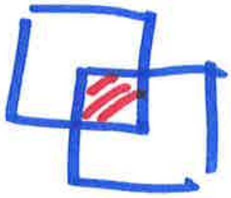
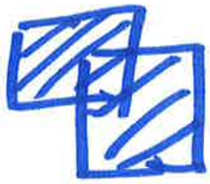
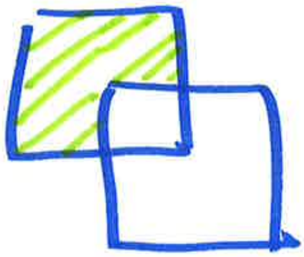
Linguaggio degli insiemi.

- A, B insiemi

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

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

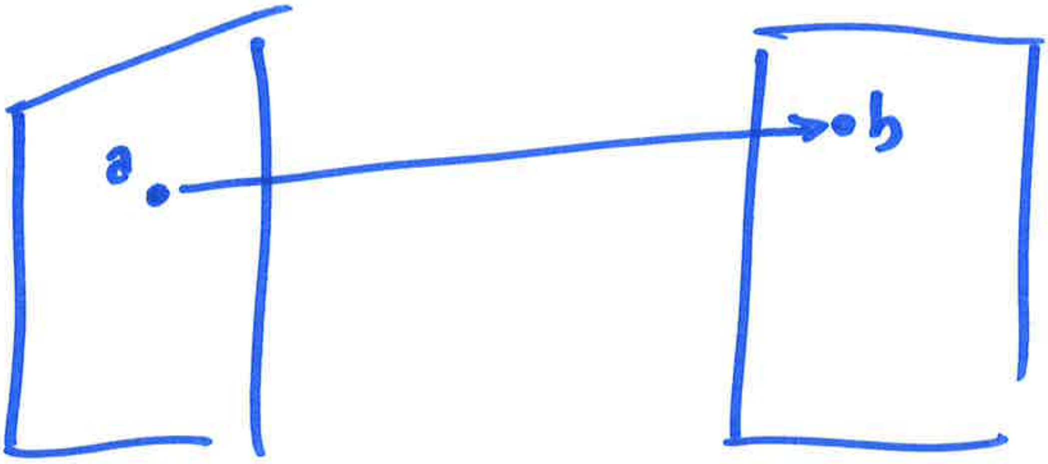
$A \setminus B = \{a \in A \mid a \notin B\}$. 

$f: A \to B$

$f \subseteq A \times B$

CORRISPONDENZA

- Funzionale
- Ovunque definita



A	B
DOMINIO	CODOMINIO

$(a, b) \in C$

DOMINIO

__Funzionale__: da ogni el. di A parte al più una freccia.

__Ovunque def__: da ogni el. di A parte almeno una freccia.

CODOMINIO

__Iniettività__: ad ogni el. di B arriva al più una freccia

__Suriettività__: ad ogni elemento di B arriva almeno una freccia.

$f: A \to B$ biiettiva

$\Rightarrow f^{-1}: B \to A$ biiettiva

funzione inversa di f.

$$f^{-1} \circ f : \begin{cases} A \to A \\ x \to x \end{cases}$$

$$f \circ f^{-1} : \begin{cases} B \to B \\ y \to y \end{cases}$$

ALGEBRA: trasformazioni di oggetti.

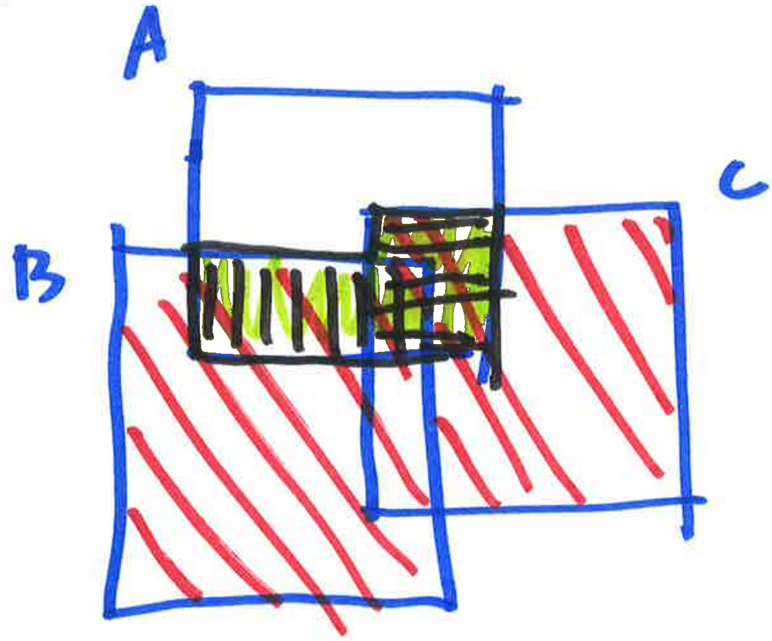
$C \subseteq A \times B$ definisco ${}^tC \subseteq B \times A$

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

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

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



operazioni su di un insieme.
(binarie).

<u>Def</u> Una operazione binaria
$*$ su di un insieme A
è una funzione $* : A \times A \longrightarrow A$
Si dice struttura algebrica una

collezione di un insieme
ed una o più operazioni
su di esso

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

$(\mathbb{N},-)$ × No

N.B per me $\mathbb{N}$ include 0

Sia A un insieme e $*$ una
operazione su A.

Si dice che:

1) $*$ ammette elemento neutro e
se $\forall a \in A$: $a * e = e * a = a$

[esempio: $0 \in \mathbb{N}$ $\forall n \in \mathbb{N}$ $0+n = n+0 = n$]

2) $*$ é associativa se $\forall a,b,c \in A$
$(a*b)*c = a*(b*c)$

3) Un elemento $a \in A$ ammette inverso rispetto $*$ se $\exists a' \in A$ tale che

$$a * a' = a' * a = e$$

4) $*$ é commutativa se $\forall a, b \in A$

$$a * b = b * a.$$

Def: $(A, *)$ é detto <u>GRUPPO</u>

se $*$ ammette el. neutro,

$\forall a \in A$ ammette inverso

$*$ é associativa.

Se $*$ é anche commutativa

$(A, *)$ é detto <u>gruppo abeliano</u>

$(\mathbb{N}, +)$

el. neutro : 0

commutativa : OK

associativa : OK.

MANCA L'INVERSO $\forall n > 0$

$3 + x \geq 3 \neq 0$

NON É UN GRUPPO

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

considerate $(\mathbb{Z}, -)$

$$a-(b-c) = a-b+c \neq$$

$$(a-b)-c = a-b-c$$

$$a+b+c$$

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

Esempio II. $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

$(\mathbb{Z}, \cdot)$ NO

$(\mathbb{Q}^*, \cdot)$ $(\mathbb{R}^*, \cdot)$ GRUPPO $(\mathbb{C}^*, \cdot)$

$$GL(2,\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}.$$

↑

Generale Lineare

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$ el. neutro ✓

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{cases} aa' + bc' = 1 \\ ab' + bd' = 0 \\ ca' + dc' = 0 \\ cb' + dd' = 1 \end{cases}$$

∃ inverso ∀ elemento.

N.B: Il prodotto di matrici NON È COMMUTATIVO

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

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

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

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

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

Def: Una struttura algebrica $(A, +, \cdot)$ è detta anello se
1) $(A, +)$ è un gruppo abeliano
2) $(A, \cdot)$ è una struttura algebrica; $\cdot$ è associativa
3) ~~———~~
4) $\forall a, b, c \in A$ $(a+b) \cdot c = ac + bc$
$a \cdot (b+c) = ab + ac$

[valgono le prop. distributive]

Def: Un Anello $(A, +, \cdot)$ é detto

→ con unitá se $\cdot$ ammette elemento neutro in A

→ commutativo se $\cdot$ é commutativa.

[es. Anello commutativo con unitá $(\mathbb{Z}, +, \cdot)$]

→ <u>CAMPO</u> se $(A \setminus \{0\}, \cdot)$ é un gruppo abeliano

<u>CORPO</u> se $(A \setminus \{0\})$ é un gruppo.

ove 0 é l'elemento neutro di +

Esempi di campo.

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

Tutta l'algebra lineare che studieremo si basa sulle proprietà di campo.

Esempio di campo finito.

$\mathbb{F}_2 = \{0, 1\}$.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$(\mathbb{F}_2, +, \cdot)$ è un campo con 2 elementi

$\mathbb{F}_3 = \{0, 1, 2\}$.

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(\mathbb{F}_3, +, \cdot)$ é un campo.

<u>N.B.</u> Un campo finito ha sempre p^t elementi con p numero primo. e per ogni potenza di primo esiste un campo con quel numero di elementi.

Esempio di corpo: (non comm.).

$\mathbb{H} = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}\}$.

con

$(a + ib + jc + kd) + (a' + ib' + jc' + kd') =$
$= (a + a') + i(b + b') + j(c + c') + k(d + d')$

$(a + ib + jc + kd) \cdot (a' + ib' + jc' + kd') = \ldots$

prodotto di polinomi in cui si pone.

$i^2 = j^2 = k^2 = -1$

$ij = k \quad jk = i \quad ki = j$

$ji = -k \quad kj = -i \quad ik = -j$

GRUPPO

↓

ANELLO

↓

CAMPO

ALGEBRA LINEARE → ALGEBRA SU CAMPI.

$$\mathbb{K} \text{ campo} \begin{cases} \mathbb{R} \\ \mathbb{C} \\ \mathbb{Q} \end{cases} \quad (\mathbb{F}_2)$$

Insieme → Coppia ordinata

Sistema (Multiinsieme)

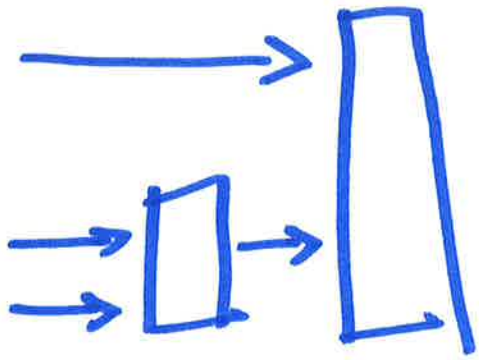
Sequenza:

Se A insieme, $k \geq 1$ intero.

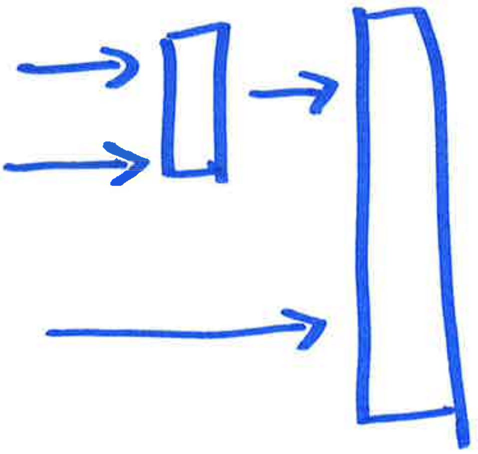
$$A^k = \underbrace{A \times (A \times \dots \times A)}_{k \text{ volte}}$$

$A\times(A\times A) \ni (a_1,(a_2,a_3))$ —

$(A\times A)\times A = \{((a_1,a_2),a_3)\ \ \}$



$A\times(A\times A)$



$(A\times A)\times A$

$$A^3 = \{(a_1,a_2,a_3) \mid a_i \in A\}.$$

Sia $I_n := \{ i \in \mathbb{N} \mid 0 < i \leq n\}$.

Una sequenza di n elementi di A una funzione $I_n \longrightarrow A$

Sia $\mathbb{K}$ un campo. e

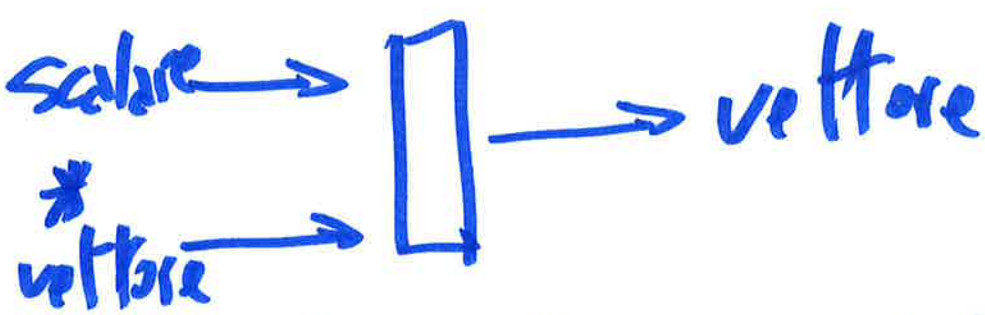
$(V, \dot{+})$ un gruppo abeliano.

Si dice che V è uno spazio vettoriale su $\mathbb{K}$ rispetto il prodotto per scalare $*$ se:

$$*: \mathbb{K} \times V \longrightarrow V$$

$\forall\, \bar{v}, \bar{w} \in V$, $\forall\, \alpha, \beta \in \mathbb{K}$ abbiamo.

1) $1 * \bar{v} = \bar{v}$
2) $(\alpha + \beta) * \bar{v} = \alpha * \bar{v} \dot{+} \beta * \bar{v}$
3) $\alpha * (\bar{v} \dot{+} \bar{w}) = \alpha * \bar{v} \dot{+} \alpha * \bar{w}$
4) $(\alpha \cdot \beta) * \bar{v} = \alpha \boxed{*} (\beta \boxed{*} \bar{v})$.



gli elementi di $\mathbb{K}$ sono detti scalari e gli elementi di V sono detti vettori.

Esempio $\mathbb{K}$ campo.

$$\mathbb{K}^3 = \{(a,b,c) \mid a,b,c \in \mathbb{K}\}.$$

Definisco $\dot{+}$ $\begin{cases} \mathbb{K}^3 \times \mathbb{K}^3 \longrightarrow \mathbb{K}^3 \\ (a,b,c),(a',b',c') \longrightarrow \end{cases}$

$$(a+a', b+b', c+c').$$

Esercizio: Verificare che $(\mathbb{K}^3, \dot{+})$ é un gruppo abeliano.

Def. $*$ $\begin{cases} \mathbb{K} \times \mathbb{K}^3 \longrightarrow \mathbb{K}^3 \\ (\alpha)(a,b,c) \to (\alpha a, \alpha b, \alpha c) \end{cases}$

prodotto componente per componente.

$(\mathbb{K}^3, \dot{+})$ é spazio vettoriale su $\mathbb{K}$.

1) $1 * (a,b,c) = (1a, 1b, 1c)$
$= (a,b,c)$

2) $(\alpha+\beta) * (a,b,c) =$
$= ((\alpha+\beta)a, (\alpha+\beta)b, (\alpha+\beta)c) =$
$= (\alpha a + \beta a, \alpha b + \beta b, \alpha c + \beta c) =$
$= (\alpha a, \alpha b, \alpha c) \dot{+} (\beta a, \beta b, \beta c) =$
$= \alpha * (a,b,c) \dot{+} \beta (a,b,c).$

3) $\alpha * ((a,b,c) \dot{+} (a',b',c')) =$
$= \alpha * (a+a', b+b', c+c') =$
$= (\alpha(a+a'), \cancel{\alpha}(b+b'), \alpha(c+c')) =$

$= \dots = \alpha(a,b,c) \dotplus \alpha(a'b'c')$.

4) $(\alpha\beta) * (a\ b\ c) =$

$= ((\alpha\beta)a\ (\alpha\beta)b\ (\alpha\beta)c) =$

$= (\alpha(\beta a)\ \alpha(\beta b)\ \alpha(\beta c)) =$

$= \alpha * (\beta a\ \beta b\ \beta c) =$

$= \alpha * (\beta * (a,b,c))$.

Esempio più concreto

$\mathbb{R}^3 = \{(a,b,c) \mid a,b,c \in \mathbb{R}\}$.

su $\mathbb{R}$.

$\mathbb{C}$ visto come s.vettoriale

su $\mathbb{R}$.

se $\mathbb{K}$ campo.

$\mathbb{K}^n$ dotato delle operazioni

di somma di vettori } componente
prodotto per scalare } per componente

$$(a_1 \dots a_n) \dotplus (b_1 \dots b_n) = (a_1+b_1 \dots a_n+b_n)$$

$$\alpha * (a_1 \dots a_n) = (\alpha a_1 \dots \alpha a_n)$$

é spazio vettoriale su $\mathbb{K}$.