

# STRUTTURE ALGEBRICHE

(136)

Per potere parlare serve innanzi tutto chiarire la  
nozione di

Operazione binaria tra due insiem  $X$  e  $Y$  a valori in  
un insieme  $Z$ .

Con questo nome indico qualunque applicazione

$$g: X \times Y \rightarrow Z$$

e per ogni coppia ordinata  $(x,y) \in X \times Y$  l'elemento

$$z = g(x,y)$$

è detto "risultato dell'operazione sulla coppia  $(x,y)$ ".

Poiché  $g$  è un'applicazione, il "risultato" esiste  
ed è unico per ogni coppia ordinata  $(x,y)$ .

Per comodità si usa denotare l'operazione con  
un simbolo, da inserire tra i due elementi di ogni  
coppia per indicare il risultato. Ad es. se indico l'ope-  
razione con  $*$ :  $g(x,y) = x * y$ .

Se i 3 insiem coincidono:  $X = Y = Z$ , si parla  
di operazione binaria interna (o legge di compo-  
sizione) e si dice che  $X$  è chiuso rispetto all'ope-  
razione \*; altrimenti si parla di operazione binaria  
esterna.

## ESEMPI

- 1) La somma e il prodotto in  $\mathbb{N}$  sono due opere-  
zioni binarie interne.
- 2) M.C.D.:  $\mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$  è un'operazione binaria  
interne

3) La differenza non è un'operazione interna  
 in  $\mathbb{N}$  poiché ad es.  $1-2 \notin \mathbb{N}$ , ma è una  
 operazione binaria esterna: (137)

$$- : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$$

4) Il prodotto scalare di vettori di  $\mathbb{R}^3$  ( $\sigma \mathbb{R}^n$  con  $n \geq 2$ )  
 definito così per ogni  $\underline{v} = (v_1, v_2, v_3)$  e  $\underline{w} = (w_1, w_2, w_3)$ :

$$\bullet : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$$

$$\underline{v} \cdot \underline{w} = v_1 w_1 + v_2 w_2 + v_3 w_3$$

è un'operazione binaria esterna

5) La distanza di due punti  $P_1, P_2$  del piano  $\mathbb{P}$

$$d : \mathbb{P} \times \mathbb{P} \rightarrow [0, +\infty)$$

$$d(P_1, P_2) = r$$

è un'operazione binaria esterna

3, 4, 5 sono esempi in cui  $X=Y \neq Z$ . Ci sono  
 anche esempi significativi in cui  $X \neq Y=Z$ .

Se

$$* : X \times Y \rightarrow Y$$

l'operazione viene talora detta "azione di X su Y"

Ne è esempio

6) il prodotto scalare-vettore definito negli spazi  
 vettoriali (su  $\mathbb{R}$ )

$$* : \mathbb{R} \times V \rightarrow V$$

$$c * \underline{v} = c \underline{v} \quad c \in \mathbb{R}, \underline{v} \in V$$

Se in particolare  $V = \mathbb{R}^3$ ,  $\forall \underline{v} = (v_1, v_2, v_3)$  sarà  
 $c * \underline{v} = (cv_1, cv_2, cv_3)$ .

Il prodotto scalar-vettore è un'azione di  $\mathbb{R}$  su  $V$   
 (infatti dilata, o restringe, o cambia verso ai vettori di  $V$ )

\*) Anche il prodotto di matrici è, in generale,  
un'operazione esterna

$$\bullet : M_{m,n}(\mathbb{R}) \times M_{n,p}(\mathbb{R}) \rightarrow M_{m,p}(\mathbb{R})$$

E' interna se si pensa  $X = M_{n,n}(\mathbb{R})$  e si fa  
il prodotto di matrici quadrate di ordine  $n$ .

Da qui ci occupiamo solo di operazioni interne,  
che chiameremo più brevemente operazioni sull'insieme  
 $X$ .

Possibili proprietà di un'operazione  $*$  su  $X$ :

1)  $*$  è associativa se  $\forall a, b, c \in X$  si ha

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

(e si scriverà brevemente  $a * b * c$ )

2)  $*$  è commutativa se  $\forall a, b \in X$  si ha

$$a * b = b * a$$

ESEMPI: già incontrati parlando di  $+$ ,  $\circ$  in  
 $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{R}[x]$ ,  $\mathbb{Z}_n$

### CONTROESEMPI

I) il prodotto righe per colonne in  $M_n(\mathbb{R})$  non è commutativo (ma è associativo)

II) la differenza in  $\mathbb{Z}$  non è commutativa  
né associativa:

$$1 - 2 \neq 2 - 1 ; (1 - 2) - 3 = -4 \neq 1 - (2 - 3) = 2$$

III) l'operazione  $\circ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  definita come

$$a \circ b = a^2 + b^2 \quad \text{non è associativa:}$$

$$(1 \circ 2) \circ 3 = (1+4) \circ 3 = 25 + 9 = 34$$

$$1 \circ (2 \circ 3) = 1 \circ (4+9) = 1 + 169 = 170$$

3) esistenza di un elemento neutro a sinistra  
 se esiste  $u_s \in X$  tale che  $\forall a \in X$   
 a sinistra!  $\rightarrow u_s * a = a$

esistenza di un elemento neutro a destra  
 se esiste  $u_d \in X$  t.c.  $\forall a \in X$   
 $a * u_d = a \rightarrow$  a destra!

esistenza di un elemento neutro (bilatero)  
 se esiste  $u \in X$  t.c.  $\forall a \in X$   
 $a * u = u * a = a$

### ESEMPI.

1. Sono elementi neutri (bilateri):

- 0 rispetto alla somma in  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $[0]_n$  " " " in  $\mathbb{Z}_n$
- la matrice nulla rispetto a + in  $M_{m \times n}(\mathbb{R})$
- il vettore nullo rispetto a + in  $\mathbb{R}^n$
- il polinomio 0 rispetto a + in  $\mathbb{R}[x]$
- 1 rispetto al prodotto in  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $[1]_n$  rispetto al prodotto in  $\mathbb{Z}_n$
- la matrice identica  $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$  risp. al prodotto  
righe per colonne in  $M_n(\mathbb{R})$
- il polinomio 1 rispetto al prodotto in  $\mathbb{R}[x]$

2. E' un neutro destro (ma non bilatero) 0 rispetto  
alla differenza in  $\mathbb{Z}$ :

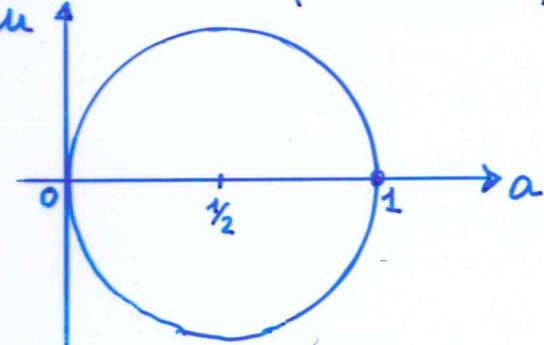
$$\forall a \in \mathbb{Z} \quad a - 0 = a$$

(ma non è vero che  $0 - a = a \quad \forall a!$ )

3. Non esiste neutro (né destro né sinistro) per l'operazione in  $\mathbb{Z}$  definita da  $a \circ b = a^2 + b^2$   
poiché

$$a \circ u = a \iff a^2 + u^2 = a$$

e questa relazione non può valere per ogni scelta di  $a \in \mathbb{Z}$



addirittura ci sono...  
solo 2 coppie di interi  
soluzione:  
 $(a, u) = (0, 0)$  e  $(a, u) = (1, 0)$

4. Non esiste neutro neppure per l'operazione di M.C.D.  
in  $\mathbb{N}^*$  poiché

$$\text{M.C.D}(a, u) = a \quad \forall a \in \mathbb{N}^*$$

Significa che  $u$  è divisibile per ogni numero naturale;  
ma sappiamo che ciò è impossibile (la relazione d'ordine di "divisibilità" non ha Sup).

L'esempio 2 dice che può esistere neutro (almeno destro)  
anche in assenza di associatività e commutatività.

L'esempio 4 dice che può non esistere anche in  
presenza di associatività e commutatività.

L'elemento neutro bilatero, se esiste, è unico. Infatti  
se  $u$  e  $v$  sono elementi neutri rispetto a  $*$  in  $X$   
si ha

$$u * v = v \quad (\text{pensando } u \text{ come neutro a sinistra})$$

$$u * v = u \quad (" \quad v \text{ come neutro a destra})$$

e quindi  $u = v$ .

(N.B. Se  $*$  è commutativa il neutro, se esiste, è sicuramente  
bilatero)

Se  $*$  è un'operazione in  $X$  rispetto alle quali:

$u_s$  è neutro a sinistra

$u_d$  è neutro a destra

allora  $u_s = u_d$  e tale elemento è il neutro bilatero.

Infatti:

$$u_s * u_d = u_d \quad \text{se penso } u_s \text{ come neutro a sin.}$$

$$u_s * u_d = u_s \quad " " \quad u_d \quad " " \text{ a destra.}$$

4) Presenza di "inverso" sinistro di un elemento  $a \in X$

Nozione PRIMA di SENSO se in  $X$  non esiste l'elemento neutro rispetto a  $*$ . Quindi

Sia  $u$  l'elemento neutro rispetto a  $*$  in  $X$  e sia  $a \in X$ .

Dico che  $\bar{a}_s$  è inverso sinistro di  $a$  se

$$\bar{a}_s * a = u$$

dico che  $\bar{a}_d$  è inverso destro di  $a$  se

$$a * \bar{a}_d = u$$

dico che  $\bar{a}$  è inverso bilatero di  $a$  se

$$\bar{a} * a = a * \bar{a} = u.$$

Se l'operazione  $*$  definita in  $X$  è associativa (e dotata di unità bilatera  $u$ ) e se l'elemento  $a \in X$  ha inversobilatero, tale inverso è unico.

Dim. Siano  $c$  e  $b$  inversi bilateri di  $a$ : essono in particolare inversi sinistri e destri (Aggiungerò a  $c$  e  $b$  il pedice s o d per indicare come li considero). Per la prop. associativa:

$$(c_s * a) * b_s = c * (a * b_d)$$

$$u * b_s = c * u$$

$$b_s = c$$

C.V.d.

ESEMPI. Non bisogna lasciarsi tradire dal nome.

(142)

- rispetto alla somma in  $\mathbb{Z}$ , l'elem. neutro è 0 e ogni elemento  $a \in \mathbb{Z}$  ha "inverso additivo":  $-a$ .
- Lo stesso vale, quando si considera come operazione la somma, in  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- rispetto alla somma in  $\mathbb{R}[x]$  l'inverso di un polin.  
nub.  $p(x)$  è il polinomio opposto  $-p(x) \dots$
- rispetto alla somma in  $M_{m,n}(\mathbb{R})$  analogamente
- rispetto alla somma in  $\mathbb{Z}_n$  ogni classe di resto  $[a]_n$  ha "inverso additivo"  $[n-a]_n$ .
- rispetto al prodotto in  $\mathbb{Z}$ , l'elemento neutro è 1 e due soli elementi hanno inverso moltiplicativo:  
 $1, -1$
- rispetto al prodotto in  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  l'elem. neutro è 1 e tutti gli elem. non nulli sono dotati di inverso
- rispetto al prodotto in  $\mathbb{R}[x]$  l'el. neutro è il polinomio 1 e sono invertibili solo i polinomi (non nulli) di grado zero
- rispetto al prodotto in  $M_n(\mathbb{R})$  l'elem. neutro è la matrice identica e sono dotate di inverso solo le matrici con determinante  $\neq 0$ .
- rispetto al prodotto in  $\mathbb{Z}_n$ ,  $[1]_n$  è l'elem. neutro e l'esistenza di un inverso per  $[a]_n$  è determinata dal fatto che

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

- rispetto alla composizione nell'insieme  $S_n$  delle permutazioni su  $n$  oggetti, il neutro è la perm. identica  $(a_1 a_2 \dots a_n)$  e ogni perm.  $(a_1 a_2 \dots a_n)$  ha inverso  $(a_1 \dots a_n)$   $(a_1 a_2 \dots a_n)$

Ci sono anche altre 3 proprietà, che incontreremo (143) più frequentemente quando entrano in gioco 2 operazioni:

5) esistenza in  $X$  di uno "zero" rispetto a  $*$ .

Chiamiamo zero un elemento  $z \in X$  tale che per ogni  $a \in X$  risulti

$$a * z = z * a = \boxed{z}$$

ATTENZIONE: non è l'elem. neutro additivo che è definito come

$$\exists u \text{ tale che } \forall a \in X \quad a + u = u + a = \boxed{a}$$

Esempio 1. Se considero in  $\mathbb{Z}$  l'operazione prodotto,

$$\forall a \in \mathbb{Z} \quad \text{si ha} \quad a \cdot 0 = 0 \cdot a = 0$$

(ove 0 è lo zero additivo di  $\mathbb{Z}$ ): 0 è zero rispetto al  $*$  in  $\mathbb{Z}$ .

Esempio 2. Se in  $\mathbb{N}^*$  considero l'operazione di M.C.D.

$$\forall a \in \mathbb{N}^* \quad \text{si ha} \quad \text{MCD}(a, 1) = \text{MCD}(1, a) = 1$$

(ove 1 è l'el. neutro moltiplicativo in  $\mathbb{N}^*$ ): 1 è zero rispetto a M.C.D. in  $\mathbb{N}^*$ .

ATTENZIONE: lo zero, se esiste, è unico. Infatti

Se  $z_1, z_2$  sono zeri per  $*$  in  $X$ . si ha

$$z_1 * z_2 = z_2 * z_1 = \begin{cases} z_1 & \text{se penso } z_1 \text{ come zero} \\ z_2 & \text{" " " } z_2 \text{ " " } \end{cases}$$

6) esistenza in  $X$  di elementi "idempotenti" rispetto a  $*$ .

Chiamiamo idempotente un elem.  $a \in X$  tale che

$$a * a = a.$$

Esempio 1. In  $M_n(\mathbb{R})$ , la matrice  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  è idempotente rispetto al prodotto.

Esempio 2. In  $\mathbb{Z}_6$  la classe di resto  $[3]_6$  è idempotente rispetto al prodotto:  $[3]_6 \cdot [3]_6 = [9]_6 = \dots$

NOTA. Se  $*$  è associativa, non esistono in  $X$  elementi idempotenti e invertibili diversi dall'elemento neutro  $u$ . (144)

In fatti se  $a$  è idempotente  $a*a=a$

se  $a$  è invertibile esiste  $\bar{a}$  t.c.  $a*\bar{a}=\bar{a}*a=u$

"Moltiplico" per  $\bar{a}$  entrambi i membri della prima:

$$(a*a)*\bar{a} = a*\bar{a} = u$$

Per la prop. associativa

$$(a*a)*\bar{a} = a*(a*\bar{a}) = a*u = a$$

Confronto le 2 uguaglianze:  $u=a$ . C.V.d.

La dizione idee-potente nasce dal pensare  $*$  come un prodotto ed estendere la simbologia in uso tutte le volte che si parla di prodotto (numeri, polinomi, matrici):

$$a*a = a^2.$$

Usando la stessa estensione di simbologia, l'inverso di un elemento  $a$  è denotato con  $a^{-1}$ .

Se poi  $*$  è associativa si può proseguire:

$$(a*a)*a = a*a*a = a^3 \text{ e in generale scrivere}$$

$$\underbrace{a*a*...*a}_{n \text{ elementi}} = a^n$$

$$\underbrace{a^{-1}*a^{-1}*...*a^{-1}}_{n \text{ elem.}} = a^{-n}$$

Se  $*$  non è associativa ma si possono "togliere le parentesi" e quindi vale si sa chi sia  $a^3$ .

Ad es. in  $\mathbb{Z}$  con l'operazione di sottrazione

$$(2-2)-2 = 0-2 = -2$$

$$2-(2-2) = 2-0 = 2$$

OSS. Se  $*$  è associativa e  $a$  è idempotente  
rispetto a  $*$  in  $X$  si ha

$$a^n = a \quad \text{per ogni } n \geq 1.$$

(14.5)

La simbologia appena introdotta può essere motivo di confusione quando  $*$  non è un prodotto, ad es.  
quando nell'insieme delle funzioni  $f: \mathbb{R} \rightarrow \mathbb{R}$   
si considera l'operazione di composizione (non  
di prodotto!). In generale

$$f^n(x) \neq (f(x))^n$$

e

$$f^{-1}(x) \neq \frac{1}{f(x)}$$

Ad es. se  $f(x) = 3^x$  si ha

$$(f(x))^2 = 3^{2x} \quad \text{ma} \quad f^2(x) = 3^{3^x}$$

e

$$\frac{1}{f(x)} = 3^{-x} \quad \text{ma} \quad f^{-1}(x) = \log_3 x.$$

Un altro motivo di confusione legato alla simbologia riguarda le proprietà delle potenze.

Siamo abituati a pensare che

$$(a * b)^n = a^n * b^n$$

e, se esistono  $a^{-1}, b^{-1}$ ,

$$(a * b)^{-1} = a^{-1} * b^{-1}$$

Ciò funziona se  $*$  è commutativa e associativa.

Ma se  $*$ , pur essendo commutativa, non è  
associativa può non valere alcuna delle 2.

ESEMPIO. Considero l'insieme  $X = \{1, 2, 3, 4\}$  con l'operazione  $*$  descritta dalla seguente TABELLA DI COMPOSIZIONE (per avere il risultato  $a * b$  leggere il valore di  $a$  nella prima colonna, a sinistra, e quello di  $b$  nella prima riga e cercare nella tabella la casella all'incrocio della riga di  $a$  e della colonna di  $b$ )

$*$	1	2	3	4
1	1	2	3	4
2	2	2	4	1
3	3	4	1	4
4	4	1	4	4

Si nota che  $*$  è commutativa, che 1 è l'elemento NEUTRO, che ogni elemento ha inverso e che 2 e 4 sono idempotenti ( $\Rightarrow *$  non è associativa). Ora:

$$(2 * 3)^2 = 4^2 = 4 \text{ mentre } 2^2 * 3^2 = 3 * 1 = 3$$

$$(2 * 3)^{-1} = 4^{-1} = 2 \text{ mentre } 2^{-1} * 3^{-1} = 4 * 3 = 4$$

OSS. Se  $*$  è associativa

$$(a * b)^n = a * b * \dots * a * b$$

$$\text{e se } \exists a^{-1} \text{ e } b^{-1}: (a * b)^{-1} = b^{-1} * a^{-1}.$$

ATTENZ.  
ALL'ORDINE

La prima delle due dice che posso dimenticare le parentesi ma non l'ordine in cui compaiono i "fattori". La seconda si motiva così:

$$\begin{aligned}
 (a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} = \\
 &\stackrel{\text{ASSOC.}}{=} a * u * a^{-1} = a * a^{-1} = u.
 \end{aligned}$$

Se  $*$  non è anche commutativa NON possiamo non tener conto dell'ordine. 147

Esempio. Su  $M_2(\mathbb{R})$  con il prodotto righe per colonne, presi  $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  e  $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

$$\text{Si ha } A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Ora

- $(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 6 \\ 0 & 4 \end{pmatrix}$  è diversa da

$$A^2 B^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ 0 & 4 \end{pmatrix}$$

- $(AB)^{-1} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}$  è diversa da

$$A^{-1} B^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

Invece  $B^{-1} A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}.$

7) (Se in  $X$  esiste lo zero  $\mathbb{Z}$  rispetto a  $*$ ). Esistenza di "divisori dello zero".

Chiamiamo divisore dello zero (rispetto a  $*$ ) un elemento  $a \neq \mathbb{Z}$  tale che esista un  $b \in X$  per cui

$$a * b = \mathbb{Z} \quad o \quad b * a = \mathbb{Z}$$

(ovviamente anche  $b$  è divisore dello zero).

**ESEMPIO 1.** Nell'insieme  $M_2(\mathbb{R})$  la matrice nulla è lo zero rispetto al prodotto righe per colonne e le matrici  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  e  $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$  sono divisori dello zero, poiché

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

**ESEMPIO 2.** In  $\mathbb{Z}_4$ ,  $[2]_4$  è div. dello zero  $[0]_4$  risp. a