Azzolini Riccardo 2018-10-23

Strutture algebriche

1 Operazione

Dato un insieme non vuoto A, un'**operazione binaria** (o semplicemente **operazione**) su A è una funzione dal prodotto cartesiano $A \times A$ in A:

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

L'immagine della coppia (a, b) tramite $*$ si indica con $a * b$ (*notazione infissa*).

1.1 Esempi

$$+ : (n, m) \in \mathbb{N} \times \mathbb{N} \mapsto n + m \in \mathbb{N}$$
$$+(n, m) = n + m \in \mathbb{N}$$

$$\cup : (X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mapsto X \cup Y \in \mathcal{P}(A)$$

1.2 Rappresentazione come tabella

Se l'insieme A è finito, allora l'operazione $*$ su A si può rappresentare con una tabella:

$$A = \{a_1, a_2, ..., a_n\} \qquad |A| = n$$

$*$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_n$

2 Struttura algebrica

Una **struttura algebrica** è una coppia $(A, *)$, dove A è un insieme e $*$ è un'operazione su A.

Esempi: $(\mathbb{N}, \cdot)$, $(\mathcal{P}(A), \cup)$

3 Proprietà commutativa

Un'operazione $*$ su A è **commutativa** se per ogni $a_1, a_2 \in A$:

$$a_1 * a_2 = a_2 * a_1$$

3.1 Nella tabella

Se un'operazione è commutativa, allora la sua tabella è simmetrica rispetto alla diagonale che va da in alto a sinistra a in basso a destra.

3.2 Esempio su insieme finito

$$A = \{a, b, c\} \qquad * : A \times A \to A$$

$*$	a	b	c
a	a	b	b
b	b	c	a
c	b	a	c

$$a * b = b * a = b$$

$$c * a = a * c = b$$

$$c * b = b * c = a$$

Quindi $*$ è commutativa.

3.3 Esempi sugli insiemi numerici

- Somma e prodotto sono operazioni commutative.
- La sottrazione su $\mathbb{Z}$ non è commutativa:

$$- : (n, m) \in \mathbb{Z} \times \mathbb{Z} \mapsto n - m \in \mathbb{Z}$$
$$n - m \neq m - n$$

- La divisione su $\mathbb{Q}$ non è commutativa:

$$\div : (r, s) \in \mathbb{Q} \times \mathbb{Q} \mapsto \frac{r}{s} \in \mathbb{Q}$$
$$\frac{r}{s} \neq \frac{s}{r}$$

4 Proprietà associativa

Un'operazione $*$ su A è **associativa** se per ogni $a_1, a_2, a_3 \in A$:

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$$

Si può quindi scrivere semplicemente:

$$a_1 * a_2 * a_3$$

4.1 Esempi

- $+$ su $\mathbb{N}$ è associativo:

$$(n + m) + h = n + (m + h) \quad \forall n, m, h \in \mathbb{N}$$

- $\cup$ su $\mathcal{P}(A)$ è associativa:

$$(X \cup Y) \cup Z = X \cup (Y \cup Z) \quad \forall X, Y, Z \in \mathcal{P}(A)$$

- La divisione su $\mathbb{Q}$ non è associativa:

$$r, s, t \in \mathbb{Q} \qquad \frac{\frac{r}{s}}{t} = \frac{r}{st} \qquad \frac{r}{\frac{s}{t}} = \frac{rt}{s}$$

5 Elemento neutro

Un'operazione $*$ su A ammette un **elemento neutro** se esiste un $e \in A$ tale che per ogni $a \in A$:

$$a * e = e * a = a$$

Se esiste, l'elemento neutro di un'insieme A rispetto a un'operazione $*$ è unico.

5.1 Nella tabella

Nella riga e nella colonna della tabella corrispondenti all'elemento neutro, sono presenti tutti gli elementi dell'insieme, nell'ordine in cui sono elencati come etichette delle colonne e delle righe.

5.2 Esempio su insieme finito

$$A = \{a, b, c\} \qquad * : A \times A \to A$$

$*$	a	b	c
a	a	a	b
b	a	b	c
c	c	c	a

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

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

Quindi b è l'elemento neutro di A rispetto a $*$.

5.3 Altri esempi

- L'elemento neutro di $(\mathbb{N}, +)$ e $(\mathbb{Z}, +)$ è 0:

$$\forall n \in \mathbb{N}, \quad n + 0 = n = 0 + n$$

- L'elemento neutro di $(\mathbb{Z}, \cdot)$ è 1:

$$\forall n \in \mathbb{Z}, \quad n \cdot 1 = n = 1 \cdot n$$

- L'elemento neutro di $(\mathcal{P}(A), \cup)$ è $\varnothing$:

$$\forall X \in \mathcal{P}(A), \quad X \cup \varnothing = X = \varnothing \cup X$$

6 Elementi invertibili

Se l'operazione $*$ su A ammette un elemento neutro, allora $a \in A$ si dice **invertibile** se esiste il suo **inverso** $b \in A$ tale che:

$$a * b = b * a = e$$

L'elemento neutro è sempre invertibile ed è inverso di se stesso.

6.1 Nella tabella

Gli elementi invertibili hanno l'elemento neutro sia nella riga che nella colonna corrispondenti della tabella.

6.2 Esempi

- In $(\mathbb{N}, +)$ è invertibile solo 0, l'elemento neutro:

$$0 + 0 = 0$$

- In $(\mathbb{Z}, +)$ (elemento neutro 0), per ogni $n \in \mathbb{Z}$ esiste l'inverso $-n$:

$$\forall n \in \mathbb{Z}, \quad n + (-n) = 0$$

- In $(\mathbb{Z}, \cdot)$ è invertibile solo l'elemento neutro 1: in generale, dato $n \in \mathbb{Z}$, se $n \neq 1$ non esiste $m \in \mathbb{Z}$ tale che $n \cdot m = 1$.
- In $(\mathbb{Q}, \cdot)$ (elemento neutro 1) sono invertibili tutti gli elementi tranne 0:

$$\forall r \in \mathbb{Q}, \quad r \neq 0 \implies r \cdot \frac{1}{r} = 1$$

  0 non è invertibile perché $0 \cdot r = 0 \neq 1$.