

**DEF.** Dico struttura algebrica su insieme  $X$  se  
ci sono definite una o più operazioni  
binarie (o non), interne (~~o esterne~~).

Se le operazioni sono denotate con  $*$ ,  $\circ$ ,  $\square$  ...

Si indica la struttura alg. con  $(X, *, \circ, \square, \dots)$

ESEMPI.

1)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}, +, \cdot)$  e simili sono strutture algebriche.

2)  $(P(X), \cup)$ ,  $(P(X), \cup, \cap)$  " " " "

3) In tutti questi casi le operazioni sono interne.

Ma è una struttura algebrica anche lo spazio vettoriale su  $\mathbb{R}$  delle coppie ordinate  $\mathbb{R}^2$ , con l'operazione (binaria interna) di somma componente per componente e l'operazione (binaria esterna) di prodotto scalare-vettore. La rappresentazione in questo caso può essere più complicata, poiché bisogna tener conto anche dell'insieme degli scalari:  $(\mathbb{R}^2, +, \mathbb{R})$  ci può ricordare che non stiamo solo facendo somma di coppie, come intendo invece con la scrittura  $(\mathbb{R}^2, +)$ .

4) Non è una struttura algebrica  $(\mathbb{Z}, \div)$

perché la divisione di un numero intero per un altro intero può non essere definita (il secondo è 0), non dar luogo a un intero cioè  $\div$  non è un'operazione in  $\mathbb{Z}$ .

Non lo è neanche in  $\mathbb{Q}$  per il problema della divisione per 0. Tuttavia

5)  $(\mathbb{Q}^*, \div)$  è una struttura algebrica, con operazione non commutativa né associativa; dotata di neutro destro ( $a \div 1 = a \forall a \in \mathbb{Q}^*$ ) ma non sinistro

### L'ESEMPIO 5

(148bis)

Verifichiamo che  $(\mathbb{Q}^*, \div)$  è una struttura algebrica con operazione non commutativa e non associativa

1)  $\div$  è un'operazione interna poiché

$\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}^*$  significa  $p, p' \neq 0$  e quindi

$\frac{p}{q} : \frac{p'}{q'} = \frac{pq'}{q'p}$  è una frazione che rappresenta un razionale ( $q'p \neq 0$ ) non nulla ( $pq' \neq 0$ )

2)  $\div$  non è commutativa. Ad es.

$$\frac{1}{1} : \frac{2}{1} = \frac{1}{2} \quad \text{mentre} \quad \frac{2}{1} : \frac{1}{1} = \frac{2}{1}$$

3)  $\div$  non è associativa. Ad es.

$$(\frac{1}{1} : \frac{2}{1}) : \frac{2}{1} = \frac{1}{2} : \frac{2}{1} = \frac{1}{4} \quad \text{mentre}$$

$$\frac{1}{1} : (\frac{2}{1} : \frac{2}{1}) = \frac{1}{1} : \frac{1}{1} = \frac{1}{1}$$

E' esattamente il "mistero" che si cela dietro il fatto che

$$\frac{\frac{1}{2}}{2} \neq \frac{1}{\frac{2}{2}}$$

PAG 149

**Esempio 2.**  $2\mathbb{Z} = \{2k, k \in \mathbb{Z}\}$ .

Il prodotto righe per colonne in  $M_2(2\mathbb{Z})$  non è commutativo. Basta prendere

$$\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} = 4 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq 4 \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

Visto la volta scorsa

PAG 149bis

Si nota nella tavola di camp. di  $S_3$  che ogni riga e ogni colonna contiene tutti gli elementi di  $S_3$ . Ciò è tipico di ogni gruppo  $(G, *)$  finito poiché in un gruppo l'equazione  $a * x = b$  è risolubile  $\forall a, b \in G$ . Infatti se  $u$  è il neutro di  $G$  e  $a^{-1}$  è l'inverso di  $a$ :  $a^{-1} * a * x = a^{-1} * b \Rightarrow u * x = a^{-1} * b \Rightarrow x = a^{-1} * b$

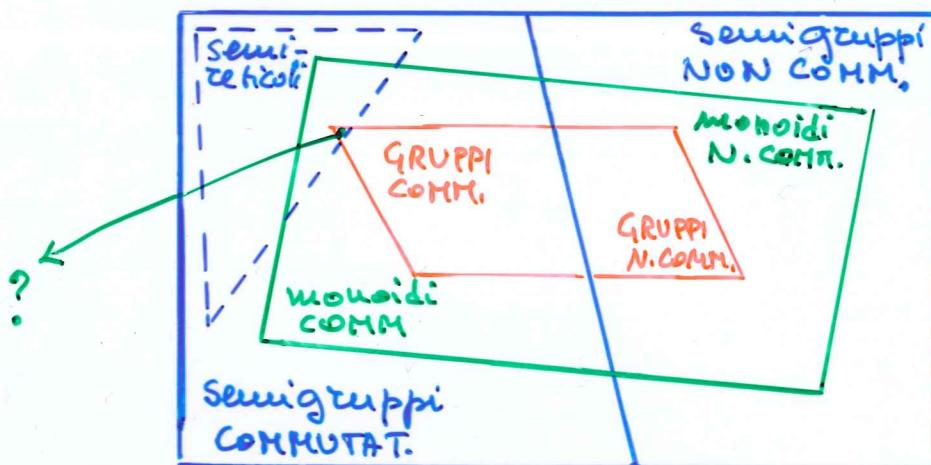
ASSOCIAТИВА

# (149)

## Strutture algebriche con una operazione interna binaria.

Le più significative sono

- semigruppo : struttura con operazione associativa
- monoide : semigruppo con elem. neutro
- gruppo : monoide in cui ogni elemento è invertibile
- semireticolato : semigruppo commutativo in cui ogni elemento è idempotente



Structure  
algebriche  
con 1 operazione

### ESEMPI

- 1)  $(2\mathbb{Z}, \cdot)$  semigruppo commutativo non monoide né semiret.
- 2)  $(M_2(2\mathbb{Z}), \cdot)$  " NON " non monoide
- 3)  $(\mathbb{Z}^*, \cdot)$  monoide comm. non semireticolato, non gruppo
- 4)  $(M_2(\mathbb{R}), \cdot)$  monoide non comm., non gruppo
- 5)  $(\mathbb{Z}, +)$  gruppo commutativo non reticolato
- 6)  $(S_3, \circ)$  gruppo non commutativo
- 7)  $(P(X), \cup)$  semireticolato con neutro  $\emptyset$  e zero  $X$ .

L'intersezione tra l'insieme dei gruppi e l'insieme dei semireticoli è costituito da un solo gruppo, formato da un sol elemento (neutro).

Esercizi:

(150)

1. Dire se i seguenti insiemi, con le operazioni indicate sono

- 1) strutture algebriche
- 2) semigruppi
- 3) monoidi
- 4) gruppi
- 5) reticolati

- $(\mathbb{R}, +)$  gruppo comm. (ABELIANO)
- $(\mathbb{Z}, *)$  con  $a * b = 2a + b$  non semigruppo
- $(\mathbb{R}^*, \cdot)$  gruppo abeliano
- $(\mathbb{R}[x], +)$  gruppo abeliano
- $(\mathbb{R}_2[x], +)$  ove  $\mathbb{R}_2[x] = \{ p(x) \in \mathbb{R}[x] \text{ con grado di } p(x) \leq 2 \}$
- $(P_2, +)$  ove  $P_2 = \{ p(x) \in \mathbb{R}[x] \text{ con grado esattamente } = 2 \}$
- $(M_2(\mathbb{R}), +)$  gruppo ABELIANO
- $(M, +)$  ove  $M = \{ A \in M_2(\mathbb{Z}) \text{ con } A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \}$  g.-ABELIANO
- $(GL_2(\mathbb{R}), \cdot)$  ove  $GL_2(\mathbb{R}) = \{ A \in M_2(\mathbb{R}) / \det A \neq 0 \}$  e il prodotto è righe per colonne
- $(M, \circ)$  ove  $M = \{ A \in M_2(\mathbb{Z}^*) \text{ con } A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \}$  mon. ABELIANO e il prodotto è righe per colonne
- $(\mathbb{R}^2, +)$
- $(\mathbb{Z}^2, *)$  ove  $(a, b) * (c, d) = (ac, bc)$  per compon.
- $(\mathbb{R}^2, *)$  ove  $(a, b) * (c, d) = (ac, b+d)$  "
- $(\mathbb{Z}_6, +)$  ove  $[a]_6 + [b]_6 = [a+b]_6$  g.-ABEL. Ripassare!
- $(\mathbb{Z}_6, \circ)$  ove  $[a]_6 \circ [b]_6 = [ab]_6$  monoido comm.
- $(\mathbb{Z}_6^*, \circ)$  come sopra  $\rightarrow$  non è interna  $\Rightarrow$  non struttura
- $(\mathbb{Z}_5^*, \circ)$  analogamente  $[2] \cdot [3] = [0] \notin \mathbb{Z}_5^*$  gruppo: VEDI PAG SUCCESSIONE

Esercizio 1

150bis

②  $(\mathbb{Z}, *) \quad a * b = 2a + b \quad \forall a, b \in \mathbb{Z}$

1) è struttura algebrica poiché  $*$  è binaria e iuterne

2) è un semigruppo? Se sviluppo:

$$(a * b) * c = (2a + b) * c = 2(2a + b) + c = 4a + 2b + c$$

$$a * (b * c) = a * (2b + c) = 2a + 2b + c$$

Sono uguali SOLO SE  $a = 0$ , quindi non  $\in \mathbb{Z}$ .

$\Rightarrow *$  non è associativa  $\Rightarrow (\mathbb{Z}, *)$  non è semigr.

$\nRightarrow$  non è un monoido  $\Rightarrow$  non è un gruppo  
non è un semireticolo

VEDI SCHEMA PAG 149

③  $(R_2[x], +)$  polinomi di grado  $\leq 2$ ; li scrivo

$$a + bx + cx^2, a' + b'x + c'x^2 \dots$$

Possono non essere di grado 2 (ad es. se  $c = 0$  e  $b \neq 0$  sono di grado 1 ecc.) ma:

- $(a + bx + cx^2) + (a' + b'x + c'x^2) = a + a' + (b + b')x + (c + c')x^2$   
ha ancora grado  $\leq 2 \Rightarrow +$  è iuterne  $\Rightarrow$  STR. algebr.
  - $+$  è associativa, poiché lo è in generale in  $R[\bar{x}] \Rightarrow$   
semigruppo
  - $+$  è commutativa, " " " " " " " " $R[\bar{x}]$
  - esiste il neutro risp. a  $+$ : il polinomio 0  $\Rightarrow$  monoido
  - ogni elem. di  $R_2[x]$  ha inverso rispetto a  $+$  in  $\underline{R_2[x]}$ :  $- (a + bx^2 + cx^2) = (-a) + (-b)x + (-c)x^2$  è ancora un poli. di gr.  $\leq 2 \Rightarrow R_2[x]$  è un gruppo  
rispetto a  $+$
- $\Rightarrow (R_2[x], +)$  non può essere un semireticolo dato che ha più di 1 elemento (ne ha infiniti) mentre c'è 1 solo gr. che è semireticolo ed è  $\mathbb{N}_0$ .

④  $(P_2, +)$  polinomi di grado esattamente 2 ( $c \neq 0 \neq c'$ )

Non è strutt. alg. poiché non è iuterne:  $(1+x^2) + (-x^2) = 1$   
ha grado 0.

2. Trovare la tavola di composizione di  $(\mathbb{Z}_{5,2}^*, \cdot)$  (151)

$\cdot_5$	[1] <sub>5</sub>	[2] <sub>5</sub>	[3] <sub>5</sub>	[4] <sub>5</sub>
[1] <sub>5</sub>	1	2	3	4
[2] <sub>5</sub>	2	4	1	3
[3] <sub>5</sub>	3	1	4	2
[4] <sub>5</sub>	4	3	2	1

gruppo  
ABEL

$+_4$	[0] <sub>4</sub>	[1] <sub>4</sub>	[3] <sub>4</sub>	[2] <sub>4</sub>
[0] <sub>4</sub>	0	1	3	2
[1] <sub>4</sub>	1	2	0	3
[3] <sub>4</sub>	3	0	2	1
[2] <sub>4</sub>	2	3	1	0

Confrontarla con quelle di  $(\mathbb{Z}_4, +_4)$ : [2]<sub>4</sub>

Si notano analogie? Pur di cambiare i nomi degli elementi e dell'operazione, le due tabelle sono SOVRAPPONIBILI.

3. Sia  $S = \{1, 2\}$  e  $X = S^S$  l'insieme delle applicazioni di  $S$  in sé; sia  $\circ$  la composizione di applicazioni. Trovare la tavola di composizione di  $(X, \circ)$  e quella di  $(S_2, \circ)$  ove  $S_2$  è l'insieme delle permutazioni di  $S$ .

Svolgimento: se  $i = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ ,  $a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ ,  $b = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ ,  $c = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$

$(S, \circ)$	$\circ$	i	a	b	c
	i	i	a	b	c
	a	a	i	c	b
	b	b	b	b	b
	c	c	c	c	c

$(S_2, \circ)$	$\circ$	i	a
	i		
	a		

b e c sono idempotenti

4. Sia  $S = \{1, 2\}$  e  $X$  l'insieme delle relazioni riflessive su  $S$ . Trovare la tavola di composizione di  $(X, \circ)$  - ove  $\circ$  è la composizione di relazioni - e di  $(X, \cap)$  - ove  $\cap$  è l'intersezione di relazioni.

Svolgimento. A ogni relazione associo la sua matrice booleana di incidenza e ricordo che le "o" corrisponde al prodotto righe per colonne della matr. della II relazione per quella della I, " $\cap$ " al prodotto elemento per elemento.

(152)  
Se  $M_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $M_a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ,  $M_b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $M_c = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$  si ha che

$$M_{aaa} = (M_a)^2 = M_a \quad M_{aob} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = M_c \quad M_{aoc} = M_c M_a = M_c$$

$$M_{boa} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = M_c \quad M_{bob} = M_b^2 = M_b \quad M_{boc} = M_c M_b = M_c$$

$$M_{coa} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = M_c \quad M_{cob} = M_b M_c = M_c \quad M_{coc} = (M_c)^2 = M_c$$

Quindi:

o	i	a	b	c
i	i	a	b	c
a	a	a	c	c
b	b	c	b	c
c	c	c	c	c

tutti gli elementi sono idempotenti e i è l'elemento neutro

o è commutativa !!  
oltre che associativa

Tuttavia

n	i	a	b	c
i	i	i	i	i
a	i	a	i	a
b	i	i	b	b
c	i	a	b	c

anche qui tutti gli elementi sono idempotenti, c'è l'elemento neutro  
i è lo zero

n è commutativa e associativa  
(come ci si aspetta).

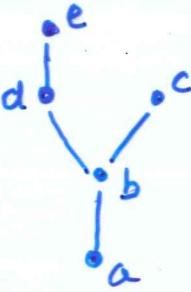
5. Sia  $(X, \leq)$  un insieme ordinato e consideriamo come operazioni  $x \wedge y = \text{Inf}(x, y)$  e  $x \vee y = \text{Sup}(x, y)$ .  
Data che non sempre esistono Inf e Sup di due elementi tali operazioni possono non essere interne e quindi non dar luogo a una struttura algebrica. In caso affermativo, detto che  $(x \wedge y) \wedge z = x \wedge (y \wedge z)$

$$x \wedge y = y \wedge x$$

$$x \wedge x = x$$

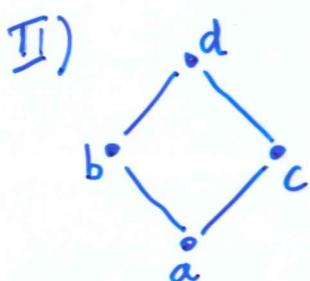
e dualmente per  $\vee$ , l'eventuale struttura è un Semireticolo.

Vedi gli esempi successivi

I)  per ogni coppia di elementi è definito ynf. Non per tutte sup.  $\Rightarrow$  si ha una struttura  $(X, \wedge)$  di semireticolato

$\wedge$	a	b	c	d	e
a					
b					
c					
d					
e					

Completare!



per ogni coppia di elem. è definito ynf e sup  $\Rightarrow$  ci sono due strutture di semireticolato:  $(X, \wedge)$  e  $(X, \vee)$

$\wedge$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

a è lo zero  
d è il neutro

$\vee$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

a è il neutro  
d è lo zero



per ogni coppia di elem. è def. sup. mentre non esiste  $a \wedge b$ . Quindi è definita solo la struttura di semireticolato  $(X, \vee)$

$\vee$	a	b	c
a			
b			
c			

IV)  in questo caso non è possibile definire alcuna struttura di semireticolato.

6. Sia  $S$  un insieme che chiamiamo alfabeto (154)  
(e i suoi elementi saranno detti lettere)

A partire da questo costruisco l'insieme  $X$  delle parole (accostamento di un numero qualunque purché finito di lettere non necessariamente distinte)

$$u = a_1 a_2 \dots a_n$$

Se  $v = b_1 b_2 \dots b_m$  definisco l'operazione di concettuazione

$$u \cdot v = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$$

Questa è un'operazione binaria, interna a  $X$  e associativa  $\Rightarrow$  SEMIGRUPPO LIBERO SULL'ALFABETO  $S$ .

Non ha elemento neutro, non ha zero, non ha idempotenti, non è commutativo a meno che l'alfabeto non sia costituito da 1 solo lettera.

Posso aggiungere all'insieme  $X$  delle parole anche la parola vuota: in questo modo si ha il monoide libero sull'alfabeto  $S$ .

Chi è il monoide libero sull'alfabeto  $S = \{a\}$ ?

Parole:  $\cdot, a, aa = a^2, aaa = a^3, \dots, a^n, \dots$

concettuazione :

in sostanza che cosa viene fuori?  $\Leftarrow$

$$\begin{aligned}\cdot \cdot &= \\ \cdot a &= \\ a \cdot &= \\ \cdot a^n &= \\ a^n \cdot &= \\ aa^n &= \\ a^m a &= \\ a^m a^n &=\end{aligned}$$