

Gruppo

Definizione

Un **gruppo** è un insieme G munito di una operazione binaria $*$, che ad ogni coppia di elementi a, b di G associa un elemento, che indichiamo con $a * b$, appartenente a G , rispettando i seguenti assiomi:

1. proprietà associativa: dati a, b, c appartenenti a G , vale $(a * b) * c = a * (b * c)$.
2. esistenza dell'elemento neutro: esiste in G un elemento *neutro* e rispetto all'operazione $*$, cioè tale che $a * e = e * a = a$ per ogni a appartenente a G .
3. esistenza dell'inverso: ad ogni elemento a di G è associato un elemento b , detto inverso di a , tale che $a * b = b * a = e$.

Un gruppo si chiama **commutativo** (o abeliano) se vale anche $a * b = b * a$ per ogni coppia a, b di elementi di G .

Esempi di gruppo

Numeri

I numeri interi

$$\mathbb{Z} = \{ \dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots \}$$

con l'operazione di somma "+" formano un gruppo abeliano. È importante evidenziare che la struttura di gruppo consiste di due oggetti: un insieme (gli interi) e una operazione (la somma). Il gruppo è quindi identificato dalla coppia

$$(\mathbb{Z}, +).$$

Ad esempio, i numeri interi *non* formano un gruppo con l'operazione di moltiplicazione: la moltiplicazione è associativa e ha un elemento neutro 1, ma la maggior parte degli elementi non ha una inversa: non esiste nessun intero che moltiplicato per 2 dia come risultato 1. Gli interi con il prodotto formano un monoide commutativo.

Anche i numeri razionali, i numeri reali e i numeri complessi formano un gruppo con l'operazione somma. Si ottengono quindi tre altri gruppi

$$(\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +).$$

I numeri razionali, privati dello zero, formano un gruppo con la moltiplicazione. Un numero razionale diverso da zero è infatti identificato da una frazione a/b con $a \neq 0$, il cui inverso (rispetto alla moltiplicazione) è la frazione b/a . Analogamente, i numeri reali o complessi senza lo zero formano un gruppo con la moltiplicazione. Un insieme numerico privato dello zero è generalmente indicato con un asterisco; sono quindi gruppi le coppie seguenti:

$$(\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

Questa costruzione non funziona con i numeri interi: ciò è correlato al fatto che i razionali, reali o complessi formano un [campo](#) con le operazioni di somma e prodotto, mentre gli interi formano soltanto un [anello](#).

Tutti i gruppi numerici descritti sono commutativi.

Permutazioni

Le [permutazioni](#) di un insieme fissato X formano un gruppo assieme all'operazione di [composizione di funzioni](#). Questo gruppo è noto come [gruppo simmetrico](#) ed è generalmente indicato con $S(X)$. Ad esempio, se X è un insieme di lettere

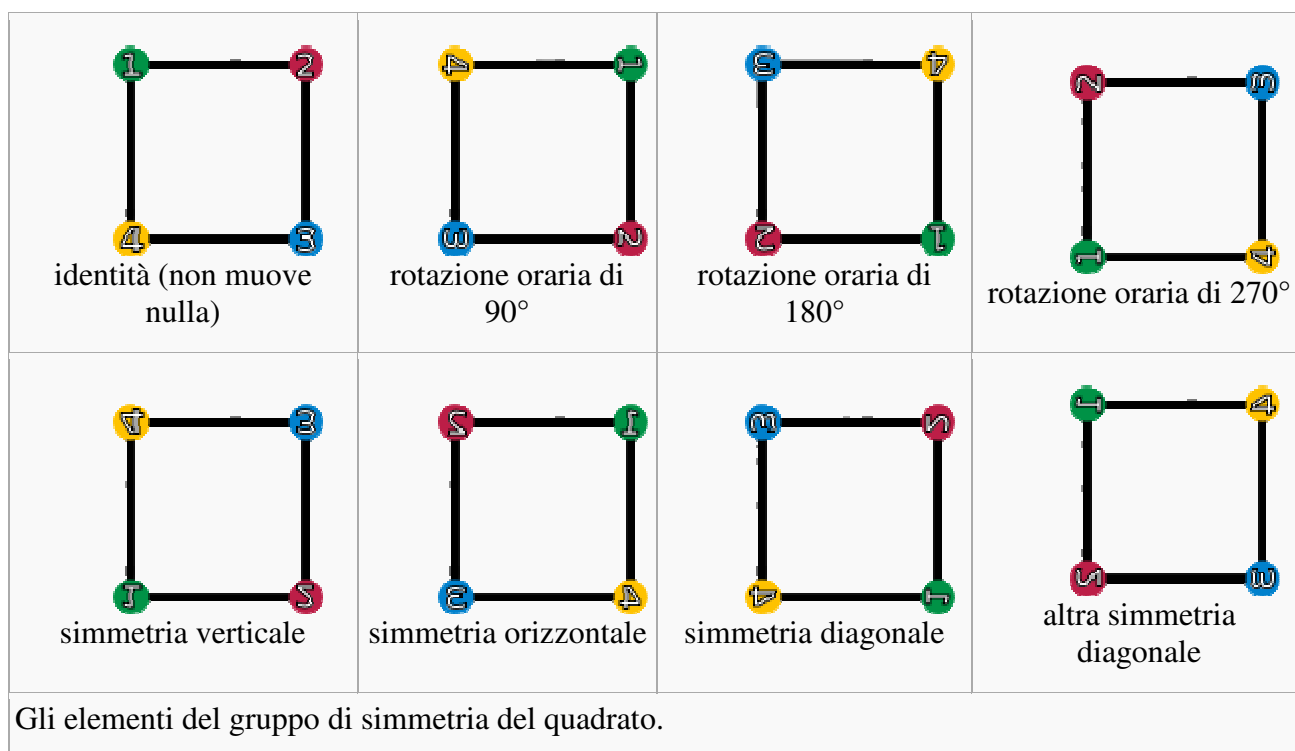
$$X = \{A, B, C\}$$

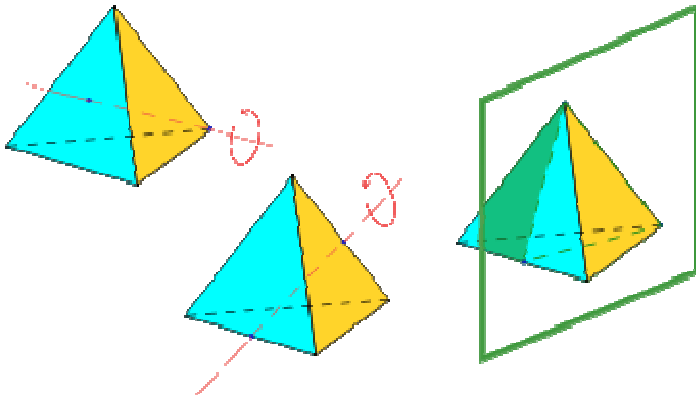
una permutazione può essere descritta da una parola nelle tre lettere A,B,C, senza ripetizioni. Ad esempio, la parola ACB indica una permutazione delle ultime due lettere (detta [trasposizione](#)), mentre la parola BAC indica una trasposizione delle prime due. Il gruppo $S(X)$ consta quindi di sei elementi: ABC, ACB, BAC, BCA, CAB, CBA.

Il gruppo simmetrico su 3 elementi S_3 è il più piccolo esempio di gruppo non abeliano. Componendo le due permutazioni ACB e BAC in due modi diversi si ottengono infatti permutazioni differenti.

Gruppi di simmetria

Le [simmetrie](#) di un oggetto geometrico formano sempre un gruppo. Ad esempio, le simmetrie di un [poligono regolare](#) formano un gruppo finito detto [gruppo diedrale](#). Le simmetrie di un [quadrato](#) sono mostrate qui sotto.





Le simmetrie di un tetraedro sono 24: oltre all'identità, ci sono 11 rotazioni intorno ad un asse, 6 riflessioni rispetto ad un piano e altre 6 operazioni ottenute componendo rotazioni e riflessioni.

Anche le simmetrie di un [poliedro](#) formano un gruppo finito. Di particolare importanza sono i gruppi di simmetria dei [solidi platonici](#). Ad esempio, il gruppo di simmetria del [tetraedro](#) consta di 24 elementi.

Algebra lineare

L'[algebra lineare](#) fornisce molti gruppi, generalmente infiniti. Innanzitutto, uno [spazio vettoriale](#) come ad esempio lo [spazio euclideo](#) \mathbf{R}^n di dimensione n è un gruppo abeliano con la usuale somma fra vettori.

Anche le [matrici](#) con m righe e n colonne sono un gruppo abeliano con la somma. Come per gli insiemi numerici, in alcuni casi è anche possibile costruire degli insiemi di matrici che formano un gruppo con il [prodotto fra matrici](#). Tra questi,

- Il [gruppo generale lineare](#) formato da tutte le matrici quadrate [invertibili](#).
- Il [gruppo ortogonale](#) formato dalle matrici quadrate [ortogonali](#).

Anello

Definizione formale [\[modifica\]](#)

L'insieme A , dotato di due operazioni binarie $+$ e \cdot , è un **anello** se valgono i seguenti [assiomi](#):

$(A, +)$ è un [gruppo abeliano](#) con elemento neutro 0 :

- $(a + b) + c = a + (b + c)$
- $a + b = b + a$
- $0 + a = a + 0 = a$
- $\exists a \exists (-a)$ tale che $a + (-a) = -a + a = 0$

(A, \cdot) è un [semigrupp](#) (cioè la moltiplicazione è associativa):

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

La moltiplicazione è distributiva rispetto alla somma:

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

(le relazioni devono valere per ogni a, b e c in A)

Come per i numeri, il simbolo \cdot per la moltiplicazione è spesso omissivo.

Spesso vengono studiati anelli che posseggono ulteriori proprietà: se anche la moltiplicazione è commutativa, A è detto anello commutativo, se ammette un elemento neutro allora l'anello è unitario.

Un corpo è un anello con unità i cui elementi non nulli hanno inverso moltiplicativo.

Un campo è un corpo commutativo.

Esempi

L'esempio più basilare della struttura di anello è l'insieme \mathbb{Z} dei numeri interi, dotato delle usuali operazioni di somma e prodotto. Tale anello è commutativo ed è un dominio d'integrità. L'insieme dei numeri naturali non è invece un anello, perché non esistono gli inversi rispetto all'addizione.

Allo stesso modo, l'insieme $A[x]$ dei polinomi con variabile x e coefficienti in un anello A formano un anello con le usuali operazioni di somma e prodotto fra polinomi. Tale anello eredita molte proprietà da quelle di A , quali la commutatività e l'assenza di divisori dello 0. Anche l'insieme $F(X, A)$ delle funzioni da un insieme qualsiasi X ad un anello A forma un altro anello con le usuali operazioni di somma e prodotto fra funzioni punto a punto, definite nel modo seguente:

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

Un anello non commutativo è invece l'anello delle matrici $n \times n$ a valori in un anello A (indicato con $M(n, A)$), con le operazioni di somma e prodotto fra matrici. Generalmente questo anello possiede anche dei divisori dello zero. Ad esempio, in $M(2, \mathbf{R})$ valgono le relazioni:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}.$$

e

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

L'esempio più importante di corpo non commutativo è il corpo \mathbb{H} dei quaternioni, mentre gli insiemi \mathbb{Q} (numeri razionali), \mathbb{R} (numeri reali) e \mathbb{C} (numeri complessi) sono esempi di campi.