

proprietá dei sottogruppi di un gruppo G

- L'unione di due sottogruppi non é in generale un sottogruppo.
- L'intersezione di un insieme di sottogruppi é un sottogruppo.
- Il *sottogruppo generato* da un sottoinsieme X di G é, per definizione, l'intersezione di tutti i sottogruppi di G che contengono X . Tale sottogruppo si denota con $\langle X \rangle$ ed é il piú piccolo (rispetto all'inclusione) sottogruppo di G contenente X .
- Un sottogruppo H di G é il sottogruppo generato da un sottoinsieme X di G se, e solo se:

(1) H é un sottogruppo di G contenente X ,

(2) ogni sottogruppo K di G contenente X contiene H .

- $\langle \emptyset \rangle = \{1\}$.
- $H \leq G$ e $X \subseteq H \Rightarrow \langle X \rangle \subseteq H$.
- $X \subseteq Y \Rightarrow \langle X \rangle \leq \langle Y \rangle$.
- $\langle X \rangle = X \Leftrightarrow X$ é un sottogruppo.
- Se X é non vuoto, risulta

$$\langle X \rangle = \{a_1 a_2 \cdots a_n : a_j \in X \cup X^{-1}, n \in \mathbb{N}\}. \quad (1)$$

Quando $\langle X \rangle = G$, si dice che X é un *generatore di G* , o anche che G é *generato da X* .

- Sia $X = H \cup K$, ove H e K sono sottogruppi di G . Allora $\langle X \rangle$ si chiama *sottogruppo generato da H e K* e si denota con $\langle H, K \rangle$. Risulta:

$$\langle H, K \rangle = \{h_1 k_1 h_2 k_2 \cdots h_n k_n : h_j \in H, k_j \in K, n \in \mathbb{N}\}. \quad (2)$$

gruppi ciclici

DEFINIZIONE 1 Un gruppo G si dice *ciclico* se esiste un elemento $a \in G$ tale che $G = \langle a \rangle$.

OSSERVAZIONE 2 Se $G = \langle a \rangle$, risulta

$$G = \{a^n : n \in \mathbb{Z}\}.$$

Ne segue che ogni gruppo ciclico \acute{e} abeliano.

ESERCIZIO 3 Sia $G = \langle a \rangle$. Provare che G \acute{e} infinito se, e soltanto se, a ha ordine infinito in G e, in questo caso, risulta $a^h \neq a^k$, per ogni due interi non negativi e distinti h e k . Provare inoltre che G \acute{e} finito d'ordine n se, e soltanto se, a ha periodo finito n in G e, in questo caso, risulta $G = \{1 = a^0, a, a^2, \dots, a^{n-1}\}$.

ESEMPI 4

- $(\mathbb{Z}, +)$ \acute{e} un gruppo ciclico, avendosi $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- $(\mathbb{Z}_m, +)$ \acute{e} un gruppo ciclico, avendosi $\mathbb{Z}_m = \langle 1 \rangle$.

ESERCIZIO 5 Provare che il gruppo delle radici n -esime dell'unit  del campo complesso \acute{e} ciclico e determinare ciascuno dei suoi generatori.

ESERCIZIO 6 Provare che il gruppo additivo dei razionali $(\mathbb{Q}, +)$ non \acute{e} ciclico.

SOLUZIONE Per assurdo, sia $\frac{n}{m} \in \mathbb{Q}$ un generatore di $(\mathbb{Q}, +)$, con n, m coprimi e osserviamo che deve essere $m \neq \pm 1$, perch  un intero non pu  generare $(\mathbb{Q}, +)$. Allora dovrebbe esistere un intero k tale che

$$\frac{n}{m^2} = k \frac{n}{m}$$

e, dovendo essere $k = \frac{1}{m}$, abbiamo un assurdo.

sottogruppi permutabili

DEFINIZIONE 7 Due sottogruppi H, K di G si dicono *permutabili* se \acute{e} $HK = KH$, cio \acute{e} se, per ogni $h \in H$ e $k \in K$, esistono $h_1, h_2 \in H$ e $k_1, k_2 \in K$ tali che $hk = k_1h_1$ e $kh = h_2k_2$.

OSSERVAZIONE 8 Notiamo esplicitamente che l'essere H e K permutabili non significa che $hk = kh$, per ogni $h \in H$ e $k \in K$.

TEOREMA 9 Siano H, K sottogruppi di G . Allora H e K sono permutabili se, e solo se, risulta $\langle H, K \rangle = HK$.

DIM. Nell'ipotesi $\langle H, K \rangle = HK$, abbiamo:

$$\bullet \langle H, K \rangle = HK \Rightarrow \boxed{KH \subseteq HK}.$$

$$\bullet hk \in HK, h \in H, k \in K \Rightarrow (hk)^{-1} = k^{-1}h^{-1} \in HK$$

$$\Rightarrow k^{-1}h^{-1} = h_1k_1 \text{ con } h_1 \in H \text{ e } k_1 \in K \Rightarrow hk =$$

$$(k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH \Rightarrow \boxed{HK \subseteq KH}.$$

Ne segue che \acute{e} $HK = KH$.

Nell'ipotesi $HK = KH$, dobbiamo provare che $\langle H, K \rangle \subseteq HK$, essendo evidente l'inclusione inversa.

\bullet Sia $h_1k_1h_2k_2 \cdots h_nk_n \in \langle H, K \rangle$, $n > 0$, $h_j \in H$, $k_j \in K$. Se \acute{e} $n = 1$ l'asserto \acute{e} vero e possiamo fare per induzione su n :

$$\underbrace{h_1k_1h_2k_2 \cdots h_{n-1}k_{n-1}} h_nk_n = hkh_nk_n \text{ con } h \in H, k \in K \Rightarrow$$

$$kh_n = h'k' \text{ con } h' \in H, k' \in K \text{ (perch\acute{e} } HK = KH) \Rightarrow$$

$$h_1k_1 \cdots h_nk_n = hh'k'k_n = h^*k^* \text{ con } h^* \in H \text{ e } k^* \in K.$$

sottogruppi permutabili

COROLLARIO 10 Se G é un gruppo abeliano e H, K due suoi sottogruppi, allora risulta $\langle H, K \rangle = HK = KH$.

COROLLARIO 11 Siano G un gruppo e H_1, H_2, \dots, H_n sottogruppi di G a due a due permutabili. Allora

$$H = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_j \in H_j\}$$

é un sottogruppo di G e risulta $H = \langle H_1, H_2, \dots, H_n \rangle$.

DEFINIZIONE 12 Siano G un gruppo e H_1, H_2, \dots, H_n sottogruppi di G a due a due permutabili. Il sottogruppo di G

$$H = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_j \in H_j\},$$

definito dal corollario precedente, si chiama *prodotto* di H_1, \dots, H_n .

ESEMPIO 13 Diamo un esempio di due sottogruppi H, K per cui risulta $\langle H, K \rangle \neq HK$. A Tale scopo, nel gruppo $G = GL(2, Q)$ consideriamo i sottogruppi

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in Q \right\}, \quad K = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in Q \right\}$$

e osserviamo che é

$$HK = \left\{ \begin{bmatrix} 1 + ab & b \\ a & 1 \end{bmatrix} : a, b \in Q \right\}.$$

Osserviamo ancora che le matrici

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \text{ e } B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

appartengono ad HK , mentre il loro prodotto

$$AB = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

non vi appartiene. Questo significa che HK non é un sottogruppo di $GL(2, Q)$ e, quindi, $\langle H, K \rangle \neq HK$.

sottogruppi di $(\mathbb{Z}, +)$

OSSERVAZIONE 14 Sia m un intero. L'insieme

$$m\mathbb{Z} = \{ma : a \in \mathbb{Z}\}$$

dei multipli di m é un sottogruppo ciclico di $(\mathbb{Z}, +)$, avendosi $m\mathbb{Z} = \langle m \rangle$. Inoltre risulta $m\mathbb{Z} = \mathbb{Z}$ se, e solo se, $m = \pm 1$.

PROPOSIZIONE 15 Ogni sottogruppo H di $(\mathbb{Z}, +)$ é del tipo

$$m\mathbb{Z} = \{ma : a \in \mathbb{Z}\},$$

ove m é il minimo fra gli interi non negativi contenuti in H . In particolare si ha che tutti i sottogruppi di $(\mathbb{Z}, +)$ sono ciclici.

COROLLARIO 16 Gli interi 1 e -1 sono gli unici generatori del gruppo $(\mathbb{Z}, +)$.

ESERCIZIO 17 Provare che $n\mathbb{Z}$ é contenuto in $m\mathbb{Z}$ se, e solo se, m divide n .

ESERCIZIO 18 Provare che in $(\mathbb{Z}, +)$ il sottogruppo $\langle a, b \rangle$ generato da due interi distinti a, b coincide col sottogruppo ciclico generato da un massimo comune divisore di a e b . Provare, inoltre, che un minimo comune multiplo di a e b é un generatore del sottogruppo intersezione di $\langle a \rangle$ e $\langle b \rangle$.

sottogruppi di $(Z_n, +)$

PROPOSIZIONE 19 Sia h un elemento non nullo del gruppo additivo $(Z_n, +)$ degli interi modulo n . Allora il sottogruppo ciclico $\langle h \rangle$ generato da h ha ordine $\frac{n}{MCD(n,h)}$. In particolare, h é un generatore di $(Z_n, +)$ se, e solo se, é coprimo con n .

PROPOSIZIONE 20 Ogni sottogruppo del gruppo additivo $(Z_n, +)$ é ciclico ed ha ordine divisibile per n .

DIM. Assumiamo $Z_n = \{0, 1, 2, \dots, n - 1\}$, sia H un sottogruppo non nullo di $(Z_n, +)$ e sia h il piú piccolo intero positivo contenuto in H . Ovviamente risulta $\langle h \rangle \leq H$. Sia ora m un elemento di H e siano q, r il quoziente e il resto della divisione fra m ed h . Poiché risulta $m - qh = r$ e $m, qh \in H$, l'intero r , che é minore di h , appartiene ad H . Ne segue che $r = 0$, cioè $H \leq \langle h \rangle$, e in definitiva abbiamo $H = \langle h \rangle$. Ora, dalla proposizione precedente abbiamo che l'ordine di H divide n e l'asserto é provato.

Le ultime due proposizioni hanno il seguente corollario.

COROLLARIO 21 Sia $(Z_n, +)$ il gruppo additivo degli interi modulo n ed h un divisore positivo di n . Allora $(Z_n, +)$ contiene un unico sottogruppo d'ordine h .

DIM. Posto $Z_n = \{0, 1, 2, \dots, n - 1\}$ e $n = hk$, il sottogruppo $\langle k \rangle$ generato da k ha ordine h . Sia ora H un sottogruppo di Z_n d'ordine h . Sappiamo che H é ciclico e che il periodo di un suo generatore m é h , per cui $hm \equiv 0 \pmod{n}$. Ne segue che esiste un intero q tale che $hm = qn$, da cui $m = qk \in \langle k \rangle$. Allora risulta $H \subseteq \langle k \rangle$ e, essendo sia H che $\langle k \rangle$ d'ordine h , risulta $H = \langle k \rangle$. L'asserto é dunque completamente provato.

sottogruppi di $(Z_n, +)$

OSSERVAZIONE 22 Notiamo esplicitamente che, se assumiamo $Z_n = \{0, 1, 2, \dots, n-1\}$, e h é un intero positivo che divide n , posto $n = hk$, il sottogruppo ciclico generato da h in $(Z_n, +)$ ha ordine k ed é dato da

$$\langle h \rangle = \{0, h, 2h, \dots, (k-1)h\}.$$

L'applicazione

$$m \in Z_k = \{0, 1, \dots, k-1\} \rightarrow mh \in \langle h \rangle$$

é evidentemente un isomorfismo fra i gruppi $(Z_k, +)$ e $\langle h \rangle$ e, per questo motivo nel seguito $\langle h \rangle$ sará impropriamente denotato con Z_k .

il gruppo simmetrico S_n

DEFINIZIONE 23 Sia X un insieme finito e non vuoto con n elementi. Una *permutazione su X* é una qualsiasi applicazione biunivoca di X su se stesso. Tutte le permutazioni su X formano un gruppo, che abbiamo denotato con $Symm(X)$ e che si chiama *gruppo simmetrico su n oggetti, o di grado n* .

OSSERVAZIONE 24 Se Y é un insieme non vuoto con n elementi e f é una funzione biunivoca di X su Y , allora l'applicazione

$$\sigma \in S(X) \rightarrow f^{-1}\sigma f \in S(Y)$$

é un isomorfismo di gruppi. Pertanto, il gruppo $S(X)$, a meno di isomorfismi, dipende solo dal numero di elementi di X .

Per non appesantire le notazioni supporremo sempre

$$X = N_n = \{1, 2, \dots, n\}$$

e denoteremo con S_n il gruppo $Symm(X)$.

Una permutazione $\sigma \in S_n$ puó rappresentarsi mediante la matrice

$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix},$$

che ha nella prima riga gli interi da 1 ad n disposti in ordine crescente e sotto ognuno di essi l'intero corrispondente in σ . Con questa notazione, la matrice

$$\begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{bmatrix}$$

rappresenta la permutazione identica.

esempi

ESEMPIO 25 Le permutazioni σ e τ di $N_4 = \{1, 2, 3, 4\}$ definite da

$$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 1 ;$$

$$\tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 2$$

si scrivono

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}.$$

In questo modo se, per esempio, vogliamo calcolare l'immagine di 2 nel prodotto $\sigma\tau$, basta leggere l'intero sotto 2 nella tabella di σ , nel nostro caso 3, e poi l'intero sotto 3 nella tabella di τ ; abbiamo così $\sigma\tau(2) = \tau(\sigma(2)) = 1$.

ESEMPIO 26 Si riportano di seguito tutti gli elementi del gruppo simmetrico S_3 :

$$1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad r_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad r_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$s_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad s_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad s_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$