TEORIA DEI GRUPPI

ENUNCIATI

Nel seguito G indica un qualsiasi gruppo, viene indicata con e l'unità del gruppo. La notazione usata è quella moltiplicativa. $H \sqsubseteq G$ indica che H è sottogruppo di G (eventualmente coincidente). $H \lhd G$ indica che H è un sottogruppo normale di G.

- Due qualsiasi laterali destri di $H \sqsubseteq G$ in G (Ha e Hb) sono in corrispondenza biunivoca attraverso la funzione $ah \mapsto bh$
- Esiste inoltre una corrispondenza biunivoca tra l'insieme dei laterali destri e quello dei laterali sinistri di uno stesso sottogruppo H
- (**Teorema di Lagrange**) G finito e $H \sqsubseteq G$, allora ord H | ord G
- G finito, $a \in G$ allora ord a | ord G e $a^{\text{ord}\, G} = e$
- (**Ciclicità degli ordini primi**) G finito con ordine primo (ord $G = p \in \mathbb{P}$), allora G è ciclico
- (**Sottogruppo prodotto**) $H, K \sqsubseteq G$. Allora $HK \sqsubseteq G \Leftrightarrow HK = KH$
- (**Ordine del prodotto**) $H, K \sqsubseteq G$ con H e K sottogruppi finiti. Supponiamo che $HK \sqsubseteq G$. Allora ord $(HK) = \frac{\text{ord}\,(H)\text{ord}\,(K)}{\text{ord}\,(H \cap K)}$
- (**Definizione di sottogruppo normale**) $N \lhd G \Leftrightarrow \forall x \in G \quad xHx^{-1} = H \Leftrightarrow \forall x \in G \quad xHx^{-1} \subseteq H \Leftrightarrow \forall x \in G \quad xH = Hx$
- (**Gruppo quoziente**) Se $N \lhd G$, allora anche G/N è un gruppo. Inoltre se G è finito, vale ord $(G/N) = \frac{\text{ord}\,(G)}{\text{ord}\,(N)}$
- (**Proiezione al quoziente**) $N \lhd G$. $\Phi : G \mapsto G/N$ definita da $\Phi(g) = Ng$ è un omomorfismo surgettivo.
- (**Gruppi abeliani hanno tutti i sottogruppi normali**) G abeliano. $N \sqsubseteq G \implies N \lhd G$.
- (**Controimmagine di un normale è normale**) $N' \lhd G'$, $\Phi : G \to G'$. Allora $\Phi^{-1}(N') \lhd G$.
- (**Immagine di un normale con morfismo surgettivo è normale**) $N \lhd G$, $\Phi : G \to G'$ omomorfismo sugettivo. Allora $\Phi(N) \lhd G'$.
- (**Normalità del Ker**) $\Phi : G \mapsto H$ omomorfismo surgettivo. $K = \text{Ker}\, \Phi \implies K \lhd G$
- (**L'immagine è un sottogruppo**) $\Phi : G \to G'$ omomorfismo. Im $\Phi \sqsubseteq G'$ (ma NON è detto che sia normale)
- (**Immagini inverse**) $\Phi : G \mapsto H$ omomorfismo. Ker $\Phi = K \implies \Phi^{-1}\Phi(x) = Kx$
- (**Primo teorema di Omomorfismo**) $\Phi : G \mapsto H$ omomorfismo surgettivo con $K = \text{Ker}\, \Phi$. Allora $G/K \cong H$
- (**Variante del Primo teorema di Omomorfismo**) $f : G \mapsto G'$ omomorfismo surgettivo. $H \lhd G, H \sqsubseteq K, K = \text{Ker}\, f$. Allora $\exists! \phi : \frac{G}{H} \to G'$ non necessariamente iniettivo tale che $f = \phi \circ \pi_{\frac{G}{H}}$
- (**"Inversi del teorema di Lagrange"**) Se G è ciclico, ord $G = n$ si ha $\forall d \mid n \quad \exists! H \sqsubseteq G$ t.c. ord $H = d$. Se G è abeliano, ord $G = n$ si ha $\forall d \mid n \quad \exists H \sqsubseteq G$ t.c. ord $H = d$ ma in generale non è unico.
- (**Condizione equivalente al prodotto diretto**) $G \equiv H \times K \Leftrightarrow \exists H, K \lhd G$ t.c. $H \cap K = (e), HK = G$
- (**Teorema di Cauchy**) Sia $p \in \mathbb{P}$ t.c. p | ord G. Esiste allora $a \neq e$ t.c. $a^p = e$
- (**Primo teorema di Sylow**) Sia $p \in \mathbb{P}$ t.c. p^α | ord $G, p^{\alpha+1} \nmid$ ord G. Allora G ha un sottogruppo di ordine p^α. Inoltre se G è abeliano tale sottogruppo è unico.

- (**Secondo teorema di Syolow**) Sia G un gruppo finito. Allora tutti i p-Sylow sono coniugati.
- (**Corollario**) Dato un gruppo finito G, il numero dei p-Sylow di G è uguale a $i_G(N_G(P))$, dove P è un qualsiasi p-Sylow di G. In particolare, un p-Syolow P è normale sse non ci sono altri p-Sylow oltre a P.
- (**Terzo teorema di Sylow**) Detto n_p il numero dei p-Sylow di un gruppo finito G, valgono $n_p \equiv 1 \pmod{p}$ e $n_p \mid \text{ord } G$.
- (**Corrispondenza tra gruppi normali**) Sia $\Phi : G \mapsto G'$ omomorfismo surgettivo. $K = \text{Ker } \Phi$. Dato $H' \sqsubseteq G'$ si definisca $H = \{x \in G \mid \Phi(x) \in H'\}$.
  Si ha che $H \sqsubseteq G$ t.c. $K \subseteq H$. Inoltre se $H' \lhd G'$ allora $H \lhd G$. L'associare H' ad H stabilisce una corrispondenza biunivoca dell'insieme di tutti i sottogruppi di G' sull'insieme di tutti i sottogruppi di G che contengono K
- (**Secondo teorema di Omomorfismo**) $\Phi : G \mapsto G'$ omomorfismo surgettivo, $K = \text{Ker } \Phi$. Si prenda ora $N' \lhd G'$ e sia $N = \{x \in G \mid \Phi(x) \in N'\}$. Allora $G/N \cong G'/N'$ oppure, in modo equivalente, $G/N \cong (G/K)/(N/K)$.
- (**Il centro è un sottogruppo normale**) $Z(G) \lhd G$, anzi è caratteristico.
- (**Caratterizzazione degli automorfismi interni**) $\text{Int } G \cong G/Z$ con $Z = Z(G)$ centro di G. Inoltre $\text{Int } G \lhd \text{Aut } G$.
- (**Teorema di Cayley**) Ogni gruppo è isomorfo ad un sottogruppo di $S(X)$, per un opportuno X.
- (**Teorema X**) Se G è un gruppo, $H \sqsubseteq G$, X l'insieme di tutti i laterali destri di H in G, esiste un omomorfismo $\Phi : G \to S(X)$. Inoltre $\text{Ker } \Phi$ è il più grande sottogruppo normale di G contenuto in H.
- (**Corollario dell'indice fattoriale**) Se G è un gruppo finito e $H \neq G$ un sottogruppo di G tale che ord $(G) \nmid$ i $_G(H)!$, allora H deve contenere un sottogruppo normale non banale di G. In particolare, G non può essere semplice.
- (**Argomento di Frattini**) Sia G un gruppo finito e $H \lhd G$; sia P un p-Sylow di H. Allora $G = HN_G(P)$.
- (**Corollario**) Dato un p-Sylow $P \sqsubseteq G$ vale $N_G(N_G(P)) = N_G(P)$.

Particolari tipi di gruppi

- (**I gruppi ciclici sono abeliani**) G ciclico $\implies$ G abeliano. (Segue dall'associatività dell'operazione di gruppo)
- (**Ciclicità dei gruppi con ordine primo**) G gruppo. $\text{ord } G = p \in \mathbb{P} \implies G$ è ciclico. (Basta usare Cauchy)
- (**Esiste un unico gruppo ciclico di ogni ordine**) G gruppo ciclico. $\text{ord } G = n \implies G \cong \mathbb{Z}_n$
- (**Abelianità di Gruppo con quoziente sul centro ciclico**) G gruppo. $G/Z(G)$ ciclico $\implies G$ abeliano

Controesempi

- (**Gruppo non abeliano con tutti i sottogruppi normali**) $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ con le regole di moltiplicazione tra quaternioni. ($i^2 = j^2 = k^2 = 1, ij = k, ji = -k, \ldots$)

Trucchi vari

- Il modo più utile di usare l'informazione MCD $(a, b) = 1$ è tramite Bèzout: $\exists s, t$ t.c. $\quad as + bt = 1$, soprattutto se a e b sono ordini di gruppi.
- Se $N \lhd G$, $x^{\mathrm{i}_G(N)} \in N$ (poiché $\mathrm{i}_G(N)$ è l'ordine del gruppo quoziente G/N)
- Se $G^k \sqsubseteq G$, allora $G^k \lhd G$. (Segue banalmente da $ga^kg^{-1} = (gag^{-1})^k$)
- Se $H \sqsubseteq G$, $\mathrm{ord}\,(H) > \frac{\mathrm{ord}\,(G)}{2} \implies H = G$

Gruppi Ciclici

- $H, K \sqsubseteq G$, $\mathrm{ord}\,(H) = a, \mathrm{ord}\,(K) = b$. Se MCD $(a, b) = 1$, allora $H \cap K = (e)$. Infatti $H \cap K \sqsubseteq H, H \cap K \sqsubseteq K \implies \mathrm{ord}\,(H \cap K) \mid \mathrm{ord}\,(H), \mathrm{ord}\,(H \cap K) \mid \mathrm{ord}\,(K) \implies \mathrm{ord}\,(H \cap K) = 1$.
- Se $H \cap K = (e)$ e $H, K \sqsubseteq G$ con G abeliano si ha: Siano $h \in H, k \in K$, $\mathrm{ord}\,(h) = r, \mathrm{ord}\,(k) = s$. Allora $\mathrm{ord}\,(hk) = \mathrm{mcm}\,(r, s)$. (Infatti $(hk)^{\mathrm{mcm}\,(r,s)} = h^{\mathrm{mcm}\,(r,s)}k^{\mathrm{mcm}\,(r,s)} = ee = e$. Inoltre supponiamo $\exists t < \mathrm{mcm}\,(r, s)$ t.c. $(hk)^t = e$ Allora $h^tk^t = e \implies h^t = k^{-t} \in H \cap K \implies h^t = k^{-t} = e \implies r \mid t, s \mid t \implies \mathrm{mcm}\,(r, s) \mid t$)

Caratteristiche di S_n

- S_n NON è abeliano per $n \geq 3$. Infatti (12) e (13) non commutano
- Il centro di S_n è banale per $n \geq 3$. Per questo motivo S_n NON è nilpotente per $n \geq 3$
- S_n è generato dalle permutazioni $(i1)$,$(i2)$,...,(in), qualsiasi sia $i = 1, ..., n$
- In S_n tutti i k-cicli sono coniugati
- Un automorfismo di S_n che manda trasposizioni in trasposizioni è interno (basta vedere dove vengono mandati i generatori): per $n \geq 7$ ciò effettivamente avviene (si esamini il centralizzante di una trasposizione), quindi ogni automorfismo di S_n è interno
- Per $n \neq 4$, l'unico sottogruppo normale proprio di S_n è A_n, il sottogruppo delle permutazioni pari (per $n = 4$ si veda la sezione dedicata)

Caratteristiche di A_n

- A_n contiene tutti i 3-cicli di S_n
- A_n è generato da $(ij1)$,$(ij2)$,...,(ijn) per $n \geq 3$, qualsiasi siano $i, j = 1, ..., n$
- In A_n tutti i k-cicli sono coniugati per $k = 1, ..., n - 2$
- Se un sottogruppo normale di A_n contiene un 3-ciclo allora coincide con A_n
- Ogni sottogruppo normale di A_n, per $n \geq 5$, contiene un 3-ciclo: quindi A_n è semplice
- Data una classe di coniugio di S_n di permutazioni pari, ci sono due possibilità per una classe di coniugio di A_n: o la classe di coniugio è uguale a una singola classe di coniugio di A_n o questa si spezza in due classi in A_n. In particolare dato $g \in A_n$ la classe di g in S_n non si spezza se $C_{S_n}(g) \not\subseteq A_n$. Equivalentemente non si spezza se esiste una permutazione dispari che commuta con g. Equivalentemente non si spezza se la decomposizione in cicli disgiunti di g contiene un ciclo pari o due cicli della stessa lunghezza.

Layout completo di S_4

S_4 è il gruppo delle permutazioni di quattro elementi. A_4 è il gruppo delle permutazioni pari. V_4 è il gruppo dei prodotti di 2-cicli disgiunti ($\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4 = \{(), (12)(34), (13)(24), (14)(23)\}$). D_8 è il gruppo diedrale di ordine otto.

S_4 contiene le seguenti permutazioni:

- 1 identità: $()$
- 6 2-cicli: $(12), (13), (14), (23), (24), (34)$
- 3 prodotti di 2-cicli: $(12)(34), (13)(24), (14)(23)$
- 8 3-cicli: $(123), (124), (132), (134), (142), (143), (234), (243)$
- 6 4-cicli: $(1234), (1243), (1324), (1342), (1423), (1432)$

Altre caratteristiche di S_4:

- Abbiamo che S_4 è risolubile considerando la catena $(e) \subseteq V_4 \subseteq A_4 \subseteq S_4$
- $A_4 \lhd S_4$ (Poiché ha indice 2)
- $V_4 \lhd S_4$ (conti)
- $S_4 \cong V_4 \rtimes \text{Aut}\,(V_4) \cong V_4 \rtimes S_3$
- $D_8 \sqsubseteq S_4$ (prendendo $D_8 = \{(), (1234), (13)(24), (1432), (12)(34), (14)(23), (13)(24)\}$)

Gruppi diedrali D_n

- **(Presentazione)** $D_n = \{s, r \mid s^2 = r^n = e, srs^{-1} = r^{-1}\}$
- **(Moltiplicazione)** $r^i s^j \cdot r^a s^b = r^{i+(-1)^j a} s^{j+b}$
- **(Sottogruppi di D_n)** Si hanno i seguenti sottogruppi: Se $m \mid n$ si ha $C_m = \{r^{\frac{n}{m}}\} \lhd D_n$, $D_m = \{r^{\frac{n}{m}}, sr^k\}$ con $k = 0, 1, \ldots, \frac{n}{m} - 1$
- **(Classi di coniugio di D_n, n pari)** Sono $\{e\}$, $\{r^k, r^{-k}\}$ $\forall k \in \{1, \ldots, \frac{n}{2}\}$, $\{s, sr^2, \ldots, sr^{\frac{n}{2}}\}$, $\{sr, sr^3, \ldots, sr^{\frac{n}{2}-1}\}$
- **(Classi di coniugio di D_n, n dispari)** Sono $\{e\}$, $\{r^k, r^{-k}\}$ $\forall k \in \{1, \ldots, \frac{n-1}{2}\}$, $\{s, sr, sr^2, \ldots, sr^{n-1}\}$
- **(Sottogruppi Normali di D_n)** $C_m \lhd D_n$, Se n dispari allora nessun altro (tranne quelli banali), se n pari si hanno i due sottogruppi $D_{\frac{n}{2}} \lhd D_n$
- **(Sottogruppi Abeliani di D_n)** Tutti i C_m e i D_1, D_2

Automorfismi di gruppi classici

n	**Aut** (A_n)	**Out** (A_n)	**Aut** (S_n)	**Out** (S_n)
$n = 1, 2$	1	1	1	1
$n = 3$	C_2	C_2	S_3	1
$n = 6$	$S_6 \rtimes C_2$	V_4	$S_6 \rtimes C_2$	C_2
$n \geq 4, n \neq 6$	S_n	C_2	S_n	1

- $\text{Aut}\,(D_n) \cong \text{Aff}\,(C_n)$
- $\text{Aut}\,(Q_8) \cong S_4$, $\text{Int}\,(Q_8) \cong Q_8/Z(Q_8) \cong V_4$, $\text{Out}\,(Q_8) = \text{Aut}\,(Q_8)/\text{Int}\,(Q_8) \cong S_4/V_4 \cong S_3$
- $\text{Aut}\,(C_p) \cong C_p^*$, $\text{Aut}\,(C_p^n) \cong \text{GL}_n(\mathbb{F}_p)$, con p primo

- $\text{Aut}\,(C_n) \cong C_n^*$, con $n \in \mathbb{N}^+$
- $\text{Aut}\,(\mathbb{Q}) \cong \mathbb{Q}^*$
- $\text{Aut}\,(V_4) \cong \text{Aut}\,(C_2^2) \cong \text{GL}_2(\mathbb{F}_2) \cong S_3$

TRUCCHI PER ESERCIZI CON AUTOMORFISMI

- Gli automorfismi conservano gli ordini degli elementi, in particolare tutti i gruppi definiti in maniera "intrinseca" usando solo proprietà di ordine sono caratteristici e.g. "$<$ {elementi di ordine 2} $>$" è caratteristico.
- Se $H \times \{e\}$ e $\{e\} \times K$ sono caratteristici in $H \times K$ allora $\text{Aut}\,(H \times K) = \text{Aut}\,(H) \times \text{Aut}\,(K)$
- Int $G \cong G/Z$ con $Z = Z(G)$ centro di G.
- Int $G \lhd$ Aut G, può essere utile per esprimere Aut (G) come prodotto semidiretto di due sottogruppi (uno normale è gratis).
- Sia α automorfismo di G e $x \in G$, allora $C_G(\alpha(x)) = \alpha(C_G(x))$. Può essere utile e.g. per capire come sono fatti gli Aut $(S_3 \times S_3)$.
- $Z(G \times K) = Z(G) \times Z(K)$
- $C_{G\times K}((x, y)) = C_G(x) \times C_K(y)$
- $(G \times K)' = G' \times K'$
- $G \cong K \rtimes_\varphi H$. Allora $(k, h) \in Z(G)$ sta nel centro $\Leftrightarrow k \in \text{Fix}\,(\text{Im}\,\varphi), h \in Z(H), \gamma_{k^{-1}} = \varphi_h$. Inoltre, se H, K sono abeliani le condizioni diventano $k \in \text{Fix}\,(\text{Im}\,(\varphi)), h \in \text{Ker}\,\varphi$, ovvero $Z(G \rtimes_\varphi H) = \text{Fix}\,(\text{Im}\,\varphi) \times \text{Ker}\,\varphi$ SE SONO ABELIANI.

ELENCO DEI GRUPPI DI ORDINE PICCOLO

Ordine	**Gruppi Abeliani**	**Gruppi Non Abeliani**
1	C_1	
2	C_2	
3	C_3	
4	$C_4, C_2 \times C_2$	
5	C_5	
6	C_6	S_3
7	C_7	
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	D_4, Q_8
9	$C_9, C_3 \times C_3$	
10	C_{10}	D_5

TEORIA DEGLI ANELLI

DEFINIZIONI

- (**Ideale primo in un anello commutativo**) Se A è un anello, allora si dice che l'ideale P di A è primo se: $P \subsetneq A$ e se $a, b \in A$ t.c. $ab \in P \implies a \in P$ oppure $b \in P$
- (**Ideale massimale**)

PROPRIETÀ DEGLI IDEALI PRIMI

- Un ideale I dell'anello commutativo A è primo se e solo se l'anello quoziente $\frac{A}{I}$ è un dominio di integrità
- Un ideale I di un anello A è primo se e solo se $A \setminus I$ è chiuso rispetto alla moltiplicazione
- In un anello commutativo unitario ogni ideale massimale è anche un ideale primo
- (**Lemma di Krull**) Ogni anello commutativo unitario ha almeno un ideale massimale (si può dimostrare usando il lemma di Zorn)
- Un anello commutativo è un dominio di integrità se e solo se $\{0\}$ è un ideale primo
- La controimmagine di un ideale primo attraverso un omomorfismo di anelli è un ideale primo