APPLICAZIONI

Def un'Applicazione (o funzione) è una relazione t.c.
$\forall a \in A \ \exists! \ b \in B$ con $(a,b) \in R$
(cioè per ogni $a \in A$ esiste unico $b \in B$ t.c. $(a,b) \in R$)

Se R è funzione e $(a,b) \in R$, (oppure aRb) allora
Scrivo $b = R(a)$ e $R: A \to B$

In questo caso A si chiama DOMINIO di R e B CODOMINIO

$R(a)$ si chiama IMMAGINE di a
un qualsiasi $a \in A$ t.c. $b = R(a)$, si chiama RETROIMMAGINE di b

Chiamo "immagine di R" l'insieme

$$\{ b \in B \mid \exists a \in A \text{ con } b = R(a) \} = R(A)$$

Scrivo $R^{-1}(b) = \{ a \in A \mid R(a) = b \} \subseteq A$

$R(A) \subseteq B$

Def: Siano $F: A \to B$ e $G: A \to B$ due funzioni, diciamo $F = G$ se e solo se $\forall a \in A \quad F(a) = G(a)$

Def: Sia $F: A \to B$ una funzione. Diciamo che F è:

→ INIETTIVA se $\underset{(a,b) \in A}{F(a) = F(b)} \Rightarrow a = b$

(elementi diversi hanno immagini diverse)
⇝ ogni elemento ha al massimo una retroimmagine

→ **SURIETTIVA** se $\forall b \in B$ esiste $a \in A$ t.c. $b = F(a)$

(cioè ogni elemento del codominio è immagine di un elemento del dominio)

⤳ ogni elemento ha almeno una retroimmagine

→ **BIIETTIVA** se è suriettiva e iniettiva

⤳ Ogni elemento in B ha esattamente una retroimmagine

Def.: Siano $F: A \to B$ e $G: B \to C$ due funzioni.

Definiamo $G \circ F: A \to C$ (composto) una funzione con dominio A e codominio C t.c. $\forall a$ $(G \circ F)(a) = G(\underbrace{F(a)}_{\in B})$

Oss: Posso "comporre" G con F se e solo se il codominio di F è il dominio di G

Proprietà della composizione:

$F: A \to B \quad G: B \to C \quad H: C \to D$

$$H \circ (G \circ F) = (H \circ G) \circ F$$

(la composizione tra funzioni è associativa)

La composizione fra funzioni NON è commutativa

cioè $F \circ G \neq G \circ F$

↓

se $A \neq B$ $\quad F: A \to B \quad G: B \to C$

$A \neq C$ $\quad G \circ F$ esiste

$B \neq C$ $\quad F \circ G$ non è definita

Def: Sia A un insieme. La funzione $id_A : A \to A$ IDENTITÀ è la funzione t.c. $\forall a \in A \quad id_A(a) = a$

Prop: se $F: A \to B$ è funzione $\Rightarrow F \circ id_A = id_B \circ F = F$

Dim: $(F \circ id_A)(a) = F(id_A(a)) = F(a)$

cioè $\forall a \in A \quad (F \circ id_A)(a) = F(a) \Rightarrow F \, id_A = F$

$(id_B \circ F)(a) = id_B(F(a)) = F(a) \Rightarrow id_B \circ F = F$

Def: Date due applicazioni $F: A \to B$, $G: B \to A$

- se $F \circ G : B \to B$ e $F \circ G = id_B$
  allora G è INVERSA DX di F
- se $G \circ F : A \to A$ e $G \circ F = id_A$
  allora G è INVERSA SX di F
- Se $G \circ F = id_A$ e $F \circ G = id_B \Rightarrow$ dico che G è INVERSA di F

Prop: F è invertibile $\Leftrightarrow$ F è biettiva

Dim: l'inversa di F associa a un elemento del codominio la sua <u>unica</u> retroimmagine per F.

STRUTTURE ALGEBRICHE

Def: Sia A un insieme. Chiamo OPERAZIONE su A una funzione

es: $\star : A \times A \longrightarrow A$
$(a, b) \longmapsto a \star b$

Se $\star$ è operazione su A dico che $(A, \star)$ è una STRUTTURA ALGEBRICA es $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$

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

es $-$ su $\mathbb{N}$ non è "un'operazione", cioè $(\mathbb{N},-)$ non è una struttura algebrica

↓

perché $(1,2) \in \mathbb{N}\times\mathbb{N}$ non associa niente $(1-2 \notin \mathbb{N})$

cioè $-: \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ non è funzione

es A insieme, $\mathcal{P}(A) = \{$ sottoinsiemi di $A\}$

$(\mathcal{P}(A), \cap)$ è struttura algebrica

$(\mathcal{P}(A), \cup)$ è " "

es $S := \{\underbrace{R: A \to A \text{ funzioni}}_{\text{funzioni da } A \text{ in } A}\}$

$(S, \circ)$ è struttura algebrica

$\circ$ composizione

Def: Sia $(A, \star)$ una struttura algebrica.

Diciamo che:

→ $\star$ è associativa se $\forall a,b,c \in A$ $(a\star b)\star c = a\star(b\star c)$

→ $\star$ è commutativa se $\forall a,b \in A$ $a\star b = b\star a$

es $+$ è commutativa e associativa

$(\mathbb{Z},-)$ è struttura algebrica, ma:

- NON è associativa perché: $5-(3-2)=4 \neq (5-3)-2=0$
- NON è commutativa perché: $2-3 \neq 3-2$

Def: (ELEMENTO NEUTRO) sia $(A, \star)$ struttura algebrica.

- Un elemento $e_s \in A$ si dice NEUTRO A SX se:
  $\forall a \in A \quad e_s \star a = a$

- Un elemento $e_D \in A$ si dice NEUTRO A DX se:
  $\forall a \in A \quad a \star e_D = a$

- Un elemento $e \in A$ si dice NEUTRO (BILATERO) se:
  $\forall a \in A \quad e \star a = a \star e = a$

  es $(\mathbb{N}, +)$ l'elemento neutro è 0
  $(\mathbb{Q}, \cdot)$ " " è 1
  $(\mathbb{Z}, -)$ esiste elemento neutro a destra 0

Def: $(A, \star)$ una struttura algebrica e sia $e \in A$ elemento neutro

- Sia $\bar{a}_s \in A$ si dice INVERSO A SX di A
  se $\bar{a}_s \star a = e$

- Sia $\bar{a}_D \in A$ si dice INVERSO A DX di A
  se $a \star \bar{a}_D = e$

- Sia $\bar{a} \in A$ si dice INVERSO (BILATERO) di A
  se $a \star \bar{a} = \bar{a} \star a = e$

Oss: l'inverso di a dipende da a
mentre l'elemento neutro non dipende da nulla

es In $(\mathbb{N}, +)$ l'inverso di $a \in \mathbb{N}$ non c'è se $a \neq 0$

In $(\mathbb{Z}, +)$ l'inverso di $a \in \mathbb{Z}$ è $-a$

In $(\mathbb{Q}, \cdot)$ l'el. 0 non ha inverso
In $(\mathbb{Q} - \{0\}, \cdot)$
$\cdot : \mathbb{Q} - \{0\} \times \mathbb{Q} - \{0\} \to \mathbb{Q} - \{0\}$ é operazione
1 é neutro e tutti gli el. hanno inverso

Prop: L'elemento neutro se esiste é unico
Sia $(A, \star)$ struttura algebrica. Se esiste un elemento neutro, esso é neutro

Dim: siano $e_1, e_2 \in A$ elementi neutri
(cioé $\forall a \in A \quad e_1 \star a = a \star e_1 = a$,
$e_2 \star a = a \star e_2 = a$)
per dimostrare $e_1 = e_2$

$$e_1 \underset{e_2 \text{ é neutro a destra}}{=} e_1 \star e_2 \overset{e_1 \text{ neutro sx}}{=} e_2$$

Prop: L'inverso se esiste é unico.
Sia $(A, \star)$ strut. alg. e sia $e \in A$ el. neutro.
Sia $\star$ associativa. Se $a \in A$ ammette inverso, l'inverso di a é unico.

Dim: siano $\bar{a}_1, \bar{a}_2 \in A$ inversi di $a \in A$

$$\overline{a_2} \underset{e \text{ neutro}}{=} e \star \overline{a_2} \underset{\substack{\bar{a}_1 \text{ é inverso di } a \\ \text{cioé } \bar{a}_1 \star a = e}}{=} (\bar{a}_1 \star a) \star \overline{a_2} \underset{\star \text{ é associativa}}{=} \overline{a_1} \star (a \star \overline{a_2}) \underset{\overline{a_2} \text{ é inverso}}{=} \overline{a_1} \star e \overset{e \text{ neutro}}{=} \overline{a_1}$$

Se A é insieme finito e $\star$ oper. allora posso considerare un diagramma "dato" da $\star$

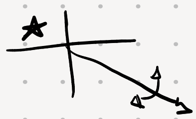
↓

$\star$	a	b	c	...
a	$a\star a$	$a\star b$		
b	$b\star a$	$b\star b$		
c				
$\vdots$				

→ tutti el di A

tutti el di A

se $\star$ è commutativa $\Rightarrow$ il diag. è simmetrico



Se e è neutro $\Rightarrow$ la riga e la colonna di e sono uguali alla prima riga e alla 1ª colonna

$\star$	e	a	b
e	e	a	b
a	a		
b	b		

=

=

Def: (MONOIDE) Un monoide è una struttura algebrica $(M, \star)$ t.c. ① : $\star$ è associativa
② : $\star$ ha elemento neutro

esempio $(\mathbb{N}, +)$ è monoide

Def: (GRUPPO) Un gruppo è una struttura algebrica $(G, \star)$ t.c. ① : $\star$ associativa
② : esiste el. neutro
③ : per ogni elemento esiste l'inverso

Def: (GRUPPO ABELIANO) Un gruppo $(G, \star)$ è abeliano se $\star$ è commutativa

es $(\mathbb{N}, +)$ non è gruppo
$(\mathbb{Z}, +)$ è gruppo abeliano/commutativo
$(P(A), \cap)$ è monoide (il neutro è A)
$(P(A), \cup)$ " " (" " è $\emptyset$)

Proprietà dei gruppi

- Il neutro è unico
- L'inverso è unico
- l'inverso dell'inverso di a è a
  $\rightarrow (g^{-1})^{-1} = g$

Notazione: $g \in G$ indico l'inverso con g^{-1}

- $(a \star b)^{-1} = b^{-1} \star a^{-1}$ (infatti $(a \star b) \star (a \star b)^{-1} = e$)

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

- Vale la legge di cancellazione
  $\forall a,b,c \in G \quad a \star b = a \star c \Rightarrow b = c$

- L'equazione di un'incognita x $\quad a \star x = b$
  $\rightarrow$ ha soluzione $x = a^{-1} \star b$