

A : insieme

Def: Operazione binaria su A :

funzione $f: A \times A \rightarrow A$

Struttura algebrica: Insieme più
una o più operazioni
in di esso.

ESEMPLI: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$,
 $(\mathbb{N}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$
etc.

Sia $(A, *)$ una struttura algebrica

Def: Si dice che $*$

a) Ammette elemento neutro se

$$\exists e \in A : \forall a \in A : a * e = e * a = a$$

b) Ammette inversi se vale "(a)" e

$$\forall a \in A \exists \bar{a} \in A : a * \bar{a} = \bar{a} * a = e$$

c) È associativa se

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

d) È commutativa se

$$\forall a, b \in A : a * b = b * a$$

Def: $(A, *)$ è detto MONOIDE se valgono
(a) e (c) ovvero

$$a) \exists e \in A: \forall a \in A: a * e = e * a = a$$

(el. neutro)

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

ESEMPIO DI MONOIDE

$$(\mathbb{N}_0, +), (\mathbb{Z}, +) \text{ etc.}$$

$\mathbb{N}_0$ = insieme dei numeri naturali
incluso lo zero.

N.B. La sottrazione non è una
operazione su $\mathbb{N}_0$.

D'altro canto anche su $\mathbb{Z}$

è priva di proprietà "interessanti"
quali l'esistenza dell'elemento
neutro o la prop. associativa.

La struttura da considerare è
sempre $(\mathbb{Z}, +)$ definendo

$$a - b := a + (-b)$$

ove $(-b)$ è l'inverso rispetto a +
di b in $(\mathbb{Z}, +)$.

Def: Si dice GRUPPO una struttura algebrica $(G, *)$ che gode delle proprietà (a), (b) e (c).

Seguovamente:

$$a) \exists e \in G : \forall g \in G : e * g = g * e = g$$

$$b) \forall g \in G \exists \bar{g} \in G : g * \bar{g} = \bar{g} * g = e$$

$$c) \forall a, b, c \in G : a * (b * c) = (a * b) * c.$$

Se vale anche la proprietà commutativa, allora il gruppo $(G, *)$ è detto

COMMUTATIVO oppure ABELIANO.

Exempis: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

$(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

ove $K^* := K \setminus \{0\}$.

N.B $(\mathbb{Q}, \cdot)$ non è un gruppo perché $0 \in \mathbb{Q}$ non è invertibile.

OSSERVAZIONE : un gruppo è un ambiente
(IMPORTANTE) in cui una equazione
del tipo

$$a * x = b$$

ammette sempre una ed una
sola soluzione.

Infatti abbiamo $a * x = b$

$$\Leftrightarrow$$

inverso $(\bar{a}) * (a * x) = (\bar{a}) * b$

$$\Leftrightarrow$$

associativo $(\bar{a} * a) * x = \bar{a} * b$

$$\Leftrightarrow$$

el. neutro $e * x = \bar{a} * b$

$$\Leftrightarrow$$

$$x = \bar{a} * b$$

N.B.: Non tutti i gruppi sono abeliani!

In particolare $\bar{a} * b \neq b * \bar{a}$
in generale.

Esempi di gruppi non abeliani:

$$1) GL(2, \mathbb{R}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

con il prodotto "righe per colonne"

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{bmatrix}$$

• elemento neutro: $I_2 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

• inversa della matrice $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} := \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

GRUPPO GENERALE LINEARE

$$2) S_3 := \{ f: \{1, 2, 3\} \rightarrow \{1, 2, 3\} \mid f \text{ biettiva} \}$$

con la composizione di funzioni.

[GRUPPO SIMMETRICO SU 3 ELEMENTI]

$$|S_3| = 3! = 6$$

possiamo scrivere esplicitamente
gli elementi di S_3

i	(23)	(12)	(123)	(132)	(13)
123	123	123	123	123	123
123	132	213	231	312	321

componendo si vede che la prop.
commutativa non vale

$$\begin{array}{ccc}
 1 & 2 & 3 \\
 & \downarrow (23) & \\
 1 & 3 & 2 \\
 & \downarrow (13) & \\
 3 & 1 & 2
 \end{array}$$

$$\begin{array}{ccc}
 1 & 2 & 3 \\
 & \downarrow (13) & \\
 3 & 2 & 1 \\
 & \downarrow (23) & \\
 2 & 3 & 1
 \end{array}$$

Def. Si dice ANELLO una struttura
algebrica $(A, +, \cdot)$ con 2 operazioni
tale che

- 1) $(A, +)$ è un gruppo abeliano
- 2) Valgono le proprietà distributive
 $\forall a, b, c \in A: a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
 $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
- 3) $\cdot$ è associativa: $\forall a, b, c \in A: a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Un anello è detto

- COMMUTATIVO se $\forall a, b \in A: a \cdot b = b \cdot a$
- CON UNITÀ se $\exists 1 \in A: \forall a \in A: 1 \cdot a = a \cdot 1$

Esempio: $(\mathbb{Z}, +, \cdot)$ è un anello
commutativo con unità.

N.B. Se $(A, +, \cdot)$ è un anello e

$0 \in A$ è l'elemento neutro per $+$
allora $\forall a \in A: 0 \cdot a = 0 = a \cdot 0$

(cioè: 0 non è mai invertibile
per il prodotto a meno che
 $A = \{0\}$ non sia l'anello banale
formato dal solo 0).

DIM:

$$0 \cdot a = (0 + 0) \cdot a =$$

$$= 0 \cdot a + 0 \cdot a$$

sommando a destra e sinistra

$$(-0 \cdot a)$$

$$\begin{aligned} 0 &= (-0 \cdot a) + (0 \cdot a) = (-0 \cdot a) + [(0 \cdot a) + (0 \cdot a)] = \\ &= [(-0 \cdot a) + (0 \cdot a)] + (0 \cdot a) = \end{aligned}$$

$$= 0 + (0 \cdot a) = (0 \cdot a)$$

Dimostrazione analoga per $a \cdot 0$.

Def: Si dice campo $(K, +, \cdot)$
un anello commutativo con unità
in cui $(K^*, \cdot)$ con $K^* := K \setminus \{0\}$
è un gruppo abeliano.

PIÙ ESPLICITAMENTE:

$(K, +, \cdot)$ è un campo se
(field)

1) $(K, +)$ è un gruppo abeliano con
el. neutro 0

2) $(K^*, \cdot)$ è un gruppo abeliano
($K^* = K \setminus \{0\}$)

3) valgono le proprietà distributive

$$\forall a, b, c \in K: a(b+c) = ab + ac$$

$$(a+b)c = ac + bc.$$

Esempi di campi

$$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$$

oss: Una struttura algebrica $(K, +, \cdot)$ in cui valgono tutte le proprietà di campo tranne la commutatività di $(K^*, \cdot)$ è detta corpo (skewfield, division ring).

OSSERVAZIONE 2: In un campo è sempre possibile discutere l'equazione lineare

$$\underline{ax + b = 0} \quad (*)$$

Infatti: se $a \neq 0 \Rightarrow \exists a^{-1} \in K$

e dunque $(*)$ diventa

$$a^{-1}(ax + b) = 0$$

$$(a^{-1})(ax) + (a^{-1}b) = 0$$

$$(a^{-1}a)x + a^{-1}b = 0$$

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

$$x = a^{-1}b$$

e dunque esiste una ed una sola soluzione.

Se $a=0 \Rightarrow (*)$ diventa

$$0 \cdot x + b = 0$$

$$b = 0 \quad (*)'$$

ci sono 2 possibilità:

1) $b=0 \Rightarrow (*)'$ è $0=0$

ed ogni valore di x è
soluzione

$\rightarrow$ equazione con ∞^1 soluzioni

2) $b \neq 0 \Rightarrow (*)'$ è sempre falsa

$\Rightarrow$ non esistono soluzioni

$\rightarrow$ equazione incompatibile.

Altri esempi di campo:

$$\mathbb{F}_2 := \{0, 1\}$$

Campo BINARIO

+	0	1
0	0	1
1	1	0

XOR

$\cdot$	0	1
0	0	0
1	0	1

AND

Le operazioni $+$ e $\cdot$ corrispondono alle
porte logiche fondamentali

(regole alla prossima lezione)