Algebra I

Andrea Gallese 25 ottobre 2017

Indice

G Teoria dei Gruppi

G.1 Automorfismi e Azioni

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

Esempi.

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

Definizione G.2 (Gruppo degli automorfismi interni)**.** Sia $\mathrm{Int}(G) = \{\varphi_g \mid g \in G\}$ 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 $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.

Teorema G.3.

$$\mathrm{Int}(G) \cong {}^{G}\!/\!_{Z(G)}$$

Dimostrazione. La funzione

$$\begin{aligned} \Phi\colon G &\to \mathrm{Int}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

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

Osservazione.

$$H \lhd G \iff \varphi_g(H) = H \quad \forall \varphi_g \in \mathrm{Int}(G)$$

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

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

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

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

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

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

$$\begin{aligned} \varphi\colon C &\to \mathcal{S}\left(\mathbb{R}^2\right) \\ z &\mapsto \mathcal{R}(O, \arg z) \end{aligned}$$

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:

$$\mathcal{O}rb(x) = \{g \cdot x \mid \forall g \in G\}$$

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

$$X = \bigcup_{x \in R} \mathcal{O}rb(x) \ \Rightarrow\ |X| = \sum_{x \in R} |\mathcal{O}rb(x)|$$

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:

$$\mathcal{S}tab(x) = \{g \in G \mid g \cdot x = x\}$$

Osservazione. è immediato osservare che $\mathcal{S}tab(x) < G$, ma non necessariamente normale.

Teorema G.8.

$$|G| = |\mathcal{O}rb(x)|\,|\mathcal{S}tab(x)|$$

Dimostrazione. La funzione f così definita

$$\begin{aligned} f\colon \{g\mathcal{S}tab(x) \mid g \in G\} &\to \{\mathcal{O}rb(x) \mid x \in X\} \\ g\mathcal{S}tab(x) &\mapsto g \cdot x \end{aligned}$$

è biunivoca, infatti:

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

♣

Osservazione. Dall'osservazione precedente

$$|X| = \sum_{x \in R} \frac{|G|}{|\mathcal{S}tab(x)|}$$

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. $H \lhd G \iff N(H) = G$

G.2 Formula delle Classi e Cauchy

Teorema G.9 (Formula delle Classi)**.** *Per ogni gruppo finito vale*
$$|G| = |Z(G)| + \sum_{x\in R'} \frac{|G|}{|Z_G(x)|}$$

Dimostrazione. Riprendiamo la partizione di X in orbite, ma separando quelle banali da quelle non
$$|X| = \sum_{\substack{x\in R\\ \mathcal{O}rb(x)=\{x\}}} 1 + \sum_{\substack{x\in R\\ \mathcal{O}rb(x)\neq\{x\}}} \frac{|G|}{|Stab\,(x)\,|}$$
Osserviamo cosa succede nel caso dell'azione di coniugo da un gruppo in se (l'esempio 3 della lezione precedente). L'orbita di x è banale se e solo se $gxg^{-1} = x$, $\forall g \in G$, 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
$$\left| {}^{G}\!/_{Z(G)} \right| = p$$
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 $|G| = pn$, 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 $kp \quad \forall k < m$ abbiamo 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 abbiamo ordine multiplo di p, dunque il centro deve coincidere con l'intero gruppo, che risulta pertanto commutativo.

♣

Dimostrazione Magica. Sia
$$X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_n = 1\}$$
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 Abeliani?
   (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 Abeliani?
   (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, $\operatorname{ord}(xy) = 6$, 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 $\mathcal{S}(G)$.*

Dimostrazione. Esibiamo un'azione fedele (ovvero, iniettiva):
$$\begin{aligned}\Phi\colon G &\to \mathcal{S}(G)\\ g &\mapsto \varphi_g(x) = gx\end{aligned}$$
è ora sufficiente verificare che Φ è ben definito (φ_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)**.**
$$\langle S\rangle = \{s_1 \cdots s_k \mid k \in \mathbb{N},\ s_i \in S \cup S^{-1}\}$$

Dimostrazione. 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 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 Commuatatori o Gruppo Derviato 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 $G' < H$.**

Dimostrazione. 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*

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

Dimostrazione. Tutti gli elementi sopra definiti possiamo ridurli a un elemento della forma ρ^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:

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

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

Osservazione. Conosciamo già un gruppo diedrale: $D_3 \cong \mathcal{S}_3$.

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

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

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 $m \mid n$.*

Dimostrazione. 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 $d \mid n$.*

Dimostrazione. 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

$$\begin{tikzcd} D_n \arrow[r, "\Phi"] \arrow[dr, "f"'] & \mathbf{O}_2(\mathbb{R}) \arrow[d, "det"] \\ & \{\pm 1\} \cong \mathbb{Z}_2 \end{tikzcd}$$

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

$$\begin{tikzcd} H \arrow[r, "f_{|H}"] \arrow[d, "id"'] & f(H) \arrow[d, "id"] \\ D_n \arrow[r, "f"] & \mathbb{Z}_2 \end{tikzcd}$$

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

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

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

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

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

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. ($\star$) Chi è $\mathrm{Aut}(D_n)$?

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

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

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

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

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

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 σ 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 del 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.*

Dimostrazione. Consideriamo

$$\begin{aligned} \operatorname{sgn} \colon \mathcal{S}_n &\to \mathbb{Z}^\times = \{\pm 1\} \\ \sigma &\mapsto \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

questo è un omomorfismo di gruppi. Infatti:

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

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

Per concludere, osserviamo che tutte le trasposizioni hanno segno negativo. ♣

Definizione G.25 (Gruppo Alterno)**.** Chiamiamo $\mathcal{A}_n$ o *gruppo alterno* il sottogruppo delle permutazioni pari

$$\ker(\operatorname{sgn}) = \mathcal{A}_n \lhd \mathcal{S}_n$$

Osservazione. Ogni sottogruppo $H < \mathcal{S}_n$ è contenuto interamente in $\mathcal{A}_n$ o viene spezzato a metà dal gruppo alterno. Questo perché possiamo restringere l'omomorfismo det al solo H, dunque l'immagine può solo restringersi.

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.*

Dimostrazione. $\Rightarrow$. Ci basta dimostrare che dato un ciclo $\sigma = (a_1 \ \cdots \ a_k)$ 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 σ, rimangono fisse

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

pertanto

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

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

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

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

Esercizio. Data una permutazione σ trovare $N(\langle\sigma\rangle)$.
Osserviamo che

$$N(\langle\sigma\rangle) = \{\tau \mid \tau\sigma\tau^{-1} = \sigma^k\}$$

dunque il normalizzatore contiene il centralizzatore di σ e, visto che il coniugio preserva la scomposizione in cicli, che possiamo prendere solo i k coprimi coll'ordine di σ. Inoltre prese due permutazioni $\tau_1, \tau_2 \in N(\langle\sigma\rangle)$ che generano lo stesso σ^k, abbiamo che

$$\tau_1\sigma\tau_1^{-1} = \tau_2\sigma\tau_2^{-1} \quad \Leftrightarrow \quad (\tau_2^{-1}\tau_1)\sigma(\tau_2^{-1}\tau_1)^{-1} = \sigma$$

Dunque $\tau_2^{-1}\tau_1 \in Z(\sigma)$, ovvero $\tau_1 \in \tau_2 Z(\sigma)$. Pertanto il normalizzatore dev'essere composto da tutti i laterali del centralizzatore indotti da permutazioni che mi danno σ^k dello stesso tipo di σ. Ovvero

$$N(\langle\sigma\rangle) = \bigcup_{(i, ord(\sigma))=1} \tau_i Z(\sigma)$$

e pertanto

$$|N(\langle\sigma\rangle)| = |Z(\sigma)| \cdot \phi(\operatorname{ord}(\sigma))$$

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

Teorema G.28. *Sia G un gruppo e $H, K \lhd G$ due sottogruppi normali. Se*

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

allora $G \cong H \times K$.

Dimostrazione. 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

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

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. $\mathrm{Int}\,(G) \cong \mathrm{Int}\,(H) \times \mathrm{Int}\,(K)$.
3. $\mathrm{Aut}\,(H) \times \mathrm{Aut}\,(K) < \mathrm{Aut}\,(G)$.

Teorema G.29. *Si ha $\mathrm{Aut}\,(H) \times \mathrm{Aut}\,(K) < \mathrm{Aut}\,(H \times K)$ e sono isomorfi se e solo se H e K sono caratteristici.*

Dimostrazione. Consideriamo l'omomorfismo

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

e verifichiamo che

- è bene definito, ovvero φ è un automorfismo. Immediata conseguenza del fatto che f e g sono a loro volta automorfismi.
- è un omomorfismo.
$$\begin{aligned} \Phi(ff', gg') &= \big(f(f'(h)), g(g'(k))\big) \\ &= \varphi_{fg}(\varphi_{f'g'}(h, k)) \\ &= \Phi(f, g)\Phi(f', g') \end{aligned}$$
- 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 Φ è suriettivo, allora tutti gli automorfismi di $H \times K$ sono della forma di cui sopra e pertanto φ_{fg} agisce sugli elementi di H come $\varphi_{fg|H} = f \in \mathrm{Aut}\,(H)$.

  $\Leftarrow$. Viceversa, supponiamo H e K caratteristici, preso un automorfismo $\varphi \in \mathrm{Aut}\,(H \times K)$ consideriamo le sue restrizioni ai due sottogruppi caratteristici.
$$f = \Pi_H\left(\varphi_{|H \times \{e_K\}}\right) \qquad g = \Pi_K\left(\varphi_{|\{e_H\} \times K}\right)$$
  Notiamo che $f \in \mathrm{Aut}\,(H)$.
  - f è iniettiva. Se $f(h) = f(h')$ allora
$$\Pi_H\left(\varphi(h, e_K)\right) = \Pi_H\left(\varphi(h', e_K)\right)$$
    poiché $H \times \{e_K\}$ è caratteristico
$$\varphi(h, e_K) = (a, e_K) \qquad \varphi(h', e_K) = (b, e_K)$$
    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 φ 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
$$f(h') = \Pi_H\left(\varphi(h', e_K)\right) = \Pi_H\left(h, e_K\right) = h$$

  Infine osserviamo che $\Phi(f, g) = \varphi$. Infatti
$$\begin{aligned} \varphi_{fg}(h, k) &= (f(h), g(k)) \\ &= \left(\Pi_H\left(\varphi(h, e_K)\right), \Pi_K\left(\varphi(e_H, k)\right)\right) \\ &= \left(\Pi_H\left(\varphi(h, k)\right), \Pi_K\left(\varphi(h, k)\right)\right) \\ &= \varphi(h, k) \end{aligned}$$
  dove la terza uguaglianza segue da
$$\begin{aligned} \Pi_H\left(\varphi(h, e_K)\right) &= \Pi_H\left(\varphi(h, e_K)\right)\Pi_H(\varphi(e_H, k)) \\ &= \Pi_H\left(\varphi(h, e_K)\varphi(e_H, k)\right) \\ &= \Pi_H\left(\varphi(h, k)\right) \end{aligned}$$

♣

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

G.6 Classificazione dei Gruppi di ordine 8

$$\begin{tikzcd}
\boxed{\exists g \mid \operatorname{ord}(g) = 8} \arrow[r, "\text{sì}"] \arrow[d, "no"'] & \mathbb{Z}_8 \\
\boxed{g^2 = e \ \ \forall g} \arrow[r, "\text{sì}"] \arrow[d, "no"'] & (\mathbb{Z}_2)^3 \\
\boxed{\varphi_h \mid h \notin C_4} \arrow[r, "\text{id}"] \arrow[d, "\text{-id}"] & \mathbb{Z}_2 \times \mathbb{Z}_4 \\
\boxed{\operatorname{ord}(h) = 2} \arrow[r, "\text{sì}"] \arrow[d, "no"'] & D_4 \\
Q_8 &
\end{tikzcd}$$

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

Dimostrazione. 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.28. 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

$$\begin{aligned} \varphi_g \colon C_4 &\to C_4 \\ x &\mapsto hxh^{-1} \end{aligned}$$

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

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

- $[\varphi_g = id, \operatorname{ord}(h) = 2]$. 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
$$G \cong \langle h\rangle \times C_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$
- $[\varphi_g = id, \operatorname{ord}(h) = 4]$. Possiamo considerare h^2 e ricondurci al caso precedente.
- $\left[\varphi_g = id^{-1}, \operatorname{ord}(h) = 2\right]$. Abbiamo che $hgh = g^{-1}$, quindi per la nostra caratterizzazione dei gruppi diedrali
$$G \cong D_4$$
- $\left[\varphi_g = id^{-1}, \operatorname{ord}(h) = 4\right]$. Anche $\operatorname{ord}(gh) = 4$. 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.31 (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.32. *Siano G un gruppo finito e H un sottogruppo che ha come indice il più piccolo primo p che divide G, allora $H \lhd G$.*

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

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

Osserviamo che

$$\begin{aligned} g \in \mathcal{S}tab\,(xH) &\Leftrightarrow gxH = xH \\ &\Leftrightarrow x^{-1}gx \in H \\ &\Leftrightarrow g \in xHx^{-1} \end{aligned}$$

dunque $\mathcal{S}tab\,(xH) = xHx^{-1}$ 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

$$\Phi' : {}^{G}\!\big/_{\ker \Phi} \to \mathcal{S}_p$$

è iniettivo e pertanto

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

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

$$\begin{aligned} \psi_n\colon G &\to G \\ x &\mapsto x^n \end{aligned}$$

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

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

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

Esercizi.

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

G.8 Prodotto Semidiretto

Definizione G.33 (Prodotto semidiretto)**.** Siano H, K due gruppi e $\varphi : K \to \mathrm{Aut}(H)$ 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 φ manda tutti gli elementi di K nell'identità su H.

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

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

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

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

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

Teorema G.34 (Teorema di decomposizione in prodotto semidiretto)**.** *Siano G un gruppo e $H, K < G$ sottogruppi, con $H \lhd G$ normale. Se*

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

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

$$\begin{aligned} \varphi\colon K &\to \mathrm{Aut}(H) \\ k &\mapsto \varphi_k : h \mapsto hkh^{-1} \end{aligned}$$

Dimostrazione. Consideriamo

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

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 Φ è un isomorfismo come desiderato. ♣

Esempi.

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

Classificazione dei gruppi di ordine pq.

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

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

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

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

per il teorema G.32. Inoltre osserviamo che $HK = G$ e i due sottogruppi hanno intersezione banale. Quindi

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

dove

$$\begin{aligned} \varphi_1\colon K &\to \mathrm{Aut}(H) \cong \mathbb{Z}_q^\times \\ y &\mapsto \varphi_y : x \mapsto yxy^{-1} = x^a \end{aligned}$$

e necessariamente dobbiamo avere che

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

ma, poiché φ è un omomorfismo, abbiamo che

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

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

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

Nel secondo caso dobbiamo avere

$$p = \mathrm{ord}(\varphi_y) \mid q - 1 = |\mathrm{Aut}(\mathbb{Z}_q)|$$

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

$$\boxed{G \cong H \rtimes K}$$

Osserviamo innanzitutto l'azione è completamente determinata dal valore che assume quando viene valutata su due fissati generatori dei due sottogruppi ciclici, x e y. E sarà del tipo

$$\varphi : y \mapsto \varphi_y : x \mapsto yxy^{-1} = x^a$$

per un certo $a \in \mathbb{Z}_q^\times$ di ordine p. Preso una diversa azione ψ avremo una valutazione x^b diversa nei generatori. Abbiamo però che esiste $m \in \mathbb{Z}$ tale che $b^m = a$, perché sono entrambi generatori del sottogruppo di ordine p di $\mathbb{Z}_q^\times$. (Questa cosa non è chiarissima, perché siamo abituati a vedere questi gruppi in notazione additiva. E' un utile esercizio provare a riscriverli in questo modo e usare impunemente il fatto che $\mathbb{Z}_r^\times \cong \mathbb{Z}_{r-1}$ per ogni r primo). Abbiamo allora

$$\psi_{y^m}(x) = x^{b^m} = x^a = \varphi_y(x)$$

e possiamo dunque costruire la funzione

$$\begin{aligned} \Phi\colon H \rtimes_\psi K &\to H \rtimes_\varphi K \\ (h, k) &\mapsto (h, k^m) \end{aligned}$$

e verificare che è un'isomorfismo:

- ► è un omomorfismo

$$\begin{aligned} \Phi(h, k)\Phi(h', k') &= (h, k^m)(h', k'^m) \\ &= (h\psi_{k^m}(h'), (kk')^m) \\ &= (h\varphi_k(h'), (kk')^m) \\ &= \Phi(h\varphi_k(h'), kk') \end{aligned}$$

- ► è iniettivo: se $\Phi(h, k) = (e, e)$, allora $h = e$ e, poiché k^m è un automorfismo di $\mathbb{Z}_p$, $k = e$.

G.9 Teorema di Sylow

Definizione G.35. Chiamiamo p-sylow ogni p-sottogruppo di ordine massimo. Ovvero $H < G$, dove $|G| = p^m n$ con $(m, n) = 1$ e $|H| = p^m$.

Teorema G.36. *Sia G un gruppo finito di ordine $|G| = p^n m$, dove p è primo e m è un intero a lui coprimo: $(p, m) = 1$. Allora sappiamo che:*

- $\exists$. *Per ogni $0 \leq \alpha \leq n$, esiste un sottogruppo $H < G$ di ordine $|H| = p^\alpha$.*
- $\subseteq$. *Ogni p-sottogruppo è incluso in un p-sylow.*
- φ_g. *Due qualsiasi p-sylow sono coniugati.*
- n_p. *Il numero n_p di p-sylow è congruo a $1 \mod p$.*

Dimostrazione. bla

- $\exists$. Fissiamo $0 \leq \alpha \leq n$. Sia $\mathcal{M}_\alpha$ l'insieme di tutti i sottoinsiemi di G di cardinalità p^α

$$\mathcal{M}_\alpha = \{M < G \mid |M| = p^\alpha\}$$

possiamo allora calcolarci

$$|\mathcal{M}_\alpha| = \binom{p^n m}{p^\alpha} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - 1}$$

e poiché $v_p(p^n m - i) = v_p(i) = v_p(p^\alpha - i)$, allora

$$v_p\left(\prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - 1}\right) = 0$$

e possiamo concludere che

$$p^{n-\alpha} \mid\mid \mathcal{M}_\alpha$$

Consideriamo ora l'azione di G su $\mathcal{M}_\alpha$ data dalla moltiplicazione a sinistra

$$\Phi \colon G \to \mathcal{S}(\mathcal{M}_\alpha)$$
$$g \mapsto \psi_g : M \mapsto gM$$

Vogliamo ora mostrare che esiste uno stabilizzatore della cardinalità giusta. Per la solita decomposizione in orbite abbiamo

$$|\mathcal{M}_\alpha| = \sum \frac{|G|}{|\mathcal{S}tab\,(M_i)\,|}$$

Per le osservazione sulla cardinalità, deve esistere un'orbita di cardinalità non divisibile per $p^{n-\alpha+1}$

$$\exists M_i \text{ tale che } p^{n-\alpha+1} \nmid |\mathcal{O}rb\,(M_i)\,|$$

Il corrispondente stabilizzatore avrà pertanto cardinalità divisibile almeno per p^α. Ma se fissiamo un elemento $x \in M_i$ e consideriamo la funzione iniettiva

$$f \colon \mathcal{S}tab\,(M_i) \to M_i$$
$$y \mapsto xy$$

ci rendiamo conto che lo stabilizzatore non avrà una cardinalità maggiore dell'insieme che stabilizza

$$p \mid |\mathcal{S}tab\,(M_i)\,| \leq |M_i| = p^\alpha$$

ed è dunque il sottogruppo che cercavamo.

- $\subseteq$. Sia $H < G$ un p-sottogruppo $|H| = p^\alpha$ e S un p-sylow. Consideriamo l'azione di H sull'insieme X delle classi laterali di S per moltiplicazione a sinistra

$$F \colon H \to \mathcal{S}(X)$$
$$h \mapsto \psi_h : gS \mapsto hgS$$

Per la decomposizione in orbite

$$m = [G : S] = |X| = \sum \frac{|H|}{|\mathcal{S}tab\,(gS)\,|} = \sum \frac{p^\alpha}{p^{e_i}}$$

ma, non potendo p dividere m, esiste un laterale $\bar{g}S$ stabilizzato da tutto H. Ovvero

$$h\bar{g}S = \bar{g}S \iff h \in \bar{g}S\bar{g}^{-1} \; \forall h \in H$$

Dunque $H \in \bar{g}S\bar{g}^{-1}$, che è il p-sylow cercato.

- φ_g. Siano A, B p-sylow. Per il punto precedente

$$\exists g \in G \text{ tale che } A < gBg^{-1}$$

che hanno la stessa cardinalità e pertanto coincidono.

- n_p. Consideriamo l'azione di coniugio di un p-sylow S sull'insieme Y dei suoi coniugati

$$\Psi \colon S \to \mathcal{S}(Y)$$
$$g \mapsto \varphi_g : H \mapsto gHg^{-1}$$

Mostriamo che l'orbita di S è l'unica banale. Infatti se $H \in Y$ ha orbita banale significa che è stabilizzato da S, dunque che i due commutano e pertanto il loro prodotto è un sottogruppo di G.

$$|HS| = \frac{|H||S|}{|H \cap S|} = \frac{p^{2n}}{|H \cap S|} \mid p^n m$$

Necessariamente $|H \cap S| = p^n$ e dunque $H = S$. Per una formula ancora mai usata

$$n_p = |Y| = \mathcal{O}rb\,(S) + \sum_{H \neq S} \frac{|S|}{\mathcal{S}tab\,(H)} \equiv 1 \mod p$$

Per concludere è sufficiente osservare che se $\mathcal{S}tab\,(H) \lneq S$ allora l'orbita corrispondente ha cardinalità divisibile per p.

♣

Teorema G.37. *Ogni gruppo G abeliano finito è prodotto diretto dei suoi p-sylow.*

Dimostrazione. Visto che i gruppi sono abeliani usiamo la nozione additiva. Per ogni divisore $d||G|$ dell'ordine del gruppo sia

$$G_d = \ker \psi_d = \{g \in G \mid dg = 0\}$$

Ci è sufficiente mostrare che se $G = p^n m$, come al solito, allora

$$G \cong G_{p^n} \times G_m$$

Osserviamo innanzitutto che G_{p^n} è un p-sylow. Dev'essere un p-gruppo perché se $|G_{p^n}|$ fosse divisibile per un primo q, allora per il Teorema di Cauhcy G.11 conterrebbe almeno un elemento di ordine q, contro la sua definizione. A questo punto, dovendo contenere l'unico p-sylow di G (il coniugio è banale negli abeliani, più sylow coinciderebbero), non può che esserlo (non può avere cardinalità maggiore). E' inoltre immediato verificare che

1. I due sottogruppi sono normali in G perché è abeliano.
2. La loro intersezione è banale, perché tutti gli elementi del p-sylow hanno ordine divisibile per un primo che non divide l'ordine m dell'altro sottogruppo.

3. La loro somma è G. Infatti per Bezout esistono interi a, b tali che
$$ap^n + bm = 1$$
che moltiplicato per un qualunque elemento di $g \in G$ diventa
$$a(gp^n) + b(gm) = g$$
Osserviamo che $gp^n \in G_m$, poiché
$$m(gp^n) = (mp^n)g = |G|g = 0$$
Analogamente $gm \in G_{p^n}$ e pertanto la somma dei due sottogruppi contiene G

♣

Esercizi.

1. Chi è il 2-sylow di $\mathcal{S}_4$?
2. Chi sono i gruppi di ordine 12?

Classificazione dei gruppi di ordine 12.
Quanti possono essere i p-sylow? I 3-sylow sono necessariamente di ordine 3, pertanto ciclici, e possono essere $n_3 = 1, 4$. I 2-sylow sono di ordine 4, quindi isomorfi a $\mathbb{Z}_2 \times \mathbb{Z}_2$ o $\mathbb{Z}_4$, e sono $n_2 = 1, 3$. Se P_3 non è normale, allora ne ho 4 copie con intersezione banale e rimane spazio solo per un P_2, che sarà normale.
Quindi uno tra un 2-sylow e un 3-sylow dev'essere normale, inoltre sono ciclici e avranno intersezione banale e il loro prodotto ha necessariamente cardinalità 12. Quindi abbiamo scoperto che G è isomorfo al prodotto semidiretto tra un sylow e l'altro. Analizziamo le varie possibilità

- $\mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_3$. Abbiamo
$$\varphi : \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$$
che è dunque necessariamente banale e otteniamo
$$\boxed{G \cong \mathbb{Z}_4 \times \mathbb{Z}_3}$$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_\varphi \mathbb{Z}_3$. Abbiamo
$$\varphi : \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathcal{S}_3$$
che avrà immagine nel sottogruppo di ordine 3, abbiamo quindi l'automorfismo banale, da cui
$$\boxed{G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3}$$
e quelli associati a σ e σ^2, che vogliamo mostrare indurre lo stesso prodotto. Infatti, scelto un ϕ non banale, possiamo far agire G sull'insieme dei suoi 3-sylow per coniugio: sia
$$\Phi\colon G \to \mathcal{S}(\text{3-sylow di G}) \cong \mathcal{S}_4$$
$$g \mapsto \varphi_g : H \mapsto gHg^{-1}$$
Osserviamo che $N(P_3) = P_3$, per la formula delle classi. Allora
$$\ker \Phi = \bigcap \mathcal{S}tab\,(H) = \bigcap N(H) = \bigcap H = \{e\}$$
dunque Φ è iniettivo e mappa G in un sottogruppo di ordine 12 di $\mathcal{S}_4$. Ma l'unico sottogruppo di questa dimensione è $\mathcal{A}_4$, quindi entrambi i gruppi generati dal prodotto non diretto sono isomorfi a questo sottogruppo.
$$\boxed{G \cong \mathcal{A}_4}$$

- $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$. Abbiamo
$$\varphi : \mathbb{Z}_4 \to \text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$$
che dunque può essere solo $\pm id$. Il caso banale ci restituisce un prodotto diretto, già considerato, l'altro è un gruppo buffo
$$\boxed{G \cong \mathbb{Z}_3 \rtimes_{-id} \mathbb{Z}_4}$$

- $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 \times \mathbb{Z}_2$. Abbiamo
$$\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$$
e abbiamo, oltre all'omomorfismo banale, 3 modi di proiettare $\mathbb{Z}_2 \times \mathbb{Z}_2$ su un suo fattore. A meno di isomorfismi di $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_3$ commuta con uno dei fattori e agisce con $-id$ sull'altro quindi
$$\boxed{G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \rtimes_{-id} \mathbb{Z}_2 \cong D_6}$$

G.10 Automorfismi di un gruppo buffo

Vogliamo scoprire chi è $\mathrm{Aut}\,(Q_8 \times D_4)$. Per far questo, possiamo scomporre un qualunque automorfismo φ nelle sue restrizioni ai due termini del prodotto e proiettarli sulle due componenti. Il seguente diagramma magico è molto esplicativo

$$\begin{tikzcd}
Q_8 \arrow[dr, "imm."'] & & & Q_8 \\
D_4 \arrow[r, "imm."'] & G \arrow[r, "\varphi"] & G \arrow[ur, "\Pi_Q"] \arrow[r, "\Pi_D"'] & D_4
\end{tikzcd}$$

Dunque possiamo scomporre l'automorfismo nei quattro omomorfismi

$$\varphi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

dove

$$\alpha : Q_8 \to Q_8 \qquad \beta : D_4 \to Q_8$$
$$\gamma : Q_8 \to D_4 \qquad \delta : D_4 \to D_4$$

Iniziamo ad analizzare i possibili omomorfismi.

β. Consideriamo le possibili immagini per dimensione, tra i sottogruppi dei quaternioni:

- $\{e\}$. [✓] Ovviamente abbiamo un omomorfismo banale.
- $\mathbb{Z}_2$. [✓] Il nucleo dev'essere un sottogruppo di indice 2 e il diedrale ne ha tre: $\langle\rho\rangle, \langle\rho^2, \sigma\rangle, \langle\rho^2, \sigma\rho\rangle$.
- $\mathbb{Z}_4$. L'unico sottogruppo di indice 4 del diedrale è $\langle\rho\rangle \cong \mathbb{Z}_4$ ed è il nucleo di un omomorfismo che uccide i termini di ordine 4.
- Q_8. Non è possibile, sarebbe un isomorfismo!

Tutti questi omomorfismi preservano necessariamente i centralizzatori, perché l'unico sottogruppo dei quaternioni di ordine 2 è il centro. Dunque sembrano accettabili tutti gli omomorfismi

$$\beta : D_4 \to Z(Q_8)$$

γ. Consideriamo le possibili immagini, per dimensione:

- $\{e\}$. [✓] Ovviamente abbiamo un omomorfismo banale.
- $\mathbb{Z}_2$. [✓] Il nucleo dev'essere un sottogruppo di indice 2 e i quaterionioni ne hanno tre: $\langle i\rangle, \langle j\rangle, \langle k\rangle$.
- $\mathbb{Z}_4$. L'unico sottogruppo di indice 4 dei quaternioni è $\{\pm 1\}$ ed è il nucleo di un omomorfismo che uccide i termini di ordine 4.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$. Possiamo mandare i quaternioni in $(\mathbb{Z}_2)^3$ usando i tre omomorfismi con immagine $\mathbb{Z}_2$, questo omomorfismo non sarà suriettivo, altrimenti sarebbe un isomorfismo, e ha almeno 4 elementi nell'immagine, visto che gli omomorfismi di sopra sono distinti. Quindi, permutando le componenti opportunamente, otteniamo 6 omomorfismi.
- D_4. Non è possibile, sarebbe un isomorfismo!

possiamo però escludere alcuni omomorfismi osservando che l'automorfismo φ deve preservare i centralizzatori. Infatti osservando il magico diagramma

$$\begin{array}{ll} Q_8 \hookrightarrow Q_8 \times D_4 & \to Q_8 \times D_4 \\ i \mapsto (i, e) & \mapsto (\alpha(i), \gamma(i)) \end{array}$$

scopriamo che $Z(i, e) \cong \mathbb{Z}_4 \times D_4$. Possiamo ora cercare di capire cosa dovrebbe essere $Z(\alpha(i)) \times Z(\gamma(i))$, per esempio elencando i possibili prodotti di sottogruppi di ordine 32

- $Q_8 \times (\mathbb{Z}_2)^2$. Che però ha solo 25 elementi di ordine 2.
- $Q_8 \times \mathbb{Z}_4$. Che ha sol 11 elementi di ordine 2.
- $\mathbb{Z}_4 \times (\mathbb{Z}_2)^2$. Che però è abeliano.
- $\mathbb{Z}_4 \times \mathbb{Z}_4$. Che è abeliano.
- $\mathbb{Z}_4 \times D_4$. [✓] Che sicuramente è il gruppo che cerchiamo.

quindi necessariamente il centralizzatore di $Z(\gamma(i)) \cong D_4$ e pertanto $\gamma(i)$ è un elemento del centro di D_4, che ha solo due elementi. Quindi gli omomorfismi γ accettabili sono solo quello banale e i tre che hanno immagine in $\mathbb{Z}_2$. Dunque sembrano accettabili tutti gli omomorfismi

$$\beta : Q_8 \to Z(D_4)$$

α. Dev'essere un isomorfismo. Se non fosse un'isomorfismo l'immagine non potrebbe avere dimensione 4, perché come già visto i sottogruppi di indice adatto eliminano gli elementi di ordine 4, e non potrebbe avere dimensione più piccola, perché altrimenti il primo termine dell'immagine di φ apparterrebbe sempre al centro di G.

δ. Analogamente dev'essere un isomorfismo.

Mostriamo ora che le condizioni trovate sono sufficienti. Ci basta mostrare che φ, costruito con le componenti sopra trovate, è iniettivo. Supponiamo di aver trovato $(x, y) \in G$ tale che

$$\varphi(x, y) = (\alpha(x)\beta(y), \gamma(x)\delta(y)) = (e, e)$$

Visto che $\beta(y)$ e $\gamma(x)$ stanno nei centri dei rispettivi insiemi, anche $\alpha(x)$ e $\delta(y)$, che sono i loro inversi, vi staranno. Ma α e δ sono isomorfismi, pertanto anche x, y staranno nei centri dei loro rispettivi gruppi! Ma β e γ contengono i centri nei loro nuclei, quindi si annullano, così come i rispettivi isomorfismi. Così x, y sono necessariamente l'elemento neutro del proprio gruppo e $\ker\varphi = \{(e, e)\}$.

Conosciamo già $\mathrm{Aut}\,(D_4)$, cerchiamo, per concludere, di capire chi sia $\mathrm{Aut}\,(Q_8)$.

Ogni automorfismo α di Q_8 deve mandare $\alpha(-x) = -\alpha(x)$, quindi le coppie

$$(i, -i) \quad (j, -j) \quad (k, -k)$$

non vengono scisse, ma solo permutate fra loro. Possiamo quindi far agire $\mathrm{Aut}\,(Q_8)$ sull'insieme di queste tre coppie, costruendo così un'omomorfismo

$$\xi : \mathrm{Aut}\,(Q_8) \to \mathcal{S}_3$$

Il nucleo di ξ è costituito dagli automorfismi che non scambiano nessuna coppia, dunque quello identico e i tre che cambiano segni a due delle coppie, ed è dunque isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Se consideriamo ora gli isomorfismi

$$S : \begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto k \end{cases} \qquad T : \begin{cases} i \mapsto j \\ j \mapsto k \\ k \mapsto i \end{cases}$$

questi generano un sottogruppo "disgiunto" da $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorfo a $\mathcal{S}_3$, quindi

$$\mathrm{Aut}\,(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \rtimes_\phi \mathcal{S}_3$$

Per una certa azione ϕ che rende il gruppo $\mathcal{S}_4$ (per ragioni magiche non dimostrate).

Teorema G.38. *Il gruppo alterno $\mathcal{A}_n$ è semplice per $n \geq 5$.*

G.11 Teorema Fondamentale dei Gruppi Abeliani Finiti

Teorema G.39. *Se G è un gruppo abeliano finito allora si decompone in modo unico come prodotto diretto di gruppi ciclici di ordine $n_1, \dots, n_s$*

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

con $n_1 \mid \cdots \mid n_s$.

Dimostrazione. Avendo già dimostrato che ogni gruppo abeliano finito si decompone nel prodotto dei suoi p-sylow ci è sufficiente dimostrare la tesi per i p-gruppi. Dato gruppo abeliano G di ordine p^n, ci basta mostrare che possiamo scriverlo come prodotto diretto del generato da un suo elemento di ordine massimo g e un altro sottogruppo K

$$G \cong \langle g \rangle \times K$$

così da poter procedere per induzione.

Mostriamo questo risultato intermedio per induzione sull'ordine del p-gruppo G. Se $|G| = p$ allora il gruppo è ciclico ed è generato da g. Supponiamo ora la tesi vera per ogni k con $1 \leq k < n$ e prendiamo g un elemento di ordine massimo, diciamo p^m. Prendiamo ora un elemento $h \in G$ che non stia nel sottogruppo $\langle g \rangle$ e in modo che abbia ordine minimo possibile, se non esiste abbiamo $G = \langle g \rangle$ e abbiamo finito.

Vogliamo ora mostrare che

$$\langle g \rangle \cap \langle h \rangle = \{e\}$$

L'ordine di h^p è ovviamente minore di quello di h, dunque $h^p \in \langle g \rangle$, ovvero esiste un intero $r \in \mathbb{Z}$ tale che

$$h^p = g^r$$

L'ordine di g^r è al più p^{m-1}, per tanto non è un generatore di $\langle g \rangle$, dunque per un qualche intero s abbiamo

$$h^p = g^r = g^{ps}$$

e succede che

$$(g^{-s}h)^p = g^{-sp}h^p = e$$

esiste un elemento di ordine p che non appartiene a $\langle g \rangle$! Quindi anche l'ordine di h è p e i due sottogruppi devono essere disgiunti.

Osserviamo ora che, detto $H = \langle h \rangle$, l'ordine di gH in ${}^{G}\!/_{H}$ è lo stesso di g in G, in particolare è ancora massimo. Se fosse più piccolo, sarebbe al più p^{m-1} e

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}}H$$

e pertanto $g^{p^{m-1}} \in H$, assurdo. Per l'ipotesi induttive e il teorema di corrispondenza

$${}^{G}\!/_{H} \cong \langle gH \rangle \times {}^{K}\!/_{H}$$

per un certo sottogruppo $H < K < G$. Mostriamo che K è il sottogruppo che cercavamo

- $\langle g \rangle \cap K = \{e\}$. Infatti se b stesse nell'intersezione, bH apparterrebbe all'intersezione $\langle gH \rangle \cap {}^{K}\!/_{H}$ che è H, dunque $b \in H$.
- $G = \langle g \rangle K$. Per ragioni di cardinalità.

L'unicità è lasciata al lettore.

♣

Classificazione dei Gruppi di Ordine 30.
Tiriamo a caso qualche gruppo di quest'ordine

$$\boxed{\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5} \qquad \boxed{D_{15}} \qquad \boxed{D_5 \times \mathbb{Z}_3} \qquad \boxed{D_3 \times \mathbb{Z}_5}$$

questi sono distinti perché il primo è l'unico abeliano e i centri di dei seguenti sono rispettivamente $\{e\}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$. Sappiamo che

$$n_5 \equiv 1 \mod 5 \qquad \text{e} \qquad n_5 \mid 6$$

per il Teorema di Sylow G.36 e perché $n_5 \mid |G|$ in quanto cardinalità dell'orbita dell'azione di coniugio, rispettivamente. E, analogamente

$$n_3 \equiv 1 \mod 3 \qquad \text{e} \qquad n_3 \mid 10$$

Allora, se P_5 non è normale, ci sono sei 5-sylow, quindi 24 elementi di ordine 5. Tra i pochi elementi che rimangono non ci stanno sicuramente dieci 3-sylow e pertanto P_3 è normale. Allora P_3 e P_5 commutano (perché uno dei due è contenuto nel normalizzatore dell'altro), dunque

$$P_3P_5 < G$$

e avendo indice 2 è normale, nonché ciclico.
Abbiamo allora che

$$G \cong \mathbb{Z}_{15} \rtimes_\varphi \mathbb{Z}_2$$

per una qualche azione di coniugio

$$\varphi \colon \mathbb{Z}_2 \to \operatorname{Aut}(\mathbb{Z}_{15}) \cong \mathbb{Z}_5^\times \times \mathbb{Z}_3^\times$$
$$y \mapsto \varphi_y : x \mapsto yxy^{-1} = x^a$$

sapendo che $\varphi_y^2(x) = x^{a^2} = x$, dobbiamo avere che

$$a^2 \equiv 1 \mod 15$$

e risolvendo il sistema di diofantee troviamo

$$a = \pm 1, \pm 4 \mod 15$$

e ognuna di questa azioni induce un prodotto semidiretto isomorfo a uno dei gruppi trovati all'inizio. In particolare $a = 1$ è l'automorfismo identico, che induce il prodotto diretto, che restituisce il gruppo abeliano, mentre $a = -1$ sappiamo già essere l'omomorfismo che genera il gruppo diedrale. Per $a = 4$ troviamo l'automorfismo che fissa $\mathbb{Z}_3$, per $a = -4$ quello che fissa $\mathbb{Z}_5$, in entrambi i casi uno dei fattori a sinistra del prodotto semidiretto commuta anche col fattore di destra, siamo così autorizzati a raccoglierlo all'esterno per ottenere, rispettivamente, $D_5 \times \mathbb{Z}_3$ e $D_3 \times \mathbb{Z}_5$.
Se invece P_5 fosse normale?

G.12 Lemmini ed esercizietti

- Dati
$$H \lhd K \lhd G$$
quali sottogruppi devono essere caratteristici per far si che H sia normale o carattertico in G?
- Sia G un gruppo di ordine $2d$, dove d è dispari. Allora esiste un sottogruppo di indice 2.
- Sia G un gruppo finito. Se esiste un sottogruppo $H < G$ di indice n, allora esiste un sottogruppo normale $N \lhd G$ di indice divisore di $n!$.
- Sia G un gruppo semplice e finito. Se esiste un sottogruppo $H < G$ di indice n, allora esiste un'immersione di G in $\mathcal{A}_n$.
- Un gruppo di ordine 112 non è semplice.
- Un gruppo di ordine 144 non è semplice.
- Quanti sono i p-sylow di $\mathbf{GL}_n(\mathbb{F}_p)$?
- Dimostrare che dato un gruppo di ordine $|G| = p^3$
  1. dimostrare che $|Z(G)| = p$.
  2. dimostrare che $G' = Z(G)$.
  3. contare il numero di classi di coniugio.