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 $\text{ord } H \mid \text{ord } G$
- G finito, $a \in G$ allora $\text{ord } a \mid \text{ord } G$ e $a^{\text{ord } G} = e$
- (**Ciclicità degli ordini primi**) G finito con ordine primo ($\text{ord } G = p \in \mathbb{P}$), 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 $\text{ord } (HK) = \frac{\text{ord } (H) \text{ord } (K)}{\text{ord } (H \cap K)}$
- (**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 $\text{ord } (G/N) = \frac{\text{ord } (G)}{\text{ord } (N)}$
- (**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. $\text{Im } \Phi \sqsubseteq G'$ (ma NON è detto che sia normale)
- (**Immagini inverse**) $\Phi : G \mapsto H$ omomorfismo. $\text{Ker } \Phi = K \implies \Phi^{-1}\Phi(x) = Kx$
- (**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, $\text{ord } G = n$ si ha $\forall d \mid n \quad \exists! H \sqsubseteq G$ t.c. $\text{ord } H = d$. Se G è abeliano, $\text{ord } G = n$ si ha $\forall d \mid n \quad \exists H \sqsubseteq G$ t.c. $\text{ord } H = d$ 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. $p \mid \text{ord } G$. Esiste allora $a \neq e$ t.c. $a^p = e$
- (**Primo teorema di Sylow**) Sia $p \in \mathbb{P}$ t.c. $p^\alpha \mid \text{ord } G, p^{\alpha+1} \nmid \text{ord } G$. 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**) $Z(G) \lhd G$.
- (**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. ord $G = p \in \mathbb{P} \implies G$ è ciclico. (Basta usare Cauchy)
- (**Esiste un unico gruppo ciclico di ogni ordine**) G gruppo ciclico. ord $G = n \implies G \equiv \mathbb{Z}_n$
- (**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. $as+bt=1$, 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 $H \sqsubseteq G$, ord $(H) > \frac{\text{ord }(G)}{2} \implies H=G$

Gruppi Ciclici

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

Caratteristiche di S_n

- S_n NON è abeliano per $n\geq 3$. Infatti (12) e (13) non commutano
- S_n ha come sottogruppo normale di indice 2 il gruppo alterno A_n formato dalle permutazioni pari
- 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 per $n\neq 2,6$ è un gruppo completo poiché non ha centro ed ogni automorfismo è interno

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 ($V_4=\{(),(12)(34),(13)(24),(14)(23)\}$). 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)
- $D_8 \sqsubseteq S_4$ (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 $k = 0, 1, \dots, \frac{n}{m} - 1$
- (**Classi di coniugio di** D_n**,** n **pari**) Sono $\{e\}$, $\{r^k, r^{-k}\} \quad \forall k \in \{1, \dots, \frac{n}{2}\}$, $\{s, sr^2, \dots, sr^{\frac{n}{2}}\}$, $\{sr, sr^3, \dots, sr^{\frac{n}{2}-1}\}$
- (**Classi di coniugio di** D_n**,** n **dispari**) Sono $\{e\}$, $\{r^k, r^{-k}\} \quad \forall k \in \{1, \dots, \frac{n-1}{2}\}$, $\{s, sr, sr^2, \dots, sr^{n-1}\}$
- (**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

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, $C_3 \times C_3$	

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