

$$f: A \rightarrow B$$

$$f \subseteq A \times B$$

$$\forall a \in A \exists ! b \in B : (a, b) \in f$$

$$f(a) = b$$

$$\text{Se } f: A \rightarrow B$$

$$g: B \rightarrow C$$

$$(g \circ f): A \rightarrow C$$

$$(a, c) \in (g \circ f) \Leftrightarrow \exists b \in B \text{ con}$$

$$(a, b) \in f \text{ e } (b, c) \in g$$

COMPOSIZIONE DI FUNZIONI È ASSOCIATIVA.

$f: A \rightarrow B, g: B \rightarrow C$ $h: C \rightarrow D$ funzioni

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

$$h \circ g \circ f$$

oss: $(g \circ f)$ si può fare $\Leftrightarrow$ il dominio di g coincide col codominio di f .

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

$$f: A \rightarrow B.$$

immagine
di f

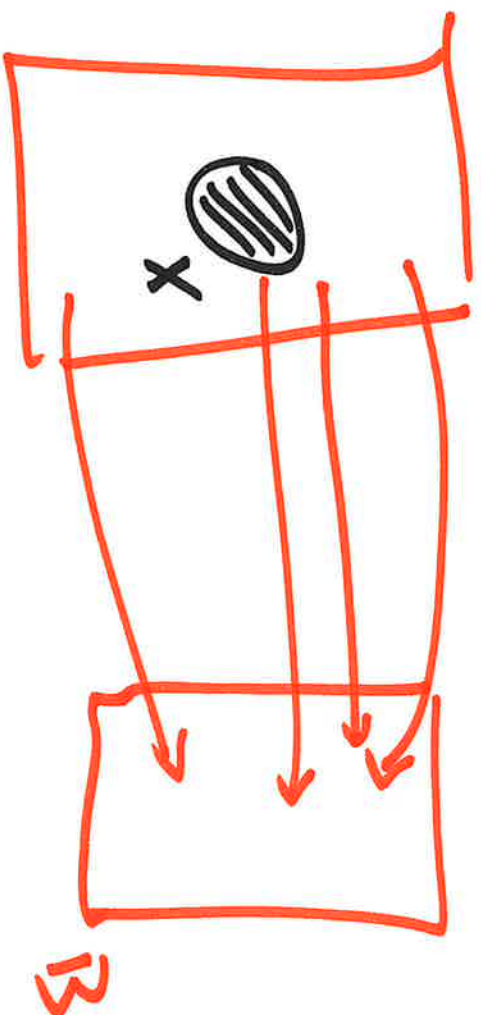
Se $X \subseteq A$

$$f(X) = \{ f(x) : x \in X \}.$$

Restrizione di f ad $X \subseteq A$

$$f|_X: X \rightarrow B.$$

$$f|_X := \{ (x, f(x)) \in X \times B \}.$$



A

B

Troncamento di f ad $Y \subseteq B$

• Serve che $\text{Im}(f) \subseteq Y$.

$$f|_Y := \{(a, b) \in f \mid a \in A\} \subseteq A \times Y$$

$$f|_Y : A \rightarrow Y$$

$$f: A \rightarrow B$$

OSS: f è suriettiva $\Leftrightarrow$

$$\forall b \in B \exists a \in A : f(a) = b$$

OGNI FUNZIONE TRONCATA ALLA SUA
IMMAGINE È SURIETTIVA.

$f|_{\text{Im } f}$ è suriettiva!

Sia $\text{Im } f$ insieme dei numeri naturali incluso lo 0.

$$f: \mathbb{N} \rightarrow \mathbb{N}$$

$$x \rightarrow 2x$$

f è iniettiva in $f|_{\text{Im } f}$

$$\text{Se } f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow$$

$$x = y$$

MA NON È SURIETTIVA: $\text{Im } f = 2\mathbb{N} =$

$= \{2n | n \in \mathbb{N}\}$ numeri naturali
pari.

$+1 \notin \text{Im } f.$

$f: 2\mathbb{N} \rightarrow \mathbb{N}$ è invece biettiva
 $x \rightarrow 2x$

Sia X un insieme.

La funzione $\text{id}_X: X \rightarrow X$ è detta

funzione identica su X

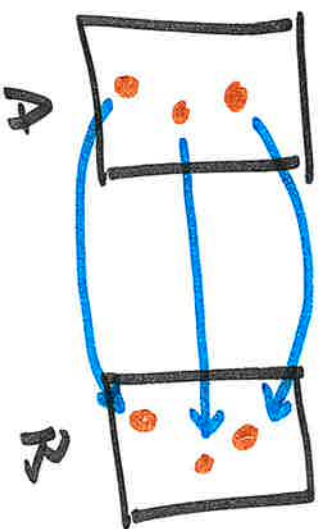
$\text{id}_X = \{ (x, x) : x \in X \}.$

Una funzione $f: A \rightarrow B$ è detta
invertibile con inversa $f^{-1}: B \rightarrow A$
se esiste f^{-1} tale che

$$\begin{cases} f \circ f^{-1} = \text{id}_B \\ f^{-1} \circ f = \text{id}_A \end{cases}$$

Teorema: f è invertibile $\Leftrightarrow f$ è biettiva

In tale caso $f^{-1} = f^{\text{opp}} = \{ (b, a) : (a, b) \in f \}$.



N.B.: 1) serve che f sia suriettiva.

Altrimenti avremmo $\text{Im}(f) \subsetneq B$

$$f \circ f^{-1} = \text{id}_B$$

e quindi $\exists b \notin \text{Im}(f)$ e dunque

$$f \circ f^{-1}(b) \neq b \quad \text{e}$$

2) serve che f sia iniettiva.

Altrimenti $\exists b \in B$ e $a, a' \in A$

$$\text{tale che } f(a) = f(a') = b.$$

$$f^{-1} \circ f = \text{id}_A$$

come possiamo definire $f^{-1}(b)$

$$(f^{-1} \circ f)(a) = a \Rightarrow f^{-1}(b) = a \quad \text{e}$$

$$(f^{-1} \circ f)(a') = a' \Rightarrow f^{-1}(b) = a' \quad \text{e}$$

$\Rightarrow f$ invertibile $\Rightarrow f$ biiettiva.

Viceversa

f biiettiva $\Rightarrow$ possiamo $f^{-1} := \{(b, a) \mid (a, b) \in f\}$.

$$\forall a \in A : (f^{-1} \circ f)(a) = f^{-1}(b) = a$$

✓

$$\forall b \in B : (f \circ f^{-1})(b) = f(a) = b$$

□

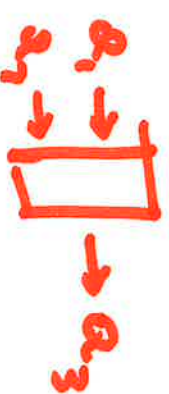
In generale se $f: A \rightarrow B$ ed $Y \subseteq B$
scriviamo $f^{-1}(Y) := \{a \in A : f(a) \in Y\}$.

PREIMMAGINE DI Y .

N.B. Non è detto che f^{-1} sia una funzione!

Si A un insieme.

Si dice operazione binaria su A
una funzione $f: A \times A \rightarrow A$.



Insiemi numerici

$\mathbb{N} \rightarrow$ insieme numeri naturali $\mathbb{N}_0 \{0, 1, \dots\}$
 $\mathbb{Z} \rightarrow$ insieme di numeri interi $\{\dots, -1, 0, 1, \dots\}$

$\mathbb{Q} \rightarrow$ insieme di numeri frazionari $\{\frac{a}{b} : a, b \in \mathbb{Z}\}$

$\mathbb{R} \rightarrow$ insieme di numeri reali

$\mathbb{C} \rightarrow$ insieme di numeri complessi.

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

$(\mathbb{N}_0, +)$ $\mathbb{N}$ include 0 con la somma.

1) $\forall a, b \in \mathbb{N}_0 : a + b \in \mathbb{N}_0$ è una operazione.

2) $\exists 0 \in \mathbb{N}_0 : 0 + a = a + 0 = a$ el. neutro.

3) $\forall a, b, c \in \mathbb{N}_0 : (a + b) + c = a + (b + c)$ prop. associativa.

4) $\forall a, b \in \mathbb{N}_0 : a + b = b + a$ prop. commutativa
 $(\mathbb{N}_0, +)$ è abeliano

Def. $(A, *)$ è una struttura algebrica con
 $* : A \times A \rightarrow A$ una operazione binaria.

Si dice che $(A, *)$ è un monoid se

1) $\exists e \in A : e * a = a * e = a \quad \forall a \in A$ el. neutro

2) $\forall a, b, c \in A : (a * b) * c = a * (b * c)$ prop. associativa

Monoid

Def: Una struttura algebrica

$(G, *)$ con $*$ op. binaria su G è detta

GRUPPO se

- 1) $\exists e \in G: \forall g \in G: e * g = g * e = g$ (EL. UNITARIO)
- 2) $\forall g \in G \exists \bar{g} \in G: g * \bar{g} = \bar{g} * g = e$ (EL. INVERSO).
- 3) $\forall a, f, g, h \in G: f * (g * h) = (f * g) * h$
(PROP. ASSOCIATIVA).

$(G, *)$ è un GRUPPO ABELIANO

Se è un GRUPPO E $\forall a, b \in G: a * b = b * a$.

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

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

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

$$\forall a, b, c \in \mathbb{Z}: (a+b)+c = a+(b+c).$$

$$\forall a, b \in \mathbb{Z}: a+b = b+a.$$

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

N.B. $(\mathbb{Z}, +)$ gruppo. $\rightarrow$

$(\mathbb{Z}, -)$ non è un gruppo.

$$a-0 = a \quad \text{ma} \quad 0-a = -a \neq a \quad (\text{ex } a \neq 0)$$

$$a-b \neq b-a$$

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

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi
abeliani.

$(\mathbb{Z}, \cdot)$ non è un gruppo perché

1) $1 \in \mathbb{Z}$ & $\forall z \in \mathbb{Z} : 1 \cdot z = z \cdot 1 = z$ el. neutro.

2) $\forall a, b, c \in \mathbb{Z} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ass.

3) Non $\exists a \in \mathbb{Z}$ tale che $z \cdot a = 1$

Non ci sono gli inversi (mult.).

$(\mathbb{Q}, \cdot)$ non è un gruppo perché

Non $\exists a \in \mathbb{Q} : a \cdot 0 = 1$

$(\mathbb{Q}^*, \cdot)$ ove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ è un gruppo.

$(\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ sono gruppi
 o.e. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Esempio di gruppo non abeliano.

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

con operazione la composizione di funzioni.

i	f_1	f_2	f_3	f_4	f_5
123	123	123	123	123	123
123	432	213	321	312	231
123				231	312

↓

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

1) $\forall f \in S_3 : i \circ f = f \circ i = f$

2) $\forall f \in S_3 \exists f^{-1} \in S_3 : f \circ f^{-1} = f^{-1} \circ f = e$

3) $\forall f, g \in S_3 : (f \circ g) \circ h = f \circ (g \circ h)$.

$$f_2 \circ f_2 \neq f_2 \circ f_2$$

$$\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array} \downarrow f_2$$

$$\begin{array}{ccc} 2 & 3 & 1 \end{array} \downarrow f_2$$

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array} \downarrow f_2$$

$$\begin{array}{ccc} 3 & 1 & 2 \end{array} \downarrow f_2$$

S_3 non è commutativo.

$S_n :=$ gruppo delle permutazioni (=f. biettive) su n elementi.

$|S_n| = n!$ e S_n se $n \geq 2$ non è mai commutativo.

In un gruppo $(G, *)$, ha senso voler risolvere l'equazione

$$a * x = b \rightarrow x = a^{-1} * b$$

in fact

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

||

$$(a^{-1} * a) * \cancel{x} = e * x = x$$

$$a * x = b \Rightarrow f(a * x) = f(b)$$

$\Downarrow$

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

⚠

N.B

$$\boxed{a^{-1} * (a * \cancel{x})} \neq (b) * \underline{a^{-1}}$$

||

in general

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

Anelli e campi

$(\mathbb{Z}, +, \cdot)$ Anello (commutativo con 1).

Anello: struttura algebrica con 2 operazioni
 $(A, *, \Delta)$ tale che

1) $(A, *)$ è un gruppo abeliano.

2) Δ è una operazione associativa

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

3) Valgono le prop. distributive. $\forall a, b, c \in A$

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

$$(a * b) \Delta c = (a \Delta c) * (b \Delta c). \quad \text{— Associativity}$$

4) commutativo se $a \Delta b = b \Delta a \quad \forall a, b \in A$
 5) con 1 (con unità) se $\exists u \in A: \forall a \in A$
 ~~$u \Delta a = a \Delta u = a$~~

$$u \Delta a = a \Delta u = a.$$

oss: Sia e l'elemento neutro di $*$

$$\text{Allora } \forall x \in A: e \Delta x = x \Delta e = e$$

$(\mathbb{Z}, +, \cdot)$ è un anello. Allora comunque
 sia definito il prodotto si ha
 $0 \cdot x = 0 \quad \forall x \in \mathbb{Z}.$

$$0+0=0$$

via $x \in \mathbb{Z}$ $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$

somma a dx e x l'elemento $(-0 \cdot x)$

$$\underbrace{(-0 \cdot x) + (0 \cdot x)}_{=} = (-0 \cdot x) + (0 \cdot x + 0 \cdot x)$$

$$\underbrace{\quad}_{0}$$

$$\underbrace{((-0 \cdot x) + (0 \cdot x))}_{0} + 0 \cdot x$$

$$\underbrace{\quad}_{0}$$

$$\underbrace{\quad}_{0 \cdot x}$$

$$0 \cdot x$$

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

Def: $(K, +, \cdot)$ è un campo se

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

2) $(K, \cdot)$ è un gruppo abeliano

3) valgono le prop. distributive.

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

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

$(K, +, \cdot)$ è un campo se è come un campo
ma $(K, \cdot)$ non è abeliano

In un campo è sempre possibile
risolvere l'equazione lineare

$$\boxed{a \cdot x + b = 0} \quad \text{con } a \neq 0$$

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

$$a \cdot x + (b + (-b)) = (-b)$$

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

$$a \cdot x = (-b)$$

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

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

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

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

✱