FATTI DI ALGEBRA

TEORIA DEI GRUPPI

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 $H \mid$ ord G
- G finito, $a \in G$ allora ord $a \mid$ 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 $G/K \cong H$.
- (**Teorema di Cauchy**) Sia $p \in \mathbb{P}$ t.c. $p \mid$ ord G. Esiste allora $a \neq e$ t.c. $a^p = e$
- (**Teorema di Sylow**) Sia $p \in \mathbb{P}$ t.c. $p^\alpha \mid$ 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.
- (**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, $K = \operatorname{Ker}\Phi$. 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**) $\operatorname{Int} G \cong G/Z$ con $Z = Z(G)$ centro di G. Inoltre $\operatorname{Int} G \lhd \operatorname{Aut} G$.
- (**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 $\operatorname{Ker}\Phi$ 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 $\operatorname{ord}(G) \nmid \mathrm{i}_G(H)!$, allora H deve contenere un sottogruppo normale non banale di G. In particolare, G non può essere semplice.

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. $\operatorname{ord} G = p \in \mathbb{P} \implies G$ è ciclico. (Basta usare Cauchy)
- (**Esiste un unico gruppo ciclico di ogni ordine**) G gruppo ciclico. $\operatorname{ord} G = n \implies G \equiv \mathbb{Z}_n$
- (**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 $\operatorname{MCD}(a, b) = 1$ 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 $ga^k g^{-1} = (gag^{-1})^k$)
- Se $H \sqsubseteq G$, $\operatorname{ord}(H) > \frac{\operatorname{ord}(G)}{2} \implies H = G$

GRUPPI CICLICI

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

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 $D_8 = \{(), (1234), (13)(24), (1432), (12)(34), (14)(23), (13)(24)\}$)