

gruppi

DEFINIZIONE 1 Un gruppo G si dice *periodico*, o *di torsione*, se ogni suo elemento é periodico. G si dice *aperiodico*, o *senza torsione*, se ogni suo elemento diverso da 1 é aperiodico. G si dice *misto* se possiede sia elementi periodici diversi da 1 che elementi aperiodici.

ESEMPI 2

- I gruppi finiti sono periodici.
- I gruppi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono aperiodici.
- I gruppi (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{C}^*, \cdot) sono misti.

PROPOSIZIONE 3 In un gruppo ogni elemento é regolare, cioè in esso vale la legge di cancellazione.

PROPOSIZIONE 4 Sia G un gruppo tale che $a^2 = 1$, per ogni $a \in G$. Allora G é abeliano.

DIM. Se $a, b \in G$, abbiamo

$$aabb = a^2b^2 = 1 \cdot 1 = 1 = (ab)^2 = abab$$

e dalla legge di cancellazione ricaviamo $ab = ba$.

ESERCIZIO 5 Provare che un gruppo G é abeliano se, e solo se, risulta

$$(ab)^{-1} = a^{-1}b^{-1}, \text{ per ogni } a, b \in G.$$

ESERCIZIO 6 Provare che un gruppo G é abeliano se, e solo se, risulta

$$(ab)^2 = a^2b^2, \text{ per ogni } a, b \in G.$$

gruppi

ESERCIZIO 7 Siano G un gruppo ed a un suo elemento di periodo 2. Provare che bab^{-1} ha periodo 2, per ogni $b \in G$. Dedurre che, se a é l'unico elemento di G di periodo 2, allora a é un elemento centrale in G .

ESERCIZIO 8 Sia K un campo. Provare che il centro del gruppo $GL(n, K)$ é l'insieme delle matrici scalari non nulle di ordine n .

DEFINIZIONE 9 Siano G un gruppo e a un suo elemento. L'applicazione

$$\tau_a^s : x \in G \rightarrow ax \in G$$

si chiama *traslazione sinistra di ampiezza a* . L'applicazione

$$\tau_a^d : x \in G \rightarrow xa \in G$$

si chiama *traslazione destra di ampiezza a* . Se G é abeliano le traslazioni sinistra e destra di ampiezza a coincidono e, in questo caso, si parla semplicemente di *traslazione di ampiezza a* e la si denota col simbolo τ_a .

ESERCIZIO 10 Provare che, se $\tau_a^s = \tau_a^d$ per ogni elemento a di un gruppo G , allora G é abeliano.

PROPOSIZIONE 11 Ogni traslazione sinistra (destra) di un gruppo G é una permutazione dell'insieme degli elementi di G .

DIM. Sia $a \in G$ e si supponga $\tau_a^s(x) = \tau_a^s(y)$, con $x, y \in G$. Allora risulta $ax = ay$ e, per la legge di cancellazione, $x = y$; cioè τ_a^s é iniettiva. Inoltre, per ogni $y \in G$, risulta $\tau_a^s(a^{-1}y) = y$; cosí τ_a^s é anche suriettiva e quindi biunivoca.

anelli

DEFINIZIONE 12 Una struttura algebrica con due operazioni interne (*addizione e moltiplicazione*) $A = (A, +, \cdot)$ si chiama *anello* se sono verificate le seguenti proprietà:

1. $(A, +)$ é un gruppo abeliano,
2. (A, \cdot) é un semigruppó,
3. la moltiplicazione é distributiva rispetto all'addizione.

L'anello A si dice *commutativo* se la moltiplicazione é commutativa, si dice *unitario* se la moltiplicazione ammette elemento neutro 1.

ESEMPI 13

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ sono anelli commutativi unitari.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono anelli commutativi unitari.
- $(\mathbb{Z}[x], +, \cdot)$, $(\mathbb{Q}[x], +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{C}[x], +, \cdot)$ sono anelli commutativi unitari.
- $(M_n(\mathbb{Z}), +, \cdot)$, $(M_n(\mathbb{Z}_m), +, \cdot)$, $(M_n(\mathbb{Q}), +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot)$, $(M_n(\mathbb{C}), +, \cdot)$ sono anelli unitari non commutativi.
- $(2\mathbb{Z}, +, \cdot)$ é un anello commutativo privo di unitá.

anelli

OSSERVAZIONE 14 In un anello $(A, +, \cdot)$ valgono le seguenti proprietà, per ogni $a, b, c \in A$ e $n \in \mathbb{Z}$.

- $a0 = 0a = 0$,
- $a(-b) = (-a)b = -ab$,
- $(-a)(-b) = ab$,
- $(na)b = a(nb) = n(ab)$,
- $a(b - c) = ab - ac$ e $(b - a)c = bc - ac$.

OSSERVAZIONE 15 Se in un anello unitario A risulta $1 = 0$, abbiamo:

$$a = a1 = a0 = 0, \text{ per ogni } a \in A \Rightarrow A = \{0\}.$$

L'anello $A = \{0\}$ si chiama *anello nullo*.

Nel seguito A denoterà un anello che, tranne esplicito avviso, supporremo sempre non nullo.

DEFINIZIONE 16 Sia $a \in A$ con $a \neq 0$. L'elemento a si dice *divisore sinistro (destro) dello zero* se esiste in A un elemento $b \neq 0$ tale che $ab = 0$ ($ba = 0$.) L'elemento a si dice *divisore dello zero* se è divisore sia sinistro che destro dello zero.

ESERCIZIO 17 *Provare che in un anello esiste un divisore sinistro dello zero se, e solo se, esiste un divisore destro dello zero.*

DEFINIZIONE 18 Un elemento $a \in A$ si dice *nilpotente* se esiste un intero positivo n tale che $a^n = 0$.

anelli

OSSERVAZIONE 19 Un elemento nilpotente a di un anello é anche un divisore sinistro dello zero. Possono però esistere elementi non nilpotenti che sono divisori sinistri dello zero. Ad esempio, per l'elemento $3 \in \mathbb{Z}_{21}$, abbiamo $3 \cdot 7 = 0$ e $3^n \neq 0$ per ogni intero positivo n .

DEFINIZIONE 20 Un anello non nullo privo di divisori sinistri dello zero si chiama *anello integro*. Un anello integro commutativo si chiama *dominio di integritá*.

DEFINIZIONE 21 Sia A unitario. Un elemento $a \in A$ si dice *invertibile* se é tale nel semigruppò (A, \cdot) .

OSSERVAZIONE 22 L'insieme degli elementi invertibili di un anello unitario A si denota con $U(A)$ ed é un gruppo rispetto alla moltiplicazione. In particolare é un gruppo moltiplicativo l'insieme $U(n)$ degli elementi invertibili di \mathbb{Z}_n .

DEFINIZIONE 23 Un anello unitario A si chiama *corpo* se é non nullo e ogni suo elemento non nullo é invertibile, cioè se $U(A) = A \setminus \{0\}$. Un corpo commutativo si chiama *campo*.

ESEMPIO 24 Le strutture algebriche $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e $(\mathbb{Z}_p, +, \cdot)$, con p primo, sono esempi di campi. Daremo nel seguito (*cfr.??*) un esempio di corpo (non commutativo).

Riportiamo senza dimostrazione il seguente importante teorema.

TEOREMA 25 (teorema di Wedderburn) *Ogni corpo finito é un campo.*

anelli

DEFINIZIONE 26 Sia A un anello per cui non esiste alcun intero positivo n tale che $na = 0$, per ogni elemento a di A . Allora si dice che A ha *caratteristica zero*. Nel caso contrario, il minimo intero positivo c per cui $ca = 0$, per ogni elemento a di A , prende il nome di *caratteristica di A* .

OSSERVAZIONE 27 L'anello nullo é l'unico anello di caratteristica 1.

ESERCIZIO 28 *Provare che:*

- Z, Q, R, C , hanno *caratteristica zero*;
- Z_m ha *caratteristica m* ;
- $M_n(A)$, $A = Z, Q, R, C, Z_m$, ha *la stessa caratteristica di A* ;
- $A[x]$, $A = Z, Q, R, C, Z_m$, ha *la stessa caratteristica di A* .

ESERCIZIO 29 *Sia K un campo. Provare che l'insieme $M_n(K)$ delle matrici quadrate d'ordine n su K é un anello commutativo unitario rispetto alle operazioni di addizione e di moltiplicazione righe per colonne. Provare, inoltre, che $M_n(K)$ ha la stessa caratteristica di K .*

sottogruppi di un gruppo G

DEFINIZIONE 30 Un sottoinsieme H di G si chiama *sottogruppo* se é una parte stabile e se é un gruppo rispetto all'operazione indotta in esso da G . Per un sottogruppo H di G si usa la notazione $H \leq G$.

OSSERVAZIONE 31 Una parte stabile di un gruppo non é necessariamente un sottogruppo. Per esempio, nel gruppo additivo degli interi, il sottoinsieme N_0 degli interi non negativi é una parte stabile ma non é un sottogruppo.

OSSERVAZIONE 32 Ogni gruppo G possiede due sottogruppi *banali* : $\{1\}$ (*sottogruppo identico*) e G . Un sottogruppo H diverso da G si dice *proprio* e per esso si usa la notazione $H < G$. Valgono, inoltre, le seguenti proprietá:

- l'unitá di H coincide con l'unitá di G ;
- l'inverso in H di un suo elemento a coincide con l'inverso di a in G ;
- $HH = \{ab : a, b \in H\} = H$.

PROPOSIZIONE 33 (test di sottogruppo) In un gruppo G valgono le seguenti equivalenze:

- $H \leq G \Leftrightarrow \left\{ \begin{array}{l} H \text{ stabile,} \\ a \in H \Rightarrow a^{-1} \in H \end{array} \right\} ;$
- $H \leq G \Leftrightarrow a^{-1}b \in H, \text{ per ogni } a, b \in H.$

sottogruppi di un gruppo

PROPOSIZIONE 34 (test di sottogruppo finito) In un gruppo G vale la seguente equivalenza:

$$H \leq G, H \text{ finito} \Leftrightarrow H \text{ sottoinsieme finito e stabile di } G.$$

DIM. Sia H un sottoinsieme finito e stabile di G . Se $b \in H$, risulta

$$bH = \{ba : a \in H\} \subseteq HH = H.$$

D'altra parte, l'applicazione

$$a \in H \rightarrow ba \in H$$

é iniettiva, onde $|bH| = |H|$ e quindi $bH = H$. Ne segue che esiste un elemento $e \in H$ tale che $be = b$, da cui ricaviamo che $e = 1$ e $1 \in H$.

Ora, poiché $1 \in H = bH$, esiste un elemento $c \in H$ tale che $bc = 1$, così $c = b^{-1}$ e abbiamo che $b^{-1} \in H$, per ogni $b \in H$. Ne segue che H é un sottogruppo di G .

ESEMPI 35 I seguenti sottoinsiemi sono sottogruppi di G :

- $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, per ogni $a \in G$.
- Il centro $Z(G)$ di G .

ESERCIZIO 36 Provare che gli insiemi

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

sono sottogruppi di $GL(2, \mathbb{Q})$.

ESERCIZIO 37 Sia $H \leq G$. Provare che ogni sottogruppo di H é anche un sottogruppo di G .

esercizi

ESERCIZIO 38 *Provare che*

$$H = \{2^n : n \in \mathbb{Z}\} \quad \text{e} \quad K = \left\{ \frac{1+2n}{1+2m} : n, m \in \mathbb{Z} \right\}$$

sono sottogruppi del gruppo moltiplicativo Q^ dei razionali.*

ESERCIZIO 39 *Provare che $H = \{0, 4, 8, 12\}$ é un sottogruppo del gruppo additivo di Z_{16} .*

ESERCIZIO 40 *Siano G_1 e G_2 due gruppi e $f: G_1 \rightarrow G_2$ un monomorfismo. Provare che $f(G_1)$ é un sottogruppo di G_2 isomorfo a G_1 .*

ESERCIZIO 41 *Se X é un sottoinsieme non vuoto di un gruppo G , si ponga*

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

ove X^{-1} denota l'insieme i cui elementi sono gli inversi degli elementi di X . Provare che:

(1) *$C(X)$ é un sottogruppo di G contenente X ,*

(2) *ogni sottogruppo K di G contenente X contiene $C(X)$.*

ESERCIZIO 42 *Provare che l'unione di una catena (rispetto all'inclusione) di sottogruppi di un gruppo é un sottogruppo.*