$f: X \to Y$

$$f \subseteq \{(x,y) \mid x \in X, y \in Y\}.$$

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

$f: \{a,b,c\} \to \{1,2\}.$

$f(a)=1$
$f(b)=1$
$f(c)=2$

$f = \{(a,1), (b,1), (c,2)\} \subseteq X \times Y$

$f^{opp} = \{(1,a), (1,b), (2,c)\} \subseteq Y \times X$

$f^{opp} := \{(y,x) \in Y \times X \mid (x,y) \in f\}.$

se f funzione, quando f^{opp} è una funzione?

Se e solamente se f è biiettiva.

1) Serve che $\forall y \in Y \; \exists (y,x) \in f^{opp}$ con qualche $x \in X$

$\Rightarrow \forall y \in Y \; \exists x \in X : (x,y) \in f \Rightarrow f$ è suriettiva

[ALTRIMENTI CI SAREBBERO ELEMENTI DI Y SU CUI f^{opp} NON È DEFINITA].

2) Serve che $\forall y \in Y \ \exists_{\leq 1} x \in X$ tale che $(y,x) \in f^{opp}$

$\iff \forall y \in Y \ \exists_{\leq 1} x \in X : (x,y) \in f \implies$

f è iniettiva

[ALTRIMENTI f^{opp} non è funzionale]

$1+2 \iff f$ è biiettiva.

→ A cosa corrisponde f^{opp} quando f biiettiva.

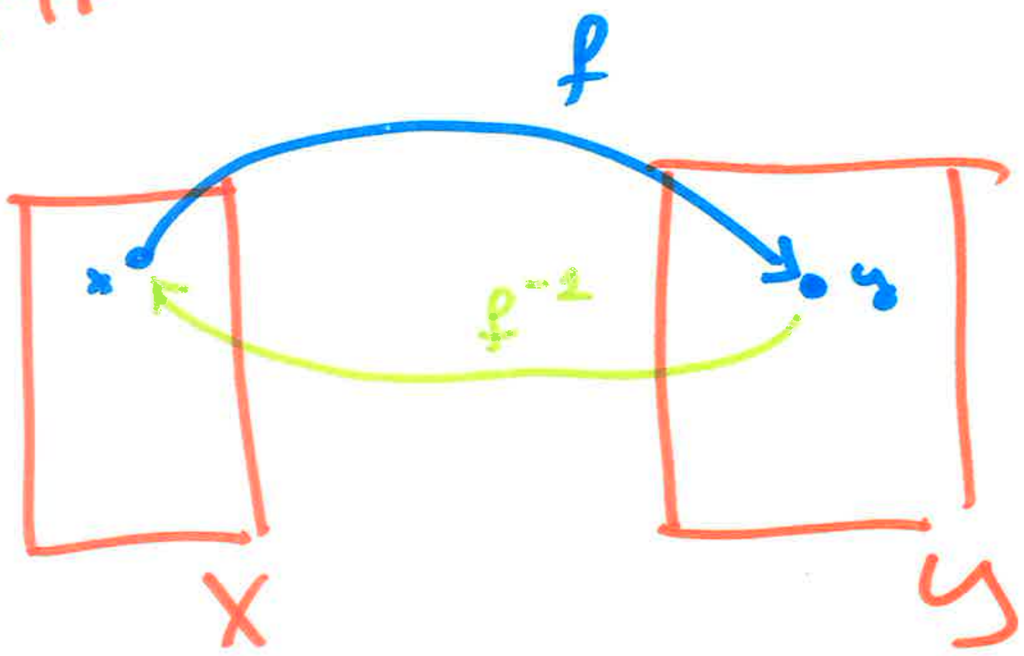
$f^{opp} \circ f : X \to X$ ed è la funzione $\iota_X(x) = x$

$f \circ f^{opp} : Y \to Y$ ed è la funzione $\iota_Y(y) = y$

ι_X, ι_Y funzioni identiche su X, Y

Si dice che f^{opp} é la funzione inversa di f

$f^{-1} = f^{opp}$



Def. <u>**Sequenza**</u>: lista ordinata con ripetizioni di elementi di un insieme.

$(a,b,c) \neq (a,c,b)$ $\quad$ $\{a,b,c\} = \{a,c,b\}$.

$(a,a,b) \neq (a,b)$ $\quad$ $\{a,a,b\} = \{a,b\}$.

sequenze di elementi $\quad$ insiemi

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

Definiamo $\mathcal{J}_n = \{1,2,\dots,n\}$ insieme dei primi n numeri naturali.

Una sequenza di n elementi di X (insieme) è una funzione $\sigma : \mathcal{J}_n \to X$
(ad ogni intero $1 \leq i \leq n$ associa un elemento di X).

$$(a,b,a) \to \{(1,a),(2,b),(3,a)\}.$$

$$(a,a,b) \to \{(1,a),(2,a),(3,b)\}.$$

⌜Nulla ci vieta di identificare gli elementi di $X \times X$ con seq. ordinate di elementi di X di lunghezza 2. ⌟

$\underbrace{(a,b)}_{\text{coppia ordinata}} = \{a,\{a,b\}\}.$

I

$\underbrace{(a,b)}_{\text{sequenza}} = \{(1,a),(2,b)\}.$

II

si comportano al medesimo modo.

OSS 2.

Siano X, Y, Z tre insiemi

$$X \times (Y \times Z) = \{(x, (y, z)) \mid x \in X, y \in Y, z \in Z\}$$

$$(X \times Y) \times Z = \{((x, y), z) \mid x \in X, y \in Y, z \in Z\}.$$

COME INSIEMI SONO DIVERSI!
però in entrambi i casi vogliamo considerare terne di elementi di cui il primo in X, il secondo in Y ed il terzo in Z.

In generale scriveremo $(X \times Y \times Z)$ e rappresenteremo i suoi elementi come (x, y, z).

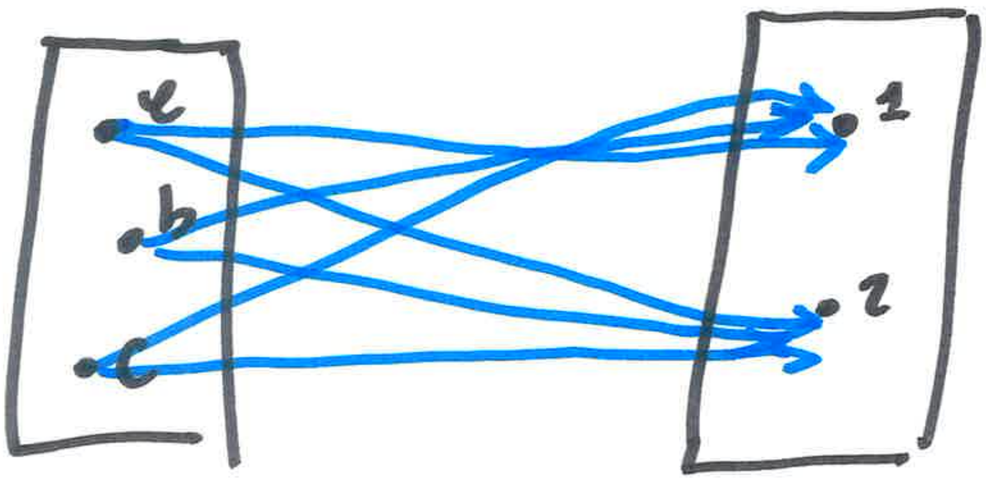
Sia X un insieme, $i \geq 1$ un intero positivo
Definiamo come X^n il prodotto cartesiano
$X \times X \times \dots \times X$ n volte ovvero (identificato con) l'insieme di tutte le sequenze ordinate di lunghezza n di elementi di X.

$$X^n = \{\sigma : J_n \to X\}.$$

$X = \{1, a, \Delta\}$

$X^2 = \{(1,1), (1,a), (1,\Delta),$
$(a,1), (a,a), (a,\Delta),$
$(\Delta,1), (\Delta,a), (\Delta,\Delta)\}.$

$X^3 = \{(1,1,1), (1,1,a), (1\ 1\ \Delta), (1\ a\ 1), (1\ a\ a),$
$(1\ a\ \Delta)$ etc etc. etc. $\}$.



Supponiamo che $|X| = m$, $|Y| = n$

$$\Rightarrow |X \times Y| = m \cdot n$$

abbiamo m possibilità per il primo elemento della coppia e n possibilità per il secondo.

$$|X^n| = |X|^n$$

Insiemi → NON ORDINATO
SENZA RIPETIZIONI

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

sequenze. → ORDINATA
CON RIPETIZIONI.

$\mathcal{J}_n \longrightarrow X$

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

sistema di elementi → NON ORDINATO
(multi insieme). CON RIPETIZIONI.

$[a,b,c] = [b,c,a]$
$[a,a,b] \neq [a,b]$

lo si implementa con una funzione $\nu : X \to \mathbb{N}$

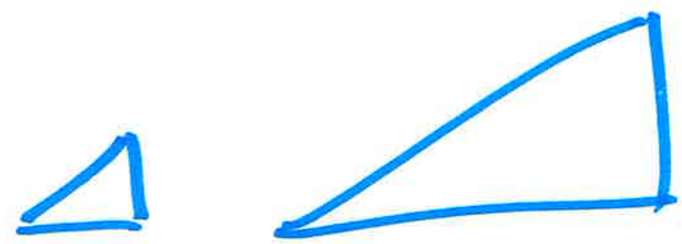
AD OGNI ELEMENTO SI ASSOCIA IL NUMERO DI VOLTE CHE COMPARE

ALGEBRA → studio di strutture.

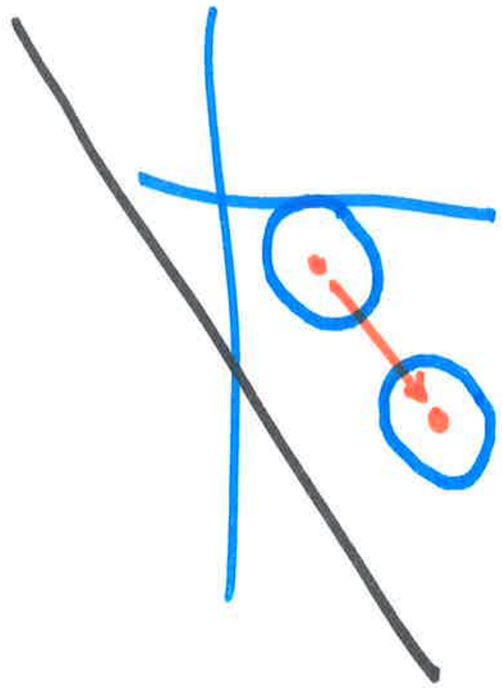
→ Insiemi A

→ Operazioni $A \times A \to A$

1) Vogliamo capire come le operazioni agiscono sugli insiemi trasformando i loro elementi.



2) In generale degli enti sono descritti "bene" dalle trasformazioni che li lasciano invarianti.



Struttura algebrica

operazione su di un insieme A
(binaria)

funzione $\quad f: A \times A \to A$

$$\mathbb{Z}_2 = \{0,1\}$$

$$\begin{matrix} a \to \\ b \to \end{matrix} \boxed{f} \to c$$

AND

$$\cdot : \begin{cases} \{0,1\} \times \{0,1\} \longrightarrow \{0,1\} \\ (x,y) \longrightarrow xy \end{cases}$$

$0 = F$
$1 = V$

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

XOR

$$\oplus \begin{cases} \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}. \\ (x,y) \longrightarrow \begin{array}{l} 1 \text{ se } x=0, y=1 \\ \quad \text{o } x=1, y=0 \\ 0 \text{ altrimenti.} \end{array} \end{cases}$$

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

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

Struttura algebrica = insieme con una o più operazioni definite su di esso.

Es. $(\mathbb{Z}_2, \oplus)$ $\quad (\mathbb{Z}_2, \cdot)$

$(\mathbb{Z}_2, \oplus, \cdot)$

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

N.B: "DIVISO" NON É UNA OPERAZIONE BINARIA SU $\mathbb{R}$.
PER ZERO NON SI PUÓ DIVIDERE!

"$-$" é una operazione binaria su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
→ NON GODE DI BELLE PROPRIETÀ
→ CONVIENE DEFINIRE IN TERMINI DI SOMMA

$(2-3)-4 = -5$
$2-(3-4) = 3$
| NON È ASSOCIATIVA :(

OSS: Se $f: A \times A \to A$ è operazione binaria

invece di $f(a,b) = c$

scriveremo $a \, f \, b = c$

$+(a,b) = c$

$a+b = c$

$(a,b)+ = c$

$3 \cdot (5+2)$ $\quad$ $(3,5,2)$ $\quad$ $\underbrace{\underbrace{5 \; 2 \, +}_{7} \; 3}_{3} \, \cdot$

$3 \cdot 7 = 21$ $\qquad\qquad\qquad\qquad = 21$

proprietà di una op. binaria.

(A, Δ) $\qquad \Delta : A \times A \to A$ operazione binaria.

Si dice che

1) Δ ammette elemento neutro in A se $\exists\, e \in A : \forall a \in A : e \Delta a = a \Delta e = a$

(esempio: in $(\mathbb{N}_0, +)$ l'elemento 0

$0 + n = n + 0 = n$

Non in $(\mathbb{N}, +)$).

2) $a \in A$ ammette inverso rispetto Δ se Δ ammette $\exists$ elemento neutro e ed

$$\exists\, \tilde{a} \in A : \tilde{a} \Delta a = a \Delta \tilde{a} = e$$

(esempio: in $(\mathbb{N}_0, +)$ l'elemento 0 ammette inverso

$$0 + 0 = 0$$

ma solo lui;

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

$$\forall a \in \mathbb{Z} \Rightarrow a + \underline{(-a)} = (-a) + a = 0$$

"sottrarre in $\mathbb{Z}$ corrisponde a sommare ad un elemento l'inverso rispetto la somma dell'altro."

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

in $(\mathbb{Q}, \cdot)$ ogni elemento diverso da zero ammette inverso.

$\frac{a}{b} \in \mathbb{Q}$ con $a, b \neq 0$

$\frac{b}{a} \in \mathbb{Q}$ $\qquad \frac{a}{b} \cdot \frac{b}{a} = 1$

1 elemento neutro.

$\mathbb{Q}^{\times} := \mathbb{Q} \setminus \{0\}$. $\quad (\mathbb{Q}^{\times}, \cdot)$ ogni el. ammette inverso.

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

$\mathbb{Z}^{\times} = \{-1, +1\}$.

se l'operazione in (A, Δ) è denotata dal simbolo $+$, allora l'elemento neutro lo si indica come 0 (oppure 0_A) e l'inverso di un elemento e è detto opposto e lo si indica con $(-a)$

se l'operazione in (A, Δ) è denotata dal simbolo $\cdot$, allora l'elemento neutro è indicato con 1 (oppure 1_A) e l'inverso di a è detto reciproco e lo si indica con a^{-1}.

3) Δ è associativa se

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

Esempi

$(\mathbb{N}, +) \quad (\mathbb{N}, \cdot)$

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

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

etc etc.

NON ASSOCIATIVA $(\mathbb{Z}, -)$

X insieme

$S(X) = \{ f : X \to X \mid f \text{ biettiva} \}$

$(S(X), \circ)$ ove $\circ$ = composizione di funzioni.

$(S(X), \circ)$ è una struttura algebrica

a) $\circ$ è una operazione su $S(X)$

b) esiste l'elemento neutro dato da $\iota_x(x) = x$

[funzione identica]

c) la operazione $\circ$ è associativa

d) ogni elemento di $S(X)$ ammette inverso rispetto "$\circ$" $\quad f \in S(X) \Rightarrow f^{-1} = f^{opp} \in S(X)$

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

GRUPPO SIMMETRICO SU X

[se $|X| = n \Rightarrow |S(X)| = n!$]

__Def:__ Una struttura algebrica $(G, \cdot)$ è detta __gruppo__ se

1) $\cdot$ ammette elemento neutro 1_G.
2) $\forall g \in G \ \exists g^{-1} \in G : g^{-1} \cdot g = g \cdot g^{-1} = 1_G$.
   ogni elemento ammette inverso
3) l'operazione $\cdot$ è associativa
   $\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

__ESEMPI:__ $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^{*}, \cdot)$ etc. etc.