Algebra I

Andrea Gallese October 4, 2017

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. $\mathrm{Aut}(\mathbb{R}) \cong \mathcal{S}(\mathbb{R}) \times \mathbb{Q}^\times$

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.

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

Proof. La funzione

$$\begin{aligned} \Phi\colon G &\to G \\ g &\mapsto \varphi_g \end{aligned}$$

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

Osservazione.

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

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:

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

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:

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

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.

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

Proof. 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. $H \lhd G \Leftrightarrow N(H) = G$

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

$$|X| = \sum_{\substack{x \in R \\ \mathcal{O}rb(x) = \{x\}}} 1 + \sum_{\substack{x \in R \\ \mathcal{O}rb(x) \neq \{x\}}} \frac{|G|}{|\mathcal{S}tab\,(x)\,|}$$

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, $\text{ord}(xy) = 6$, 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 $\mathcal{S}(G)$.*

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

$$\Phi\colon G \to \mathcal{S}(G)$$
$$g \mapsto \varphi_g(x) = gx$$

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)**.**

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

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 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 $H \lhd G$, il quoziente ${}^{G}\!/_{H}$ è abeliano se e solo se $G' < H$.**

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 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:

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

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 $m \mid n$.*

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

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

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

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

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

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

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

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

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. ($\star$) 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

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

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

Osservazione. I cicli sono orbite dell'applicazione di immersione.

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.*

Proof. Consideriamo

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

questo è un omomorfismo di gruppi. Infatti:

1. Chiaramente $|\mathrm{sgn}(\sigma)| = 1$: infatti tutte le differenze che compaiono a denominatore compaiono anche a numeratore, poiché σ è una permutazione, semplicemente con ordine, ed eventualmente segno, differente .
2. Si comporta bene con la composizione

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

inoltre tutte le trasposizioni hanno tutte segno negativo. ♣

Definizione G.25 (Gruppo Alterno)**.** Chiamiamo A_n o *gruppo alterno* il sottogruppo delle permutazioni pari

$$\ker(\mathrm{sgn}) = A_n \lhd \mathcal{S}_n$$

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 $\sigma = (a_1 \ \cdots \ a_k)$ 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. ♣