# **Gara di Gruppi 2022**, Recap della Teoria

**Nota Bene.** Le pagine seguenti contengono i risultati essenziali necessari alla soluzione degli esercizi della Gara, e sono scritte principalmente allo scopo di "rinfrescare la memoria" ai partecipanti. Tuttavia, né i risultati, né il modo in cui sono esposti, sono vincolanti in alcun modo per la scrittura delle soluzioni: usare, senza dimostrarlo, un risultato non presente in queste pagine ma ugualmente noto è del tutto ammissibile, e scrivere le soluzioni con notazioni o nomenclature (comprensibili ma) diverse da quelle qui usate è certamente possibile.
Questo documento potrebbe essere aggiornato nei prossimi giorni.

**Teoremi di Lagrange e di Isomorfismo.** Se $G$ è un gruppo, $H$ è un sottogruppo di $G$, un *laterale destro* di $H$ in $G$ è una classe di equivalenza per la relazione $x \sim y$ se e solo se $y = xh$ per qualche $h \in H$. I laterali sinistri di $H$ si definiscono analogamente.

Teorema 1 *(Lagrange).* *Se $H$ è un sottogruppo di un gruppo $G$, l'ordine di $H$ divide quello di $G$. In particolare, l'*indice *di $H$ in $G$, definito come $[G : H] = |G|/|H|$, è un intero positivo che divide $|G|$.*

*Dimostrazione.* Per ogni laterale destro $Hx$ di $H$, la mappa $H \to Hx$ indotta dal prodotto per $x$ è una bigezione. □

Un sottogruppo $N < G$ è *normale* se $Ng = gN$ per ogni $g \in G$; se $N$ è normale, e $G/N$ è l'insieme delle classi laterali di $N$, la proiezione naturale $G \to G/N$ induce una struttura di gruppo su $G/N$, che si dice il *quoziente* di $G$ per $N$. Si vede subito che i nuclei degli omomorfismi sono normali, e viceversa ogni sottogruppo normale è nucleo della rispettiva proiezione al quoziente. In altre parole

Proposizione 2. *Se $G$ è un gruppo, un sottogruppo $N$ è normale se e solo se $N$ è il nucleo di un opportuno omomorfismo di dominio $G$.*

Il *prodotto* di due sottoinsiemi $S, T$ di un gruppo $G$ è definito come $ST = \{st \mid s \in S, t \in T\}$. È immediato che, se $S, T < G$, $ST$ è un sottogruppo se e solo se $S$ e $T$ commutano (nel senso che $ST = TS$). In generale, vale la seguente formula.

Proposizione 3. *Se $S, T$ sono sottoinsiemi finiti di $G$,*

$$|ST| = \frac{|S| \cdot |T|}{|S \cap T|}.$$

*Dimostrazione.* La mappa (di insiemi) $S \times T \longrightarrow ST$ indotta dal prodotto è tale che la preimmagine di un punto ha cardinalità $|S \cap T|$ □

I risultati seguenti sono anche noti come *primo, secondo, terzo teorema di isomorfismo* (le numerazioni tra il secondo e il terzo sono arbitrarie) e *teorema di corrispondenza* (*lattice theorem*, in inglese), o (complessivamente) *teoremi di Noether*.

Teorema 4. *Sia* $\varphi : G \to H$ *un omomorfismo di gruppi, e sia* $N$ *un sottogruppo normale di* $G$ *contenuto in* $\ker(\varphi)$. *Allora,* $\varphi$ *fattorizza in modo unico a un omomorfismo* $G/N \to H$*; in altre parole, se* $p : G \to G/N$ *è la proiezione al quoziente, esiste un unico omomorfismo* $\overline{\varphi} : G/N \to H$ *tale che il diagramma*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow{\scriptstyle p} & \nearrow{\scriptstyle \overline{\varphi}} & \\ G/N & & \end{array}$$

*sia commutativo. Inoltre,* $\overline{\varphi}$ *è iniettivo se e solo se* $N = \ker(\varphi)$*, e surgettivo se e solo se lo è* $\varphi$.

*Dimostrazione.* L'unica definizione possibile è $\overline{\varphi}(gN) = \varphi(g)$ per ogni $g \in G$; dato che $N \subset \ker(\varphi)$, si vede subito che l'immagine di $gN$ non dipende dalla scelta di un sollevamento. A questo punto, il resto è chiaro. □

Corollario 5. *Un omomorfismo* $\varphi : G \to H$ *induce un isomorfismo* $G/\ker(\varphi) \simeq \mathrm{im}(\varphi)$. *In particolare, a meno di isomorfismo, le immagini omomorfe di* $G$ *sono esattamente i suoi quozienti.*

Corollario 6. *Se* $K, N < G$*, e* $N$ *è normale in* $G$*,* $K \cap N$ *è normale in* $K$ *e* $KN/N \simeq K/K \cap N$.

*Dimostrazione.* La mappa naturale $K \to KN/N$ ha nucleo $K \cap N$, per cui $K \cap N$ è normale in $K$ e la tesi segue dal Teorema 4. □

Corollario 7. *Se* $K < H$ *sono sottogruppi normali di* $G$*,* $H/K$ *è normale in* $G/K$ *e* $(G/K)/(H/K) \simeq G/H$.

*Dimostrazione.* La mappa naturale $G/K \to G/H$ ha nucleo $H/K$. □

Teorema 8. *Sia* $N$ *un sottogruppo normale di* $G$*. La proiezione* $p$ *al quoziente induce un isomorfismo di reticoli tra il reticolo* $\mathcal{L}$ *dei sottogruppi di* $G$ *contenenti* $N$ *e il reticolo* $\overline{\mathcal{L}}$ *dei sottogruppi di* $G/N$*, che preserva gli indici e la normalità.*

*Dimostrazione.* La mappa $\mathcal{L} \to \overline{\mathcal{L}}$ descritta da $H \mapsto p(H) = H/N$ è tale che $p(H \cap H') = p(H) \cap p(H')$ e $p(\langle H, H' \rangle) = \langle p(H), p(H') \rangle$ per ogni $H, H' \in \mathcal{L}$. Inoltre, si inverte ponendo $\widetilde{H} \mapsto p^{-1}(\widetilde{H})$ per ogni $\widetilde{H} < G/N$. Che $p$ preservi gli indici segue dal Corollario 7, che preservi la normalità è una semplice verifica. □

**Azioni di gruppo.** Se $G$ è un gruppo e $X$ è un insieme, un'*azione* sinistra $G \curvearrowright X$ è una mappa $G \times X \to X$ che associa a ogni coppia $(g, x)$ un elemento $gx \in X$ rispettando l'identità il prodotto di $G$, nel senso che $1x = x$ per ogni $x \in X$ e $(gh)x = g(hx)$. Indicando con $S(X)$ il gruppo simmetrico su $X$ (l'insieme delle bigezioni di $X$) con l'operazione $\sigma\tau = \sigma \circ \tau$, otteniamo

Proposizione 9. *Un'azione sinistra* $G \curvearrowright X$ *induce un omomorfismo* $G \to S(X)$.

*Dimostrazione.* È sufficiente notare che la restrizione ${}_g\sigma$ dell'azione a $\{g\} \times X$ è una bigezione con $X$, e pertanto induce un elemento ${}_g\sigma \in S(X)$. Dato che, per definizione, la mappa $g \mapsto {}_g\sigma$ così ottenuta è un omomorfismo, si ottiene la tesi. □

Viceversa, è immediato che ogni omomorfismo $G \to S(X)$ induca un'azione naturale su $X$, vale a dire la mappa di valutazione $(g, x) \to g(x)$ ottenuta identificando ogni $g \in G$ con la sua immagine in $S(X)$. Pertanto, le azioni sinistre di $G$ su $X$ sono esattamente gli omomorfismi $G \to S(X)$.
C'è un naturale concetto duale di azione destra $X \curvearrowleft G$, cioè una mappa $X \times G \to G$ per cui $x1 = 1$ e $x(gh) = (xg)h$: chiaramente, ciò che cambia nei due casi è l'ordine di composizione degli elementi di $G$. D'altra parte, un'azione destra di $G$ su $X$ induce evidentemente un'azione sinistra $G \curvearrowright X$ data da $gx = xg^{-1}$ (dato che l'inversione su $G$ è un antiomomorfismo, cioè scambia l'ordine di composizione), e viceversa. Detto in altri termini, sia $G^{op}$ il *gruppo opposto* a $G$, cioè l'insieme $G$ su cui il prodotto è definito come $g \cdot_{op} h = h \cdot g$. La mappa $g \mapsto g^{-1}$ è un chiaro isomorfismo (involutivo) tra $G$ e $G^{op}$, e vale

PROPOSIZIONE 10. *Ogni azione destra $X \curvearrowleft G$ induce un'azione sinistra $G^{op} \curvearrowright X$ e viceversa.*

*Dimostrazione.* Se $\sigma_g : x \mapsto xg$ è la permutazione indotta dall'azione destra di $g \in G$ in $S(X)$, la mappa $G^{op} \to S(X)$ data da $g \mapsto \sigma_g$ è un omomorfismo. Il viceversa è del tutto analogo. □

Il discorso è inerentemente ambiguo, dato che scegliere l'ordine di composizione su $S(X)$ (cioè, scambiare $S(X)$ con $S(X)^{op}$) ribalta tutte le definizioni (qui si è scelto di comporre le permutazioni come funzioni). Tuttavia, i risultati sopra assicurano che, comunque scelti il verso delle azioni e della composizione su $S(X)$, esistono identificazioni canoniche tra gli oggetti in questione. In particolare, possiamo ridurci a studiare le azioni sinistre, come definite sopra, ottenendo analoghi risultati in tutti gli altri casi.

Dati un'azione $G \curvearrowright X$, un punto $x \in X$ e un elemento $g \in G$, diciamo

- ◇ *orbita* di $x$ l'insieme $Gx = \{gx \mid g \in G\}$;
- ◇ *stabilizzatore* di $x$ il sottogruppo $G_x = \{g \in G \mid gx = x\} < G$;
- ◇ *carattere* di $g$ il numero naturale $\chi(g) = |\{x \in X \mid gx = x\}|$.

PROPOSIZIONE 11. *Le orbite degli elementi di $X$ inducono una partizione di $X$. Inoltre, per ogni $x \in X$, esiste una bigezione tra $Gx$ e i laterali (sinistri) di $G_x$.*

*Dimostrazione.* Che avere la stessa orbita sia una relazione di equivalenza segue dalla definizione di azione. Inoltre, la mappa $gG_x \mapsto gx$ è evidentemente ben definita, dato che $(gh)x = gx$ se $h \in G_x$, e bigettiva. □

Diciamo inoltre che l'azione di $G$ su $X$

- ◇ è *finita* se $G$ e $X$ sono finiti;
- ◇ è *fedele* se l'omomorfismo $G \to S(X)$ che induce è iniettivo;
- ◇ è *libera* se gli stabilizzatori dei punti sono banali;
- ◇ è *transitiva* se ha un'unica orbita (i.e. $Gx = X$ per ogni $x \in X$);
- ◇ *fissa* un punto $x \in X$ se $G_x = G$ (equivalentemente, $Gx = \{x\}$).

Il *nucleo* dell'azione di $G$ è il nucleo dell'omomorfismo $G \to S(X)$ che induce, i.e. l'intersezione $\bigcap_{x \in X} G_x$ degli stabilizzatori. Un *trasversale* per l'azione di $G$ è un insieme di rappresentanti per le orbite dell'azione. In particolare, un *trasversale* di $H < G$ è un trasversale per l'azione di $H$ per moltiplicazione su $G$ (i.e., un insieme di rappresentanti per i laterali di $H$).

Corollario 12 *(Equazione delle orbite).* *Sia $G \curvearrowright X$ un'azione finita, $F$ l'insieme dei punti fissi di $X$. Allora,*

$$|X| = \sum_{x \in T} |G|/|G_x| = |F| + \sum_{x \in T \setminus F} |G|/|G_x|,$$

*dove $T$ è un trasversale per l'azione di $G$.*

*Dimostrazione.* Segue immediatamente dal fatto che $X$ è unione disgiunta delle sue orbite, e $|Gx| = |G|/|G_x|$ per ogni $x \in X$. □

Il *quoziente* di $X$ per l'azione di $G$ è l'insieme $X/G$ delle sue orbite.

Corollario 13 *(Lemma di Burnside).* *Sia $G \curvearrowright X$ un'azione finita. Vale*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

*Dimostrazione.* Un double counting mostra che vale l'equazione

$$\sum_{g \in G} \chi(g) = \sum_{x \in X} |G_x|.$$

D'altra parte, raccogliendo gli elementi nella stessa orbita si ha

$$\sum_{x \in X} |G_x| = \sum_{x \in T} |Gx| \cdot |G_x|,$$

con $T$ un trasversale di $X/G$. Il fatto che $|Gx| \cdot |G_x| = |G|$ per ogni $x$ fornisce l'ulteriore uguaglianza $\sum_x |Gx| \cdot |G_x| = |X/G| \cdot |G|$. □

Se $H < G$, un'azione di $G$ su $X$ induce un'azione di $H$ per restrizione. Se $N < G$ è normale, è ben definita l'azione di $G/N$ su $X/N$ via $(Ng)(Nx) = N(gx)$. Vale (per la definizione di coniugio, vedi i punti **2**, **3.** della sezione successiva)

Proposizione 14. *Sia $N < G$ un sottogruppo normale. Se l'azione di $G$ su $X$ è transitiva,*

*i) gli stabilizzatori dell'azione di* $G$ *sono coniugati,*

*ii) le orbite dell'azione di* $N$ *su* $X$ *sono equipotenti,*

*iii) l'azione di* $G/N$ *su* $X/N$ *è transitiva.*

*Dimostrazione.* Se $x, y \in X$ e $gx = y$, $hy = y$ se e solo se $h^g x = x$, da cui $(G_y)^g = G_x$, che mostra (i). Per (ii), si osserva che $N_x = (G_x) \cap N = (G_y)^g \cap N = (N_y)^g$ per normalità di $N$, per cui $|N_x| = |N_y|$ e dalla Proposizione 11 segue $|Nx| = |Ny|$. La (iii) è immediata. □

**Azioni notevoli.** Ricordiamo di seguito le principali azioni naturali di un gruppo $G$, e le loro importanti conseguenze.

**1.** Se $G$ è un gruppo finito, e $p$ è un numero primo che divide $|G|$, sia $G_1^{\times p}$ il sottoinsieme del prodotto cartesiano di $p$ copie di $G$ costituito dalle $p$-uple $(g_1, \dots, g_p)$ tali che $\prod_i g_i = 1$. L'azione naturale di $\mathbb{Z}/p\mathbb{Z}$ su $G_1^{\times p}$ per traslazione ciclica ha come punti fissi le $p$-uple della forma $(g, \dots, g)$, corrispondenti agli elementi di ordine $1$ o $p$.
Dato che $|G_1^{\times p}| = |G|^{p-1}$, dall'equazione delle orbite segue subito che, se $F$ è l'insieme dei punti fissi, $|F|$ è un multiplo positivo di $p$ (si noti che $(1, \dots, 1) \in F$). Di conseguenza, $G$ ha un elemento di ordine $p$. Riassumendo,

TEOREMA 15 *(Cauchy).* *Se* $G$ *è un gruppo finito e* $p$ *è un primo che divide* $|G|$, $G$ *contiene un elemento di ordine* $p$. *Inoltre, il numero di tali elementi è congruo a* $-1$ *modulo* $p$.

**2.** Ogni elemento $g \in G$ induce un automorfismo di $G$, il *coniugio* (a destra)

$$\gamma_g : x \mapsto g^{-1}xg = x^g$$

(la sua versione sinistra è ${}_g\gamma : x \mapsto gxg^{-1} = {}^g x$), e l'insieme $\mathrm{Inn}(G)$ degli automorfismi di coniugio è un sottogruppo normale di $\mathrm{Aut}(G)$. La mappa naturale $G \to \mathrm{Inn}(G) < S(G)$ induce un'azione (destra o sinistra rispettivamente) di $G$ su sé stesso, il cui nucleo (e anche l'insieme dei punti fissi) è il *centro* $Z(G)$ di $G$. Notiamo il fatto seguente.

PROPOSIZIONE 16. *Il quoziente* $G/Z(G)$ *è ciclico se e solo se è banale, ed è isomorfo a* $\mathrm{Inn}(G)$.

*Dimostrazione.* Se $G/Z(G) = \langle tZ(G) \rangle$, e $x, y \in G$, $x = t^m z, y = t^n z'$ per certi $m, n \in \mathbb{N}$, $z, z' \in Z(G)$. Da qui, si ottiene subito che $xy = yx$, per cui $G$ è abeliano, cioè $Z(G) = G$. L'isomorfismo segue dall'azione sopra e dal Teorema 4. □

Le orbite di tale azione si chiamano *classi di coniugio* di $G$, e si scrive $\mathrm{cl}(x) = Gx$, mentre lo stabilizzatore di $x \in G$ è il suo *centralizzatore*, scritto $C_G(x)$. Il Corollario 12 si specializza nella forma seguente.

Teorema 17 *(Equazione delle classi).* *Dato un gruppo finito* $G$*, vale l'equazione*

$$|G| = |Z(G)| + \sum_{x \in T \setminus Z(G)} |G|/|C_G(x)|$$

*dove* $T$ *è un trasversale per l'azione di coniugio.*

*Dimostrazione.* Dato che $Z(G)$ è l'insieme dei punti fissi dell'azione, la formula segue immediatamente dal Corollario 12. □

3. Un gruppo $G$ agisce naturalmente per coniugio anche sull'insieme dei suoi sottogruppi: ogni $g \in G$ mappa $H < G$ in $H^g = g^{-1}Hg$ (nel caso destro, o in ${}^gH = gHg^{-1}$ nel caso sinistro). Se $H < G$, lo stabilizzatore di $H$ in quest'azione è detto *normalizzatore* di $H$ in $G$, e indicato con $N_G(H)$; in particolare, si vede facilmente che i punti fissi di quest'azione sono esattamente i sottogruppi normali, cioè $N < G$ è normale se e solo se $N_G(N) = G$.
   Se $H < G$, ogni elemento $g \in N_G(H)$ è tale che la restrizione della mappa $\gamma_g$ ad $H$ è un automorfismo di $H$: l'omomorfismo $N_G(H) \to \mathrm{Aut}(H)$ ottenuto mappando $g$ nella restrizione ad $H$ di $\gamma_g$ è un'azione $N_G(H) \curvearrowright H$ (per automorfismi). Il nucleo di quest'azione consiste degli elementi di $G$ che commutano con $H$ elemento per elemento, ed è detto il *centralizzatore* $C_G(H)$ di $H$ in $G$. Il Teorema 4 fornisce subito il risultato seguente.

   Proposizione 18 *(Lemma N/C).* *Se* $H < G$*, il quoziente* $N_G(H)/C_G(H)$ *è isomorfo a un sottogruppo di* $\mathrm{Aut}(H)$.

4. Se $p$ è un primo, un $p$*-gruppo* è un gruppo $P$ in cui ogni elemento ha per ordine una potenza di $p$. Nel caso in cui $P$ sia finito, ciò è equivalente a chiedere che l'ordine di $p$ sia una potenza di $P$ per il Teorema 15.

   Teorema 19. *Sia* $P$ *un* $p$*-gruppo finito, e sia* $N$ *un suo sottogruppo normale. Allora, l'intersezione* $N \cap Z(P)$ *è non banale. In particolare,* $Z(P)$ *è non banale.*

   *Dimostrazione.* Applicando l'equazione delle orbite all'azione $P \curvearrowright N$ per coniugio, si ottiene $|N| = |Z(P) \cap N| + \sum_x |P|/|P_x|$ al variare di $x$ tra rappresentanti di orbite non banali, dato che $Z(P) \cap N$ è l'insieme dei punti fissi dell'azione. Ne segue immediatamente che $p$ divide $|Z(P) \cap N|$. □

5. Un gruppo $G$ agisce su sé stesso per moltiplicazione (a destra o a sinistra). Tale azione è evidentemente libera e transitiva e, in particolare, fedele. Si ottiene il risultato seguente, notando che, se $G$ è finito e $|G| = n$, fissare una numerazione $\{g_1, \ldots, g_n\}$ degli elementi di $G$ induce un isomorfismo $S(G) \simeq S_n$.

   Teorema 20 *(Cayley).* *Un gruppo finito di ordine* $n$ *si immerge in* $S_n$.

**6.** Se $H < G$ ha indice finito, $G$ agisce sui laterali di $H$ per moltiplicazione (a destra sui laterali destri, a sinistra sui laterali sinistri). Tale azione è certamente transitiva, e lo stabilizzatore (ad esempio, nel caso destro) di un punto $Hg$ è $H^g$. Il nucleo di quest'azione, l'intersezione dei coniugati di $H$, è detto *nucleo* di $H$, e indicato con $H_G$. Il Teorema 4 fornisce una mappa iniettiva $G/H_G \to S_n$, se $n = [G : H]$. Si ottiene quindi che

PROPOSIZIONE 21 *(Lemma di Poincaré).* *Se $H < G$ ha indice $n$, $[G : H_G]$ divide $n!$. In particolare, se $G$ ha un sottogruppo di indice finito, ha un sottogruppo* normale *di indice finito.*

Notiamo che $N < G$ è normale se e solo se $N_G = N$.

PROPOSIZIONE 22. *Sia $G$ un gruppo finito e sia $p$ il minimo primo che divide $|G|$. Se $H < G$ ha indice $p$, $H$ è normale.*

*Dimostrazione.* Dal fatto che $G/H_G$ si immerge in $S_p$ segue subito che $H_G = H$, e ciò equivale alla tesi. □

**Teoremi di Sylow.** Se il teorema di Lagrange fornisce una condizione necessaria affinché un gruppo finito $G$ ammetta un sottogruppo di ordine $d$, per un certo $d \in \mathbb{N}$, tale condizione non è sufficiente. Il più piccolo controesempio è fornito dal gruppo alternante su 4 elementi (si veda la sezione successiva).

OSSERVAZIONE 23. *$A_4$ non ha sottogruppi di ordine 6.*

*Dimostrazione.* Un sottogruppo di indice 2 in $A_4$ conterrebbe i quadrati degli elementi di $A_4$; ma $A_4$ è generato dai 3-cicli (Proposizione 29), e il quadrato di un 3-ciclo è un 3-ciclo. □

Sorge quindi il "problema inverso di Lagrange": dare condizioni su $G$ e/o su $d$ affinché $G$ ammetta un sottogruppo di ordine $d$. La prima risposta è il Teorema 15, che chiede che $d$ sia primo. Le più elementari condizioni su $G$ sono le seguenti.

PROPOSIZIONE 24. *Un gruppo finito $G$ risolve il problema inverso di Lagrange (cioè, se $d$ divide l'ordine di $G$, esiste $H < G$ di ordine $d$) se vale una delle seguenti:*

*i)* *$G$ è abeliano*

*ii)* *$G$ è un $p$-gruppo*

*In entrambi i casi, si può chiedere che $H$ sia normale.*

*Dimostrazione.* Per assurdo, sia $G$ abeliano di ordine minimo tra i gruppi abeliani finiti che non risolvono il problema inverso di Lagrange: allora $G$ non è ciclico, e se $H$ è un suo sottogruppo non banale, $|H| < |G|$ e $|G/H| < |G|$. Per il Teorema 8, si ottiene un assurdo. Nel caso (ii), il Teorema 19 permette di considerare $P/Z(P)$ e ragionare per induzione; ancora una volta, il Teorema 8 conclude. □

Senza dare condizioni su $G$, la miglior condizione su $d$ che si può chiedere è probabilmente quella del teorema seguente. Un $p$-*sottogruppo di Sylow* di $G$ è un $p$-sottogruppo di $G$ di indice coprimo con $p$.

Teorema 25 *(Teorema di esistenza di Sylow).* *Siano $G$ un gruppo finito, $p$ un primo. Se $d = p^k$ divide l'ordine di $G$, con $k \in \mathbb{N}$, $G$ ammette un sottogruppo di ordine $d$.*

*Dimostrazione.* Per la Proposizione 24, basta mostrare che $G$ ammette un $p$-Sylow. Supponiamo che $p^n$ divida esattamente $|G|$, e consideriamo l'azione di $G$ per moltiplicazione sui suoi sottoinsiemi: se $g \in G$, e $X \subset G$, $gX$ è l'insieme dei $gx, x \in X$. Dato che l'azione preserva la cardinalità dei sottoinsiemi, e il numero dei sottoinsiemi di cardinalità $p^n$ è $\binom{|G|}{p^n}$, che si verifica facilmente non essere multiplo di $p$, la restrizione dell'azione a $\binom{G}{p^n}$ ammette un'orbita la cui cardinalità non è divisibile per $p$, diciamo $\mathcal{O}$. Se quindi $X \in \mathcal{O}$, il suo stabilizzatore $G_X$ è tale che $|G_X| = |G|/|\mathcal{O}|$ è un multiplo di $p^n$. D'altra parte, si vede subito che dev'essere $|G_X| \leqslant p^n$, dato che $gx = y$, con $x, y \in X$, implica $g \in X$: in conclusione, $G_X$ è il $p$-Sylow cercato. □

Indichiamo con $\mathrm{Syl}_p(G)$ l'insieme dei $p$-Sylow di un gruppo finito $G$, e con $n_p(G)$ il $p$-*numero di Sylow*, cioè il numero di $p$-Sylow, di $G$.

Teorema 26 *(Teorema di unicità di Sylow).* *Sia $P$ un $p$-Sylow di $G$. Se $Q < G$ è un $p$-sottogruppo di $G$, esiste un coniugato $P^g$ di $P$ tale che $Q \subset P^g$. In particolare, $G$ agisce transitivamente per coniugio sui suoi $p$-Sylow, e $n_p(G) = [G : N_G(P)]$.*

*Dimostrazione.* L'equazione delle orbite per l'azione di $Q$ sui laterali di $P$ si scrive

$$[G : P] = |F| + \sum_{gP \in T \setminus F} |Q|/|Q_{Pg}|,$$

con la solita scelta di $g$, e con $F$ l'insieme dei punti fissi dell'azione. Pertanto si ottiene che $p$ non divide $|F|$, da cui $Q$ fissa un laterale $Pg$ di $P$, e da $PgQ = Pg$ si deduce ${}^gQ \subset P$, cioè $Q \subset P^g$. L'ultima affermazione segue dalla Proposizione 11. □

Un sottogruppo di $G$ è *caratteristico* se è fissato dall'azione naturale di $\mathrm{Aut}(G)$ su $G$. Quanto appena mostrato evidenzia che, se un $p$-Sylow $P$ è normale in $G$, vale $n_p(G) = 1$, e pertanto $P$ è caratteristico. In particolare, $N_G(P)$ ha sempre un unico $p$-Sylow, che è appunto $P$.

Teorema 27 *(Teorema del numero di Sylow).* *Sia $n_p(G) > 1$, e siano $S, T \in \mathrm{Syl}_p(G)$ distinti tali che $S \cap T$ abbia ordine massimo tra le intersezioni di due $p$-Sylow di $G$. Allora,*

$$n_p(G) \equiv 1 \pmod{[S : S \cap T]}.$$

*In particolare, $n_p(G)$ è sempre congruo a $1$ modulo $p$.*

*Dimostrazione.* Nell'azione di $S$ per coniugio su $\mathrm{Syl}_p(G)$, sia $\mathcal{O}$ un'orbita diversa da $\{S\}$. Se $P \in \mathcal{O}$, e $Q = S_P$, vale $Q \subset N_G(P)$: dato che $Q$ è un $p$-gruppo, e $QP \subset N_G(P)$ è un sottogruppo poiché $Q$ normalizza $P$, dev'essere $Q \subset P$. Di conseguenza, $|Q| \leqslant |S \cap P| \leqslant |S \cap T|$, e quindi $|\mathcal{O}| = [S : Q]$ è un multiplo di $[S : S \cap T]$. Per l'arbitrarietà di $\mathcal{O}$, si conclude. □

**Gruppi simmetrici.** Sia $S_n$ è il gruppo simmetrico su $n$ elementi. In questa sezione, per $\sigma\tau$ intendiamo la permutazione $\tau \circ \sigma$ (cioè, identifichiamo $S_n$ col gruppo opposto a quello considerato parlando delle azioni).
Ricordiamo che ogni permutazione $\sigma \in S_n$ ammette, a meno di trasposizione ciclica, un'unica scrittura in *cicli disgiunti*, dove un ciclo $(i_0 \cdots i_k)$ è un'orbita di dell'azione naturale di $\langle\sigma\rangle < S_n$ su $\{1, \ldots, n\}$, scritta in modo che $\sigma^j(i_0) = i_j$ per $j \leqslant k$.

Proposizione 28. *Se $\sigma, \tau \in S_n$, e $\sigma = (c_{11} \cdots c_{1k_1}) \cdots (c_{t1} \cdots c_{tk_t})$ in cicli disgiunti, $\sigma^\tau$ è la permutazione $(\tau(c_{11}) \cdots \tau(c_{1k_1})) \cdots (\tau(c_{t1}) \ldots \tau(c_{tk_t}))$.*

*Dimostrazione.* È sufficiente verificare l'uguaglianza sui cicli, su cui la verifica è immediata. □

La mappa $S_n \to \{1, -1\}$ data da

$$\sigma \mapsto \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

induce un omomorfismo surgettivo a valori in $C_2$, che mappa le trasposizioni (cioè i cicli di lunghezza 2) in $-1$. Il suo nucleo è il *gruppo alternante* $A_n < S_n$, e una permutazione $\sigma \in A_n$ si dice *pari*, una in $S_n \setminus A_n$ è invece *dispari*.

Proposizione 29. *$S_n$ è generato dalle trasposizioni della forma $(1\,k)$, $A_n$ è generato dai 3-cicli.*

*Dimostrazione.* Ogni elemento di $S_n$ è prodotto di cicli, e un ciclo $(c_1 \cdots c_k)$ si scrive come prodotto $(c_1\,1)(c_2\,1) \cdots (c_n\,1)$ di trasposizioni. Poiché il segno è un omomorfismo, $\sigma \in S_n$ è prodotto di un numero pari di trasposizioni se e solo se è pari. In tal caso, $\sigma = \tau_1 \cdots \tau_k$ con $\tau_k$ 2-cicli e $k$ pari, e può essere

i) $\tau_1 = \tau_2$, per cui $\tau_1\tau_2 = 1$;

ii) $\tau_1\tau_2 = (a\,b)(b\,c)$ per certi $a, b, c$ distinti, nel qual caso $\tau_1\tau_2 = (a\,b\,c)$ è un 3-ciclo;

iii) $\tau_1\tau_2 = (a\,b)(c\,d)$ per $a, b, c, d$ distinti, e in tal caso $\tau_1\tau_2 = (a\,b)(b\,c)(b\,c)(c\,d)$ è prodotto di due 3-cicli.

Iterando e usando il fatto che $k$ è pari si ottiene che $\sigma$ è prodotto di 3-cicli. □

Un gruppo $G$ è *semplice* se non ha sottogruppi normali non banali. I gruppi abeliani semplici sono solo quelli isomorfi a $C_p$ (il gruppo ciclico di ordine $p$) per $p$ primo. L'esempio più elementare di gruppi semplici non abeliani è il seguente. Notiamo che, poiché fissato dall'azione di $\mathrm{Inn}(G)$, un sottogruppo normale di un gruppo $G$ è unione di classi di coniugio.

Teorema 30. *Per $n \geqslant 5$, $A_5$ è semplice.*

*Dimostrazione.* Il caso $n = 5$ si ottiene verificando direttamente che nessuna unione non banale di classi di coniugio di $A_5$ ha cardinalità un divisore di $|A_5| = 60$. Per $n > 5$, si ragiona induttivamente: per ogni $i = 1, \dots, n$, lo stabilizzatore $G_i$ del punto $i$ nell'azione naturale di $G = A_n$ su $\{1, \dots, n\}$ è isomorfo ad $A_{n-1}$, e quindi semplice per ipotesi induttiva. Inoltre, poiché l'azione considerata è transitiva, è facile vedere che i $G_i$ sono tutti coniugati: nello specifico, $G_{\sigma(i)} = {}^{\sigma}G_i$ per ogni $\sigma \in A_n$ e per ogni $i$. Infine, $A_n = \langle G_1, \dots, G_n \rangle$.
Se ne ottiene che, se $N$ è normale in $A_n$,

i) o $N$ interseca non banalmente uno dei $G_i$, e allora lo contiene perché $G_i$ è semplice; ma questo implica che $N \supset G_i$ per ogni $i$, da cui $N = A_n$;

ii) o $N$ interseca ognuno dei $G_i$ banalmente, da cui ogni elemento di $N$ non fissa alcun punto. Ma, usando $n > 4$, si conclude facilmente che $N = 1$. □

Corollario 31. *Per $n > 4$, l'unico sottogruppo normale non banale di $S_n$ è $A_n$.*

*Dimostrazione.* Se $N$ è normale in $S_n$, la sua intersezione con $A_n$ è normale in $A_n$ e quindi banale. Ne segue che, se $N \not\supset A_n$, l'ordine di $N$ è al più 2. Osservando che, nelle ipotesi fatte, il sottogruppo generato da un'involuzione di $S_n$ non può essere normale, si conclude $N = 1$. □

Un gruppo si dice *completo* se ha centro banale e $\mathrm{Inn}(G) = \mathrm{Aut}(G)$: il prototipo dei gruppi completi è fornito dai gruppi simmetrici per $n \neq 2, 6$.

Proposizione 32. *Un automorfismo di $S_n$ è interno (cioè è un coniugio) se e solo se mappa trasposizioni in trasposizioni.*

*Dimostrazione.* Un'implicazione segue dalla Proposizione 28. Per l'altra, sia $\varphi \in \mathrm{Aut}(S_n)$, e supponiamo mappi trasposizioni in trasposizioni. Induttivamente, mostriamo che esistono elementi $\gamma_i \in \mathrm{Inn}(S_n)$ tali che $\gamma_k^{-1} \cdots \gamma_2^{-1} \varphi$ fissa $(1\,i)$ per $i = 1, \dots, k$. Il caso base è chiaro; per il passo induttivo, notiamo che, se $\psi = \gamma_k^{-1} \cdots \gamma_2^{-1} \varphi$, e $\psi(1\,k+1) = (s\,t)$, allora

i) $(s\,t)$ e $(1\,2)$ non sono disgiunti, il che si può facilmente dedurre dal fatto che $(1\,k+1)$ e $(1\,2)$ non lo sono, e pertanto $(s\,t) = (1\,t)$ o $(s\,t) = (2\,t)$;

ii) se $k \geqslant 3$, lo stesso argomento applicato a $(1\,3)$ mostra che $(s\,t) = (1\,t)$;

iii) di sicuro, $t > k$, per iniettività di $\psi$.

Basta allora definire $\gamma_{k+1}$ come il coniugio per $(1\,2)(k+1\,t)$ se $(s\,t) = (2\,t)$, per $(k+1\,t)$ se $(s\,t) = (1\,t)$. Prendendo $k = n$, si ha che $\varphi = \gamma_2 \cdots \gamma_n$. □

Teorema 33. *Per $n \neq 2, 6$, $S_n$ è completo.*

*Dimostrazione.* Che $S_n$ sia senza centro per $n \geqslant 3$ è immediatamente verificabile. Se $T_k$ è la classe di coniugio, in $S_n$, dei prodotti di $k$ trasposizioni disgiunte, si vede facilmente che $|T_k| = |T_h|$ se e solo se $k = h$, oppure $k = 1$, $h = 3$ e $n = 6$; la conclusione segue dal fatto che un automorfismo di $S_n$ mappa classi di coniugio in classi di coniugio, e dalla Proposizione 32. □

Un sottogruppo di $S_n$ è *transitivo* se lo è la sua azione naturale su $\{1, \ldots, n\}$. Se $n = 6$, si osserva che

1. l'azione di $S_5$ sui suoi 5-Sylow induce un omomorfismo $S_5 \to S_6$, certamente iniettivo perché l'azione è transitiva e l'unico nucleo non banale sarebbe $A_5$. Di conseguenza, l'immagine $K$ di tale omomorfismo è un sottogruppo transitivo di $S_6$ di ordine 120;

2. Per il Teorema 15, $K$ ha un elemento di ordine 5, che è un 5-ciclo. Se $K$ contenesse una trasposizione, per transitività si otterrebbe facilmente che $K$ contiene $(k\,6)$ per ogni $k = 1, \ldots 5$. Dato che, per un argomento analogo a quello della Proposizione 29, tali trasposizioni generano $S_6$, ciò è impossibile.

3. L'azione di $S_6$ sui laterali di $K$ induce un automorfismo $\varphi$ di $S_6$. Se tale automorfismo fosse interno, mapperebbe $(1\,2)$ in una trasposizione, cioè l'azione di $(1\,2)$ fisserebbe quattro laterali di $K$. Tuttavia, se fosse $(1\,2)\sigma K = \sigma K$ per qualche $\sigma$, la trasposizione $(1\,2)^\sigma$ sarebbe un elemento di $K$. Quindi, $\varphi$ è un automorfismo in $\mathrm{Aut}(S_6) \setminus \mathrm{Inn}(S_6)$;

4. se $\varphi, \psi \in \mathrm{Aut}(S_6) \setminus \mathrm{Inn}(S_6)$, per quanto osservato nel Teorema 33, devono scambiare entrambi $T_1$ e $T_3$: perciò, la loro composizione manda trasposizioni in trasposizioni, ed è quindi un elemento di $\mathrm{Inn}(S_6)$ per la proposizione 32.

Un elemento non banale di $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ è detto un automorfismo *esterno* di $G$. Riassumendo,

Teorema 34 *(Hölder). Esiste un unico automorfismo esterno di $S_6$.*

**Serie normali e subnormali.** Una catena finita di sottogruppi

$$G = G_0 > G_1 > \cdots > G_n = 1$$

è una *serie subnormale* se $G_{i+1}$ è normale in $G_i$ per ogni $i$, ed è una *serie normale* se ogni $G_i$ è normale in $G$. I suoi *quozienti* sono i quozienti $G_i/G_{i+1}$, le cui cardinalità sono i *fattori* della serie. Due serie subnormali per $G$ sono *isomorfe* se hanno quozienti isomorfi, a meno dell'ordine.
Rispetto alla naturale relazione di raffinamento (una serie raffina un'altra se tutti i termini della seconda compaiono nella prima), una serie subnormale massimale per $G$ è detta *serie di composizione*, una serie normale massimale è detta *serie principale*. Notiamo che una serie subnormale è di composizione se e solo se ha quozienti semplici. Vale il

Teorema 35 *(Schreier).* *Due serie subnormali di un gruppo* $G$ *ammettono raffinamenti isomorfi.*

Lemma 36 *(Zassenhaus).* *Siano* $A, C$ *sottogruppi di un gruppo* $G$. *Se* $B$ *è normale in* $A$, *e* $D$ *è normale in* $C$, *vale l'isomorfismo*

$$\frac{(A \cap C)B}{(A \cap D)B} \simeq \frac{(A \cap C)D}{(B \cap C)D}.$$

*Dimostrazione.* Si verifica immediatamente che $(A \cap D)B$ e $(B \cap C)D$ sono normali in $(A \cap C)B, (A \cap C)D$ rispettivamente. Se $E = (B \cap C)(A \cap D)$, $E$ è normale in $C \cap D$ e l'omomorfismo $(A \cap C)B \to (A \cap C)/E$ che associa a un elemento $ab \in (A \cap C)B$ il laterale $aE$ è ben definita ($ab = a'b'$ implica $(a')^{-1}a = b'b^{-1} \in E$), e si vede facilmente essere surgettiva con nucleo $(A \cap D)B$. Pertanto, si ottiene

$$\frac{(A \cap C)B}{(A \cap D)B} \simeq \frac{A \cap C}{E}.$$

Ragionando analogamente a partire da $(A \cap C)D$ si ottiene la tesi. □

*Dimostrazione.* Prese due serie subnormali

$$G = G_0 > G_1 > \cdots > G_n = 1,$$
$$H = H_0 > H_1 > \cdots > H_m = 1,$$

inseriamo una copia della seconda serie tra $G_i$ e $G_{i+1}$ per ogni $i$ e viceversa, ponendo $G_{ij} = G_{i+1}(G_i \cap H_j)$ e $H_{ij} = H_{i+1}(H_i \cap G_j)$. In tal modo, $G_{ij} > G_{i,j+1}, G_{i,0} = G_i$ e $G_{i,m} = G_{i+1}$, per cui $G_{ij}$ è una serie subnormale per $G$ che raffina $G_i$, e analogamente $H_{ij}$ raffina $H_i$. Per il Lemma 36, $G_{ij}/G_{i,j+1} \simeq H_{ij}/H_{i+1,j}$ per ogni $i, j$, il che conclude. □

Corollario 37 *(Jordan-Hölder).* *Un gruppo finito* $G$ *ha un'unica serie di composizione a meno di isomorfismo.*

*Dimostrazione.* Due serie di composizione hanno raffinamenti isomorfi per il Teorema 35, e per massimalità sono isomorfe. □

**Sottogruppo derivato e gruppi risolubili.** Se $G$ è un gruppo, il *commutatore* (destro) di due elementi $g, h \in G$ è definito da $[g, h] = g^{-1}h^{-1}gh$ (la versione sinistra è, ovviamente, $[g, h] = ghg^{-1}h^{-1}$). Il sottogruppo *derivato* di $G$ è

$$G' = \langle [g, h] \mid g, h \in G \rangle$$

(si noti che la definizione non dipende dalla scelta di un verso per i commutatori). È immediato vedere che $G'$ è caratteristico in $G$; la sua proprietà fondamentale è la seguente.

Proposizione 38. *Sia* $N$ *un sottogruppo normale di* $G$. *Il quoziente* $G/N$ *è abeliano se e solo se* $N \supset G'$.

*Dimostrazione.* Poiché $gh = hg[g,h]$ per definizione, si ha che $gh = hg \bmod N$ (nel senso che $gh$ e $hg$ hanno la stessa immagine tramite la proiezione al quoziente) se e solo se $[g,h] = 0 \bmod N$, cioè $[g,h] \in N$. □

È naturale iterare induttivamente la definizione di $G'$, definendo $G^{(0)} = G, G^{(1)} = G'$ e, induttivamente, $G^{(i+1)} = \left(G^{(i)}\right)'$ per ogni $i > 1$. Ciò fornisce una catena discendente di sottogruppi caratteristici di $G$, detta *serie derivata* di $G$, che è una serie normale se e solo se è finita.

Proposizione 39. *Se $G$ è un gruppo, sono equivalenti:*

*i) la serie derivata di $G$ è finita;*

*ii) $G$ ha una serie subnormale a quozienti abeliani.*

*Dimostrazione.* Che (i) implichi (ii) segue dalla Proposizione 38. Viceversa, se $G = G_0 > G_1 > \cdots > G_n = 1$ è una serie subnormale di $G$ a quozienti abeliani, la Proposizione 38 permette di concludere, induttivamente, che $G_i \supset G^{(i)}$. Pertanto $G^{(n)} = 1$. □

Se vale una delle condizioni sopra, $G$ si dice *risolubile*, e il minimo $n$ tale che $G^{(n)} = 1$ si dice *lunghezza derivata* di $G$. Notiamo che $G$ è abeliano se e solo se ha lunghezza derivata 1. Sottogruppi e quozienti di gruppi risolubili sono a loro volta risolubili, come mostra il risultato seguente.

Proposizione 40. *Siano $H, N < G$ con $N$ normale in $G$. Se $G$ è risolubile, $H$ e $G/N$ sono risolubili. Viceversa, se $N$ e $G/N$ sono risolubili, anche $G$ lo è.*

*Dimostrazione.* Se $G = G_0 > G_1 > \cdots > G_n = 1$ è una serie normale a quozienti abeliani, basta porre $H_i = G_i \cap H$ e $\overline{G}_i = G_i N/N$ per ottenere due serie normali di $H, G/N$ rispettivamente, per cui l'abelianità dei quozienti viene dal Corollario 6. Viceversa, una serie normale di $G/N$ è della forma $G/N = G_0/N > G_1/N > \cdots > G_n/N = 1$ per il Teorema 8, e fornisce una catena $G_0 > G_1 > \cdots > G_n = N$ con i $G_i$ normali in $G$. Proseguendo con una serie normale di $N$ si ottiene una serie normale di $G$, e l'abelianità dei quozienti è conseguenza del Corollario 7. □

**Prodotti diretti e semidiretti.** Il prodotto cartesiano di due gruppi $H, K$ ha una naturale struttura di gruppo, con il prodotto fatto per componenti. Il gruppo $H \times K$ così ottenuto è detto *prodotto diretto* di $H, K$. Più in generale, se $\{H_i \mid i \in I\}$ è una famiglia di gruppi, il loro prodotto diretto è definito analogamente come l'insieme $\prod_{i \in I} H_i$ con l'operazione naturale. Vale

Proposizione 41. *Un gruppo $G$ è isomorfo a un prodotto diretto $\prod_{i=1}^{n} G_i$ se e solo esistono sottogruppi $H_1, \ldots, H_n < G$ tali che:*

*i) per ogni $i$, $H_i$ è normale in $G$ ed è isomorfo a $G_i$;*

*ii)* $G = \langle H_1, \dots H_n \rangle$;

*iii)* *per ogni* $i$, *l'intersezione* $H_j \cap \langle H_i \mid i \neq j \rangle$ *è banale.*

*Dimostrazione.* Per (i) e (ii), $G = H_1 \cdots H_n$, e la mappa naturale $\prod_{i=1}^n H_i \to G$ data da $(h_1, \dots, h_n) \mapsto h_1 \cdots h_n$ è surgettiva. Inoltre, l'iniettività è garantita dalla condizione (iii): pertanto, tale mappa induce un isomorfismo $\prod_{i=1}^n G_i \to G$. Viceversa, un isomorfismo $\varphi : \prod_{i=1}^n G_i \to G$ identifica sottogruppi $H_i = \varphi(1 \times \cdots \times G_i \times \cdots \times 1)$, e le proprietà richieste sono immediate. □

Nel caso di due gruppi, il loro prodotto cartesiano possiede altre strutture naturali di gruppo. Ogni scelta di un omomorfismo $\varphi : H \to \mathrm{Aut}(G)$ induce una struttura di gruppo su $G \times H$ ponendo $(g, h)(g', h') = (g\varphi(h)(g'), hh')$. Con tale struttura, $G \times H =: G \rtimes_\varphi H$ si dice un *prodotto semidiretto* (sinistro) di $G$ per $H$ via $\varphi$ (al solito, la versione destra è $H \ltimes_\varphi G := H \times G$ con il prodotto $(h, g)(h', g') = (hh', \varphi(h)(g)g')$). Vale

Proposizione 42. *Un gruppo* $G$ *è isomorfo a un prodotto semidiretto* $G_1 \rtimes_\varphi G_2$ *se e solo se esistono sottogruppi* $H_1, H_2 < G$ *tali che*

*i)* $H_1$ *è normale in* $G$, $H_1 \simeq G_1$ *e* $H_2 \simeq G_2$;

*ii)* $G = \langle H_1, H_2 \rangle$;

*iii)* $H_1 \cap H_2$ *è banale.*

*Dimostrazione.* È chiaro che $G_1, G_2$ verificano le proprietà richieste per $G_1 \rtimes_\varphi G_2$. Viceversa, se $H_1, H_2 < G$ sono come sopra, $H_2$ agisce su $H_1$ per coniugio e induce un omomorfismo $\gamma : H_2 \to \mathrm{Aut}(H_1)$. La mappa $H_1 \rtimes_\gamma H_2 \to G$, $(h_1, h_2) \to h_1 h_2$ è quindi un omomorfismo, ed è bigettivo per (ii) e (iii). □

**Gruppi abeliani finitamente generati.** Un gruppo $G$ è detto *finitamente generato* se $G = \langle g_1, \dots, g_n \rangle$ per certi elementi $g_i \in G$. Nel caso dei gruppi abeliani, quelli finitamente generati sono classificati a meno di isomorfismo.
Per una famiglia $\{A_i \mid i \in I\}$ di gruppi abeliani, la *somma diretta* $\bigoplus_{i \in I} A_i$ è il sottogruppo del prodotto diretto $\prod_{i \in I} A_i$ formato dagli elementi nulli in quasi ogni coordinata, cioè dagli $(a_i) \in \prod_{i \in I} A_i$ tali che $a_i \neq 0$ per al più un numero finito di $i$. Nel caso in cui $I$ sia finito, vale quindi $\bigoplus_{i \in I} A_i = \prod_{i \in I} A_i$.
Enunciamo solamente il seguente risultato.

Teorema 43 *(Struttura dei GAFG). Sia* $A$ *un gruppo abeliano finitamente generato. Allora, esistono un unico* $k \in \mathbb{N}$ *e unici* $q_1, \dots, q_t \in \mathbb{N}$ *a meno dell'ordine tali che, per ogni* $i$, $q_i$ *è una potenza di un primo* $p_i$ *e*

$$A \simeq \mathbb{Z}^k \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_t\mathbb{Z}.$$

*In particolare, se* $A$ *è finito, è isomorfo a una somma diretta di gruppi ciclici di ordine una potenza di un primo.*