

Ricordiamo: dati due insiemi non vuoti $A \neq B$, un'applicazione o funzione $f: A \rightarrow B$ è una relazione (o corrispondenza) $f \subseteq A \times B$ tale che:

$$\forall a \in A, \exists! b \in B : (a, b) \in f \quad [a R b]$$

$A = \text{dominio di } f$

$$\text{Scriveremo} \quad f: A \rightarrow B \quad \text{e} \quad f(a) = b$$

$B = \text{codominio di } f$

Se $X \subseteq A$, $f(X) = \{f(x) \mid x \in X\}$. In particolare, $f(A) =: \text{Im } f$
IMMAGINE di f

$$\text{Se } Y \subseteq B, \quad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

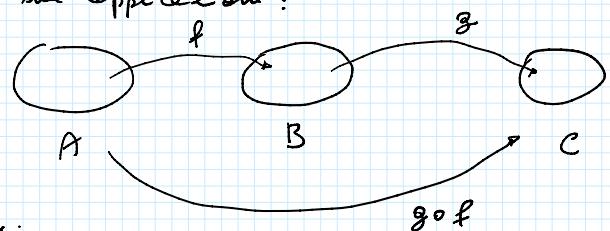
contrarioimmagine di Y
(o immagine inversa)

$$\text{Se } Y = \{y\}, \quad f^{-1}(\{y\}) =: f^{-1}(y).$$

Abbriamo enunciato la definizione di applicazione iniettiva, suriettiva, biiettiva (o bimbirocca).

Consideriamo tre insiemi non vuoti A, B, C e due applicazioni:

$$f: A \rightarrow B \quad g: B \rightarrow C$$



$g \circ f: A \rightarrow C$ è l'applicazione tali che:

$$\forall a \in A, \quad g(f(a)) := g(f(a))$$

Esempio: $A = \mathbb{N}$, $B = \mathbb{Z}$, $C = \mathbb{N}$ $f: \mathbb{N} \rightarrow \mathbb{Z}$, $g: \mathbb{Z} \rightarrow \mathbb{N}$
 $f: x \in \mathbb{N} \rightarrow \begin{cases} -\frac{x+1}{2}, & \text{se } x \text{ è dispari} \\ \frac{x}{2}, & \text{altrimenti} \end{cases} \in \mathbb{Z}$ oss: f è biiettiva

$$g: \mathbb{Z} \rightarrow \mathbb{N} \quad y \rightsquigarrow |y|$$

In questo esempio, poniamo considerare sia $g \circ f$ sia $f \circ g$:

$$g \circ f: \mathbb{N} \rightarrow \mathbb{N}$$

$$\begin{aligned} x \in \mathbb{N}, \text{ se } x \text{ è dispari: } g(f(x)) &= g\left(-\frac{x+1}{2}\right) = \left|-\frac{x+1}{2}\right| = \frac{x+1}{2} \\ \text{altrimenti: } g(f(x)) &= g\left(\frac{x}{2}\right) = \left|\frac{x}{2}\right| = \frac{x}{2} \end{aligned}$$

$$\xrightarrow{\text{es:}} g \circ f(1) = g(-1) = 1$$

$$f \circ g: \mathbb{Z} \rightarrow \mathbb{Z} \quad y \in \mathbb{Z} \quad f(g(y)) = f(|y|) = \begin{cases} -\frac{|y|+1}{2}, & \text{se } y \text{ è dispari} \\ \frac{|y|}{2}, & \text{altrimenti.} \end{cases}$$

esempio:

$$f \circ g(-3) = f(g(-3)) = f(3) = -2$$

$$f \circ g(4) = f(4) = 2$$

Si può dimostrare: $f: A \rightarrow B$, $g: B \rightarrow C$

f, g sono iniettive (opp. suriettive) $\Rightarrow g \circ f$ è iniettive (opp. suriettive)

Definizione: $f: A \rightarrow B$ è invertibile se esiste un'applicazione $f': B \rightarrow A$

tale che: $f \circ f': B \rightarrow B$, $f \circ f' = \text{id}_B: B \rightarrow B$ f' si dice

Definizione: $f: A \rightarrow B$ è invertibile se esiste un'applicazione $f': B \rightarrow A$ tale che:

$$f \circ f': B \rightarrow B, \quad f \circ f' = \text{id}_B: B \rightarrow B \quad \begin{matrix} b \rightsquigarrow b \\ f' \text{ si dice applicazione inversa di } f \end{matrix}$$

$$e \quad f' \circ f: A \rightarrow A, \quad f' \circ f = \text{id}_A: A \rightarrow A \quad \begin{matrix} a \rightsquigarrow a \\ f^{-1} \text{ relazione inversa della relazione } f \end{matrix}$$

Proposizione: $f: A \rightarrow B$ è invertibile $\Leftrightarrow f$ biettiva

Infatti, se f è invertibile, allora la sua inversa è f^{-1} relazione inversa della relazione f .

Esempio. Consideriamo di nuovo l'applicazione:

$$f: \mathbb{N} \rightarrow \mathbb{Z}$$

$$x \rightsquigarrow \begin{cases} -\frac{x+1}{2}, & \text{se } x \text{ è dispari} \\ \frac{x}{2}, & \text{altrimenti} \end{cases}$$

Come si comporta l'applicazione inversa f^{-1} di f ?

$$f^{-1}: \mathbb{Z} \rightarrow \mathbb{N}$$

$$y \rightsquigarrow \begin{cases} -2y-1, & \text{se } y \text{ è negativo} \\ 2y, & \text{altrimenti} \end{cases}$$

Dobbiamo trovar l'elemento $x \in \mathbb{N}$ tale che $f(x) = y$.

Se y è negativo, $y = -\frac{x+1}{2}$, quindi: $2y = -x-1 \Rightarrow x = -2y-1$

Altrimenti, $y = \frac{x}{2} \Rightarrow x = 2y$

Esercizio. Dimostriamo il seguente fatto: $f: A \rightarrow A$ iniettiva $\Rightarrow f \circ \dots \circ f = f^m: A \rightarrow A$ è iniettiva

usando il principio di induzione.

$m=1$ $f^1 = f$ è iniettiva, per ipotesi. base induttiva

$m>1$ $f^m = f \circ f \circ \dots \circ f \underset{m-1}{=} f \circ f^{m-1}$ per ipotesi di induzione, f^{m-1} è iniettiva

Th: f^m è iniettiva. Quindi: $x, x' \in A, f^m(x) = f^m(x') \Rightarrow x = x'$

$$\begin{array}{ccc} f^m(x) = f^m(x') & & \\ \overset{\text{f è iniettiva}}{\Rightarrow} f \circ f^{m-1}(x) = f \circ f^{m-1}(x') & & \\ \overset{\text{f è iniettiva}}{\Rightarrow} f(f^{m-1}(x)) = f(f^{m-1}(x')) & & \\ \overset{\text{f è iniettiva}}{\Rightarrow} f^{m-1}(x) = f^{m-1}(x') \Rightarrow x = x' & & \end{array}$$

Def. Siano A e B due insiem. Si dice che A e B hanno la stessa potenza o cardinalità se esiste un'applicazione biettiva $f: A \rightarrow B$ ($f^{-1}: B \rightarrow A$). Si dice che A e B sono equipotenti.

Esempio. Se A è un insieme finito e contiene n elementi, allora esiste una applicazione biettiva $f: A \rightarrow \{1, \dots, n\}$

$$\text{Card}(A) = |A| = |\{1, \dots, n\}| = \text{Card}(\{1, \dots, n\})$$

$$A = \{x_1, x_2, x_3\} \quad A \rightarrow \{1, 2, 3\}$$

$$x_1 \rightsquigarrow 1$$

$$x_2 \rightsquigarrow 2$$

$$x_3 \rightsquigarrow 3$$

(Questa approccio ci suggerisce la seguente definizione rigorosa di parotto co-ordinato:

(Quanto appena si raggiunge la seguente definizione rigorosa di prodotto di insiemi:
il prodotto cartesiano di insiemi A_1, A_2, \dots, A_m è l'insieme di tutte le applicazioni $f: \{1, \dots, m\} \rightarrow A_1 \cup A_2 \cup \dots \cup A_m$ tali che $f(i) \in A_i$)

Osservazione:

- Se A è un insieme equipotente a N si dice che è numerabile. $|A| = |N|$
- Qualsiasi insieme A consideriamo, $|A| < |\mathcal{P}(A)|$.
In particolare $|N| < |\mathcal{P}(N)| = |\mathbb{R}|$ potenza del continuo.
- Si può osservare che un insieme è infinito se è equipotente a una sua parte propria: esempio $|N| = |\mathbb{Z}|$ e $N \subsetneq \mathbb{Z}$.

Dato un'applicazione $f: A \rightarrow B$, poniamo "restringere" il dominio e anche il codominio di f .

- $\forall A' \subseteq A$, $f|_{A'}: A' \rightarrow B$ tali che:
 $\forall a' \in A'$, $f|_{A'}(a') \stackrel{\text{def.}}{=} f(a')$

$f|_{A'}$ è l'applicazione f RISTRETTA ad A' .

- Se $B' \subseteq B$ tali che $\text{Im } f \stackrel{\text{def.}}{=} f(A) \subseteq B'$, allora poniamo considerare:
 $g: A \rightarrow B'$ tali che: $\forall a \in A$, $g(a) = f(a)$

Esempio: $A = \{1, 3, 5\}$ $B = \{x, y, z, t\}$ $f: A \rightarrow B$ $\text{Im } f = \{z, t, y\}$

1	~	z
3	~	t
5	~	y

$$A' = \{1, 5\}, \quad f|_{A'}: \{1, 5\} \rightarrow B$$

1	~	z
5	~	y

$$B' = \{z, t, y\} \supseteq \text{Im } f, \quad g: A \rightarrow B'$$

1	~	z
3	~	t
5	~	y

Se invece $B'' = \{x, t, y\} \not\supseteq \text{Im } f$, allora NON POSSO RESTRINGERE il codominio a B'' .

Dati tre insiemi (non vuoti) A, B, C , un'operazione binaria su A si dice mappamento o operazione $A \times B \rightarrow C$. Se $A = B = C$, allora l'operazione si dice interna.

Se $B = C$, $A \times B \rightarrow B$, allora diciamo che l'operazione è esterna con operatore in A .

Esempi: $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ addizione "normale"
 $\cdot: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ moltiplicazione "normale"

Una mappa costituita da insiemi e da operazioni su essi definite si dice STRUTTURA ALGEBRICA.

Una struttura algebrica costituita da un insieme e una operazione interna su questo insieme si chiama gruppoide: $(N, +)$ è un gruppoide, (\mathbb{Q}, \cdot) è un gruppoide.

(G, \perp) $\perp: G \times G \rightarrow G$ gruppoide. Quali proprietà poniamo chiedendo che l'operazione \perp sia un gruppoide soddisfici?

- \perp è associativa se: $\forall x, x', x'' \in G$, $(x \perp x') \perp x'' = x \perp (x' \perp x'')$
- \perp è commutativa se: $\forall x, x' \in G$, $x \perp x' = x' \perp x$

• \perp ammette elemento neutro x : $\exists e \in G : \forall x \in G, e \perp x = x \perp e = x$

l'elemento "e" si dice elemento neutro rispetto a \perp

Se \perp ammette elementi:

• \perp è tale che ogni elemento di G ammette inverso (opp. simmetrico), ovvero:

$$\forall x \in G, \exists \bar{x} \in G : x \perp \bar{x} = \bar{x} \perp x = e.$$

$+: N^* \times N^* \rightarrow N^*$

Esempio: $(N^*, +)$ è associativa, commutativa, ma non ha elemento neutro

$(N, +)$ " " " " , ammette elemento neutro, ma non tutti gli elementi hanno inverso.

$+: N \times N \rightarrow N$

• Se \perp è $+$, l'inverso si dice **OPPOSTO**

• Se \perp è \circ , " " " " RECIPROCO.

Esempio: $X \neq \emptyset \quad \text{Hom}(X) = \{f: X \rightarrow X \mid f \text{ applicazione}\}$

$(\text{Hom}(X), \circ)$ è associativa (in più dimensione)
non è commutativa

ha elemento neutro = id_X

non tutti gli elementi di $\text{Hom}(X)$ hanno inverso

$G(X) \subseteq \text{Hom}(X)$

" $\{f: X \rightarrow X \mid f \text{ applicazione invertibile}\}$

$(G(X), \circ)$ è associativa, (non è commutativa), ammette elemento neutro id_X
e ogni elemento di $G(X)$ ha inverso (si dice anche che è invertibile)

Def. (G, \perp) si dice gruppo se: \perp è associativa, ammette elemento neutro e
ogni elemento di G ha inverso (si dice anche che è invertibile)

Esempio: $(G(X), \circ)$ è un gruppo.

$(Z, +)$ è un gruppo, $(N, +)$ non è un gruppo

Def. Un gruppo (G, \perp) si dice abeliano se \perp è commutativa.

Esempio: $(G(X), \circ)$ è un gruppo non abeliano, $(Z, +)$ è un gruppo abeliano,

(Q^*, \cdot) è un gruppo abeliano

Esempio: $f: \{1, 3, 5\} \rightarrow \{x, y\}$

1	\rightsquigarrow	x
3	\rightsquigarrow	y
5	\rightsquigarrow	y

$g: \{x, y\} \rightarrow \{1, 3, 5\}$

x	\rightsquigarrow	3
y	\rightsquigarrow	1

$g \circ f: \{1, 3, 5\} \rightarrow \{x, y\} \rightarrow \{1, 3, 5\}$

1	\rightsquigarrow	x	\rightsquigarrow	3
3	\rightsquigarrow	y	\rightsquigarrow	1
5	\rightsquigarrow	y	\rightsquigarrow	1

$f \circ g: \{x, y\} \xrightarrow{g} \{1, 3, 5\} \xrightarrow{f} \{x, y\}$

È ovvio che $f \circ g \neq g \circ f$ perché

hanno dominio e codominio DIVERSI

$f: \{1, 3, 5\} \rightarrow \{1, 3, 5\}$

1	\rightsquigarrow	3
3	\rightsquigarrow	1
5	\rightsquigarrow	3

$g: \{1, 3, 5\} \rightarrow \{1, 3, 5\}$

1	\rightsquigarrow	5
3	\rightsquigarrow	5
5	\rightsquigarrow	1

$g \circ f: \{1, 3, 5\} \xrightarrow{f} \{1, 3, 5\} \xrightarrow{g} \{1, 3, 5\}$

1	\rightsquigarrow	3	\rightsquigarrow	5
3	\rightsquigarrow	1	\rightsquigarrow	5
5	\rightsquigarrow	3	\rightsquigarrow	5

$f \circ g: \{1, 3, 5\} \xrightarrow{g} \{1, 3, 5\} \xrightarrow{f} \{1, 3, 5\}$

1	\rightsquigarrow	5	\rightsquigarrow	3
3	\rightsquigarrow	5	\rightsquigarrow	3
5	\rightsquigarrow	1	\rightsquigarrow	3

Proprietà: se (G, \perp) un gruppoide.

Proprietà: sia (G, \perp) un gruppoide.

(1) Se \perp ha elemento neutro e , questo elemento è unico.

(2) Se \perp è associativa & ammette elemento neutro e :

- se $x \in G$ ammette inverso \bar{x} , \bar{x} è unico
- se $x, x' \in G$ ammettono inversi \bar{x}, \bar{x}' , rispettivamente, allora:
 $x \perp x'$ ammette inverso $= \bar{x}' \perp \bar{x}$

DIM. (2) per definizione, $\forall x \in G \quad x \perp e = e \perp x = x$

Sia e' un altro elemento neutro. Th: $e = e'$

$$e' = e \perp e' = e' \perp e = e$$

\nwarrow e è elemento neutro \nearrow e' è elemento neutro

(2) • per definizione: $x \perp \bar{x} = \bar{x} \perp x = e$

Sia $\bar{\bar{x}}$ un altro inverso di x : $x \perp \bar{\bar{x}} = \bar{\bar{x}} \perp x = e$ \leftarrow NB

$$\bar{x} = \bar{x} \perp e = \bar{x} \perp (x \perp \bar{x}) = (\bar{x} \perp x) \perp \bar{x} = e \perp \bar{x} = \bar{\bar{x}}$$

\nwarrow \perp è associativa

• per definizione $x \perp \bar{x} = \bar{x} \perp x = e$ Th: $(x \perp x') \perp (\bar{x}' \perp \bar{x}) =$
 $x' \perp \bar{x}' = \bar{x}' \perp x = e$ $= (\bar{x}' \perp \bar{x}) \perp (x \perp x') = e$

$$(x \perp x') \perp (\bar{x}' \perp \bar{x}) = x \perp (x' \perp (\bar{x}' \perp \bar{x})) = x \perp ((x' \perp x') \perp \bar{x}) =$$

\nwarrow \perp è associativa
 $= x \perp (e \perp \bar{x}) = x \perp \bar{x} = e$

$$(x' \perp \bar{x}) \perp (x \perp x') = \bar{x}' \perp (\bar{x} \perp (x \perp x')) = \bar{x}' \perp ((\bar{x} \perp x) \perp x') = \bar{x}' \perp (e \perp x') =$$
 $= \bar{x}' \perp x' = e$

Def. Sia K un insieme non vuoto e due operazioni interne $+: K \times K \rightarrow K$
 $\cdot: K \times K \rightarrow K$

$(K, +, \cdot)$ si dice campo se:

(a) $(K, +)$ è un gruppo abeliano. Denotiamo con 0 l'elemento neutro.

Posto $K^* = K \setminus \{0\}$ e denotato ancora con \cdot la restrizione dell'operazione $\cdot: K^* \times K^* \rightarrow K^*$

(b) (K^*, \cdot) è un gruppo abeliano; denotato con \circ l'elemento neutro

(c) $\forall a, b, c \in K$, $a \cdot (b+c) = ab + ac$ (oss.: $1 \neq 0$)
 $(a+b) \cdot c = ac + bc$

Esempio: $(\mathbb{R}, +, \cdot)$ è un campo, $(\mathbb{Q}, +, \cdot)$ è un campo, con le operazioni che già conosciamo.

$$K = \{0, 1\}$$

$$\oplus: K \times K \longrightarrow K$$

$(0, 0)$	\rightsquigarrow	0
$(0, 1)$	\rightsquigarrow	1
$(1, 0)$	\rightsquigarrow	1
$(1, 1)$	\rightsquigarrow	0

$$\odot: K \times K \longrightarrow K$$

$(0, 0)$	\rightsquigarrow	0
$(0, 1)$	\rightsquigarrow	0
$(1, 0)$	\rightsquigarrow	0
$(1, 1)$	\rightsquigarrow	1

(K, \oplus, \odot) è un campo.