Algebra e Geometria 2022-23

Luca Giuzzi

luca.giuzzi@unibs.it

- ALGEBRA LINEARE
- GEOMETRIA ANALITICA
  (applicazione dell'algebra lineare)

ALGEBRA: strutture e loro trasformazioni.

Notazione: teoria "intuitiva" degli insiemi

ZF + Assioma della scelta

<u>Insieme</u> → collezione di elementi
non ordinata e priva
di ripetizioni.

$A = \{a, b, c, d\} = \{b, c, d, a\} = \{a, b, c, a, d, d\}$.

CARDINALITÀ DI UN INSIEME A

$|A|$ = numero di elementi di A

propr. fondamentale $x \in A$ x appartiene ad A

$x \notin A$ x non appartiene ad A

<u>Multiinsieme</u> – <u>sistema</u>: Insieme
con molteplicità =
collezione non ordinata
di elementi con ripetizioni.

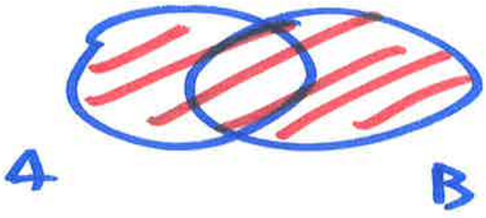
$[a, b, c] = [c, b, a] \neq [a, a, b, c]$

Sequenza: collezione ordinata di
elementi

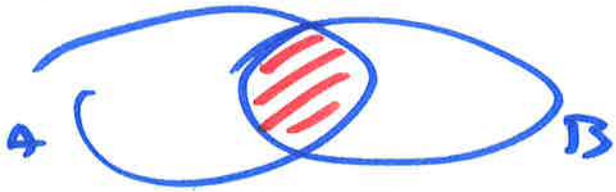
$(a, b, c) \neq (c, b, a) \neq (a, a, b, c)$.

Dati due insiemi A, B definiamo

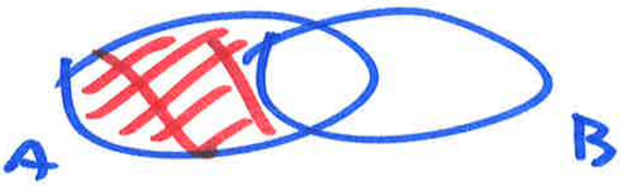
$$A \cup B = \{x \mid x \in A \text{ oppure } x \in B\}.$$



$$A \cap B = \{x \in A \mid x \in B\}.$$



$$A \setminus B = \{x \in A \mid x \notin B\}.$$



$$A \times B = \{(a,b) \mid a \in A,\ b \in B\}.$$

sequenze.

$$(a,b) := \{\{a\}, \{a,b\}\}.$$

$$(a,b) = \boxed{\{\{a\},\{a,b\}\}}.$$

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

$$= \boxed{\{\{a\}\}}.$$

$$(b,a) = \{\{b\},\{b,a\}\} = \boxed{\{\{b\},\{a,b\}\}}.$$

<u>coppia ordinata.</u>

<u>Def</u>: Siano A, B insiemi.

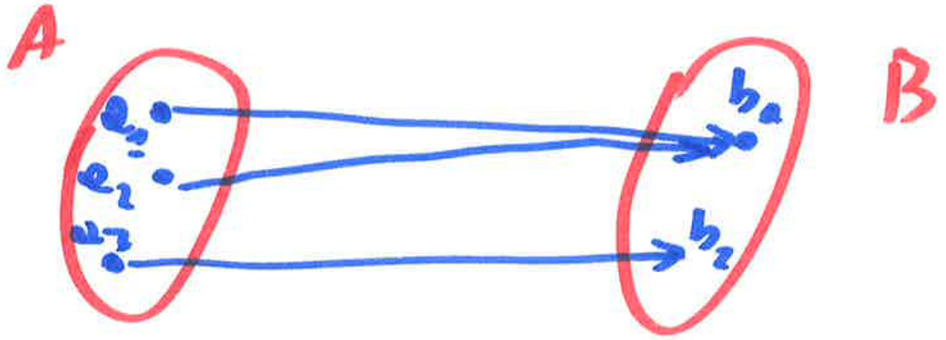
Si dice ~~[illegible]~~ <u>funzione</u> fra A e B un sottoinsieme

$$C \subseteq A \times B$$

tale che ~~$\forall (x,y) \in C$~~

$\forall a \in A \ \exists! b \in B$ tale che

$$(a,b) \in C$$



$$C = \{(a_1,b_2),(a_2,b_1),$$
$$(a_3,b_2)\}.$$

Scriveremo $\quad b_1 = C(a_1)$

$b_1 = C(a_2)$

$b_2 = C(a_3)$

Insiemi famosi:

$\mathbb{N} = \{0,1,2\dots\}$ numeri naturali

$\mathbb{Z} = \{\dots -1, 0, +1 \dots\}$ numeri interi

$\mathbb{Q}$ = numeri razionali

$\mathbb{R}$ = numeri reali

$\mathbb{C}$ = numeri complessi.

$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ $\quad \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\quad \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

$\mathbb{N}_0$

Sia $f \subseteq A \times B$ una funzione

$$f : A \to B.$$

~~Allora f è detta iniettiva se~~

Allora A é detto <u>dominio</u> di f

e B é detto <u>codominio</u> di f

<u>N.B.</u> $f : A \to B$

$g : A \to C$ con $C \subseteq B$

e tali che $\forall a \in A : f(a) = g(a)$

sono 2 funzioni diverse.

Es. $g : \begin{cases} \mathbb{N} \longrightarrow \mathbb{Z} \\ n \longrightarrow 2n \end{cases}$ $\qquad \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

$f : \begin{cases} \mathbb{N} \longrightarrow \mathbb{R} \\ n \longrightarrow 2n \end{cases}$

Def $f: A \to B$ si dice

immagine di f

l'insieme $\mathrm{Im}\, f := \{ b \in B \mid \exists a \in A$

con $f(a) = b \}$.

Def: Data $f: A \to B$ e ~~X~~ $\mathrm{Im}\, f \subseteq$

si dice **troncatura** di f

ad X la funzione

$f^X \subseteq A \times X$ tale che

$$f^X := \{ (a,x) \in A \times X \mid (a,x) \in A \times B \}.$$

Il codominio viene ristretto!

$$\boxed{\mathrm{Im}\, f \subseteq X}$$

$g = f^{\mathbb{Z}}$ $\quad$ g è f troncata a $\mathbb{Z}$

$f: A \to B$ $\quad Y \subseteq A$ si dice **restrizione** di f ad Y la funzione $f_Y := \{(a,b) \in Y \times B$ tali che $a \in Y\}$.

In generale: prima si restringe e poi si tronca una funzione.

$$f: \begin{cases} \mathbb{N} \longrightarrow \mathbb{R} \\ x \longrightarrow 2x \end{cases}$$

Sia $Y = 2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$.

si può considerare

$$f_Y: \begin{cases} 2\mathbb{N} \longrightarrow \mathbb{R} \\ x \longrightarrow 2n \end{cases}$$

calcoliamo $Im(f_y) = 4\mathbb{N}$

e consideriamo la restrizione troncata

$$f_{2\mathbb{N}}^{4\mathbb{N}} : \begin{cases} 2\mathbb{N} \to 4\mathbb{N} \\ x \to 2n \end{cases}$$

$f: A \to B$ é detta iniettiva se $\forall b \in B$ esiste al più un elemento $a \in A$ tale che $f(a) = b$.

In altre parole se $\forall x, y \in A$

$$f(x) = f(y) \Rightarrow x = y$$

implica

$f: A \to B$ é detta suriettiva se $\forall b \in B \; \exists a \in A : f(a) = b$

cioè $Im(f) = B$

f è <u>biiettiva</u> se $\forall b \in B \ \exists! \, a \in A$

esiste uno ed un solo

tale che $f(a) = b$.

$\to$ iniettiva + suriettiva.

<u>OSS</u>: Se A, B sono insiemi

$f: A \to B$ biiettiva $\Leftrightarrow |A| = |B|$.

<u>N.B</u> $|A|$ e $|B|$ possono essere infiniti e $|\mathbb{N}| < |\mathbb{R}|$

$|X| < |Y| \Leftrightarrow \exists$ una funzione iniettiva $X \to Y$ ma non $\exists$ biiettiva da $X \to Y$

<u>N.B</u> biiettiva è anche detta corrispondenza 1-1

Composizione di funzioni

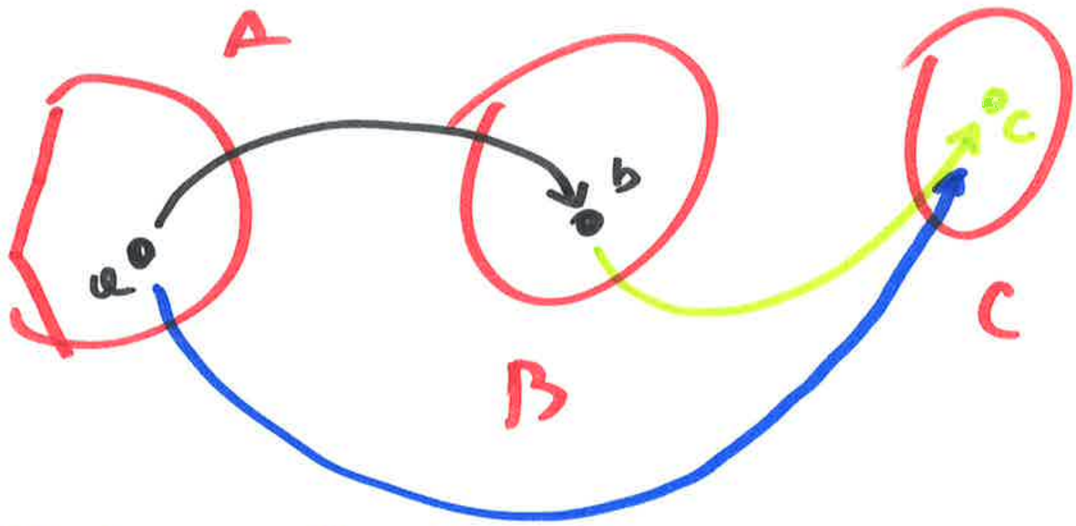
$f: A \to B$ funzione

$g: B \to C.$ funzione

$(g \circ f): A \to C$ ed è definita

come

$$(g \circ f) = \{ (a,c) \mid \exists b : (a,b) \in f \;\&\; (b,c) \in g \}.$$



oss: l'elemento b che compare in $(g \circ f)$ è unico $\forall a \in A$

Def: Sia M un insieme.
Si dice <u>operazione binaria</u> su M una funzione
$$\circ : M \times M \rightarrow M$$
che prende come input 2 elementi di M e fornisce come risultato un elemento di M.

Una <u>struttura algebrica</u> è una n-upla (sequenza) data da un insieme ed una o più operazioni su di esso. $(M, \circ)$

<u>ESEMPI</u>

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

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

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +)$

$(\mathbb{R}^*, :)$ $(\mathbb{C}, +, \cdot)$ etc.

Def: Sia $(A, *)$ un insieme con una operazione binaria

$$* \; A \times A \to A$$

$$*(a,b) = a * b$$

Si dice che $e \in A$ è un elemento neutro per $*$ se

$$\forall a \in A : \; e * a = a * e = a$$

~~Si dice che~~

Se $(A, *)$ ammette elemento neutro si dice che $b \in A$ ammette inverso destro b' se $\exists\, b' \in A$ tale che

$$b * b' = e$$

inverso sinistro se $\exists\, b'' \in A$ tale che

$$b'' * b = e.$$

inverso se $\exists$ inversi destri e sinistri

Si dice che $*$ è commutativa se $\forall a,b \in A : a*b = b*a$

Si dice che $*$ è associativa se $\forall a,b,c \in A : a*(b*c) = (a*b)*c$.

Def: $(A,*)$ è detto MONOIDE se $*$ ammette elemento neutro ed è associativa.

è detto GRUPPO se è un MONOIDE ed ogni elemento di A ammette inverso (necessariamente unico, destro e sx).

è detto GRUPPO ABELIANO o COMMUTATIVO se oltre ad essere gruppo $\forall a,b \in A : a*b = b*a$.

Esempi

$(\mathbb{N},+)$ MONOIDE COMM. MA NON GRUPPO

$(\mathbb{Z},+)$ GRUPPO ABELIANO

$(\mathbb{Z}, -)$ NON HA ELEM. NEUTRO
NON È ASSOCIATIVO
NON È COMMUTATIVO

$5-0 \neq 0-5$ NO COMM.

$a-0=a \quad \forall a \in \mathbb{Z}$

$0-a \neq a \quad \forall a \in \mathbb{Z} \setminus \{0\}$.

NO EL. NEUTRO.

$(2-3)-4=-5$

$2-(3-4)=3$

NON È ASSOC.!!

<u>N.B</u> la sottrazione è definita come somma con l'opposto di un elemento in $(\mathbb{Z}, +)$.

$a-b: \quad a+(-b)$