.

## G.8 Prodotto Semidiretto

**Definizione G.34** (Prodotto semidiretto). Siano  $H, K$  due gruppi e  $\varphi : K \rightarrow \text{Aut}(H)$  un'omomorfismo. Si dice prodotto semidiretto

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

l'insieme dato dal prodotto cartesiano, dotato dell'operazione

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

*Osservazione.* Il prodotto semidiretto è un gruppo.

*Osservazione.* Il prodotto diretto è un prodotto semidiretto in cui  $\varphi$  manda tutti gli elementi di  $K$  nell'identità su  $H$ .

*Osservazione.* Sia  $\bar{H} = H \times e_k$ . Si ha

$$\ker \Pi_K = \bar{H} \triangleleft H \rtimes_{\varphi} K$$

qualunque sia l'omomorfismo  $\varphi$ . Infatti  $\bar{H}$  è il nucleo dell'omomorfismo di proiezione su  $K$ .

*Osservazione.* Inoltre  $\bar{K}$  se e solo se il prodotto è diretto.

$$\bar{K} \triangleleft H \rtimes_{\varphi} K \Leftrightarrow \rtimes = \times$$

**Teorema G.35** (Teorema di decomposizione in prodotto semidiretto). Siano  $G$  un gruppo e  $H, K < G$  sottogruppi, con  $H \triangleleft G$  normale. Se

$$1. HK = G$$

$$2. H \cap K = \{e\}$$

allora  $G \cong H \rtimes_{\varphi} K$  dove  $\varphi$  manda  $k$  nella corrispondente azione di coniugio

$$\varphi : K \rightarrow \text{Aut}(H)$$

$$k \mapsto \varphi_k : h \mapsto hkh^{-1}$$

*Proof.* Consideriamo

$$\begin{aligned} \Phi : H \rtimes_{\varphi} K &\rightarrow G \\ (h, k) &\mapsto hk \end{aligned}$$

questo

► è un omomorfismo, perché

$$\begin{aligned} \Phi((h, k)(h', k')) &= \Phi(h\varphi_k(h'), kk') \\ &= \Phi(hkh'k^{-1}, kk') \\ &= hkh'k^{-1}kk' \\ &= hkh'k' \\ &= \Phi(h, k)\Phi(h', k') \end{aligned}$$

► è iniettivo e suriettivo per le ipotesi, come nella decomposizione in prodotto diretto.

dunque  $\Phi$  è un isomorfismo come desiderato. ♣

**Esempi.**

1.  $\mathcal{S}_n \cong A_n \rtimes_{\varphi} \langle (1\ 2) \rangle$ , con  $\varphi$  di coniugio.

2.  $D_n \cong \langle \rho \rangle \rtimes_{\varphi} \langle \sigma \rangle$ , con  $\varphi$  di coniugio.

## G.9 Sottogruppi di Ordine $pq$

Se  $p = q$ , allora  $|G| = p^2$ , quindi  $G$  è abeliano. Allora necessariamente

$$G \cong \mathbb{Z}_{p^2} \quad \text{oppure} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Se  $p < q$ , allora ho due elementi  $x, y$  di ordine, rispettivamente,  $p$  e  $q$ , che generano relativi gruppi ciclici. Il più grande dei quali sarà normale

$$K = \langle x \rangle < G \quad \text{e} \quad H = \langle y \rangle \triangleleft G$$

per il teorema G.33. Inoltre osserviamo che  $HK = G$  e i due sottogruppi hanno intersezione banale. Quindi

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

dove

$$\begin{aligned} \varphi_1: K &\rightarrow \text{Aut}(H) \cong \mathbb{Z}_q^{\times} \\ y &\mapsto \varphi_y: x \mapsto xyx^{-1} \end{aligned}$$

e necessariamente dobbiamo avere che

$$yxy^{-1} = x^k \quad \text{con} \quad (k, q) = 1$$

ma, poiché  $\varphi$  è un omomorfismo, abbiamo che

$$\text{ord}(\varphi_y) \mid \text{ord}(y) = p$$

quindi abbiamo solo due casi:  $\text{ord}(\varphi_y) = 1$  e  $\text{ord}(\varphi_y) = p$ . Nel primo caso  $\varphi$  manda ogni elemento nell'identità, dunque il prodotto semidiretto è in realtà diretto e dunque

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q$$

Nel secondo caso dobbiamo avere

$$p = \text{ord}(\varphi_y) \mid \text{ord}(x^k) \mid q - 1$$

Vogliamo mostrare che qualunque omomorfismo  $\psi$  da  $K$  a  $\text{Aut}(H)$ , non banale, costruisce un prodotto semidiretto isomorfo a  $G$  e ci è pertanto concesso scrivere

$$G \cong H \rtimes K$$

Osserviamo innanzitutto che le azioni del tipo

$$\varphi_i: y \mapsto \varphi_{y^i}: x \mapsto y^i x y^{-i} \quad 0 \leq i < p$$

sono tutte e sole le azioni di  $K$  su  $H$ .

Queste sono  $p$  e sono tutte distinte.

Inoltre una qualunque azione è un omomorfismo da  $K$  ad  $\text{Aut}(H) \cong \text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}^{\times}$ . Dovendo l'azione avere ordine  $p$ , dev'essere un omomorfismo da  $K$  al sottogruppo ciclico di ordine  $p$  di  $\text{Aut}(H)$ . Pertanto, escluso l'omomorfismo banale  $\varphi_0$ , gli omomorfismi sono isomorfismi del gruppo ciclico sopracitato e perciò sono in totale  $1 + |\text{Aut}(\mathbb{Z}_p)| = 1 + (p-1) = p$ . A questo punto è facile convincersi che la mappa

$$\begin{aligned} \Phi: H \rtimes_{\varphi_1} K &\rightarrow H \rtimes_{\varphi_i} K \\ (x, y) &\mapsto (x, y^k) \end{aligned}$$

è un'isomorfismo tra tutti i possibili prodotti semidiretti.