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

$f \subseteq A \times B$.

1) $\forall a \in A \; \exists_{\leq 1} b \in B: (a,b) \in f$

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

1) funzionale
2) ovunque definita

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

Se f funzione $A \to B$ si dice immagine di f il sottoinsieme $Im(f) \subseteq B$

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

$f: A \to B$ funzione

sia $C \subseteq A$: restrizione di f a C:

$$f|_C : C \to B$$

tale che $\{(c,b) \in C \times B \mid (c,b) \in f\}$.

ni D tale che $\operatorname{Im} f \subseteq D \subseteq B$:

troncamento di f a D $f^{|D}$

$$f^{|D} : A \to D$$

tale che $\{(a,d) \in A \times D \mid (a,d) \in f\}$.

Oss: se si scrive $f|_C^{|D} : C \to D$ e prima si applica la restrizione e poi il troncamento.

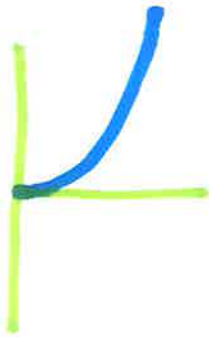
$f: A \to B$

$f|^{D}_{Ic}: C \to D$ si richiede $\operatorname{Im} f_{|c} \subseteq D$

non $\operatorname{Im} f \subseteq D$

$$f: \begin{cases} \mathbb{R} \to \mathbb{R} \\ x \to x^3 \end{cases}$$

$$f_{|\mathbb{R}^+}: \begin{cases} \mathbb{R}^+ \to \mathbb{R} \\ x \to x^3 \end{cases}$$



$f^{|\mathbb{R}^+}$ non si può fare!

perché $\operatorname{Im} f = \mathbb{R} \not\subseteq \mathbb{R}^+$

$$f^{|\mathbb{R}^+}_{|\mathbb{R}^+}: \begin{cases} \mathbb{R}^+ \to \mathbb{R}^+ \\ x \to x^3 \end{cases}$$

COMPOSIZIONE DI FUNZIONI

$$f: A \to B$$

$$g: B \to C$$

Definiamo $(g \circ f): \begin{cases} A \to C \\ a \to c = g(f(a)) \end{cases}$

(*) $(g \circ f) = \{(a,c) \in A \times C \mid \exists b \in B \text{ con } (a,b) \in f \text{ e } (b,c) \in g\}$.

Teorema: *La composizione di funzioni è associativa nel senso che* $\forall\ f: A \to B,\ g: B \to C,\ h: C \to D$

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

DIM: si usa la definizione (*)

Def: Sia $I_n = \{1, 2, \dots n\} \subseteq \mathbb{N}$ e X un insieme

si dice **sequenza** di elementi di X

ogni funzione $f: I_n \to X$.

↓

lista di elementi di X

con ripetizioni e in cui l'ordine è importante.

$X = \{x_1, x_2, x_3\}$

$\{(1, x_1), (2, x_2), (3, x_1), (4, x_3)\}$

↓

(x_1, x_2, x_1, x_3)

↑ ↑ ↑ ↑

1 2 3 4

N.B:

Sequenze

$(1,2,3) \neq (3,2,1)$

$(1,2,2) \neq (1,2)$

$(1,2,2) \neq (2,2,1)$

Insiemi

$\{1,2,3\} = \{3,2,1\}$.

$\{1,2,2\} = \{1,2\}$.

SISTEMA = SEQUENZA NON ORDINATA

= MULTI-INSIEME.

↓

funzione $f: X \to \mathbb{N} \cup \{0\}$.

ad ogni el. di X si associa una molteplicità che può anche essere $= 0$.

$[1,2,2] \neq [1,2]$

$[1,2,2] = [2,2,1] = [2,1,2]$

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

$[a, a, b, b, b] = [b, b, a, a, b]$

$\{(a, 2), (b, 3), (c, 0)\}$

Indichiamo con X^n l'insieme di tutte le sequenze di n elementi di X.

N.B. X^n "si comporta come" $X \times (X \times X) \ldots$

più in generale se A e B sono 2 insiemi scriveremo B^A per indicare l'insieme di tutte le funzioni $f : A \to B$.

oss: $|B^A| = |B|^{|A|}$

per ogni elemento $a \in A$ devo ~~posso~~ scegliere uno ed un solo elemento $b \in B$ in modo arbitrario → ci sono $|B|$ possibilità.

$$\underbrace{|B| \cdot |B| \cdot \ldots \cdot |B|}_{|A| \text{ volte}} = |B|^{|A|}$$

Esempio: ~~[illegible]~~

A insieme, $B = \{0,1\}$.

B^A corrisponde all'insieme di tutte le funzioni $A \to \{0,1\}$ dette funzioni caratteristiche e corrisponde anche all'insieme di tutti i sottoinsiemi di A

A insieme $= \{ a, b, c, \dots \omega, x, y, z \dots \}$.

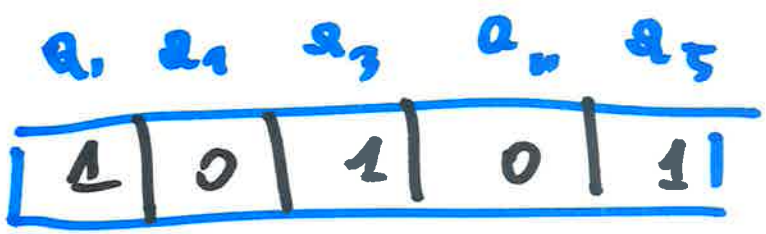
Sia $X \subseteq A$ definiamo $\chi_X : \begin{cases} A \to \{0,1\} \\ a \to \begin{cases} 0 \text{ se } a \notin X \\ 1 \text{ se } a \in X \end{cases} \end{cases}$

viceversa: data $f : \begin{cases} A \to \{0,1\} \\ a \to \eta \end{cases}$ possiamo sempre

vedere $X = \{ x \in A \mid f(x) = 1 \} \subseteq A$

CORRISPONDENZA BIUNIVOCA FRA sottoinsiemi di A e funzioni caratteristiche

$$X \to \chi_X$$



$\sim \{a_1, a_3, a_5\}$.

0 0 1 1 1 — $\{a_3\ a_4\ a_5\}$.

0 0 0 0 0 — ϕ

$\mathcal{P}(A) = \{X \mid X \subseteq A\}$.

$2^A := \{f : A \to \{0,1\}\}$.

$B \in \mathcal{P}(A) \xrightarrow{\psi} \chi_B \in 2^A$

$f \in 2^A \xrightarrow{\theta} C = \{a \in A : f(a) = 1\}$

$(\theta \circ \psi)(B) = B$

$(\psi \circ \theta)(f) = f$

SOTTOINSIEMI → FUNZIONI BINARIE

X ←

- $\{1,2,3,4\}$

- $X=\{2,3\}$.

$(0,1,1,0) \sim \{(1,0),(2,1),(3,1),(4,0)\}$.

*

$1\ 2\ 3\ 4 = \{2,3\}$.

x ✓ ✓ x

i sottoinsiemi di un insieme A con $|A|=n$ sono 2^n

DEF Sia A un insieme. Una funzione

$f: A^n \to A$ è detta operazione n-aria su A.

In particolare se $f: A \times A \to A$ allora f è una operazione binaria su A.

Def: Struttura algebrica Data di un insieme ed alcune operazioni su di esso.

(N.B. a volte si ammettono anche fam. op. fra l'insieme dato e

altri insiemi).

STRUTTURA ALGEBRICA

INSIEMI + OPERAZIONI

$(\mathbb{N}, +)$ $\mathbb{N}$ = insieme dei numeri naturali

+ = somma di 2 numeri naturali

$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

$(\mathbb{Z}, +)$ $\mathbb{Z}$ = insieme dei numeri interi

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

$(\mathbb{Q}, +)$ $(\mathbb{Q}, \cdot)$, $(\mathbb{Q}^x, \cdot)$ etc. etc.

$\mathbb{Q}^x$ → numeri razionali meno lo 0

$\mathbb{N}$ → insieme dei numeri naturali (incluso 0)

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

$\mathbb{Q}$ → insieme dei numeri razionali

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

$\mathbb{C}$ → insieme dei numeri complessi.

analisi

algebra + analisi.

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

$(\mathbb{N}, +)$ incluso lo 0

- $\forall a, b \in \mathbb{N}: \quad a+b = b+a$ commutativa
- $\exists 0 \in \mathbb{N}: \forall a \in \mathbb{N}: \quad 0+a = a+0 = a$ el. neutro.
- $\forall a, b, c \in \mathbb{N}: \quad a+(b+c) = (a+b)+c$ associativa.

→ monoide

equazione $a+x=b$

$(\mathbb{Z},+)$ proprietà di $(\mathbb{N},+)$ ed inoltre

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

(esistenza inverso).

$$\boxed{a+x=b}$$

possiamo risolverla sempre.

esist. inverso.

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

ass.

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

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

el. neutro

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

Def: Sia G un insieme e $*: G\times G \to G$ una operazione binaria su G.

$(G,*)$ è un gruppo se

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

2) $\forall g \in G \; \exists\, g' \in G : g*g' = g'*g = e$ ($\exists$ inverso).

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

(prop. associativa).

In particolare in $(G,*)$ sappiamo sempre risolvere una equazione del tipo $a*x = b$

ed anche $x*a = b$

$(G,*)$ è detto commutativo o abeliano se

$\forall a,b \in G : \; a*b = b*a$.

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

$(\mathbb{Q}, +)$

$(\mathbb{R}, +)$

$(\{0\}, +)$ ← gruppo banale.

$(\{0,1\}, \oplus)$ = $(\mathbb{Z}_2, +)$

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

el neutro ✓
commutativa ✓
inverso di ogni el. ✓
associativa

a	b	c	
0	0	0	$(0+0)+0 = 0+(0+0)$
0	0	1	$(0+0)+1 = 0+(0+1)$
0	1	0	$(0+1)+0 = 0+(1+0)$
0	1	1	$(0+1)+1 = 0+(1+1)$
1	0	0	$(1+0)+0 = 1+(0+0)$
1	0	1	$(1+0)+1 = 1+(0+1)$
1	1	0	$(1+1)+0 = 1+(1+0)$

a	b	c	
1	1	1	$1+(1+1) = 1+(1+1)$

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

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

$(\mathbb{Z}_5, +)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

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

+	0	1
0	0	1
1	1	0

→ pari/dispari

→ tabella di verità di XOR

$(\mathbb{Z}_n, +)$ $\quad \mathbb{Z}_n = \{0, 1, \dots, n-1\}$.

somma in $\mathbb{Z}_n$: si sommano i numeri, li si divide per n e si viene il resto

$(\mathbb{Z}_3^\times, \cdot) \cong (\mathbb{Z}_2, +)$

$1 \longrightarrow 0$

$2 \longrightarrow 1$

·	1	2
1	1	2
2	2	1

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_5^\times, \cdot)$ GRUPPO

·	1	2	3
1	1	2	3
→ 2	2	0	2
3	3	2	1

!!

!! $(\mathbb{Z}_4^\times, \cdot)$ non è un gruppo!

$(\mathbb{Z}_p^\times, \cdot)$ GRUPPO $\Leftrightarrow$ p è primo.

oss: Sia $(G, *)$ un gruppo $\Rightarrow$

in ogni riga (colonna) della tabella moltiplicativa di G devono comparire tutti gli elementi di G una e una sola volta.

Teorema $(G, *)$ un gruppo $\Rightarrow$ le funzioni

$$\vartheta_x : \begin{cases} G \to G \\ g \to x * g \end{cases} \quad \text{e} \quad \delta_x : \begin{cases} G \to G \\ g \to g * e \end{cases}$$

sono biiettive.

DIM: ϑ_x è invertibile infatti sia $\hat{x}$ tale che

$$\hat{x} * x = e \Rightarrow \vartheta_{\hat{x}} \circ \vartheta_x (g) = \hat{x} * (x * g) =$$

$= (\hat{x} * x) * g = g$

$(\vartheta_x \circ \vartheta_{\hat{x}})(g) = x * (\hat{x} * g) = (x * \hat{x}) * g = g$ ∎

$(\mathbb{R}^*, \cdot)$ è un gruppo

$(\mathbb{R}, \cdot)$ NON è UN GRUPPO! ∎ non ammette reciproco!

$(\mathbb{Q}^*, \cdot)$ è un GRUPPO

$\{-1, +1\} \subseteq \mathbb{Z}$ $(\{-1, +1\}, \cdot)$ è UN GRUPPO

$\cdot$	-1	$+1$
-1	1	-1
$+1$	-1	1

$+$	0	1
0	0	1
1	1	0

Sia X un insieme e sia

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

$\Rightarrow (S(X), \circ)$ è un gruppo, detto gruppo simmetrico su X.

NON È COMMUTATIVO.

- $id_X : \begin{cases} X \to X \\ x \to x \end{cases}$ è l'identità di questo gruppo
- $\forall f \in S(X) \ \exists f^{-1} \in S(X)$ in quanto f biiettiva.
  con $f^{-1} \circ f = f \circ f^{-1} = id_X$
- vale la prop. associativa perché vale per la composizione di funzioni.

Se $|X|=n \Rightarrow |S(X)| = n!$

$n(n-1)\dots 1 = n!$

oss: Se $(G,*)$ gruppo e $\vartheta_x : \begin{cases} g \to g \\ g \to x*g \end{cases}$

$\Rightarrow \vartheta_x \in S(G)$

ed abbiamo anche che

$$\vartheta_{\hat{x}} = (\vartheta_x)^{-1}$$

$$\vartheta_{xy} = \vartheta_x \circ \vartheta_y$$

la funzione ϑ_x "trasforma le operazioni in G in operazioni in $S(G)$"

OMOMORFISMO (DI GRUPPI).

$(G, *)$ ed (H, Δ) due gruppi

indichiamo con $\hat{x}$ l'inverso di x in G

e con $\tilde{y}$ l'inverso di y in H

Funzione $\psi : G \to H$ tale che

$$\begin{cases} \psi(g * e) = \psi(g) \Delta \psi(e) \\ \psi(\hat{g}) = \widehat{\psi(g)} \end{cases}$$

$G = \{e^x \mid x \in \mathbb{Z}\}$ con il prodotto

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

$$\psi : \begin{cases} G \longrightarrow \mathbb{Z} \\ a \longrightarrow \log a \end{cases}$$

$$\log(\alpha \cdot \beta) = \log \alpha + \log \beta$$

$$\psi^{-1} : \begin{cases} \mathbb{Z} \longrightarrow G \\ n \longrightarrow e^n \end{cases}$$

Def: Un omomorfismo $\psi : G \to H$ invertibile è detto <u>isomorfismo</u>

$\mathbb{R}^{++} := \{x \in \mathbb{R} \mid x > 0\}$ rispetto il prodotto e $(\mathbb{R}, +)$ sono isomorfi.

$$\log : \begin{cases} \mathbb{R}^{+*} \longrightarrow \mathbb{R} \\ x \longrightarrow \log x \end{cases}$$

$$\exp : \begin{cases} \mathbb{R} \to \mathbb{R}^{+*} \\ x \to e^x \end{cases}$$

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

<u>OSS</u>: $(\mathbb{Z}, +)$ è un gruppo

$(\mathbb{Z}, -)$ <u>NO!!</u> $\quad 7 - 0 = 7$

$0 - 7 = -7 \neq 7$

$(1-2)-3 \neq 1-(2-3)$

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

in $\mathbb{Q}^*$ $\quad a/b := a \cdot (b^{-1})$

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

$(\mathbb{Z}, \cdot)$ monoide

1 elemento

$a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$

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

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

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

$(a+b) \cdot c = ac + bc$.

Def: Sia A un insieme e $+ : A \times A \to A$ e $\cdot : A \times A \to A$ due operazioni binarie su A.

A è detto **anello commutativo con unità** se

ANELLO

1) $(A, +)$ è un gruppo abeliano
2) $\cdot : A \times A \to A$ è associativa
3) valgono le proprietà distributive
$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(a+b) \cdot c = ac + bc$$

UNITÀ

4) $\exists 1 \in A : \forall a \in A : 1 \cdot a = a \cdot 1$ (unità).

COMMUTATIVO

5) $\forall a, b \in A : a \cdot b = ba$ (commutativo).

$(\mathbb{Z}, +, \cdot)$ $\qquad$ $(\mathbb{Z}[x], +, \cdot)$

ove $\mathbb{Z}[x]$ = insieme di tutti i polinomi in x a coeff. in $\mathbb{Z}$

$$f(x) \in \mathbb{Z}[x] \iff f(x) = f_0 + f_1 x + \dots + f_n x^n = \sum_{i=0}^{n} f_i x^i$$

con somma di polinomi

$$(f+g)(x) = \sum_{i=0}^{n} (f_i + g_i) x^i$$

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

Def: $(\mathbb{K}, +, \cdot)$ **campo** se

1) $(\mathbb{K}, +)$ gruppo commutativo con el. neutro $= 0$

2) $(\mathbb{K} \setminus \{0\}, \cdot)$ gruppo commutativo

3) valgono le distributive

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(a+b)c = ac + bc.$$

CAMPO = anello commutativo con 1 in cui ogni el. diverso da 0 ammette inverso moltiplicativo

□