

Note di Matematica Discreta

GRUPPI

Un gruppo G è un insieme su cui è definita una *operazione binaria* $*$, cioè un'applicazione

$$\begin{aligned} * : G \times G &\rightarrow G \\ (x, y) &\mapsto x * y, \end{aligned}$$

che soddisfi le seguenti proprietà:

- (1) $*$ è associativa ovvero

$$\forall x, y, z \in G \quad (x * y) * z = x * (y * z)$$

- (2) esiste in G un elemento neutro rispetto a $*$ cioè

$$\exists e \in G : \forall x \in G \quad x * e = x = e * x$$

- (3) ogni elemento di G ha un inverso rispetto all'operazione $*$ cioè

$$\forall x \in G \exists \bar{x} \in G : \quad x * \bar{x} = e = \bar{x} * x$$

Osservazioni.

- Il fatto che $*$ sia una applicazione da $G \times G$ in G implica, in particolare, che per ogni x, y in G , $x * y \in G$.
- L'operazione $*$ non è necessariamente commutativa. Se questo accade cioè se

$$\forall x, y \in G \quad x * y = y * x$$

allora diciamo che il gruppo è commutativo (o *abeliano*).

- Osserviamo senza dimostrarlo che l'elemento neutro di un gruppo è unico così come, fissato arbitrariamente x in G , l'inverso di x è unico.

ESEMPI

1) L'insieme degli interi \mathbb{Z} con la somma è un gruppo con elemento neutro 0 e, per ogni $n \in \mathbb{Z}$, l'inverso di n è $-n$. La somma è commutativa così abbiamo un esempio di gruppo abeliano.

2) In analogia al caso 1) sono gruppi abeliani anche i razionali \mathbb{Q} rispetto alla somma e i reali \mathbb{R} rispetto alla somma.

3) L'insieme dei razionali non nulli, \mathbb{Q}^* rispetto alla moltiplicazione è un gruppo abeliano con elemento neutro 1 e, fissato arbitrariamente $\frac{m}{n} \in \mathbb{Q}^*$, il suo inverso è $\frac{n}{m}$. Notiamo che, poichè $\frac{m}{n} \neq 0$ risulta $m \neq 0$ e $n \neq 0$ così ha senso considerare $\frac{n}{m}$.

4) In modo analogo al caso 3) i numeri reali non nulli formano un gruppo rispetto alla moltiplicazione. Notiamo anche che i numeri interi non nulli non formano un gruppo rispetto alla moltiplicazione.

5) L'insieme Z_n delle classi di resto nella congruenza modulo n formano un gruppo rispetto alla somma definita come

$$[a] + [b] = [a + b]$$

Ponendo $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ abbiamo che l'elemento neutro è la classe $[0]$ mentre l'inverso della classe $[i]$ è la classe $[n-i]$. Di nuovo si tratta di un gruppo commutativo.

6) Il gruppo S_n delle permutazioni su n oggetti. Sia X l'insieme $\{1, 2, \dots, n\}$. Una permutazione di X è una applicazione biettiva di X in se stesso. Sia S_n l'insieme di tutte le permutazioni di X , pertanto:

$$S_n = \{\sigma : X \rightarrow X : \sigma \text{ è una biiezione}\}$$

Affermiamo che S_n è un gruppo rispetto all'operazione composizione di applicazioni:

$$\begin{aligned} \circ : S_n \times S_n &\rightarrow S_n \\ (\sigma, \tau) &\rightarrow \sigma \circ \tau : \begin{array}{ccc} X & \rightarrow & X \\ k & \rightarrow & (\sigma \circ \tau)(k) = \sigma(\tau(k)) \end{array} \end{aligned}$$

Infatti la composizione definisce una operazione binaria in S_n perchè se σ e τ sono due permutazioni di X allora anche $\sigma \circ \tau$ lo è. Inoltre la composizione di applicazioni è associativa e l'applicazione identica

$$\begin{aligned} \iota : X &\rightarrow X \\ k &\rightarrow k \end{aligned}$$

è l'elemento neutro rispetto alla composizione. Infine se σ è una permutazione di X , l'applicazione inversa σ^{-1} è ancora una permutazione di X .

Determiniamo il numero di elementi di S_n , cioè il numero di permutazioni di X . Osserviamo innanzitutto che una funzione da X in X che sia iniettiva è anche suriettiva e pertanto è una permutazione. Infatti se $f : X \rightarrow X$ è una funzione iniettiva allora la sua immagine, $Im(f)$, è un sottoinsieme di n elementi contenuto in X . Ne segue che $Im(f) = X$, ovvero f è anche suriettiva. Si tratta allora di contare le applicazioni iniettive da X in sé. Una funzione iniettiva $\sigma : X \rightarrow X$ è assegnata una volta che sono assegnati i valori $\sigma(k)$, per $k = 1 \dots n$. Ora per il valore $\sigma(1)$ abbiamo n scelte possibili, infatti $\sigma(1)$ può essere un valore qualsiasi tra 1 e n . Una volta assegnato il valore $\sigma(1)$, per il valore $\sigma(2)$ abbiamo $n-1$ scelte, infatti $\sigma(2)$ deve essere un valore tra 1 e n diverso da $\sigma(1)$ perchè σ è iniettiva. Procedendo in questo modo abbiamo $n(n-1)(n-2) \dots 2 \cdot 1$ modi di scegliere una funzione iniettiva da X in X e pertanto $n(n-1)(n-2) \dots 2 \cdot 1$ modi di scegliere una permutazione di X .

Per $n \in \mathbb{N}$, si definisce *fattoriale* di n e si indica con $n!$ il numero

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$$

Il gruppo S_n ha ordine $n!$ e si tratta di un gruppo non commutativo.

Per semplificare la notazione per un gruppo generico G indichiamo la sua operazione con il simbolo del prodotto \cdot (e spesso ometteremo anche di scriverlo), l'elemento neutro con 1 e l'inverso dell'elemento x con x^{-1} . Per un gruppo G abeliano l'operazione si indica usualmente con il simbolo della somma, $+$, l'elemento neutro con 0 e l'inverso di un elemento x in G con l'opposto, $-x$.

Un anello A è un insieme non vuoto dotato di due operazioni binarie, che indichiamo con somma e prodotto

$$\begin{aligned} + : A \times A &\rightarrow A \\ (x, y) &\mapsto x + y, \end{aligned}$$

e

$$\begin{aligned} \cdot : A \times A &\rightarrow A \\ (x, y) &\mapsto x \cdot y, \end{aligned}$$

che soddisfi le seguenti proprietà. L'insieme A rispetto alla operazione di somma è un gruppo abeliano, cioè:

- (1) per ogni a, b e c in A , $a + (b + c) = (a + b) + c$,
- (2) esiste un elemento $0 \in A$ tale che, per ogni $a \in A$, $a + 0 = a = 0 + a$,
- (3) per ogni a in A esiste un elemento $-a \in A$ tale che $a + (-a) = 0 = (-a) + a$,
- (4) per ogni $a, b \in A$, si ha $a + b = b + a$.

Inoltre l'operazione prodotto è associativa e distributiva rispetto alla somma, cioè:

- (1) per ogni $a, b, c \in A$, si ha $(ab)c = a(bc)$;
- (2) per ogni $a, b, c \in A$, si ha $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$.

Un anello A si dice poi commutativo se l'operazione prodotto è commutativa, cioè se per ogni $a, b \in A$ si ha $ab = ba$ e si dice unitario se esiste un elemento neutro rispetto all'operazione prodotto, cioè se esiste un elemento $u \in A$ tale che per ogni $a \in A$ risulti $a \cdot u = a = u \cdot a$. L'elemento u si indica con 1.

ESEMPI

- (1) L'insieme \mathbb{Z} dei numeri interi, con le usuali operazioni di somma e prodotto, è un anello commutativo e unitario. Analogamente son anelli rispetto alle usuali operazioni di somma e prodotto, gli insiemi \mathbb{Q} ed \mathbb{R} .
- (2) Per n naturale, l'insieme delle classi di resto \mathbb{Z}_n , con le operazioni di somma e prodotto definite da:

$$[a]_n + [b]_n = [a + b]_n \quad [a]_n \cdot [b]_n = [a \cdot b]_n$$

è un anello commutativo e unitario (con unità $[1]_n$).

ELEMENTI SPECIALI DI UN ANELLO

Sia A un anello commutativo unitario. Un elemento $a \in A$ si dice *invertibile* se esiste $b \in A$ tale che

$$ab = 1 = ba$$

L'elemento b si dimostra essere unico e si indica con a^{-1} .

ESEMPI

In \mathbb{Z} gli elementi invertibili sono $\{1, -1\}$. In \mathbb{Q} ogni elemento non nullo $\frac{n}{m}$ è invertibile, con inverso $\frac{m}{n}$. In $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ gli elementi invertibili sono tutti e soli gli elementi $[a]_n$ con $(a, n) = 1$. \diamond

Sia A un anello commutativo unitario. Un elemento $a \in A$ si dice un *divisore dello zero* se $a \neq 0$ ed esiste $b \in A$, con $b \neq 0$, tale che $ab = 0 = ba$.

ESEMPIO

In \mathbb{Z}_{12} l'elemento $[3]_{12}$ è un divisore dello zero infatti $[3]_{12} \cdot [4]_{12} = [0]$ con $[3]_{12} \neq [0]_{12}$ e $[4]_{12} \neq [0]_{12}$.

Una osservazione. Un elemento invertibile a di un anello A non è mai un divisore dello zero. Infatti se lo fosse esisterebbe $b \in A$ con $ab = 0 = ba$. Ma a è invertibile, dunque $1 = aa^{-1}$. Moltiplicando questa ultima uguaglianza per b si trova che $b = b \cdot 1 = b(aa^{-1}) = (ba)a^{-1} = 0$. contro l'ipotesi che $b \neq 0$.

Descriviamo gli elementi invertibili e i divisori dello zero di \mathbb{Z}_n . abbiamo già visto che una classe $[a]_n \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$. Sia ora $[a]_n \in \mathbb{Z}_n$ con $1 \leq a \leq n-1$ e $(a, n) = d > 1$. Considero $b = \frac{n}{d}$ sicchè b è un intero e $1 < b < n$. Inoltre

$$[a]_n [b]_n = [ab]_n = [a \frac{n}{d}]_n = [\frac{a}{d} n]_n = [0]_n.$$

Abbiamo trovato allora che $[a]_n$ è un divisore dello zero. Riassumendo in \mathbb{Z}_n ogni elemento $[a]_n$ (diverso da $[0]_n$) o è invertibile o è un divisore dello zero. Inoltre $[a]_n$ è invertibile se e solo se $(a, n) = 1$ e $[a]_n$ è un divisore dello zero se e solo se n non divide a e $(a, n) \neq 1$.