Funzioni e composizione di funzioni.

A, B

$f: A \to B$ $\qquad$ $f \subseteq A \times B$

1) f è ovunque definita $\quad \forall a \in A \ \exists b \in B : (a,b) \in f$
2) f è funzionale $\quad \forall a \in A \ \exists_{\leq 1} b \in B : (a,b) \in f$

se f funzione

a) f è iniettiva se $\forall b \in B \ \exists_{\leq 1} a \in A : (a,b) \in f$
b) f è suriettiva se $\forall b \in B \ \exists a \in A : (a,b) \in f$

Data $f \subseteq A \times B$ diciamo corrispondenza opposta di f $f^{opp} \subseteq B \times A$ tale che $f^{opp} = \{(b,a) \in B \times A \mid (a,b) \in f\}$.

f è iniettiva $\Leftrightarrow$ f^{opp} è ~~illegib~~ funzionale

f è suriettiva $\Leftrightarrow$ f^{opp} è ovunque definita.

f è biiettiva (iniettiva + suriettiva) $\Leftrightarrow$ f^{opp} è una funzione $B \to A$

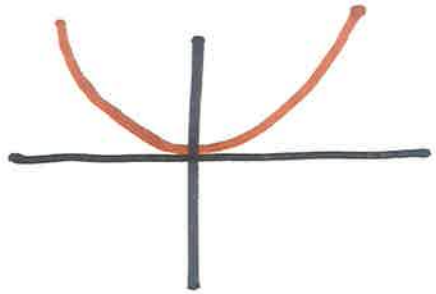
$$Im(f) := \{ b \in B : \exists a \in A \text{ con } f(a) = b \}.$$

immagine di f

$\Rightarrow$ $Im(f) \subseteq B$ codominio

f è suriettiva su $Im(f)$.

$$f : \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to x^2 \end{cases}$$



$Im(f) = \mathbb{R}^+$

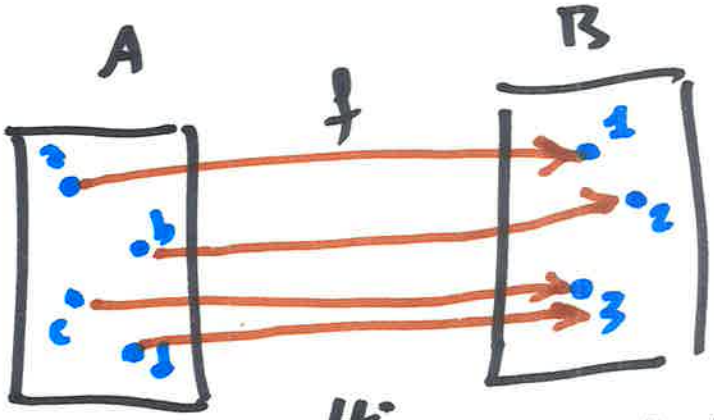
Def: Una funzione $f: A \to B$ si dice ammette inversa se $\exists\ f^{-1}: B \to A$ tale che

$$\begin{cases} f^{-1} \circ f = id_A : A \to A \\ f \circ f^{-1} = id_B : B \to B \end{cases}$$

ove $id_A : \begin{cases} A \to A \\ a \to a \end{cases}$ $\quad id_B \begin{cases} B \to B \\ b \to b. \end{cases}$

Oss: $f: A \to B$ ammette inversa $\Leftrightarrow f$ è bigettiva e in questo caso $f^{-1} = f^{opp}$

$|B| \leq |A|$

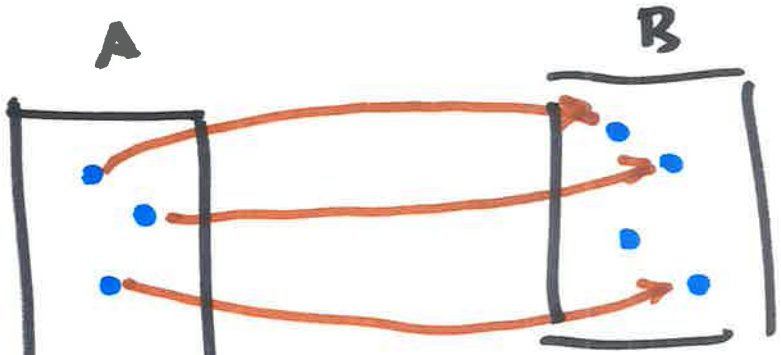


$\rightarrow = \{(a,1),(b,2),(c,3),(d,3)\}$.

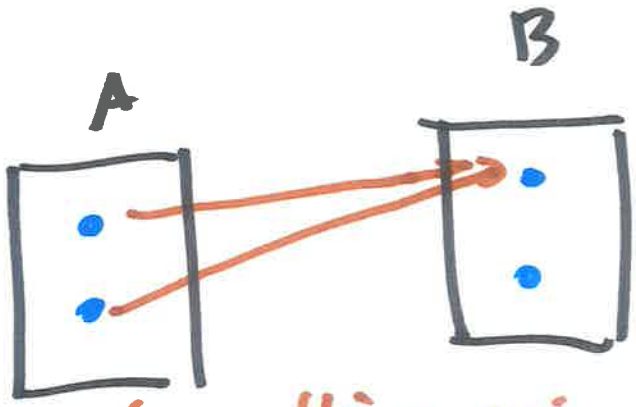
$f(c) = 3 = f(d)$

suriettiva, non iniettiva

$|B| \geq |A|$



iniettiva ma non suriettiva.



né iniettiva né suriettiva.

$|B| = |A|$

biiettiva.

$\mathbb{N}$ insieme dei numeri naturali con zero

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

$2\mathbb{N}$ insieme dei numeri naturali pari

$$2\mathbb{N} = \{0, 2, 4, 6, \dots\}.$$

La funzione $f: \begin{cases} \mathbb{N} \to 2\mathbb{N} \\ a \to 2a \end{cases}$

è biiettiva.

$2\mathbb{N} \subsetneq \mathbb{N}$

↑ contenuto propriamente = contenuto ma non uguale.

DIM: $f^{OPP}: 2\mathbb{N} \to \mathbb{N}$ è una funzione.

$b \to \frac{b}{2}$

pari

Si dice che un insieme X è infinito se $\exists Y \subsetneq X$ con Y e X una funzione biiettiva $X \to Y$.

Restrizione → rimpicciolire il dominio

Sia $C \subseteq A$ $\quad f_{|C} = \{(c,b) \mid (c,b) \in f\}$.

$f_{|C} : C \to B$

Troncamento

Sia $f: A \to B$

$C \subseteq B$ con

$Im(f) \subseteq C$

Il troncamento di f a C è la funzione $f^{|C} : A \to C$

tale che $f^{|C} = \{(a,c) \in A \times C \mid (a,c) \in A \times B\} = f$.

$f: A \to B$

$$f \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to x^2 \end{cases}$$

$$f_{|\mathbb{R}^+} : \begin{cases} \mathbb{R}^+ \to \mathbb{R} \\ x \to x^2 \end{cases}$$

$$f: \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to x^2 \end{cases}$$

NO INI.
NO SUR.

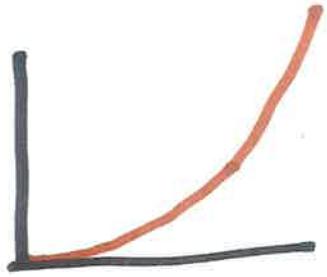
$$f|_{\mathbb{R}^+} \begin{cases} \mathbb{R}^+ \to \mathbb{R} \\ x \to x^2 \end{cases}$$

INI.
NO SUR

$$f^{|\mathbb{R}^+}: \begin{cases} \mathbb{R} \to \mathbb{R}^+ \\ x \to x^2 \end{cases}$$

NO INI
SUR.

$$f^{|\mathbb{R}^+}_{|\mathbb{R}^+}: \begin{cases} \mathbb{R}^+ \to \mathbb{R}^+ \\ x \to x^2 \end{cases}$$



BIIETTIVA

N.B. $\sqrt{x^2} = |x|$

Sia A un insieme.

Si dice operazione (binaria) su A una funzione

$$f: A \times A \to A$$

Esempio $A = \mathbb{N}$

$$f: \begin{cases} A \times A \to A \\ (a,b) \to a+b \end{cases}$$

$$+(a,b) = a+b$$

$5+7 = 12$

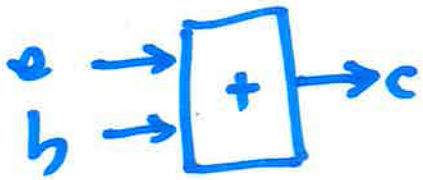
$5, 7, +$

$352+\cdot$

$(3(5+2))+$

$((3\cdot 5)+2)$

$35\cdot 2+$



$\mathbb{N} = \{0, 1, 2 \dots\}$ insieme dei numeri naturali

$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2 \dots\}$ insieme dei numeri interi

$\mathbb{Q} = \{ a/b : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \}$ insieme dei numeri razionali.

$\mathbb{R}$ = insieme dei numeri reali

$\mathbb{C}$ = insieme dei numeri complessi =

$= \{ a + ib \mid a, b \in \mathbb{R} \}$.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

(con un abuso di notazione).

$(\mathbb{N}, +)$ $(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

$(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$

$$*: \begin{cases} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (a,b) \to \max((a-b), 0). \end{cases}$$

- non è una operazione su $\mathbb{N}$

$(\mathbb{Z}, -)$ sì: - è una operazione (brutta) su $\mathbb{Z}$

Def: Si dice <u>struttura algebrica</u> un insieme A dotato di una o più operazioni.

$(\mathbb{N}, +)$ $(\mathbb{Z}, +)$

$(\mathbb{Q}, :)$ non è una struttura algebrica!

$(\mathbb{Q} \setminus \{0\}, :)$ è una struttura algebrica.

Def: Un **gruppo** è una struttura algebrica

$(G, *)$

data da un insieme G ed una operazione binaria $*: G \times G \to G$ tale che:

1) $\exists\, e \in G : \forall g \in G : \; e * g = g * e = g$

(elemento neutro).

es. in $(\mathbb{Z}, +)$
$e = 0$

2) $\forall a \in G \; \exists\, a' \in G : \; a * a' = a' * a = e$

(inverso)

es in $(\mathbb{Z}, +)$
$a \in \mathbb{Z}$
$a + (-a) =$
$= (-a) + a = 0$

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

(prop. associativa)

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

→ Se $\forall a,b \in G : a*b = b*a$

allora il gruppo G è detto **ABELIANO**

o **COMMUTATIVO**.

Esempi

$(\mathbb{N},+)$ non è un gruppo

el. neutro $0 \in \mathbb{N}$ e $0+a = a+0 = a$ ✓

prop. associativa: $\forall a,b,c \in \mathbb{N}$ $a+(b+c) = (a+b)+c$ ✓

inverso cioè $\forall a \in \mathbb{N}\ \exists b \in \mathbb{N}$ con $a+b=0$ ✗

No

Non ci sono gli INVERSI.

$(\mathbb{Z},+)$ è un gruppo abeliano. ✓

$(\mathbb{Z},\cdot)$ el neutro = 1 mancano gli inversi.

associativo OK

$(\mathbb{Q}, \cdot)$ non è un gruppo

perché $\forall$ elemento di $\mathbb{Q} \neq 0$

ammette inverso, ma 0 no!

$(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo abeliano.

perché parliamo di $(\mathbb{Z}, +)$ e non $(\mathbb{Z}, -)$.

partendo da $(\mathbb{Z}, +)$ posso definire

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

ove $(-b)$ è l'inverso di b rispetto l'operazione $+$

In $(\mathbb{Z}, -)$ non c'è manco l'elemento neutro!

$a - 0 = a$ $\qquad$ $0 - a = -a \neq a$ se $a \neq 0$

$(a-b)-c \neq a-(b-c) = a-b+c$!!

Gruppi infiniti

Esempio di gruppo finito

$\mathbb{Z}_1 = \{0\}$ con $+$ GRUPPO BANALE

XOR

$\oplus$	0	1
0	0	1
1	1	0

$\mathbb{Z}_2 = \{0,1\}$ con $+$ è un gruppo commutativo.

con 0 = el. neutro.

AND

$\wedge$	0	1
0	0	0
1	0	1

RISPETTO $\wedge$ $\mathbb{Z}_2$ non è un gruppo.

ma $\mathbb{Z}_2 \setminus \{0\}$ sì.

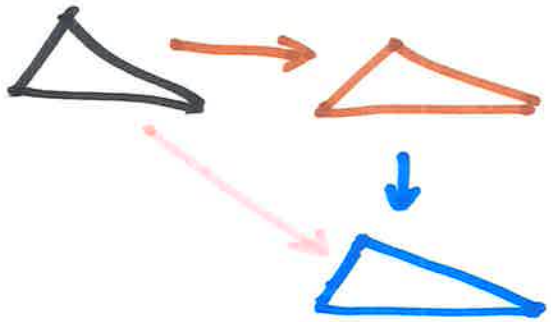
Esempi di gruppi: → ROTAZIONI DEL PIANO

→ TRASLAZIONI DEL PIANO

TRASLAZIONE: funzione $A_2 \longrightarrow A_2$

piano affine — piano affine

MANDA PUNTI IN PUNTI.



Sia A un insieme e sia

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

$\Rightarrow S(A)$ con la composizione di funzioni è un gruppo.

(detto gruppo Simmetrico su A).

<u>oss</u> 1) Se $f, g \in S(A) \Rightarrow f \circ g \in S(A)$

2) $id_A : a \to a \in S(A)$ e $f \circ id_A = id_A \circ f = f$

identità $\in S(A)$.

3) $\forall f \in S(A)$, $f^{-1} \in S(A)$ ed è una funzione e

$f^{-1} \circ f = f \circ f^{-1} = id_A$

4) $\forall f, g, h \in S(A)$

$$f \circ (g \cdot h) = (f \circ g) \cdot h$$

$S(A)$ è un gruppo. NON COMMUTATIVO!

Se X è un insieme di funzioni biiettive

$$A \to A$$

tale che $\forall f \in X,\ f^{-1} = f^{-} \in X$

e $\forall f, g \in X : f \circ g \in X$

$\Rightarrow X$ è un gruppo SOTTOGRUPPO di $S(A)$

GRUPPO = st. algebrica con 1 operazione

ANELLO (commutativo con unità) = st. algebrica con 2 operazioni

CAMPO

MODELLO DI ANELLO (commutativo con 1) $\longrightarrow (\mathbb{Z}, +, \cdot)$

MODELLO DI CAMPO $\longrightarrow (\mathbb{Q}, +, \cdot)$

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

Def: Una struttura algebrica $(A, +, \cdot)$ è detta anello se

1) $(A, +)$ è un gruppo abeliano
2) $\exists 1 \in A : \forall b \in A : 1 \cdot b = b \cdot 1 = 1$

3) $\forall a, b \in A : \quad a \cdot b = b \cdot a$

4) $\forall a, b, c \in A: \quad a \cdot (b+c) = a \cdot b + a \cdot c$

5) $\forall a, b, c \in A: \quad a \cdot (b+c) = a \cdot b + a \cdot c$

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

[proprietà ~~associative~~ distributiva]

Esempio $\mathbb{R}[x] = \{ a_0 + a_1 x + \dots \mid a_i \in \mathbb{R} \}$

polinomi nella indeterminata x
a coeff. in $\mathbb{R}$
con somma e prodotto di polinomi

$$(a_0 + a_1 x + \dots + a_n x^n) + (b_0 + b_1 x + \dots + b_n x^n) =$$

$$= (a_0 + b_0) + (a_1 + b_1) x + \dots (a_n + b_n) x^n$$

$$f(x) = \sum_{i=0}^{h} a_i x^i \qquad g(x) = \sum_{j=0}^{m} b_j x^j$$

$$(f \cdot g)(x) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

$$(2+X+X^2)\cdot(1-X) = 2+X+X^2-2X-X^2-X^3$$

comm. con 1

CAMPO $(\mathbb{K}, +, \cdot)$ è un anello ^{v} in cui $(\mathbb{K}\setminus\{0\}, \cdot)$ è un gruppo.

- $(\mathbb{K}, +)$ gruppo abeliano
- $(\mathbb{K}\setminus\{0\}, \cdot)$ gruppo abeliano

$\mathbb{K}\setminus\{0\} = \mathbb{K}^*$

- $(a+b)\cdot c = ac+bc$
  $a\cdot(b+c) = ab+ac$ | ASSOCIATIVE

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

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

$(\mathbb{Z}_2, \oplus, \wedge)$ campo

$\mathbb{K}$

$\oplus$	0	1
0	0	1
1	1	0

$\wedge$	0	1
0	0	0
1	0	1

$(\mathbb{Z}_3, +, \cdot)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

0...

$(\mathbb{Z}_4, +, \cdot)$ é um 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

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

No!

$(\mathbb{F}_4, +, \cdot)$

+	(00)	(10)	(11)	(01)
(00)	(00)	(10)	(11)	(01)
(10)	(10)	(00)	(01)	(11)
(11)	(11)	(01)	(00)	(10)
(01)	(01)	(11)	(10)	(00)

·	(00)	(10)	(11)	(01)
(00)	(00)	(00)	(00)	(00)
(10)	(00)	(10)	(11)	(01)
(11)	(00)	(11)	(01)	(10)
(01)	(00)	(01)	(10)	(11)

$\mathbb{Z}_n = \{0, 1, 2 \ldots n-1\}$.

$(a+b)_n :=$ $(a+b)$ diviso n prendendo il resto. $= (a+b) \% n$

$(a \cdot b)_n =$ $(a \cdot b)$ diviso n prendo il resto $= (a \cdot b) \% n$

n è un primo $\Rightarrow$ $(\mathbb{Z}_n, +, \cdot)$ è un campo

n non è primo $\Rightarrow$ $(\mathbb{Z}_n, +, \cdot)$ anello ma non campo.