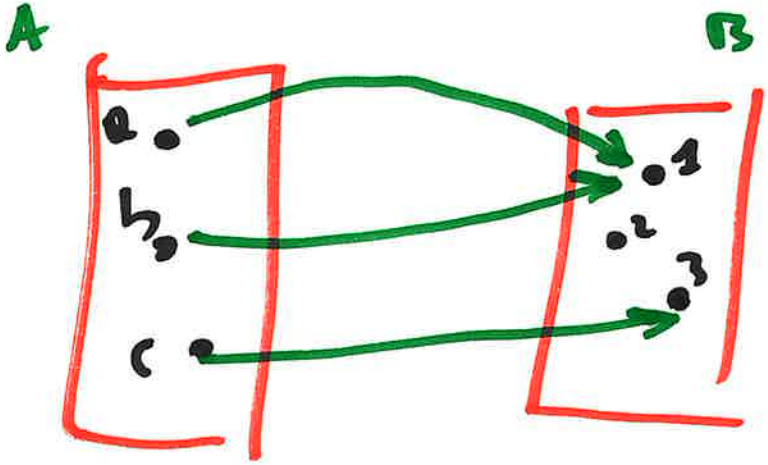
$f \subseteq A \times B$ $\quad$ $f: A \to B$

$f: A \to B$ $\quad$ $f^{\leftarrow}: B \to 2^A$

$\forall b \in B: \; f^{\leftarrow}(b) := \{a \in A : f(a) = b\}.$



$f^{\leftarrow}(2) = \phi$

$f^{\leftarrow}(3) = \{c\}.$

$f^{\leftarrow}(1) = \{a, b\}.$

$$2^A := \{ X \subseteq A \}.$$

$$f : A \to \{0,1\}.$$

$$\chi : A \to \{0,1\}.$$

$$\forall X \subseteq A : \chi_X : \begin{cases} A \to \{0,1\}. \\ x \to \begin{cases} 1 \text{ wenn } x \in X \\ 0 \text{ wenn } x \notin X \end{cases} \end{cases}$$

Strutture algebriche

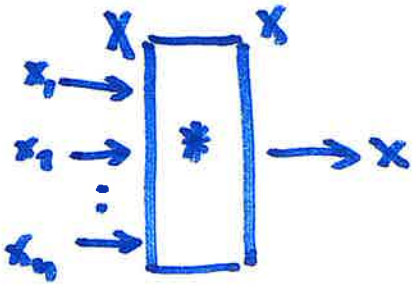
Insieme con una o più operazioni definite su di esso

Def: Sia X un insieme. Una **operazione n-aria** su X $(n \geq 0)$ è una funzione

$$*: X^n \to X$$

CASO PARTICOLARE

- $n=2$ → operazione **binaria** $X \times X \to X$



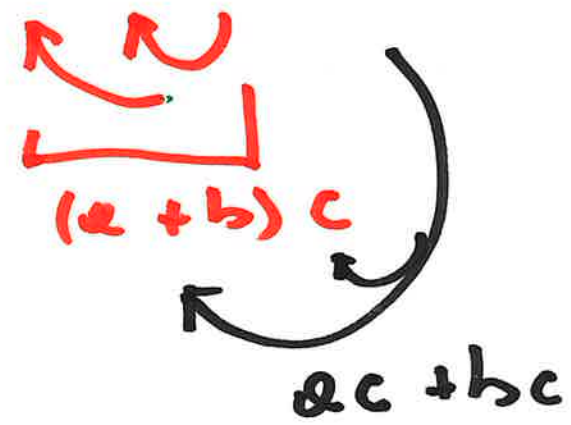
* operazione binaria

$* (a, b) \longrightarrow a * b$

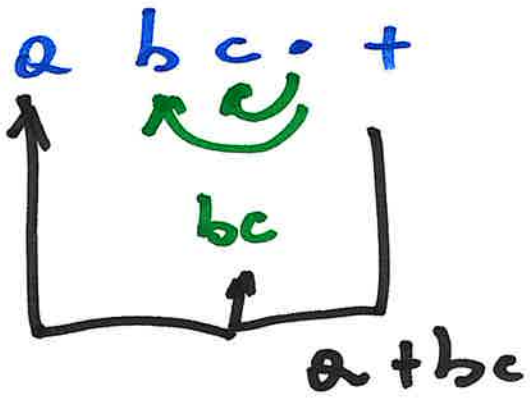
$(\mathbb{N}, +)$ $\qquad +(a, b) \longrightarrow a + b$

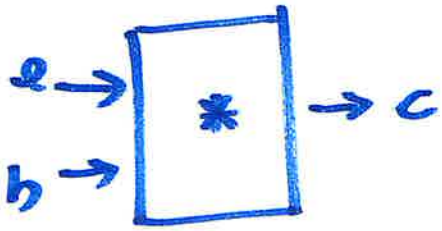
$(a, b) + \longrightarrow a + b$

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



$(a + b\cdot c)$





$\mathbb{N}$: insieme dei numeri naturali

$\mathbb{N}_0$ incluso lo 0

$\mathbb{N} \setminus \{0\}$ senza zero.

$\mathbb{Z}$: insieme dei numeri interi

$\mathbb{Q}$: insieme dei numeri razionali $\quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

$\mathbb{R}$: insieme dei numeri reali $\quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$\mathbb{C}$: insieme dei numeri complessi $\quad \mathbb{C}^* = \mathbb{R} \setminus \{0\}$.

$-: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ non è una operazione.

$-: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ è una operazione binaria.

$\dot{-}: \begin{cases} \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \\ a, b \to \max(a-b, 0) \end{cases}$ è una operazione.

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

1) el. neutro • $\exists\, 0 \in \mathbb{N}_0 : \forall a \in \mathbb{N} : 0+a = a+0 = a$
el. neutro

2) associativa • $\forall a,b,c \in \mathbb{N}_0 : a+(b+c) = (a+b)+c$

3) commutativa $\forall a,b \in \mathbb{N}_0 : a+b = b+a$

1+2 → MONOIDE

1+2+3 → MONOIDE ABELIANO o COMMUTATIVO

$(\mathbb{Z}, +)$

GRUPPO

- el. neutro · $\exists 0 \in \mathbb{Z} : \forall a \in \mathbb{Z} : 0 + a = a + 0 = a$
- associativo · $\forall a, b \in \mathbb{Z}: \quad a + (b + c) = (a + b) + c$
- inverso · $\forall a \in \mathbb{Z} \; \exists (-a) \in \mathbb{Z} : a + (-a) = (-a) + a = 0$

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

Esempi

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

2) $(\{0,1\}, +)$

+	0	1
0	0	1
1	1	0

3) $X = \{a, b\}$ e consideriamo su $X^2 \setminus \{(x,x) : x \in X\}$

$= \{(a,b), (b,a)\} = A$

le due funzioni: $b_A : \begin{cases} (a,b) \to (a,b) \\ (b,a) \to (b,a) \end{cases}$

$\sigma : \begin{cases} (a\,b) \to (b\,a) \\ (b\,a) \to (a,b) \end{cases}$

$G = \{\iota_A, \sigma\}$ con la composizione di funzioni è un gruppo.

1)

$\circ$	ι_A	σ
ι_A	ι_A	σ
σ	σ	ι_A

$(G, \circ)$

$+$	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, +)$

$$\varphi : G \longrightarrow \mathbb{Z}_2$$

$$\varphi(\iota_A) = 0$$

$$\varphi(\sigma) = 1$$

$\forall x, y \in G$:

$$\varphi(x \circ y) = \varphi(x) + \varphi(y)$$

$$\varphi(x^{-1}) = -\varphi(x)$$

] OMOMORFISMO DI GRUPPI.

OMOMORFISMO $f : G \to H$ con G, H strutture algebriche

CHE PRESERVA LE OPERAZIONI

$$f(a * b) = f(a) *' f(b)$$

$(G, *)$, $(H, *')$

$$f(a^{-1 *}) = f(a)^{-1 *'}$$

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

$$\exp: a \longmapsto e^a$$

$$\exp(a+b) = e^{a+b} = e^a \cdot e^b =$$

$$= \exp(a) \cdot \exp(b)$$

$$\exp(-a) = e^{-a} = (e^a)^{-1} = \exp(a)^{-1}$$

$$\exp: (\mathbb{Z}, +) \to (\mathbb{R}^*, \cdot)$$

NON è SURIETTIVA

è iniettiva.

$$\exp(a) = \exp(b) \Rightarrow e^a = e^b \Rightarrow$$

$$\Rightarrow e^{a-b} = 1$$

$$\Rightarrow a - b = 0 \Rightarrow a = b$$

Def: Sia $f: G \to H$ un omomorfismo di Gruppi.

Sia 1_H l'elemento neutro di H e
0_G l'elemento neutro di G.

$(G, +)$
$(H, \cdot)$

$$\underline{\ker(f)} := \{ g \in G \mid f(g) = 1_H \}.$$

NUCLEO DI f

Oss 1) $\ker(f) \leq G$ è un sottogruppo di G.

1) $0_G \in \ker f$
2) $\forall x, y \in \ker f : x + y \in \ker f$
3) $\forall x \in \ker f : -x \in \ker f$

DIM 2) $x, y \in \ker f \Rightarrow f(x) = 1_H$

$f(y) = 1_H$

$\Rightarrow f(x) f(y) = 1_H \cdot 1_H = 1_H$

$\Rightarrow f(x+y) = 1_H \Rightarrow x+y \in \ker f$

1+2) $x \in \ker f \Rightarrow f(x) = 1_H \Rightarrow f(x)^{-1} = 1_H^{-1} = 1_H$

$\Rightarrow f(x) \cdot f(x)^{-1} = 1_H$

$\Rightarrow f(x-x) = f(0_G)$

D'altro canto $f(0_G - 0_G) = f(0_G) \cdot f(0_G)^{-1}$

$= 1_H$

e $0_G - 0_G = 0_G \Rightarrow f(0_G) = 1_H$

$\Rightarrow (-x) \in \ker f \; ; \; 0_G \in \ker f.$

□

Teorema

La funzione $f: G \to H$ è iniettiva $\Leftrightarrow \ker f = \{0_G\}$.

$\forall y \in \mathrm{Im}(f)$ esiste una biiezione fra gli elementi di $\ker(f)$ e quelli di $f^{\leftarrow}(y)$

→ le proprietà di f sono controllate da come f si comporta in 0_G

DM: Se $\ker f = f^{\leftarrow}(1_H)$ contiene più di un elemento $\Rightarrow$ f non è iniettiva!

Supponiamo di avere $a, b \in G$

tali che $f(a) = f(b) \Rightarrow$

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

$$\Rightarrow f(a) + f(-b) = 1_H \Rightarrow$$

$$\Rightarrow a - b \in \ker f$$

se $\ker f = \{e_G\} \Rightarrow a - b = e_G \Rightarrow a = b$

in ogni caso

$a \in$ ~~blah~~

$$\ker(f) + (+b) =$$

$$= \{ x+b \mid b \in \ker f \}.$$

oss: $\ker(f) \trianglelefteq G$ sottogruppo normale.

cioè $b + \ker(f) = \ker(f) + b$

come insiemi $\forall b \in G$.

$x \in b + \ker(f) \Rightarrow x = (b+y)$ e $f(x) = f(b+y) =$
$y \in \ker f$
$= f(b) \Rightarrow$

$$\Leftrightarrow f(x) = f(h) = 0 + f(h) = f(y+h) \Leftrightarrow$$

$$\Leftrightarrow x \in \ker f + h \qquad \square$$

Se $\ker(f) \neq \{0\} \Rightarrow f$ è iniettiva ed in particolare biiettiva sulla sua immagine.

Un omomorfismo $f: G \to H'$ biiettivo è detto isomorfismo.

X insieme

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

GRUPPO SIMMETRICO SU X

↓

Tutte le possibili permutazioni di oggetti di X

$|X|$

$\#S(X) = \#X!$

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

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

3!

a	b	c	
a	b	c	ι_X
b	a	c	$(b\ a)$
b	c	a	$(b\ c\ a)$
a	c	b	$(c\ b)$
c	a	b	$(c\ b\ a)$
c	b	a	$(c\ a)$

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

$$b \to c \to c$$
$$c \to a \to b$$
$$a \to b \to a$$

$$\iota_A \circ X = X \circ \iota_A = X$$

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

$(S(X), \circ)$ NON È COMMUTATIVO.