# GRUPPI

sabato 15 ottobre 2022 15:12

## AZIONI

**definizione**

$G$ gruppo $\quad \varphi_g : G \longrightarrow G$
$\qquad\qquad x \longrightarrow \underbrace{gxg^{-1}}_{\text{coniugato di } x}$

coniugio

**Proposizione**

1) $\forall g \in G \quad \varphi_g \in Aut(G)$

2) $Inn(G) = \{\varphi_g \mid g \in G\} \trianglelefteq Aut\, G$
 ↳ gruppo degli automorfismi interni

**Proposizione**

$Inn\, G \cong G/Z(G)$

**conseguenze**

1) $G/Z(G)$ ciclico $\Rightarrow$ $G$ abeliano

2) $G$ abeliano $\Rightarrow$ $Inn(G) = \{e\}$ dato che $G = Z(G)$

---

azione

$G$ gruppo, $X$ insieme $\quad G \curvearrowright X \quad$ $G \times X \longrightarrow X$ è un'azione
$\qquad\qquad\qquad\qquad\qquad\qquad (g, x) \longrightarrow g \cdot x$
se verifica 2 proprietà:

**1.** $e \cdot x = x \quad \forall x$

**2.** $(g_1 g_2) x = g_1 \cdot (g_2 x) \quad \forall g_1, g_2 \in G \quad \forall x \in X$

es di azioni

**1.** azione di $G$ su se stesso per coniugio $\quad G \curvearrowright G$
$G \times G \to G$
$(g, x) \to gxg^{-1} \quad \forall x, g \in G.$

**2.** azione sui laterali
$G$ gruppo $\quad G/H = X$ insieme $\quad H < G \quad G \curvearrowright X = G/H$
$G \times G/H \longrightarrow G/H$
$(g, g_1 H) \longrightarrow (g g_1) H$

---

**definizione**

$G$ gruppo, $X$ insieme, un' azione di $G$ su $X$ è un omomorfismo $\phi : G \longrightarrow S(X)$
$\qquad\qquad g \longrightarrow \varphi_g \quad$ dove $\varphi_g : X \to X \quad$ con $\varphi_g$ bigettiva $\forall g \in G$
$\qquad\qquad\qquad\qquad\qquad\qquad x \mapsto \underbrace{\varphi_g(x)}_{g * x \text{ (azione di } g \text{ su } x)}$

$G \circlearrowleft X$

**relazione di equivalenza**

$\varphi$ definisce una relazione di equivalenza su $X$

$x \sim y \iff \exists\, g \in G$ t.c. $\varphi_g(x) = y$ cioè due elt. sono in relazione se $\exists$ un'applicazione $\varphi_g \in S(X)$ per cui un elt. è immagine dell'altro mediante $\varphi_g$

orbite

Data $\sim$ le classi di equivalenza di $X$ sono le orbite $Orb(x) = \{\varphi_g(x) \mid g \in G\} \subseteq X$

$X = \dot{\bigcup}_{x \in R} Orb_G(x)$

Quindi l'orbita = {tutte le immagini di un elt in un insieme mediante tutte le possibili applicazioni dell'insieme $\varphi(G)$}

Stabilizzatore

$St(x) = \{g \in G \mid \varphi_g(x) = x\}$

cioè lo stabilizzatore = {elt di $G$ che danno origine alle applicazioni $\varphi_g \in S(X)$ mediante $\varphi$ che lasciano fisso un det. elt}

- $St(x) \leq G$

Relazione tra orbite e stabilizzatore

$Orb(x) \longleftrightarrow$ classi laterali di $St(x)$ in $G$

$$orb(x) \longleftrightarrow G/St(x)$$

$$|G| = |St(x)|\,[G : St(x)]$$

$$|G| = |St(x)| \cdot |orb(x)|$$

$\begin{cases} |St(x)| \mid |G| & \text{perchè } St(x) \leq G \text{ la Grange} \\ |orb(x)| \mid |G| & \text{anche se } orb(x) \not\leq G. \end{cases}$

Se $|X| < +\infty$ $\quad |X| = \sum_{x \in R} |orb(x)| = \sum_{x \in R} \frac{|G|}{|St(x)|}$ perchè $X = \dot{\bigcup}_{x \in R} orb(x)$

azione di coniugio

$G \circlearrowleft G = X$ $\quad \varphi : G \longmapsto Inn\, G \trianglelefteq S(G)$

$\varphi$ azione perchè $\varphi$ omo $\quad g \longmapsto \varphi_g : G \longmapsto G$

$x \longmapsto gxg^{-1} = \varphi_g(x)$

Orbite

$Orb(x) = \{\varphi_g \mid g \in G\} = \{gxg^{-1} \mid g \in G\} = C_x$ = classe di coniugio di $x$

Stabilizzatore

$St(x) = \{g \in G \mid \varphi_g(x) = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = Z_G(x)$ = centralizzatore di $x$
tutti gli elt di $G$ che commut con $x$

Formule

$|G| = |St(x)| \cdot |orb(x)| = |Z_G(x)|\,|C_x|$

⚠ $C_x \not\leq G$ perchè $\{e\} \not\subseteq C_x$

$$|G| = \sum_{x \in R} |C_x| = \sum_{x \in R} \frac{|G|}{|Z_G(x)|}$$

Osservazioni

1 $Z_G(x) = G \iff x \in Z(G)$ (centralizzatore) infatti se $x \in Z(G)$ allora $\forall g \in G$ $gx = xg \Rightarrow Z_G(x) = G$.

2 Per azione di coniugio si ha che $x \in Z(G) \iff orb(x) = \{x\}$ cioè $\varphi_g(x) = gxg^{-1} = gg^{-1}x = x$ $\forall g \in G$.

3 $|G| = \sum_{x \in Z(G)} \frac{|G|}{|Z_G(x)|} + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$ se $x \in Z(G) \Rightarrow \frac{|G|}{|Z_G(x)|} = |C_x| = \{x\}$ Quindi $\sum_{x \in Z(G)} |\{x\}| = |Z(G)|$

$$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|} \quad := \text{formula delle classi}$$

definizione

- Si definisce p-gruppo un gruppo di ordine $p^n$ con p primo e $n \geq 1$
- Se G è un p-gruppo la formula delle classi diventa $p^n = |G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} \left| \frac{|G|}{|Z_G(x)|} \right|$ con $|Z(G)| = p^z$ $1 \leq z \leq n$
- Il centro di un p-gruppo non è mai banale

$p \mid |G| = p^n$ $\quad p \mid \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}$ $\quad \Rightarrow p \mid |Z(G)|$

$\hookrightarrow$ perché $\frac{|G|}{|Z_G(x)|} > 1$

- Un gruppo di ordine $p^2$ e' abeliano $\quad |G| = p^2 \Rightarrow |Z(G)| =$
  - $\to 1$ NO perché il centro di un p-gruppo non è banale
  - $\to p$ No perché $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ ciclico $\Rightarrow$ G abel $\Rightarrow$ $G = Z(G)$
  - $\to p^2$ SI

- Teorema di Cauchy

Dato un gruppo G di ordine p primo se $p \mid |G| \Rightarrow \exists\, x \in G$ t.c. $ord(x) = p$.

- Teorema di Cayley

Ogni gruppo e' isomorfo ad un sgr. di un gruppo di permutazioni. In particolare se $|G| = n \Rightarrow G \cong H \leq S_n$

per dimostrarlo uso $\lambda : G \to S(G)$ $\quad$ $\lambda :=$ rappresentazione regolare a sx di G.

$g \longmapsto \varphi_g : G \to G$

$g \longmapsto gx$

Teorema

Se G è gr. finito e $H \leq G$ se $[G:H] = p$ con p il più piccolo primo che divide $|G| \Rightarrow H \trianglelefteq G$.

Piccolo Teorema di Fermat

p primo, se $n \in \mathbb{Z}$ $(n,p) = 1 \Rightarrow n^{p-1} \equiv 1 \pmod p$

azione transitiva

G gruppo e X insieme $\varphi : G \to S(X)$, $g \mapsto \varphi_g$ $\quad$ $\varphi$ azione si dice transitiva se $\forall\, x,y \in X$ $\exists\, g \in G$ t.c. $\varphi_g(x) = y$ o equivalent. se $orb(x) = G$ $\forall x \in X$

Proprieta'

- G gruppo finito e $H \lneq G \Rightarrow G \neq \bigcup_{g \in G} gHg^{-1}$
- Se $\varphi$ e' transitiva allora
  - $\forall\, x,y \in X$ $\exists\, g \in G$ t.c. $g\,St(x)\,g^{-1} = St(y)$
  - Se $|X| \geq 2 \Rightarrow \exists\, g \in G$ che agisce su X senza punti fissi cioè tale che $\varphi_g(x) \neq x$ $\forall x \in X$

## azione di coniugio su un sottogruppo

Sia $X = \{H \leq G\}$ $\quad \varphi : G \longrightarrow S(X)$

$\varphi$ azione $\quad g \longmapsto \varphi_g(X) : X \longrightarrow X$, $\quad H \longrightarrow gHg^{-1}$

### Orbite

$Orb(H) = \{\varphi_g(H) \mid g \in G\} = \{gHg^{-1} \mid g \in G\} = \{$insieme dei coniugati di $H\}$

### Stabilizzatore

$St(H) = \{g \in G \mid \varphi_g(H) = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H) =$ normalizzatore di $H$

Proprietà normalizzatore

$H \trianglelefteq G \iff N_G(H) = G$

$N_G(H)$ è un sgr.

$H < N_G(H)$

$H \trianglelefteq N_G(H)$

$N_G(H)$ è il max sgr in cui $H$ è normale

### Osservazioni

$H \trianglelefteq G \iff Orb(H) = \{H\} \iff N_G(H) = G \iff H$ è chiuso per coniugio in $G$.

### Formule

- $|G| = |orb(H)| \cdot |St(H)| = |orb(H)|\,|N_G(H)|$

$H < G$.
- $\#\{gH\} = [G : H]$
- $\#\{gHg^{-1}\} = [G : N_G(H)]$

### Osservazioni

$H \trianglelefteq G \iff H = \bigcup_{h \in H} C_h$ $\quad$ dove $C_h = \{ghg^{-1} \mid h \in H\} \leq H$

$\boxed{\subseteq}$ $H \subseteq \bigcup C_h$

$\boxed{\supseteq}$ $H \supseteq \bigcup C_h$

"H è chiuso per coniugio"

$H \trianglelefteq G \iff ghg^{-1} \in H$ cioè $ghg^{-1} = h' \in H \ \forall h \in H$ e $\forall g \in G$

$\hookrightarrow C_h = \{ghg^{-1} \mid h \in H\} \leq H \ \forall h \in H \Rightarrow \bigcup_{h \in H} C_h \leq H$

# PRODOTTO DIRETTO

Lemmi utili

(1)

$\left.\begin{matrix} G = H \times K \quad \text{finiti} \\ 1 = (|H|, |K|) \end{matrix}\right\} \Rightarrow H \times \{e\}$ e $\{e\} \times K$ sono caratteristici in $G$
in tal caso $\mathrm{Aut}\, G \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$

$$f: \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(H) \times \mathrm{Aut}(K)$$
$$\varphi \longmapsto (\varphi_H, \varphi_K)$$

dove $\varphi_H(h) = \pi_1(\varphi(h,e))$ con $\pi_1: G \to H$

$\varphi_K(k) = \pi_2(\varphi(e,k))$ con $\pi_2 = G \to K$

(2) Dati $x, y \in G$ se $x, y$ commutano allora $\mathrm{ord}(xy) = [\mathrm{ord}(x), \mathrm{ord}(y)]$ anche se $G$ non è abeliano

(3) Se $H, K \leq G$ $HK \not\leq G$ in generale

$HK = \{hk \mid h \in H \text{ e } k \in K\} \ntrianglerighteq G$

$S_3 = G$ $M = \{e, (12)\}$ $N = \{e, (13)\}$

$MN = \{e, e(13), (12).e, \underbrace{(12)(13)}_{(132)}\}$ $MN \not\leq S_3$

(4) Se $H, K \leq G$ $HK \leq G \iff HK = KH$

(5) Se $H \trianglelefteq G$ e $K \leq G \Leftarrow HK \leq G$

$\Rightarrow$ in tal caso $\downarrow$ $|H_1 H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = |H_2 H_1|$

(6) $H \times K \leq G \times G$.

(7) $H, K \trianglelefteq G$ e $H \cap K = \{e\} \Rightarrow hk = kh$ $\forall h \in H$ e $\forall k \in K$ cioè commutano

In questo caso $HK < G$ e $\underbrace{HK}_{\text{prodotto interno}} \cong \underbrace{H \times K}_{\text{prodotto diretto esterno}}$

$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$

(8) Teorema

$\left.\begin{matrix} H, K \trianglelefteq G \\ HK = G \\ H \cap K = \{e\} \end{matrix}\right\} \Rightarrow G \cong H \times K$

(9) $G_1, G_2 \leq G$ $G = G_1 \times G_2 \Rightarrow H = G_1 \times \{e_2\} \trianglelefteq G$ e $K = \{e_1\} \times G_2 \trianglelefteq G$

Esempio importante

$|G| = p^2 \Rightarrow G$ abeliano $\Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$ oppure $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
gruppo di ordine $p^2$

Se $G$ è ciclico $\Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z}$ Se $G$ non è ciclico $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Sia $x \in G$ $H = \langle x \rangle$ $H \trianglelefteq G$
perché $G$ abeliano

Sia $y \in G/H$ e $K = \langle y \rangle$ $K \trianglelefteq G$

$\Rightarrow H \cap K = \{e\}$
Infatti $H$ e $K$ sono sgr ciclici di $G$ di ordine $p$ e quindi hanno in comune solo $e$

$HK = G$ per $\# \Rightarrow |HK| = \frac{|H||K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2$

Rispetta le hp. del Teo $\Rightarrow G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

## ALTRO

- Un'azione $\lambda$ si dice fedele se è inj.
- L'azione di rappresentazione regolare a sx è inj. $Ker(\lambda) = \{g \in G \mid \lambda(g) = id\} = \{g \in G \mid \lambda_g(e) = e\} = \{g \in G \mid ge = e\} = \{e\}$
- $\rho: G \longmapsto S(G) \cong S_n$ se $|G| = n$
  $g \longmapsto \rho_g : x \longrightarrow xg^{-1}$
  $\rho$: rappresentazione regolare a dx

- Se $G$ è abeliano di ordine $n \Rightarrow \forall d \mid n \; \exists H \leq G$ t.c. $|H| = d$
- $G$ gruppo se $|G| = p^n \Rightarrow \exists \; \{e\} = H_n < H_{n-1} < \dots < H_1 < G$ con $H_j \trianglelefteq G$ e $|H_j| = p^{n-j}$ $\forall j \in \{1, \dots, n\}$

commutatore

$G$ gruppo $x, y \in G$ $[x,y] = xyx^{-1}y^{-1}$ =: commutatore di $x$ e $y$

sgr derivato

$G' = \langle \{[x,y] \mid x, y \in G\} \rangle$ =: sgr dei commutatori o sgr derivato

osservazioni

- $[x,y] = e \iff x$ e $y$ commutano
- $G'$ è un sgr caratteristico di $G$.
- $G/G'$ è un gruppo abeliano
- Dato $A$ gruppo abeliano e $\varphi \in Hom(G,A) \Rightarrow G' \leq Ker\,\varphi$
- $G/G'$ è il più grande quoziente abeliano di $G$ o equivalentemente che $G'$ è il più piccolo sgr di $G$ che produce un quoziente abeliano. $G'$ misura quanto è abeliano $G$.
- Dato $A$ gruppo abeliano il 1 Teo di omo produce una bij $Hom(G,A) \longmapsto Hom(G/G', A)$

$$\begin{tikzcd} G \arrow[r, mapsto, "\varphi"] \arrow[d, "\pi_{G'}"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\ G/G' \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

$\varphi \in Hom(G,A)$ $\quad \pi_{G'}$ proiez. al quoz.

Viceversa sia $\bar{\varphi}: G/G' \longrightarrow A$ omo $\Rightarrow \pi_{G'} \circ \bar{\varphi} = \varphi: G \longrightarrow A$

Esempio $S_3$

1. $(S_3)' \neq id$ poichè se $(S_3)' = \{id\} \Rightarrow S_3/(S_3)' = S_3/id \cong S_3$ dovrebbe essere abeliano ma non lo è.
2. Ho 2 possibilità $(S_3)' = S_3$ oppure $(S_3)' = \langle (1\,2\,3) \rangle$ perchè gli unici sgr $\trianglelefteq$ di $S_3$ sono $S_3$ e $\langle (1,2,3) \rangle$
3. $S_3/\langle(1\,2\,3)\rangle \cong \mathbb{Z}/2\mathbb{Z}$ abeliano $\Rightarrow (S_3)' \leq \langle(1\,2\,3)\rangle \Rightarrow (S_3)' = \langle(1\,2\,3)\rangle$

$$\begin{tikzcd} S_3 \arrow[r, mapsto, "\varphi"] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \\ S_3/\langle(1\,2\,3)\rangle \arrow[ur] & \end{tikzcd}$$

$$\left.\begin{array}{l} (S_3)' \leq Ker\,\varphi = \langle (1\,2\,3) \rangle \\ (S_3)' \leq S_3 \end{array}\right] \Rightarrow (S_3)' = \langle(1\,2\,3)\rangle$$

4. In generale $(S_n)' = A_n$ e $(S_n)' \leq A_n$ $\quad S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$
5. $[(i,j),(j,k)] = (i\,k\,j)$
6. $Hom(S_n, H) = Hom(S_n/S_n', H) = Hom(S_n/A_n, H) = Hom(\mathbb{Z}_2, H)$ $\qquad \varphi: S_n \to H$

- Teorema di Poincaré

Dato $G$ finito e $H \leq G$ se $[G:H] = n \Rightarrow \exists N \trianglelefteq G$ t.c.:
- $N \leq H \leq G$
- $n \mid [G:N] \mid n!$

Se $G$ ha un sgr di indice $n$ e $n! \leq |G| \Rightarrow G$ ha sgr $\trianglelefteq$ non banali.

## Classi di coniugio in $A_n$

$\sigma \in A_n$ $\quad C_{A_n}(\sigma) :=$ classe di coniugio ottenuta coniugando $\sigma$ solo con elt. di $A_n$

$C_{S_n}(\sigma) :=$ classe di coniugio ottenuta coniugando $\sigma$ con tutti gli elt di $S_n$

$$|A_n| = |C_{A_n}(\sigma)|\,|Z_{A_n}(\sigma)| \quad \text{e} \quad Z_{A_n}(\sigma) = Z_{S_n}(\sigma) \cap A_n \implies |C_{A_n}(\sigma)| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{1}{2}\frac{|S_n|}{|Z_{S_n}(\sigma) \cap A_n|}$$

Dato che $[S_n : A_n] = 2 \implies [Z_{S_n}(\sigma) : Z_{S_n}(\sigma) \cap A_n] \in \{1,2\}$

$$\# Cl_{A_n}(\sigma) = \frac{\# A_n}{\# Z_{A_n}(\sigma)} = \frac{\# S_n/2}{\#(Z_{S_n}(\sigma) \cap A_n)} = \frac{\# S_n/2}{\# Z_{S_n}(\sigma)/2} = \# Cl_{S_n}(\sigma) \quad \text{se } Z_{S_n}(\sigma) \not\subseteq A_n$$

$$= \frac{\# S_n/2}{\# Z_{S_n}(\sigma)} = \frac{1}{2} \# Cl_{S_n}(\sigma) \quad \text{se } Z_{S_n}(\sigma) \subseteq A_n$$

# PRODOTTO SEMIDIRETTO

## Prodotto semidiretto

Dati due gruppi H e K e l'azione $\varphi: K \longrightarrow Aut(H) \leq S(H)$, $k \longmapsto \varphi_k$ $\quad H \rtimes_\varphi K$ è un gruppo

$(h,k)(h',k') = (h \cdot_H \varphi_k(h'), k \cdot_K k')$ , $(h,k)^{-1} = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$

## Osservazione

$H \rtimes_\varphi K$ è il prodotto diretto $\iff \varphi_k = id \;\; \forall k \in K$

infatti $(h,k)(h',k') = (h\varphi_k(h'), kk') = (hh', kk') \iff \varphi_k(h') = h' \iff \varphi_k = id \;\; \forall k \in K$

## Teorema

G gruppo $H, K \leq G$

$$\left.\begin{array}{l} H \trianglelefteq G \\ HK = G \\ H \cap K = \{e\} \end{array}\right\} \Rightarrow G \cong H \rtimes_\varphi K \quad \text{dove } \varphi: K \to Aut(H), \; k \mapsto \varphi_k: H \to H, \; h \to khk^{-1}$$

- $\varphi_k$ è la restrizione al sgr H di $\varphi_g: g \to kgk^{-1}$ $\varphi_g \in Inn\, G$.
  poiché $\trianglelefteq G$ $\varphi_{g|_H} = \varphi_k$ è aut (H)
- $\overline{H} = H \times \{e_K\}$ $\quad \overline{K} = \{e_H\} \times K \Rightarrow \overline{H}, \overline{K} \leq G \quad G = H \rtimes_\varphi K$
  chiusi per . $(h, e_K)(h', e_K) = (h\varphi_{e_K}(h'), e_K) = (h\, id(h'), e_K) = (hh', e_K)$
  $(e_H, k)(e_H, k') = (e_H \cdot \varphi_k(e_H), kk') = (e_H, kk')$

  $\overline{H} \trianglelefteq G$ $\quad H = Ker\, \pi$ con $\pi: H \rtimes_\varphi K \longmapsto (h,k) \longmapsto k$ $\quad \pi$ omo

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

  $\overline{H}\overline{K} = G \quad \overline{H} \cap \overline{K} = \{e\} \Rightarrow \overline{H} \times \overline{K} \cong G \cong H \rtimes_\varphi K$

  ⚠ $\overline{K}$ in generale non è $\trianglelefteq$

### $S_n \cong A_n \rtimes \langle(1,2)\rangle$

Sia $K = \langle(1,2)\rangle$

$A_n \trianglelefteq S_n$

$A_n \cdot K = S_n$ infatti $\underbrace{|A_n|}_{\frac{n!}{2}} \underbrace{|K|}_{2} = \underbrace{|S_n|}_{n!}$

$A_n \cap K = \{e\}$ $\quad K = \langle(1,2)\rangle = \{\overset{\text{dispari}}{(1,2)}, e\}$ $\qquad A_n = \{\text{permutazioni pari}\} = Ker\, sgn$

$S_n \cong A_n \rtimes_\varphi \langle(1,2)\rangle$

$\varphi: \langle(1,2)\rangle \longmapsto Aut(A_n)$

$(1,2) \longmapsto \varphi_{(1,2)}: A_n \longmapsto A_n$, $\; \rho \longmapsto (1\,2)\rho(1\,2)$

$id \longmapsto id$

### $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$

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

$ord(r) = n \Rightarrow |\langle r \rangle| = n$

$[D_n : \langle r \rangle] = 2 \Rightarrow \langle r \rangle \trianglelefteq D_n$

$\langle r \rangle \cap \langle s \rangle = \{id\}$ perchè $\det(r_j) = 1$ e $\det(s r_j) = -1 \quad \forall i = 1, \dots, n$

$|\langle s \rangle| = 2$

$$|\langle r \rangle \langle s \rangle| = \frac{|\langle r \rangle| \, |\langle s \rangle|}{|\langle r \rangle \cap \langle s \rangle|} = \frac{2n}{1} = 2n$$

$\langle r \rangle \langle s \rangle = D_n$

Quindi $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ con $\varphi : \langle s \rangle \longrightarrow Aut(\langle r \rangle)$

$s \longmapsto \varphi_s : \langle r \rangle \longrightarrow \langle r \rangle$, $r \longrightarrow srs^{-1} = r^{-1}$

deve valere che $ord\, \varphi_s \mid ord(s) = 2 \Rightarrow \varphi_s = \begin{cases} id & \rightsquigarrow \text{p. diretto} \\ r \to r^{-1} & \rightsquigarrow \text{p. semidiretto} \end{cases}$

Se in $Aut\, \mathbb{Z}/n\mathbb{Z}$ ci sono altri elt. di ordine 2 si possono definire altri p. semidiretti $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

## Gruppi di ordine pq

Cauchy.

Se $|G| = pq$ per il Teo di Cauchy $\exists\, x, y \in G$ tali che $ord(x) = q$, $ord(y) = p$ Sia $q > p$

Trovo un sgr $\trianglelefteq$

si ha che • $H = \langle x \rangle \trianglelefteq G$ perchè $[G : H] = p$ con $p$ primo più piccolo che divide $|G|$

Alternativamente posso vedere che $H$ è caratt. in $G$ poichè è unico sgr. di quell' ordine

Infatti se per assurdo $\exists\, H' < G$ con $|H'| = q$ e $H \neq H' \Rightarrow H \cap H' = \{e\} \Rightarrow |HH'| = \frac{|H|\,|H'|}{|H \cap H'|} = q^2 > pq$ perchè $q > p$.

Quindi $H' \not< G$. e quindi $H$ caratt $\Rightarrow H$ normale

applico il Teo di decomp. in prodotto semidiretto.

• Sia $K = \langle y \rangle$.

$$\left.\begin{array}{l} H \cap K = \{e\} \\ HK = G \\ H \trianglelefteq G \end{array}\right\} \Rightarrow G \cong H \rtimes_\varphi K$$

$\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$ $\quad \langle x \rangle = H \cong \mathbb{Z}/q\mathbb{Z}$ e $\langle y \rangle = K \cong \mathbb{Z}/p\mathbb{Z}$

$\varphi : \langle y \rangle \longmapsto Aut(\langle x \rangle) \cong \mathbb{Z}/(q-1)\mathbb{Z}$

$y \longmapsto \varphi_y : \langle x \rangle \cong \mathbb{Z}_q \to \mathbb{Z}_q \cong \langle x \rangle$, $x \longmapsto x^e$ con la condizione che $\left.\begin{cases} ord\, \varphi_y \mid ord\, y = p \\ ord\, \varphi_y \mid q - 1 = |Aut(\mathbb{Z}/q\mathbb{Z})| \end{cases}\right] \Rightarrow ord\, \varphi_y \mid (p, q-1)$

poichè gli aut. di un gr. ciclico mandano un elt in una sua potenza o prodotto se la not. è additiva.

Distinguo 2 casi

1) $p \nmid q-1 \Rightarrow ord\, \varphi_y \mid 1 \Rightarrow ord\, \varphi_y = 1 \Rightarrow \varphi_y = id \Rightarrow$ ho p. diretto $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$

2) $p \mid q-1 \Rightarrow ord\, \varphi_y = 1 \;\vee\; ord\, \varphi_y = p$

$\varphi_y = \{id\}$

ho $p-1$ elt. di ordine $p$ in $\mathbb{Z}/q-1\mathbb{Z}$ ho $p-1$ scelte per $\varphi_y$ che danno un $\rtimes$ (tutti $\cong$)

analizzo meglio caso 2

in particolare considero un omo $\mathbb{Z}_p \longrightarrow Aut(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$

$\bar{1} \longmapsto$ elt di ordine che divide $p$ cioè 1 o $p$.

- se ha ordine 1 siamo nuovamente nel caso banale, e dunque del prodotto diretto, già trattato.

- se ha ordine $p$ abbiamo la possibilità di scegliere l'immagine come $1\left[\frac{q-1}{p}\right]_{q-1}, 2\left[\frac{q-1}{p}\right]_{q-1}, \dots, (p-1)\left[\frac{q-1}{p}\right]_{q-1}$
  che sono tutti gli elt. di ordine $p$ in $\mathbb{Z}_{q-1}$
  In definitiva abbiamo $p-1$ omo non banali che chiameremo $\phi_1, -, \phi_{p-1}$
  Mostriamo che questi semidiretti sono $\cong$
  vogliamo mostrare che tutti questi omo non banali inducono la stessa struttura sul prodotto semidiretto
  Consideriamo $\phi_1$ e $\phi_J$ con $J \neq 1$
  Usiamo il criterio per capire se due o più semidiretti sono $\cong$

  $\alpha = id \in Aut(\mathbb{Z}_q)$ e $\forall J = 1, -, p-1$ $\beta_J \in Aut(\mathbb{Z}_p)$ tale che $\beta_J([1]_p) \overset{*}{=} [J]_p$
  visto che $\alpha$ è l'id devo verificare che $\phi_J([1]_p)$ e $\phi_1(\beta_J[1]_p)$ coincidono
  infatti $\phi_J([1]_p) = J\left[\frac{q-1}{p}\right]_{q-1} = \phi_1(\underbrace{[J]_q}) \overset{*}{=} \phi_1(\underbrace{\beta_J[1]_q})$

  ↓ basta verif. sui generatori

  $\exists$ dunque a meno di iso al più due gr. di ordine $pq$.

Mostriamo che i due gruppi così ottenuti sono tra loro distinti

$G_1 = \mathbb{Z}_q \times \mathbb{Z}_p$ e $G_2 = \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ con $\varphi = \phi_i$ $\forall i = 1, -, p-1$

$G_1 \neq G_2$ $G_1$ è abeliano mentre $G_2$ non lo è

Sia $a \in \mathbb{Z}_q$ e $b \in \mathbb{Z}_p$

$$(a,b)(0,b) = (a + \varphi_b(0), b+b) = (a + \varphi_b(0), 2b) = (a+0, 2b) = (a, 2b)$$

ricorda! $\varphi_K(e_H) = e_H$

$$(0,b)(a,b) = (0 + \varphi_b(a), b+b) = (\varphi_b(a), 2b)$$

↳ $\varphi$ è non banale $\Rightarrow \exists\, b \in \mathbb{Z}_p$ t.c. $\varphi_b \neq id$ e $\exists\, a \in \mathbb{Z}_q$ t.c. $\varphi_b(a) \neq a$ scelti questi $a$ e $b$ possiamo concludere che $(a,b)(0,b) \neq (0,b)(a,b)$ e che quindi $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ non è ab.

Criterio per capire se due prodotti semidiretti sono $\cong$

Hp $\begin{cases} \text{Dati due gruppi } H \text{ e } K \text{ e due omomorfismi } \varphi \text{ e } \psi : K \to Aut(H) \\ \text{Se } \left.\begin{array}{l} \alpha \in Aut(H) \\ \beta \in Aut(K) \end{array}\right\} \text{ t.c. } \quad \alpha \circ \psi(k) \circ \alpha^{-1} = \varphi(\beta(k)) * \ \forall k \in K \end{cases}$

$\alpha \in Aut(H) \iff \alpha : H \to H$
$\beta \in Aut(K) \iff \beta : K \to K$

Allora $H \rtimes_\varphi K \cong H \rtimes_\psi K$

dim.

$\phi : H \rtimes_\varphi K \xrightarrow{\cong} H \rtimes_\psi K$

$(h, k) \longrightarrow (\alpha(h), \beta(k))$

$\boxed{\phi \text{ è iso}}$

1) $\phi$ è omo

$\beta$ è aut.

$\phi((h,k)(h',k')) = \phi(h \, \psi_k(h'), kk') = (\alpha(h\psi_k(h')), \beta(kk')) = (\alpha(h)\alpha(\psi_k)(h'), \beta(k)\beta(k'))$

$= (\alpha(h)(\varphi(\beta_k)\alpha)(h'), \beta(k)\beta(k')) \overset{?}{=} (\overbrace{\alpha(h), \beta(k)}^{A})(\overbrace{\alpha(h'), \beta(k')}^{B}) = \phi(h,k)\,\phi(h',k')$

facccio il prodotto tra A e B

$(\alpha(h)\varphi_{\beta_k}(\alpha(h')), \beta(k)\beta(k')) =$

$\alpha\psi_k\alpha^{-1} = \varphi(\beta_k)$
molt. per $\alpha$ a sx
$\alpha\psi_k\alpha^{-1}\alpha = \varphi(\beta_k)\alpha \implies \alpha\psi_k = \varphi(\beta_k)\alpha$

2) Iniettività:

$\phi(h,k) = (e_H, e_K) \iff (\alpha(h), \beta(k)) = (e_H, e_K) \iff (h,k) = (e_H, e_K)$

$\alpha, \beta$ sono aut $\Rightarrow$ inj

3) Surgettività segue dal fatto che $\alpha$ e $\beta$ sono automorf $\Rightarrow$ sono anche surj

# TEOREMA DI STRUTTURA

## Enunciato Teorema di Struttura

$G$ gruppo abeliano finito $|G| = n = p_1^{e_1} \cdots p_l^{e_l}$ $p_i$ primi distinti $\Rightarrow$ $\underbrace{G \cong \mathbb{Z}/_{n_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{n_s\mathbb{Z}}}_{}$ $G$ è $\cong$ al p. diretto di gruppi ciclici

questa struttura è unica con la condizione $n_{i+1} \mid n_i \quad \forall i = 1, \dots, s-1$

a) $G(p) = \{ g \in G \mid \operatorname{ord} g = p^k \quad k \in \mathbb{N} \}$ $p$-Sylow o componente di $p$-torsione di $G$.

- $G(p) < G$ perché $G$ è ab. $\Rightarrow \operatorname{ord}(xy) \mid [\operatorname{ord}(x), \operatorname{ord}(y)]$
- $G(p)$ è caratteristico perché gli aut cons. l'ordine ($G(p)$ è mandato in $G(p)$)

b) Teorema 1 I gr. ab. sono prodotto delle loro componenti di $p$-torsione

$G$ abeliano $|G| = p_1^{e_1} \cdots p_s^{e_s}$ con $p_i \neq p_j \quad \forall i \neq j \Rightarrow G \cong G(p_1) \times \dots \times G(p_s)$

Tale deco. è unica

c) Teorema 2 I $p$-gruppi si spezzano come prodotto di $p$-gruppi ciclici

$|G| = p^n$, $G$ abeliano $\Rightarrow \exists!\ r_1 \geq r_2 \geq \dots \geq r_t$ t.c. $G \cong \mathbb{Z}/_{p^{r_1}} \times \dots \times \mathbb{Z}/_{p^{r_t}\mathbb{Z}}$

L'ordine degli esp. garantisce l'unicità della fatt.

T1 + T2 $\Rightarrow$ Teo di Struttura

- $\exists$

$$G \underset{T1}{\cong} G(p_1) \times \dots \times G(p_s) \underset{T2}{\cong} \underbrace{\mathbb{Z}/_{p_1^{r_{11}}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p_1^{r_{1t_1}}\mathbb{Z}}}_{G(p_1)} \times \dots \times \underbrace{\mathbb{Z}/_{p_s^{r_{s1}}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p_s^{r_{st_s}}\mathbb{Z}}}_{G(p_s)} \underset{TCR}{\cong}$$

ad ogni $G(p_i)$

con $r_{i1} \geq \dots \geq r_{it_1}$ (gli esp sono in ord decr.)

$$\underset{TCR}{\cong} \mathbb{Z}/_{n_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{n_t\mathbb{Z}}$$

dove $m_1 = p_1^{r_{11}} \cdots p_s^{r_{s1}}$ $\quad n_j = p_1^{r_{1j}} \cdots p_s^{r_{sj}}$

$m_t = p_1^{r_{1t}} \cdots p_s^{r_{st}}$

dove $t = \max\{t_1, \dots, t_s\}$ e $r_{i_k} = 0$ se $k > t_i$

$n_t \mid n_{t-1} \mid \dots \mid n_i$

- Unicità

Se $G$ avesse 2 decomposizioni $\neq$ con ordini che si dividono in catena potrei spezzarlo con il TCR e troverei almeno due $p$-gruppi ciclici $\neq$ tra le 2 decomposizioni

$\lightning$ per unicità Teo 2.

Per dim Teorema 2 mi serve un Lemma

- Lemma

Sia $G$ un $p$-gruppo abeliano e sia $x_1$ un elt. di ordine max in $G$

preso $\bar{x} \in G/_{\langle x_1 \rangle}$ $\exists\, y \in \pi^{-1}(\bar{x})$ t.c. $\operatorname{ord}_G(y) = \operatorname{ord}_{G/\langle x_1 \rangle}(\bar{x})$

ovvero preso un elt nel quoziente $\exists$ sempre un elt nella sua fibra con lo stesso ordine.

c'è controes.

es

$|G| = 2000 = 2^4 \cdot 5^3$

$G \cong G_{(2)} \times G_{(5)}$ con $|G_{(2)}| = 2^4$ $|G_{(5)}| = 5^3$

$G_{(2)} =$
- $\mathbb{Z}/_{2^4\mathbb{Z}} = \mathbb{Z}/_{16\mathbb{Z}}$
- $\mathbb{Z}/_{2^3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} = \mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$
- $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}$
- $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$
- $(\mathbb{Z}/_{2\mathbb{Z}})^4 = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$

$G_{(5)} =$
- $\mathbb{Z}/_{5^3\mathbb{Z}} = \mathbb{Z}/_{125\mathbb{Z}}$
- $\mathbb{Z}/_{5^2\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}$
- $(\mathbb{Z}/_{5\mathbb{Z}})^3 = \mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}$.

P- Sylow $\longrightarrow$ scrittura

$(\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}) \times (\mathbb{Z}_{7^2} \times \mathbb{Z}_{7^3}) \times (\mathbb{Z}_{11^4} \times \mathbb{Z}_{11^6})$

1) Prendo da ogni p- Sylow i più grandi.

$\boxed{\mathbb{Z}_{2^2 \cdot 7^3 \cdot 11^6}}$

2) Poi i secondi

$\boxed{\mathbb{Z}_{2^2 \cdot 7^2 \cdot 11^4}}$

3) Poi la parte più piccola

$\boxed{\mathbb{Z}_2}$

$\mathbb{Z}_2 \times \mathbb{Z}_{2^2 \cdot 7^2 \cdot 11^4} \times \mathbb{Z}_{2^2 \cdot 7^3 \cdot 11^6}$

# TEOREMI DI SYLOW

Dato un gr. G finito cosa posso dire dell'$\exists$ di elt. e sgr di un certo ordine?

- $H \leq G \Rightarrow |H| \mid |G|$ Teo Lagrange
- $\forall p$ primo t.c. $p \mid |G|$, $\exists x \in G$ t.c. $ord_G(x) = p$ Teo Cauchy
- Se $G$ è ciclico $\forall d \mid |G|$, $\exists x \in G$ t.c. $ord_G(x) = d$ (deriva dalla def di G ciclico)
  $G$ ciclico $\Leftrightarrow$ $d = |G|$ ($\exists x \in G$ t.c. $ord_G(x) = d$)
- Se $G$ è $\boxed{\text{abeliano}}$ $\forall d \mid |G|$, $\exists H \leq G$ t.c. $|H| = d$ (deriva dal Teo struttura)

Lemma

Se $G$ è un p-gruppo e $H \lneq G \Rightarrow H \lneq N_G(H)$

Def

$G$ gruppo finito e $p$ primo t.c. $|G| = p^n \cdot m$ con $\underbrace{p^n \| |G|}_{p^n \text{ è la max potenza di p che divide } \# G}$ e $n \geq 1$, $(m,p) = 1 \Rightarrow$ Un sgr di G di ordine $p^n$ (potenza di p max) prende il nome di P-Sylow.

**Teorema 1.98** (Teorema Di Sylow)
Sia $G$ un gruppo finito, con $|G| = p^n m$, con $p$ primo, $n \geq 1$ e $(m,p) = 1$ [a], allora:

(1) $\forall \alpha : 0 \leq \alpha \leq n$, $\exists H \leqslant G : |H| = p^\alpha$. (Esistenza)

(2) $\forall \alpha : 0 \leq \alpha \leq n-1$, ogni sottogruppo di ordine $p^\alpha$ è contenuto in un sottogruppo di ordine $p^{\alpha+1}$. In particolare, ogni $p$-sottogruppo è contenuto in un $p$-sottogruppo di Sylow. (Inclusione)

(3) Due qualunque $p$-sottogruppi di Sylow di $G$ sono coniugati (quindi tutti i $p$-sottogruppi di ordine massimale sono isomorfi). (Coniugio) (c'è un'unica orbita)

(4) Sia $n_p$ il numero di $p$-sottogruppi di Sylow di $G$, allora: (Numero)

$$n_p \mid |G| \qquad \text{e} \qquad n_p \equiv 1 \pmod p \qquad \text{e} \qquad n_p = [G : N_G(S)]^b$$

[a] Ovvero $p^n \| |G|$, o anche $\nu_p(|G|) = n$ (dove con $\nu_p$ intendiamo la valutazione $p$-adica).
[b] Con $S$ ci si riferisce a un qualsiasi $p$-Sylow, per un $p$ fissato.

$Q_8$

$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = j^3 i \rangle$

$ord(i) = 4 = ord(j)$

$\langle i \rangle, \langle j \rangle$ ciclici di ordine 4

$\langle i \rangle \cap \langle j \rangle = \{1, i^2 = j^2\}$

$Q_8 = \{1, \underbrace{i, j}_{ord\ 4}, \underbrace{i^2 = j^2}_{ord\ 2}, \underbrace{i^3, j^3, ij, i^3 j}_{ord\ 4}\}$

$|Q_8| = 8$

$Q_8$ non è ab.

Tutti i sgr di $Q_8$ sono ab.

$H \lhd G$ $|H| = 2$ è normale $\Leftrightarrow$ $H \lhd Z(G)$

$|Z(Q_8)| = 2$ e $Z(Q_8) = \langle i^2 \rangle$

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ $ij = k$, $j \cdot i = -k$

$i^2 = -1$ $i^3 = -i$ $j^3 = -j$, $i^3 j = -k$

$Q_8 \ncong D_4$ perchè $Q_8$ ha 6 elt di ord. 4
$D_4$ ne ha solo 2

$Q_8$ non è un semi diretto $\forall H_1, H_2 < Q_8$ $H_1 \cap H_2 = \{1,-1\} \neq \{1\}$.

Classif. dei gr. di ordine 8

**Esempio 1.112** (Classificazione dei gruppi di ordine 8)
Distinguiamo innanzitutto i gruppi in base all'abelianità:

- Se $G$ è abeliano, allora per il Teorema di Struttura abbiamo che $G \cong G(2)$ e per la 2-componente abbiamo le seguenti possibilità:
$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
- Se $G$ non è abeliano, allora ha almeno un elemento di ordine 4 (se avesse tutti elementi di ordine 2 sarebbe isomorfo a $(\mathbb{Z}/2\mathbb{Z})^3$), sia $a \in G$ tale che $\text{ord}(a) = 4$, allora $\langle a \rangle \triangleleft G$ e:
$$G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\} \qquad b \in G \setminus \langle a \rangle$$
dove deve essere $b^2\langle a \rangle = \langle a \rangle$, infatti se fosse $b^2\langle a \rangle = b\langle a \rangle \implies b\langle a \rangle = \langle a \rangle \implies b \in \langle a \rangle$, che è assurdo, dunque:
$$b^2\langle a \rangle = \langle a \rangle \implies b^2 \in \{e, a, a^2, a^3\}$$
ma non può essere che $b^2 = a, a^3$, altrimenti $b$ avrebbe ordine 8, dunque rimangono soltanto i casi $b^2 = 1$ e $b^2 = a^2$.
  (1) Se $a^4 = 1$ e $b^2 = 1$, allora $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$ da cui (si verificano facilmente le ipotesi del Teorema 1.78) segue:
  $$G \cong \langle a \rangle \rtimes_\varphi \langle b \rangle \cong D_4$$
  dove $\varphi : \langle b \rangle \longmapsto \text{Aut}(\langle a \rangle) \cong \mathbb{Z}/2\mathbb{Z} : b \longmapsto \varphi_b$ e $\varphi_b : \langle a \rangle \longmapsto \langle a \rangle : a \longmapsto a^{-1}$ (ovvero $\varphi_b = -id$, se avessimo scelto l'identità avremmo ottenuto uno dei prodotti diretti già visti sopra).
  (2) Se $a^4 = 1$ e $b^2 = a^2$, osserviamo che $bab^{-1} \in \langle a \rangle$ (essendo il generato da $a$ normale in $G$), inoltre non può essere che $bab^{-1} = 1$ (altrimenti $a = 1$) o $bab^{-1} = a^2$ (poiché il coniugio conserva l'ordine degli elementi) e non può nemmeno essere che $bab^{-1} = a$ (poiché abbiamo supposto che $G$ non sia commutativo). Pertanto abbiamo necessariamente $bab^{-1} = a^3 \iff ba = a^3b$, da cui segue:
  $$G \cong Q_8$$
  dove l'isomorfismo manda $a \longmapsto i$ e $b \longmapsto j$.

$\langle g \rangle$

Dunque i gruppi di ordine 8 sono:
$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad D_4 \qquad Q_8$$