

Strutture algebriche

Sia $A \neq \emptyset$ un insieme. Un'operazione bimaria (interna in A) è una qualunque applicazione $f: A \times A \rightarrow A$

Si dice STRUTTURA ALGEBRICA (Semplice) una coppia costituita da un insieme A e da un'operazione bimaria su A : (A, f) .

Consideriamo $\forall m \geq 1 \quad \mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$

In tale insieme possiamo definire una somma:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m \\ ([a]_m, [b]_m) \mapsto [a+b]_m$$

e possiamo anche definire un prodotto:

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m \\ ([a]_m, [b]_m) \mapsto [a \cdot b]_m$$

Sia $(A, *)$ una struttura algebrica.

d'operazione $*$ si dice **COMMUTATIVA** se
 $a * b = b * a \quad \forall a, b \in A$

Si dice **ASSOCIAUTIVA** se $a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$

Un elemento $e \in A$ si dice **NEUTRO** se
 $a * e = a = e * a \quad \forall a \in A \rightarrow \text{È UNICO}$

Un elemento $b \in A$ si dice **SIMMETRICO** di $a \in A$ se
 $a * b = e = b * a$

Un elemento $a \in A$ che possiede almeno un simmetrico si dice **SIMMETRIZZABILE**.

d'insieme di tutti gli elementi simmetrizzabili di $(A, *)$
si denota con

$$\mathcal{U}(a) = \{x \in A : a \text{ è simmetrizzabile}\}$$

$$= \{x \in A : \exists y \in A \text{ con } a * b = \underline{\underline{x}} * a\}$$

Th. Sia $m > 0$ e si consideri la struttura algebrica (\mathbb{Z}_m, \cdot)
allora

$$\mathcal{U}(\mathbb{Z}_m) = \{[a]_m : \text{MCD}(a, m) = 1\}$$

Se $A \supseteq \mathbb{Z}_m$ tutti i numeri ai numeri di A si dicono \mathbb{Z}_m

$$\text{MCD}(a, m) = 1 \Leftrightarrow \text{MCD}(a, m) = 1$$

Se A è finito, dati a_1, \dots, a_m gli elementi di A , si può ricevere la TABELLA MOLTIPLICATIVA di $(A, *)$

*	a_1	a_2	\dots	a_m
a_1	.	.		
a_2	.	.		
a_i	- - -	- - -		- - -
a_m	.	.		.

- L'operazione $*$ è commutativa

↑
la tabella è simmetrica rispetto
alla diagonale principale.

- $a_i \in A$ è neutro rispetto a $*$

↓
la riga e la colonna i -esima
contengono tutti gli elementi di A
nell'ordine scelto

Sia $(A, *)$ una struttura algebrica e sia $B \subseteq A$.

Un sottoinsieme B si dice STABILE (rispetto a $*$) $\Leftrightarrow x + y \in B, \forall x, y \in B$

Una struttura algebrica $(A, *)$ si dice:

SEMI GRUPPO $\stackrel{\text{def}}{\Leftrightarrow} *$ è associativa

MONOIDE $\stackrel{\text{def}}{\Leftrightarrow}$ $\begin{cases} * \text{ è associativa} \\ \exists \text{ el. neutro} \end{cases}$

GRUPPO $\stackrel{\text{def}}{\Leftrightarrow}$ $\begin{cases} * \text{ è associativa} \\ \exists \text{ el. neutro} \\ \text{ogni elemento di } A \text{ è simmetrabile} \end{cases}$

Se $\forall x \in A$ ^{im più} è commutativa si parla di SEMI GRUPPO COMMUTATIVO, o di MONOIDE COMMUTATIVO o di GRUPPO ABELIANO.

Sia $(A, *)$ un semigruppo. Un sottoinsieme $B \subseteq A$ si dice SOTTOSEMI GRUPPO di A $\stackrel{\text{def}}{\Leftrightarrow} B$ è stabile rispetto a $*$

Sia $(A, *)$ un monoide. Un sottoinsieme $B \subseteq A$ si dice

SOTTONOIDE di A $\stackrel{\text{def}}{\Leftrightarrow} \begin{cases} B \text{ è stabile rispetto a } * \\ \forall a \in B \\ \text{elemento neutro di } A \end{cases}$

Sia $(A, *)$ un gruppo. $B \subseteq A$ è un SOTTOGRUPPO di A $\stackrel{\text{def}}{\Leftrightarrow}$

$\begin{cases} B \text{ è stabile rispetto a } * \\ \forall a \in B \\ \text{per ogni elemento } b \in B, \text{ il simmetrico} \\ \text{di } b \in B \end{cases}$

Def.-

ANELLO: struttura algebrica $(A, +, *)$ dotata di $+ : A \times A \rightarrow A$

MOTTO: struttura algebrica $(A, +, \cdot)$ dotata di $+ : A \times A \rightarrow A$
 $\cdot : A \times A \rightarrow A$

$\left\{ \begin{array}{l} (A, +) \text{ gruppo abeliano} \\ (A, \cdot) \text{ semigruppo} \\ \cdot \text{ è distributivo rispetto a } + \end{array} \right.$

poss' essere:

- **COMMUTATIVO** se \cdot è commutativa
- **UNITARIO** $\Leftrightarrow \exists 1 \in A : a \cdot 1 = a = 1 \cdot a \quad \forall a \in A$
- **COMMUTATIVO UNITARIO** $\Leftrightarrow (A, \cdot)$ monoide commutativo

CAMP $\stackrel{\text{def}}{\Leftrightarrow} \forall a \in A \text{ s.t. } \exists a^{-1} \in A : a \cdot a^{-1} = 1$

Esercizi

① Nell'insieme \mathbb{Q} dei numeri razionali, si consideri l'operazione bimaria $*$ definita ponendo

$$a * b = a + b - 4ab$$

- ① Si dimostri che la struttura algebrica $(\mathbb{Q}, *)$ è un monoide commutativo.
- ② Si determinino tutti gli elementi invertibili del monoide $(\mathbb{Q}, *)$.
- ③ Si stabilisca se l'insieme \mathbb{Z}_2 è un sottomonoide di $(\mathbb{Q}, *)$.

①

$(\mathbb{Q}, *)$ MONOIDE COMMUTATIVO $\Leftrightarrow \left\{ \begin{array}{l} * \text{ commutativa} \\ * \text{ associativa} \\ \exists \text{ el. neutro} \end{array} \right.$

* commutativa ($a * b = b * a$)

$$[a * b = a + b - 4ab]$$

$$\forall a, b \in \mathbb{Q} \quad \underline{b * a = b + a - 4ba} = a + b - 4ab = \underline{a * b} \Rightarrow * \text{ è commutativa}$$

* associativa $\rightarrow (a * (b * c)) = (a * b) * c$

$$\begin{aligned} a * (b * c) &= a * \underbrace{(b + c - 4bc)}_b = \underbrace{a + b + c - 4bc - 4a}_{b} (b + c - 4bc) = \\ &= a + b + c - 4bc - 4ab - 4ac + 16abc \end{aligned}$$

$$= a + b + c - 4ab - 4ac + 16abc$$

$$\bullet (a+b)*c = (a+b-4ab)+c = a+b-4ab+c-4c(a+b-4ab) = \\ = a+b+c-4ab-4ac-4cb+16abc$$

Sono uguali $\Rightarrow *$ è associativa

\exists l-mutro ($a+\cancel{a}=a$)

$$a*\cancel{b}_0 = a+\cancel{b}_0-4\cancel{ab}_0$$

$0 \in \mathbb{Q}$ è l-mutro per *

$$\forall a \in \mathbb{Q}, a*0 = a+0-4a \cdot 0 = a$$

(2) $a \in \mathbb{Q}$

a è invertibile in $(\mathbb{Q}, *) \Leftrightarrow \exists \overset{\text{elemento inverso}}{b} \in \mathbb{Q}: a*b = 0 \Leftrightarrow$ l-mutro

$$\Leftrightarrow \exists b \in \mathbb{Q}: \underline{a+b-4ab=0}$$

$$\Leftrightarrow \exists b \in \mathbb{Q}: b-4ab = -a \leftarrow (\text{porta } \underline{a} \text{ a destra})$$

$$\Leftrightarrow \exists b \in \mathbb{Q}: b(1-4a) = -a \leftarrow (\text{mettendo in evidenza } b)$$

$$\Leftrightarrow \exists b \in \mathbb{Q}: b = \frac{-a}{1-4a} \quad \left(\begin{array}{l} b \text{ avete solo } \neq 0 \text{ denominatore} \\ \bar{a} \neq 0 \end{array} \right)$$

$$\Leftrightarrow 1-4a \neq 0 \Leftrightarrow a \neq \frac{1}{4}$$

$$\overset{\uparrow}{(\mathcal{U}(\mathbb{Q}), *)} = \mathbb{Q} \setminus \left\{ \frac{1}{4} \right\}$$

Oss. Chi è l'inverso di $\frac{3}{5}$? $(\mathbb{Q}, *)$

l'inverso di $\frac{3}{5}$ è

$$\frac{-3/5}{1-4 \cdot \frac{3}{5}} = \frac{-3/5}{1-\frac{12}{5}} = -\frac{3}{5} \cdot \left(-\frac{5}{7}\right) = \frac{3}{7}$$

$$\frac{3}{5} * \frac{3}{7} = \frac{3}{5} + \frac{3}{7} - 4 \cdot \frac{3}{5} \cdot \frac{3}{7} = \frac{3}{5} + \frac{3}{7} - \frac{36}{35} = \frac{21+15-36}{35} = 0$$

(3) $2\mathbb{Z}$ è un sottomonoido $\Leftrightarrow \left\{ \begin{array}{l} 2\mathbb{Z} \text{ è stabile rispetto a } * \\ 0 \in 2\mathbb{Z} \Leftrightarrow 0 \in \mathbb{Z} \end{array} \right.$

• $0 \in 2\mathbb{Z} \rightarrow$ vero

• $\forall a, b \in 2\mathbb{Z}$

Tr: $a * b \in 2\mathbb{Z}$

$$a * b = \underbrace{a + b - 4ab}_{\in \mathbb{Z}_L} \in \mathbb{Z}_L$$

Quindi \mathbb{Z}_L è stabile rispetto a $*$ e contiene l'elemento neutro di $(\mathbb{Q}, *)$; pertanto \mathbb{Z}_L è un sottogruppo di $(\mathbb{Q}, *)$

- ② Nell'insieme \mathbb{N} si consideri l'operazione bimaria $*$ definita ponendo

$$a * b = \begin{cases} a & \text{se } a \in \mathbb{N}_P \\ b & \text{se } a \in \mathbb{N}_d \end{cases}$$

per ogni $a, b \in \mathbb{N}$

- ① Si dimostri che la struttura algebrica $(\mathbb{N}, *)$ è un semigruppo

- ② Si stabilisce se l'operazione $*$ è commutativa

- ③ Si dimostri che la struttura algebrica $(\mathbb{N}, *)$ non è un monoido.

- ① * associativa $(\underline{\underline{a * b}} * c) = a * (\underline{\underline{b * c}})$

$$a * b = \begin{cases} a & \text{se } a \in \mathbb{N}_P \\ b & \text{se } a \in \mathbb{N}_d \end{cases}$$

$$\begin{aligned} (\underline{\underline{a * b}} * c) &= \frac{a \in \mathbb{N}_P}{\cancel{a * b}} \frac{a * c = a \rightarrow a \in \mathbb{N}_P = a * (\cancel{b * c})}{\cancel{b * c}} \\ &\quad \frac{b \in \mathbb{N}_P}{\cancel{b * c}} = b \rightarrow a \in \mathbb{N}_d, b \in \mathbb{N}_P \\ &\quad \frac{c \in \mathbb{N}_d}{\cancel{b * c}} = c \rightarrow a \in \mathbb{N}_d, b \in \mathbb{N}_d \end{aligned}$$

$$\begin{aligned} b &= b * c = a * (\cancel{b * c}) \\ &\quad \frac{b \in \mathbb{N}_P}{\cancel{b * c}} \quad \frac{a \in \mathbb{N}_d}{\cancel{b * c}} \\ c &= b * c = a * (\cancel{b * c}) \\ &\quad \frac{b \in \mathbb{N}_d}{\cancel{b * c}} \quad \frac{a \in \mathbb{N}_d}{\cancel{b * c}} \end{aligned}$$

$$a * (\cancel{b * c}) = a \quad \text{se } a \in \mathbb{N}_P$$

$\Rightarrow *$ è associativa

$\Rightarrow (\mathbb{N}, *)$ è un semigruppo

② $2 * 4 = 2$

$$4 * 2 = 4$$

* non è commutativa

- ③ $\nexists z \in \mathbb{N}$ neutro rispetto a $*$:

Per assurdo sia $z \in \mathbb{N}$ neutro

$$a * b = \begin{cases} a & \text{se } a \in \mathbb{N}_P \\ b & \text{se } a \in \mathbb{N}_d \end{cases}$$

$$\Rightarrow \forall a \in \mathbb{N}_0 \quad a + e = a = e + a$$

Se $a = 1$ deve valere $1 + e = 1 \Rightarrow e = 1 \Rightarrow 1 \text{ è l'el.- neutro}$

Prendiamo $a = 3$ allora $3 + 1 = 3$

$$\Downarrow 1 = 3 \Downarrow$$

Quindi c'è assurdo
supponendo che \exists el.- neutro

③ Si consideri il monide moltiplicativo $A = \mathbb{Z}_{10}$ e sia U il gruppo degli elementi invertibili di A .

① Si compili la tabella moltiplicativa di U .

② Si determini un sottogruppo di ordine 2 di U .

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, [2]_{10}, [3]_{10}, [4]_{10}, [5]_{10}, [6]_{10}, [7]_{10}, [8]_{10}, [9]_{10}\}$$

$$U(\mathbb{Z}_m) = \{[a]_m : \text{MCD}(a, m) = 1\}$$

$$(U(\mathbb{Z}_{10}), \cdot) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \{1, 3, 7, 9\}$$

①

1	3	7	9
1	1	3	7
3	3	9	1
7	7	1	9
9	9	7	3

$\Rightarrow 21 = 1 \pmod{10}$

1 è el.- neutro perché
la riga e la colonna
correspondenti contengono tutti
gli elementi nell'ordine
scelto $(1, 3, 7, 9)$

②

Per determinare
un sottogruppo B di ordine
2 di U , questo deve contenere
l'elemento neutro di U che è 1

$$\Rightarrow B = \{1, a\}$$

$$B = \{1, a\}$$

$$a \cdot b = 1$$

b: inverso di a

Siccome vogliamo che B sia un sottogruppo
ed $a \in B$, anche a^{-1} dovrà $\in B$

$$\text{quindi } a^{-1} = 1 \circ a^{-1} = a$$

Ma $a^{-1} = 1$ è impossibile perché in qualunque
monide l'inverso dell'el.- neutro è se stesso.

$$a \cdot a^{-1} = 1$$

$$\Rightarrow \underset{''}{a^{-1}} = a \quad a^2 = 1 \quad 3, 7, 9$$
$$\frac{1}{a} = a \Rightarrow a^2 = 1$$

X CASA.

$$\mathbb{Q} \quad a+b = a+b + |ab|$$

$(\mathbb{Q}, *)$ è commutativa, non associativa e dotata di el. neutra