

APPLICAZIONI

Def un'Applicazione (o funzione) è una relazione t.c.

$$\forall a \in A \exists! b \in B \text{ con } (a, b) \in R$$

(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 $a R b$) allora

Scrivo $b = R(a)$ e $R: A \rightarrow B$

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

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

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

$$R(A) \subseteq B$$

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

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

→ **INiettiva** se $F(a) = F(b) \Rightarrow a = b$
 $(a, b) \in A$

(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

→ **BIETTIVA** se è suriettiva e iniettiva
 ↳ ogni elemento in B ha esattamente una retroimmagine

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

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

Proprietà delle composizioni:

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

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

(la composizione tra funzioni è **associativa**)

la composizione tra funzioni **NON** è **commutativa**

$$\text{cioè } F \circ G \neq G \circ F$$

$$\downarrow$$

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

$$A \neq C \quad G \circ F \text{ esiste}$$

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

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

Prop: se $f: A \rightarrow B$ 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 $\forall a \in A \quad (f \circ id_A)(a) = f(a) \Rightarrow f \circ id_A = f$

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

Def: Date due applicazioni $f: A \rightarrow B$, $g: B \rightarrow A$

• se $f \circ g: B \rightarrow B$ e $f \circ g = id_B$

allora g è INVERSA DX di f

• se $g \circ f: A \rightarrow A$ 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 unica retroimmagine per f .

STRUTTURE ALGEBRICHE

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

es: $\star: A \times A \rightarrow A$
 $(a, b) \mapsto a \star b$

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

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

$(P(A), \cap)$ è struttura algebrica

$(P(A), \cup)$ è " "

es $S := \{ R : A \rightarrow A \text{ funzioni} \}$

funzioni da A in A

(S, \circ) è struttura algebrica

↗ composizione

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

Diciamo che:

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

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

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

$$\text{se } \bar{a}_s \star a = e$$

- Sia $\bar{a}_d \in A$ si dice INVERSO A DX di a

$$\text{se } a \star \bar{a}_d = e$$

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

$$\text{se } a \star \bar{a} = \bar{a} \star a = e$$

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 $(\mathbb{Q} - \{0\}, \cdot)$

$\cdot : \mathbb{Q} - \{0\} \times \mathbb{Q} - \{0\} \rightarrow \mathbb{Q} - \{0\}$ è operazione
1 è neutro e tutti gli el. hanno inverso

Prop: L'elemento neutro se esiste è unico

Sia (A, \star) struttura algebrica. Se esiste un elemento neutro, esso è neutro

Dimo: siano $e_1, e_2 \in A$ elementi neutri

(cioè $\forall a \in A \quad e_1 \star a = a \star e_1 = a$,

$e_2 \star a = a \star e_2 = a$)

per dimostrare $e_1 = e_2$

$e_1 = e_1 \star e_2 = e_2$ (per e_1 neutro sx)

↓
 e_2 è neutro a destra

Prop: L'inverso se esiste è 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 è unico.

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

$$\bar{a}_2 = e \star \bar{a}_2 = (\bar{a}_1 \star a) \star \bar{a}_2 = \bar{a}_1 \star (a \star \bar{a}_2) = \bar{a}_1 \star e = \bar{a}_1$$

↓
 e neutro ↓
 \bar{a}_1 è inverso di a
cioè $\bar{a}_1 \star a = e$ ↓
 \star è associativa ↓
 \bar{a}_2 è inverso ↑
 e neutro

Se A è insieme Finito e \star oper. allora posso considerare un diagramma "dato" da \star



\star	a	b	c	...	→ tutti el di A
a	$a \star a$	$a \star b$			
b	$b \star a$	$b \star b$			
c					
⋮					

| 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.

Tutti el di A

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

Def: (**MONOIDE**) Un monode è una struttura algebrica

(M, \star) t.c. ①: \star è associativa

②: \star ha elemento neutro

esempio $(\mathbb{N}, +)$ è monode

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

$$\begin{aligned} & (a \star b) \star (b^{-1} \star a^{-1}) = \\ & \downarrow \\ & = a \star (b \star b^{-1}) \star a^{-1} = \\ & \downarrow \\ & = a \star e \star a^{-1} = a \star a^{-1} = e \end{aligned}$$

⊙ 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 $a \star x = b$

$$\rightarrow \text{ha soluzione } x = a^{-1} \star b$$