$f: A \to B$ biiettiva

$\Leftrightarrow$ $f^{opp}: B \to A$ è una funzione

(in tal caso biiettiva e

$$f^{opp} \circ f = \iota_A \qquad f \circ f^{opp} = \iota_B$$

ove $\iota_A : \begin{cases} A \to A \\ x \to x \end{cases}$ $\iota_B : \begin{cases} B \to B \\ x \to x \end{cases}$

Sia X un insieme (finito) e consideriamo l'insieme $S(X) = \{f : X \to X$ tali che f biiettiva$\}$.

oss: se $|X| = n$ $|S(X)| = n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$.

$X = \{a, b, c \dots\}$. $f : X \to X$ biiettiva

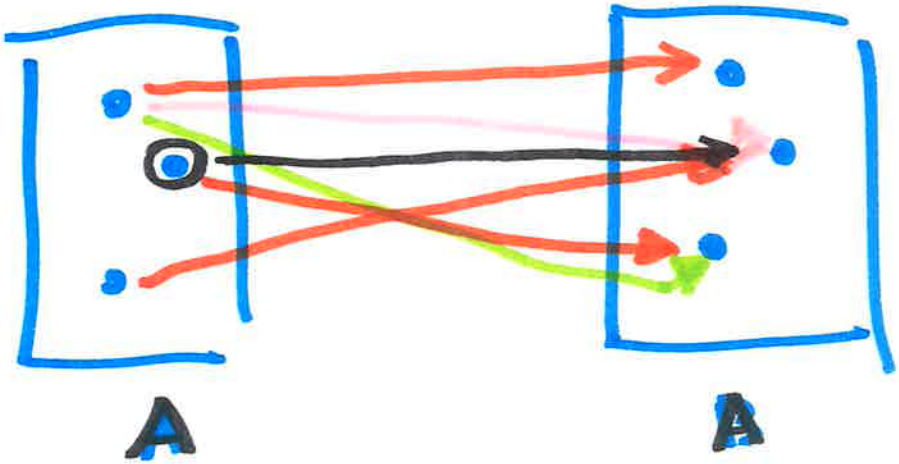
$f(a) =$ n possibilità

$f(b) =$ $n-1$ possibilità
(ogni elemento di X tranne $f(a)$)

$\vdots$

$f(z) =$ 1 possibilità
(ogni elemento di X tranne quelli già indicati ... ma quelli indicati sono tutti tranne 1)

$n!$



1 - arrivo

$3 \times 2 \times 1 = 6$

Siano $f : X \to X$, $g : X \to X$ due elementi di $S(X)$

[$S(X)$ gruppo simmetrico su X]

$\Rightarrow (g \circ f) : X \to X$ biiettiva

$\forall x \in X \; \exists! \, y \in X : f(x) = y$ & $\forall y \in X \; \exists! \, x \in X : f(x) = y$

$\forall x \in X \; \exists! \, y \in X : g(x) = y$ & $\forall y \in X \; \exists! \, x \in X : g(x) = y$

Sia $z \in X \Rightarrow \exists\, y \in X$ tale che $g(z) = y$

perché g suriettiva

$\forall\, y \in X \Rightarrow \exists\, x \in X$ tale che $f(x) = y$

$\Rightarrow (g \circ f)(x) = g(f(x)) = g(y) = z$

e quindi $(g \circ f)$ è suriettiva.

Supponiamo $(g \circ f)(x) = (g \circ f)(x')$

allora $g(f(x)) = g(f(x'))$ ma g

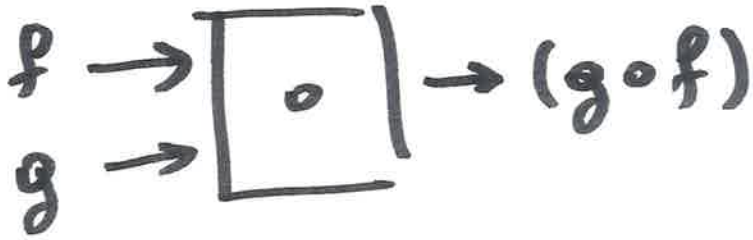
è iniettiva $\Rightarrow$ $f(x) = f(x')$

ma anche f è iniettiva $\Rightarrow$ $x = x'$

$\rightarrow (g \circ f)$ è iniettiva.

insieme $S(X)$

$$\circ : S(X) \times S(X) \to S(X)$$



Def: Sia A un insieme. Si dice operazione (binaria) su A una funzione Δ

$$\Delta : A \times A \to A$$

Si dice struttura algebrica una lista formata da un insieme ed una o più operazioni su di esso.

ALGEBRA → STUDIO DELLE STRUTTURE ALGEBRICHE.

Esempi $(S(X), \circ)$ dove X insieme, $\circ$ composizione di funzioni.

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

$(\mathbb{N}_0, +)$ $(\mathbb{Z}, -)$ BRUTTA

$(\mathbb{N}_0, \cdot)$ $(\mathbb{Z}, \cdot)$ $(\mathbb{Z}, +, \cdot)$

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

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

NON É STRUTTURA ALGEBRICA $(\mathbb{N}, -)$

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

proprietà di $(S(X), \circ)$

1) $\exists$ la funzione $\iota_x : \begin{cases} X \to X \\ z \to x \end{cases}$

tale che $\boxed{\iota_x \circ f = f \circ \iota_x = f}$

$$f(\iota_x(x)) = f(x) = \iota_x(f(x))$$

esiste l'elemento neutro.

2) $\forall\, f \in S(X) \quad \exists\, f^{opp} \in S(X)$

$$\boxed{(f^{opp} \circ f)(x) = (f \circ f^{opp})(x) = x} \qquad \forall x \in X$$

$f^{opp} =: f^{-1}$ è detto inverso dell'elemento f

perché $\boxed{f^{opp} \circ f = f \circ f^{opp} = \iota_x}$

3) vale la proprietà associativa.

$\forall f,g,h \in S(X)$: $\boxed{f \circ (g \circ h) = (f \circ g) \circ h}$

ed in $(\mathbb{Z}, +)$?

1) $\forall a \in \mathbb{Z}$ $\boxed{a + 0 = 0 + a = a}$

0 el. neutro

2) $\forall a \in \mathbb{Z}$ $\exists (-a) \in \mathbb{Z}$: $\boxed{a + (-a) = (-a) + a = 0}$

esiste "inverso".

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

Def: Una struttura algebrica $(G, *)$ è detta **gruppo** se $* : G \times G \to G$ è una operazione binaria su G e

1) $\forall \exists\, e \in G : \forall g \in G : e * g = g * e = g$
(elemento neutro)

2) $\forall g \in G \; \exists\, \tilde{g} \in G : g * \tilde{g} = \tilde{g} * g = e$
(ogni elemento ammette inverso)

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

Esempi $(S(X), \circ)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
$(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}^*, \cdot)$

ove $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ $\quad$ $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$.

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

$(\mathbb{N}, +)$ → non c'è nemmeno l'elemento
neutro (però vale la
prop. associativa).

$(\{-1, +1\}, \cdot)$ è un gruppo

$(\mathbb{Z}, \cdot)$ non lo è

$(\mathbb{Z}, -)$ NON È UN GRUPPO.
NON SODDISFA NESSUNA DELLE PROP.

In $(\mathbb{Z}, -)$ non esiste elemento neutro

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

a maggior ragione non si può parlare di inverso anche se $\forall a : a - a = 0$

NON VALE LA PROPRIETÀ ASSOCIATIVA

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

$$2 - (3 - 5) \neq (2 - 3) - 5$$

$$\| \qquad\qquad \|$$

$$4 \qquad\qquad -6$$

In generale in $\mathbb{Z}$ si definisce la

sottrazione di due numeri come

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

somma

opposto di b rispetto la somma.

$(\mathbb{Z}, +)$

similmente in $(\mathbb{R}^\times, \cdot)$ definiamo $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.

$$a/b := a \cdot b^{-1}$$

prodotto

reciproco = opposto di b rispetto al prodotto.

Def: Un gruppo $(G, *)$ è detto **commutativo** o **abeliano** se $\forall g, h \in G : g * h = h * g$

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$] sono gruppi commutativi

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

$GL_n(\mathbb{K})$ con prodotto di matrici.
gruppo delle matrici $n \times n$ in $\mathbb{K}$
con determinante $\neq 0$
rispetto prodotto righe per colonne
(gruppo generale lineare delle
matrici di ordine n in $\mathbb{K}$)

Gruppo banale

$(\{1\}, *)$ $\quad 1*1=1$

$1 = 1*(1*1) = (1*1)*1 = 1$

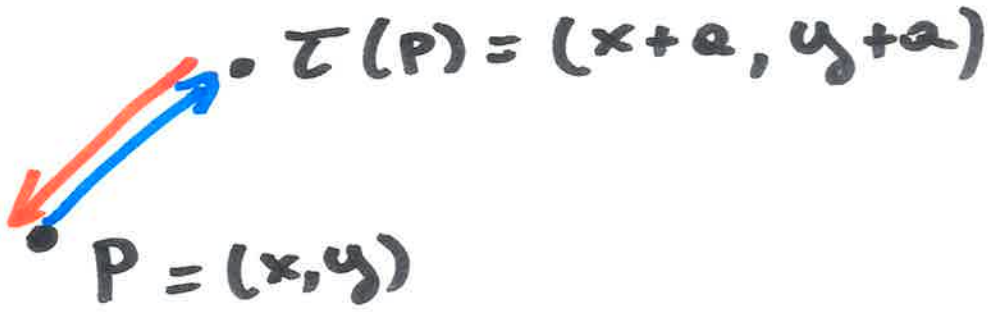
$(\{0\}, +)$

Gruppo delle traslazioni in un piano euclideo.

(x, y)

$P=(x,y) \longrightarrow \tau_{(a,b)}(x,y) =$

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



TRASLARE CON $\tau_{(0,0)}$ lascia tutti i punti invariati.

$$\tau_{(a,b)} \circ \tau_{(0,0)} = \tau_{(a,b)}$$

$$\tau_{(0,0)} \circ \tau_{(a,b)} = \tau_{(a,b)}$$

$\exists$ elemento neutro rispetto la comp. di funzioni

$$\tau_{(a,b)} \circ \tau_{(-a,-b)} = \tau_{(-a,-b)} \circ \tau_{(a,b)} = \tau_{(0,0)}$$

$$= \tau_{(a+c,\, b+d)} \left(x+e \quad y+f \right)$$

$$= \left[x+(a+c)+e,\; y+(b+d)+f \right]$$

$$= \left(x+(a+e)+c,\; y+(b+f)+d \right)$$

$$= \left(x+(c+e)+a,\; y+(d+f)+b \right)$$

$$= \tau_{(a,b)} \left(x+(c+e),\; y+(d+f) \right)$$

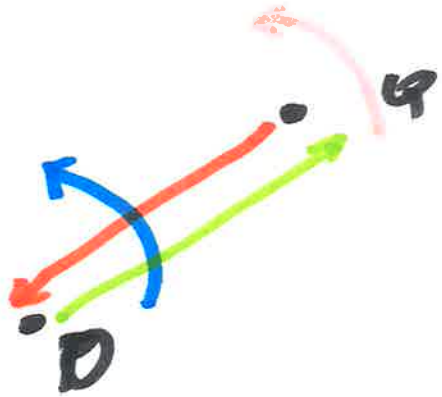
$$= \tau_{(a,b)} \left(\tau_{(c,d)} \left(x+e,\; y+f \right) \right)$$

$$= \tau_{(a,b)} \left(\tau_{(c,d)} \left(\tau_{(e,f)} (x,y) \right) \right)$$

$$= \tau_{(a,b)} \circ \left(\tau_{(c,d)} \circ \tau_{(e,f)} \right) (x,y)$$

$$\tau_{(a+c,b+d)} \circ \tau_{(e,f)} \quad (x,y) =$$

$$= \left(\tau_{(a,b)} \circ \tau_{(c,d)}\right) \circ \tau_{(e,f)} \quad (x,y)$$



Un gruppo é l'ambiente in cui si può sempre risolvere una equazione

$$a \cdot x = b$$

(ove indico con $\cdot$ l'operazione di gruppo)

$ax = b$ $\quad\quad$ $\exists!$ soluzione

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

N.B. $a^{-1}b \neq ba^{-1}$ in generale

in particolare per le matrici

$A^{-1}B \neq BA^{-1}$

oss: G gruppo $\Rightarrow$ l'operazione è denotata con $+$ si indicherà l'elemento neutro con 0 o 0_G o $\underline{0}$

e l'opposto di $g \in G$ con $(-g)$

NOTAZIONE ADDITIVA

G gruppo e l'operazione è denotata con $\cdot$ si indicherà l'elemento neutro con 1, 1_G. I e l'opposto di $g \in G$ con g^{-1}

NOTAZIONE MOLTIPLICATIVA

DI SOLITO I GRUPPI IN NOTAZIONE ADDITIVA SONO COMMUTATIVI, cioè

$a+b = b+a \quad \forall a, b.$

Def: Sia X un insieme, si dice **sequenza** di elementi di X una funzione

$s : \mathbb{N}_n \longrightarrow X$ ove $\mathbb{N}_n = \{1, 2, \dots n\}$.

Una sequenza è una "struttura dati" che raccoglie elementi di X con ripetizioni e preservando l'ordine.

$$s = (x_1, x_2 \dots x_n) \qquad x_i \in X$$

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

SEQUENZA $(a,b,c) \neq (c,b,a) \neq (a,a,b,b,c) \neq$

$\neq (a,b\ b\ b,c)$

Si come i-esimo elemento di $s = s(i)$

Dato X chiamiamo X^n l'insieme di tutte le possibili sequenze di lunghezza n di elementi di X

$X = \{a, b, c\}$

$|X| = 3$

$|X^3| = 3^3 = 27$

$X^3 = \{$ (a a a) (a b a) (a c a)
(a a b) (a b b) (a c b)
(a a c) (a b c) (a c c)
(b a a) (b b a) (b c a)
(b a b) (b b b) (b c b)
(b a c) (b b c) (b c c)
(c a a) (c b a) (c c a)
(c a b) (c b b) (c c b)
(c a c) (c b c) (c c c) $\}$.

$\neq (X \times X) \times X \neq X \times (X \times X)$

formalmente sono diversi:

PRATICAMENTE LI IDENTIFICHIAMO!

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

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

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

Sia $(G, *)$ un gruppo.

Allora $(G^n, *^n)$ dove con

$(g_1 \dots g_n) *^n (h_1 \dots h_n) :=$

$(g_1 * h_1 \dots g_n * h_n)$ è un gruppo.