Gruppi

Sono note allo studente alcune *operazioni* elementari sugli insiemi numerici; ad esempio l'addizione e la moltiplicazione su $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Ciò che tali operazioni hanno in comune è il seguente fatto: ad ogni coppia di numeri viene associato un altro numero (il risultato dell'operazione). Questa semplice osservazione è alla base della seguente definizione di *operazione su un insieme*.

DEFINIZIONE **1**. *Sia A un insieme non vuoto. Sia*

$$A \times A = \{(a,b),\ \forall\, a \in A,\ \forall\, b \in A\}$$

il prodotto cartesiano di A per se stesso. Ogni applicazione

$$* : A \times A \to A$$

è detta ***operazione su*** *A. L'operazione $*$ associa quindi ad ogni coppia $(a,b) \in A \times A$ la sua immagine $*(a,b)$, che, per semplificare le notazioni, denoteremo con $a * b$. L'operazione $*$ è detta:*

(i) ***associativa****, se risulta:*

$$a * (b * c) = (a * b) * c, \quad \forall\, a,b,c \in A;$$

(ii) ***commutativa****, se risulta:*

$$a * b = b * a, \quad \forall\, a,b \in A.$$

Inoltre:

(iii) l'operazione $*$ ***ammette elemento neutro*** *$e \in A$, se risulta:*

$$a * e = e * a = a, \quad \forall\, a \in A;$$

(iv) l'operazione $*$ ***ammette reciproco*** *(o* ***opposto*** *o* ***inverso****)* ***di ogni elemento*** *se verifica (iii) e se per ogni $a \in A$ esiste $a' \in A$ [dipendente da a] tale che*

$$a * a' = a' * a = e.$$

ESEMPIO **1.** È evidente che l'addizione e la moltiplicazione sono operazioni su $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ verificanti le proprietà $(i),(ii),(iii)$ [con 0 elemento neutro dell'addizione e 1 elemento neutro della moltiplicazione]. Relativamente alla proprietà (iv) si osserva subito che:

(a) l'addizione verifica la proprietà (iv) su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ [il reciproco (o, più propriamente, l'opposto) di a è $-a$] ma non su $\mathbb{N}$ [infatti 1 non ha opposto in $\mathbb{N}$].

(b) la moltiplicazione non verifica la proprietà (iv): infatti 0 non ha reciproco. Ci chiediamo ora cosa avviene se eliminiamo 0. Per $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, denotiamo $A - \{0\}$ con A^*. È evidente che la moltiplicazione verifica la proprietà (iv) come operazione su $\mathbb{Q}^*$, su $\mathbb{R}^*$ e su $\mathbb{C}^*$ [il reciproco (o, meglio, l'inverso) di a è $a^{-1} = \frac{1}{a}$] ma non su $\mathbb{N}^*$ e su $\mathbb{Z}^*$ [infatti ad esempio 2 non ha inverso in $\mathbb{N}^*$ o $\mathbb{Z}^*$].

Veniamo ora alle altre due operazioni elementari: sottrazione e divisione. È evidente che la sottrazione è un'operazione su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (ma non lo è su $\mathbb{N}$) e che la divisione è un'operazione soltanto su $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$. Entrambe le operazioni non verificano alcuna delle proprietà $(i), .., (iv)$.

ESEMPIO **2.** Sia A un insieme non vuoto. Denotiamo con $\mathcal{F}(A)$ l'insieme di tutte le applicazioni di A in sè. Ricordiamo che, $\forall\, f, g \in \mathcal{F}(A)$, si chiama *composizione* (o *prodotto operatorio*) di f e g l'applicazione $g \circ f \in \mathcal{F}(A)$ così definita:

$$(g \circ f)(a) = g(f(a)), \quad \forall\, a \in A.$$

Resta pertanto definita l'operazione di *composizione di applicazioni*:

$$\circ : \mathcal{F}(A) \times \mathcal{F}(A) \to \mathcal{F}(A)$$

tale che:

$$(f, g) \to g \circ f.$$

Tale operazione verifica le proprietà (i) e (iii), cioè è associativa [semplice verifica] ed ammette elemento neutro [che è l'*applicazione identica* (o *identità di* A):

$$\mathbf{1}_A : A \to A \text{ tale che } \mathbf{1}_A(a) = a, \ \forall\, a \in A].$$

Limitiamoci ora a considerare le *applicazioni biunivoche* (o *biiezioni*) su un insieme A e denotiamo con $\mathcal{S}(A)$ l'insieme di tali applicazioni. Poiché la composizione di due biiezioni è ancora una biiezione [semplice verifica], l'operazione $\circ$ si può *restringere* ad $\mathcal{S}(A)$ e dunque è definita l'operazione:

$$\circ : \mathcal{S}(A) \times \mathcal{S}(A) \to \mathcal{S}(A)$$

(*composizione di applicazioni biunivoche*). Tale operazione verifica, oltre alle proprietà (i) e (iii), anche la proprietà (iv). Infatti, assegnata $f \in \mathcal{S}(A)$ e definita l'applicazione $g : A \to A$ tale che:

$$g(a) = b \iff f(b) = a, \quad \forall\, a \in A,$$

si verifica subito che $g \in \mathcal{S}(A)$ e che $g \circ f = f \circ g = \mathbf{1}_A$ [cioè g è l'elemento reciproco di f]. L'applicazione g è usualmente denotata con f^{-1} ed è detta *applicazione inversa di* f.

Con facili esempi si verifica che in generale la composizione di applicazioni (anche biunivoche) non è un'operazione commutativa (cfr. Eserc. **3**).

Gli esempi precedenti ci introducono al concetto di *gruppo*, cioè un insieme dotato di un'operazione verificante le proprietà $(i), (iii)$ e (iv). Riformuliamo questa definizione.

DEFINIZIONE **2.** *Sia A un insieme non vuoto. Sia $*$ un'operazione su A. La coppia $(A,*)$ è un* ***gruppo*** *se valgono i tre seguenti assiomi:*

(G_1) $a*(b*c)=(a*b)*c, \quad \forall a,b,c \in A$ *[proprietà associativa].*

(G_2) $\exists e \in A$ *[**elemento neutro** di A] tale che* $a*e=e*a=a, \quad \forall a \in A.$

(G_3) $\forall a \in A, \ \exists a' \in A$ *[**reciproco** di a] tale che* $a*a'=a'*a=e.$

Il gruppo $(A,*)$ è detto ***gruppo commutativo*** *se vale l'ulteriore assioma:*

(G_4) $a*b=b*a, \quad \forall a,b \in A$ *[proprietà commutativa].*

OSSERVAZIONE **1.** (i) È immediato verificare che in un gruppo $(A,*)$ l'elemento neutro e ed il reciproco a' di ogni elemento $a \in A$ sono unici. Infatti, se e, e' sono due elementi neutri di A, risulta:

$$e'=e*e'=e'*e, \quad e=e'*e=e*e'.$$

Ne segue che $e=e'$. Se poi a', a'' sono due reciproci di a, risulta:

$$a'=a'*e=a'*(a*a'')=(a'*a)*a''=e*a''=a''.$$

Una conseguenza immediata di tale unicità è la seguente formula (la cui verifica è lasciata al lettore):

$$(a*b)'=b'*a', \quad \forall a,b \in A.$$

(ii) In $(A,*)$ valgono le seguenti *regole di cancellazione* (o di *semplificazione*) *a sinistra* e *a destra*:

$$a*b=a*c \implies b=c, \quad a*b=c*b \implies a=c,$$

$\forall a,b,c \in A$. Proviamo la prima [e per la seconda si proceda in modo analogo]. Denotato, al solito, con a' il reciproco di a, si ha:

$$b=e*b=(a'*a)*b=a'*(a*b)=a'*(a*c)=(a'*a)*c=e*c=c.$$

(iii) Spesso i gruppi vengono presentati con *notazione additiva* [l'operazione viene indicata con $+$, l'elemento neutro con 0 ed il reciproco di a con $-a$ (ed è chiamato *opposto*)] ovvero con *notazione moltiplicativa* [l'operazione viene indicata con $\cdot$, l'elemento neutro con 1 ed il reciproco di a con a^{-1} oppure $\frac{1}{a}$ (ed è chiamato *inverso*)]. Tradizionalmente i gruppi presentati con notazione additiva vengono supposti commutativi.

ESEMPIO **3.** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ sono esempi di gruppi commutativi.

2.9. Definizione di campo. Sia S un insieme munito di due operazioni, per la prima delle quali si usi la notazione additiva, $+$, per la seconda la notazione moltiplicativa, $\cdot$. L'insieme S si dice un *campo* rispetto alle due operazioni $+$ e $\cdot$ quando valgono le seguenti proprietà:

α) S è un gruppo commutativo rispetto all'addizione $+$,

β) $S - \{0\}$ è un gruppo commutativo rispetto all'operazione di moltiplicazione $\cdot$,

γ) l'operazione di moltiplicazione è distributiva rispetto all'addizione.