- Funzione fra 2 insiemi

$$f: A \to B.$$

- Composizione di funzioni

- $G: I \to A$

con $I \subseteq \mathbb{N} \setminus \{0\}$.

$I = \{1, 2 \dots n\}$

sequenza (ordinata).

- $A \to \mathbb{N} \setminus \{0\}$

ad ogni elemento associa la sua molteplicità.

$A = [a, a, b, c]$

$f(a) = 2$

$f(b) = 1$

$f(c) = 1$

(a, b, c, a, c)

$f: I_5 \to \{a, b, c\}$.

$f(1) = a \quad f(2) = b \quad f(3) = c$

$f(4) = a \quad f(5) = c$

NOTAZIONE: Se A insieme

denotiamo con A^n l'insieme

di tutte le seq. ordinate di elementi

di A.

Si identifica $A \times A$ con A^2

$A \times A \times \dots \times A$ con A^n

$$(A \times A) \times A = \{((a,b),c) \mid a,b,c \in A\}.$$

$$A \times (A \times A) = \{(a,(b,c)) \mid a,b,c \in A\}.$$

$$A^3 = \{(a,b,c) \mid a,b,c \in A\}.$$

Operazioni binarie su insiemi

$$f : A \times A \longrightarrow A$$

$$+ : \begin{cases} \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (a,b) \longrightarrow a+b \end{cases}$$

N.B. - NON É UNA OP. SU $\mathbb{N}$

ALGEBRA → STUDIO DI STRUTTURE ALGEBRICHE = INSIEMI DOTATI DI UNA O PIÚ OPERAZIONI

Sia A un insieme e

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

una operazione binaria.

$(A, *)$ é una struttura algebrica

1) Si dice che $e \in A$ è elemento neutro per $*$ se

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

[esempio: 0 in $(\mathbb{N}, +)$]
[1 in $(\mathbb{Z}, \cdot)$]

2) Si dice che $*$ è associativa se $\forall a, b, c \in A$:

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

[esempio: $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$, etc.
ma anche la composizione di funzioni sull'insieme 2^A di tutte le possibili funzioni $A \to A$]

Una struttura algebrica in cui valgono 1+2 è detta <u>monoide</u>

[es. $(\mathbb{N}, +)$]

3) Si dice che $a \in A$ ammette inverso rispetto $*$ se $\exists \bar{a} \in A$ tale che $a * \bar{a} = \bar{a} * a = e$ (deve esserci anche el. neutro).

es. in $(\mathbb{Z}, +)$ ogni elemento ammette inverso.

$z \in \mathbb{Z}$ $\exists -z \in \mathbb{Z}$:

$z + (-z) = (-z) + z = 0$

in $(\mathbb{N}, +)$ l'unico elemento che ammette inverso è 0

in $(\mathbb{Z}, \cdot)$ gli unici elementi che hanno inverso sono ± 1

in $(\mathbb{R}, \cdot)$ l'unico elemento che non ha inverso è 0.

Def: Si dice **Gruppo** una st. alg. $(A, *)$ tale che

1) $\exists$ elemento neutro e
2) $\forall a \in A \ \exists \bar{a} \in A: \ a * \bar{a} = \bar{a} * a = e$
3) $\forall a, b, c \in A: \ a * (b * c) = (a * b) * c$

Un gruppo è detto **commutativo** o **abeliano** se vale la proprietà commutativa

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

Esempi: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$

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

gruppi abeliani

Sia A un insieme

$S(A) := \{ f : A \to A \mid f \text{ biiettiva} \}$.

$(S(A), \circ)$ è un gruppo non commutativo.

$\circ$ comp. di funzioni

1) comp. di funzioni è associativa.

2) $\exists\, \iota : A \to A$, $a \to a$ che agisce come l'identità rispetto la comp. di funzioni

$$f \circ \iota = \iota \circ f = f$$

3) Ogni funzione bigettiva ammette inversa.

$A = \{a, b, c\}$.

	a	b	c
I	a	b	c
→ II	a	c	b
→ III	b	a	c
IV	b	c	a
V	c	a	b
VI	c	b	a

$(III \circ II) = IV$

$(b\ c\ a)$

$(II \circ III) = (c\ a\ b) = V$

$I = I^{-1}$ $\quad II = II^{-1}$

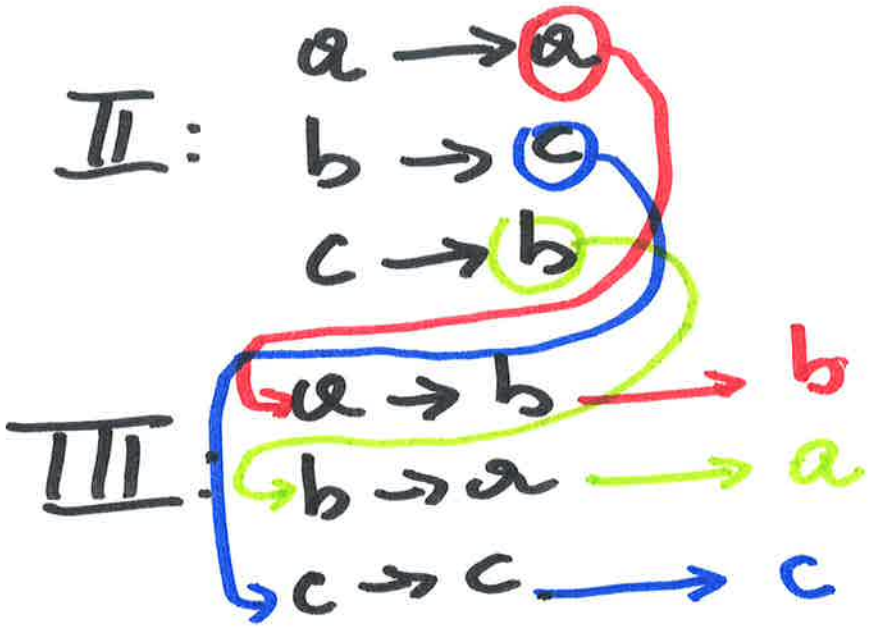
$III^{-1} = III$

$IV^{-1} = V$

$V^{-1} = IV$

$VI^{-1} = VI$

$(III \circ II)$



$a \to b$
$b \to c$
$c \to a$ $\quad IV$

Sia A un insieme e $+, \cdot$ due operazioni su A.

La struttura algebrica $(A, +, \cdot)$ è detta anello (commutativo con unità) se:

1) $(A, +)$ è un gruppo abeliano
2) l'operazione $\cdot : A \times A \to A$ è associativa.
3) valgono le proprietà distributive

$\forall a, b, c \in A$: $(a+b)\cdot c = ac + bc$

$a \cdot (b+c) = ab + ac$

4) $\exists\, 1_A \in A$ tale che $1_A \cdot a = a \cdot 1_A = a$ $\forall a \in A$

5) $\cdot$ è commutativo cioè $\forall a, b \in A$ $a \cdot b = b \cdot a$

Esempi $(\mathbb{Z}, +, \cdot)$

$(\mathbb{R}[x], +, \cdot)$

↙ insieme di tutti i polinomi a coeff. reali rispetto somma e prodotto di polinomi.

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

- $(\mathbb{K}, +)$ gruppo abeliano
- $(\mathbb{K} \setminus \{0\}, \cdot)$ gruppo abeliano
- prop. distributive $\forall a, b, c$: 

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

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

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

ma ce ne sono anche altri.

$(\mathbb{F}_2, \tilde{+}, \tilde{\cdot})$ $\quad \mathbb{F}_2 = \{0, 1\}$.

$\tilde{+}$	0	1
0	0	1
1	1	0

$\tilde{\cdot}$	0	1
0	0	0
1	0	1

0 = "pari"

1 = "dispari"

$(\mathbb{F}_3, +', \cdot')$

$+'$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot'$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Sia p un numero primo

e definiamo

$$\mathbb{F}_p = \{0, 1, \dots, p-1\}$$

$$+_p : \begin{cases} \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p \\ (a, b) \to (a+b) \,\%\, p \end{cases}$$

$$\cdot_p \begin{cases} \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p \\ (a, b) \to (a \cdot b) \,\%\, p \end{cases}$$

resto della divisione per p

$(\mathbb{F}_p, +_p, \cdot_p)$ è un campo

$(\mathbb{Z}_4, +_4, \cdot_4)$ ANELLO MA NON CAMPO

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Teorema (legge di annullamento del prodotto).

Sia $(\mathbb{K}, +, \cdot)$ un campo.

Allora $\forall a, b \in \mathbb{K}$: $a \cdot b = 0 \iff a = 0$ oppure $b = 0$

DIM: ($\Leftarrow$) mostriamo che

$a \cdot 0 = 0 \quad \forall a \in \mathbb{K}$

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

sommare a Sx e dx $-(a \cdot 0)$

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

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

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

($\Rightarrow$) Supponiamo $a \cdot b = 0$

$\Rightarrow$ se $a = 0 \rightarrow$ FINE

se $a \neq 0 \Rightarrow \exists\, a^{-1} \in \mathbb{K} : a^{-1} \cdot a = 1$

$\Rightarrow$ moltiplico per a^{-1} a dx e sx

$$a^{-1}(ab) = a^{-1} \cdot 0 = 0$$

$$\| $$

$$(a^{-1}a) \cdot b = 1 \cdot b = b$$

$$b = 0$$ □

Un campo $(\mathbb{K}, +, \cdot)$ è l'ambiente algebrico in cui si può scrivere una equazione

$$\boxed{ax + b = 0}$$

e se $a \neq 0 \Rightarrow$ tale eq. ha 1 e 1 sola soluzione.

$$ax+b=0 \qquad a\neq 0$$

$\Rightarrow$ soluzione è

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

N.B. In generale la teoria dei sistemi di eq. di primo grado dipende solo dall'avere un campo.

Per equazioni di grado >1 servono proprietà extra!

Se devo studiare

(*) $aX^2+b=0 \qquad a\neq 0$

se $ab>0$ l'eq. (*) non ha soluzioni reali

$x^2 = -ab < 0$

$x^2 - 2 = 0$ non ha soluzioni in $\mathbb{Q}$ ma ne ha in $\mathbb{R}$.