$(\mathbb{K},+,\cdot)$ campo

$(\mathbb{K},+)$: gruppo abeliano con el neutro 0

$(\mathbb{K}\setminus\{0\},\cdot)$: gruppo abeliano

valgono le distributive

$\forall a,b,c \in \mathbb{K}$: $a(b+c) = ab+ac$

$(a+b)c = ac+bc$

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

$a-b := a+(-b)$

$a/b := a\cdot(b)^{-1}$ $\quad b\neq 0$

$(\mathbb{Z}_2,+,\cdot)$ $\qquad \mathbb{Z}_2=\{0,1\}$

+	0	1
0	0	1
1	1	0

~~AND~~ XOR

·	0	1
0	0	0
1	0	1

AND

$0 = F$
$1 = V$

$NOT = \neg$ $\qquad$ $NOT(x) := 1 + x$

x	$x+1$
0	1
1	0

x OR y

OR	0	1
0	0	1
1	1	1

$= (x+y) + xy$

x	y	$x+y$	xy	$(x+y)+xy$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	0	1	1

$x \Rightarrow y$ significa $\neg x$ OR y $\qquad$ $\neg x = (x+1)$

$$(x+1+y) + (x+1)y = x+y+1+xy+y =$$

$$= x + xy + 1$$

$x \Rightarrow y$ è eq. $\neg(x \text{ XOR } (x \,\&\, y))$

$(b \cdot a) \cdot b^{-1} = a$ $\quad b \neq 0$

$ba = b(a+c)$

$(\mathbb{Z}_2, +, \cdot)$ campo finito

Sia p un primo $\Rightarrow \forall n \geq 1$ esiste un campo con p^n elem.

$\mathbb{F}_{p^n}$

Se $n = 1$ $\quad \mathbb{F}_p = \mathbb{Z}_p$ $\quad \mathbb{Z}_p = \{0, 1, \dots p-1\}$

$(a+b)$ in $\mathbb{Z}_p$ = resto di $(a+b)/p$ in $\mathbb{Z}$

$(a \cdot b)$ in $\mathbb{Z}_p$ = resto di $(a \cdot b)/p$ in $\mathbb{Z}$

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

non è invertibile

NON È UN CAMPO

$\mathbb{F}_4 = \{(00), (01), (10), (11)\}$

$\quad\;\; 0 \quad\;\; 1 \quad\;\; 2 \quad\;\; 3$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

resto divisione polinomio dati:

$\downarrow$

$(a\ b) = ax+b$ per x^2+x+1

$\{0, 1, x, x+1\} \in \mathbb{Z}_2[x]$

$x \cdot (x+1) = (x^2+x)$ resto divid. per (x^2+x+1)

$$x^2+x = (x^2+x+1)\cdot 1 - 1 = (x^2+x+1)+1 \Rightarrow 1$$

$\uparrow$ quoz. $\uparrow$ div.

$$(2)\cdot(3) = (1)$$

$$(x+1)\cdot(x+1) = x^2+x+x+1 = x^2+1$$

divido per x^2+x+1

mi resta resto $= x = (2)$

$\mathbb{Z}_3$

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

$2 = -1$

$2 + 1 = 0$

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\frac{1}{2} = 2$

$\mathbb{Z}_9 = \mathbb{Z}_3[x]$

$p(x) = x^2 + 2x + 1 = (x+1)^2$

NO

$p(0) = 1$

$p(1) = 4 = 1 \neq 0$

$p(2) = 4 + 4 + 1 = 9$

$q(x) = x^2 + 2x + 2$

OK

$q(0) = 2 \neq 0$

$q(1) = 2 \neq 0$

$q(2) = 10 = 1 \neq 0$

$0 \quad 1 \quad 2 \quad x \quad x+1 \quad x+2 \quad 2x \quad 2x+1 \quad 2x+2$

$$(x+2)(2x+2) = 2x^2+2x+4x+4 =$$

$$= 2x^2+6x+4 =$$

$$= 2x^2+1$$

DIVIDO per x^2+2x+2

$$2x^2+1 = (x^2+2x+2)\cdot 2 + r(x)$$

$$r(x) = 2x^2+4x+4-2x^2-1 = 4x+4-1 = x$$

Insiemi: collezioni non ordinate senza ripetizioni.

Sistema di elementi di un insieme = multiinsieme

: collezione non ordinata di elementi con molteplicità.

↓

funzione $f: A \to \mathbb{N}$ (escluso 0).

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

$$\shortparallel$$

$$[a, c, b, b]$$

Sequenza di n elementi di un insieme A = collezione ordinata anche con el. ripetuti

→ funzione $g: \{1 \dots n\} \to A$

Insieme

$$\{a, b, c\} = \{a, c, b\} = \{a, b, b, c\}$$

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

Sequenze: $(a, b, c) \neq (a, c, b) \neq (a\ b\ b\ c) \neq (a, b, c)$

Dato un insieme A definiamo

$$A^n = \{(a_1, \dots a_n) \mid a_i \in A\} =$$

$$= \{f : \{1, \dots n\} \to A \mid f \text{ funzione}\}.$$

$A^2 = \{(a,b) \mid a,b \in A\}.$

$A \times A$

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

$(A \times A) \times A \approx A^3$

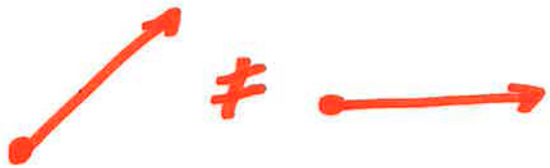
$\{((a,b),c) \mid a,b,c \in A\}.$

$A \times (A \times A) = \{(a,(b,c)) : a,b,c \in A\}.$

(a,b,c)

vettore

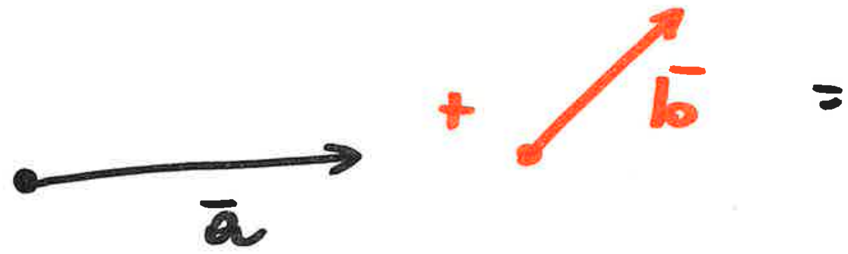
 = (direzione, verso, lunghezza).

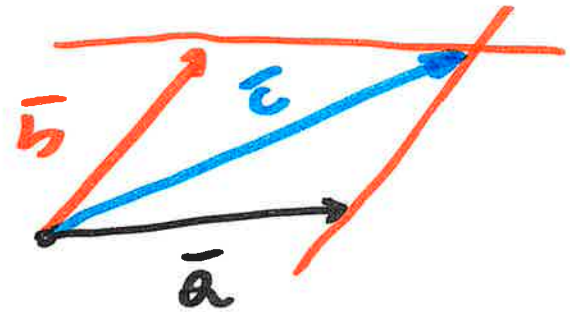
 dir. diversa

 verso differente

 lunghezza differente.

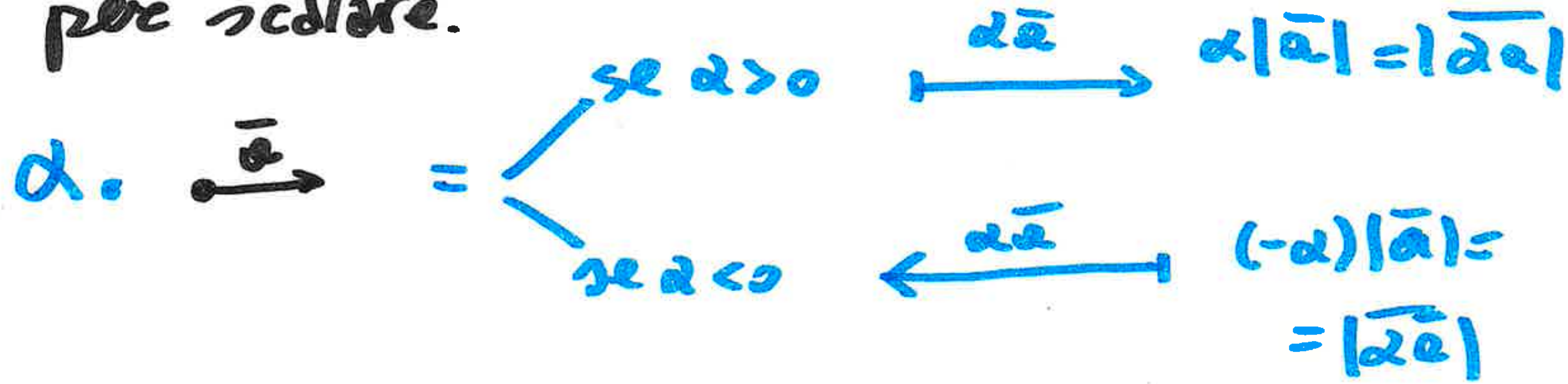
somma di vettori





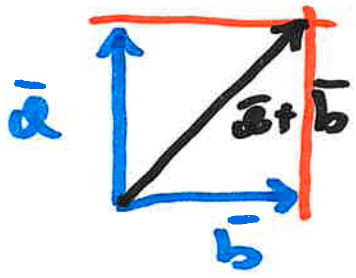
$\bar{c} = \bar{a} + \bar{b}$

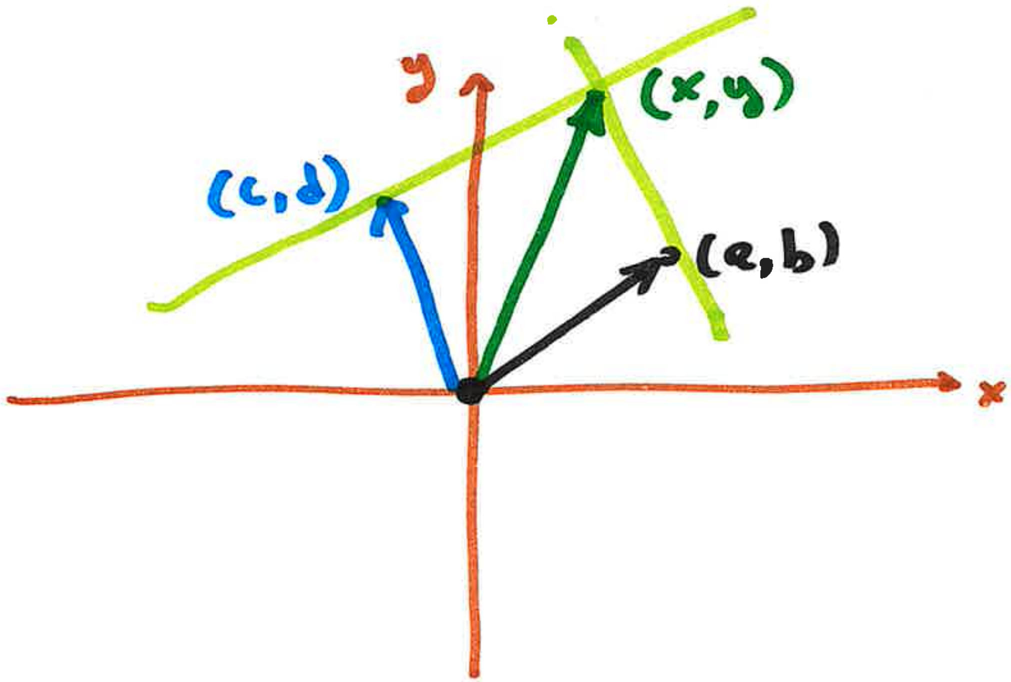
prodotto per scalare.



$2\bar{a}$ 

$\frac{1}{2}\bar{a} = \bar{b}$ $\quad 2\bar{b} = \bar{a}$





$\bar{a} = (a,b) \in \mathbb{R}$

$\bar{b} = (c,d)$

$\bar{c} = (x,y) =$

$= \bar{a} + \bar{b}$

r retta per (a,b) parallela a (c,d)

$$\frac{x-a}{c} = \frac{y-b}{d} \rightarrow x = \frac{y-b}{d}c + a$$

s retta per (c,d) parallela ad (a,b)

$$\frac{x-c}{a} = \frac{y-d}{b} \rightarrow x = \frac{y-d}{b}a + c$$

Intersechiamo risolvendo il sistema in 2 equazioni nelle incognite x, y

$$\frac{y-b}{d}c+a=\frac{y-d}{b}a+c$$

$$(y-b)(cb)+adb=(y-d)ad+cbd$$

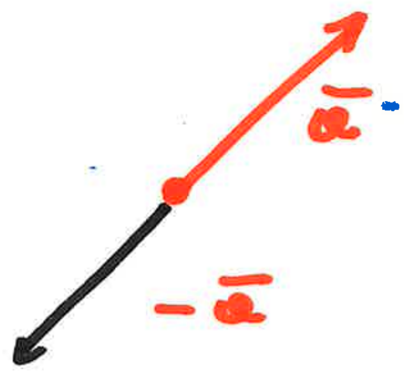
$$y(cb-ad)=-adb+cbd-add+cbb$$
$$=(cb-ad)(b+d)$$

$cb-ad\neq 0$

$y=b+d \qquad x=a+c.$

$$\rightarrow \boxed{(a,b)+(c\ d)=(a+c,\ b+d)}$$

$$-1\cdot(a,b)=-\overline{a}$$



$$(x,y)+(a,b)=(0\ 0)$$

$$\Rightarrow x=-a\,,\ y=-b$$

$$2\cdot(a,b)=(a,b)+(a,b)=(2a,2b)$$

$$\rightarrow \boxed{\alpha\cdot(a,b):=(\alpha a,\alpha b)}$$

__Def__: Sia $(\mathbb{K}, +, \cdot)$ un campo.

Uno spazio vettoriale $V(\mathbb{K})$ sul campo $\mathbb{K}$ è una struttura algebrica $(V, \hat{+})$ tale che.

1) $(V, \hat{+})$ è un gruppo commutativo.

[el. di V = vettori, $\hat{+}$ somma di vettori].

2) $\exists$ una funzione $\hat{\cdot} : \mathbb{K} \times V \longrightarrow V$ tale che

unitarietà a) $1 \hat{\cdot} \bar{v} = \bar{v} \quad \forall \bar{v} \in V$

pseudo distrib. b) $\forall \alpha, \beta \in \mathbb{K}: \ (\alpha + \beta) \hat{\cdot} \bar{v} = (\alpha \hat{\cdot} \bar{v}) \hat{+} (\beta \hat{\cdot} \bar{v})$

c) $\forall \bar{u}, \bar{v} \in V: \ \alpha \hat{\cdot} (\bar{u} \hat{+} \bar{v}) = (\alpha \hat{\cdot} \bar{u}) \hat{+} (\alpha \hat{\cdot} \bar{v})$.

pseudo associativa d) $\forall \alpha, \beta \in \mathbb{K} \ \forall \bar{v} \in V: \ (\alpha \cdot \beta) \hat{\cdot} \bar{v} = \alpha \hat{\cdot} (\beta \hat{\cdot} \bar{v})$

$\mathbb{R}^2 = \{(a,b) : a, b \in \mathbb{R}\}$ $\qquad (a,b) \hat{+} (c,d) = (a+c, b+d)$

$\alpha \hat{\cdot} (a,b) = (\alpha a, \alpha b)$

1) $(\mathbb{R}^2, \hat{+})$ gruppo abeliano. $(0,0) \in \mathbb{R}^2$

1) $(a,b) \hat{+} (0\,0) = (a+0, b+0) = (a,b)$

$(0,0) \hat{+} (a,b) = (0+a, 0+b) = (a,b)$

2) $(a,b) \in \mathbb{R}^2 \Rightarrow (-a,-b) \in \mathbb{R}^2$ e

$(a,b) \hat{+} (-a,-b) = (a-a, b-b) = (0,0)$

$(-a,-b) \hat{+} (a,b) = (0\,0)$.

3) $\forall (a,b), (c,d), (e,f) \in \mathbb{R}^2$

$(a,b) \hat{+} [(c,d) \hat{+} (e,f)] = (a,b) \hat{+} (c+e, d+f)$

$= (a+(c+e), b+(d+f)) = ((a+c)+e, (b+d)+f) =$

$$([a+c),(b+d)]\,\hat{+}\,(e,f) = [(a,b)\,\hat{+}\,(c,d)]\,\hat{+}\,(e,f).$$

4) $(a,b)\,\hat{+}\,(c,d) = (a+c,\ b+d) =$

$$=(c+a,\ d+b) = (c,d)\,\hat{+}\,(a,b).$$

2a) $1 \hat{\cdot} (a,b) = (1\cdot a,\ 1\cdot b) = (a,b)$ ✓

2b) $(\alpha+\beta)\hat{\cdot}(a,b) = ((\alpha+\beta)a,\ (\alpha+\beta)b) =$

$$= (\alpha a+\beta a,\ \alpha b+\beta b) =$$

$$= (\alpha a,\ \alpha b)\,\hat{+}\,(\beta a,\ \beta b) =$$

$$= \alpha\hat{\cdot}(a,b)\,\hat{+}\,\beta\hat{\cdot}(a,b).$$

2c) $\alpha\hat{\cdot}[(a,b)\,\hat{+}\,(c,d)] = \alpha\hat{\cdot}(a+c,\ b+d) =$

$$= (\alpha(a+c),\ \alpha(b+d)) = (\alpha a+\alpha c,\ \alpha b+\alpha d) =$$

$$= (\alpha a, \alpha b) \hat{+} (\alpha c, \alpha d) =$$

$$= \alpha \hat{\cdot} (a,b) \hat{+} \alpha \hat{\cdot} (c,d)$$

d) $$(\alpha\beta) \hat{\cdot} (a,b) = ((\alpha\beta)a, (\alpha\beta)b) =$$

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

$$= \alpha \hat{\cdot} (\beta a, \beta b) = \alpha \hat{\cdot} (\beta \hat{\cdot} (a,b))$$

$\square$

<u>OSS</u> 1 : i conti non dipendono dal fatto che stiamo usando $\mathbb{R}$. Bastano le proprietà di campo.

$\mathbb{K}^2$ con somma e prodotto comp. per componente è uno s. vettoriale su $\mathbb{K}$.

2) La stessa dim. funziona se prendiamo $\mathbb{K}^n$ con $^{n>0}$ op. componente per componente.

$\boxed{(\mathbb{K}^n, +)}$ $\quad (a_1 \dots a_n) + (b_1 \dots b_n) := (a_1 + b_1 \dots a_n + b_n)$

$\cdot : \mathbb{K} \times \mathbb{K}^n \to \mathbb{K}^n \quad \alpha \cdot (a_1 \dots a_n) := (\alpha a_1 \dots \alpha a_n).$

$\underbrace{\alpha \in \mathbb{K}}_{\text{scalare}} \quad \underbrace{(a_1 \dots a_n) \in \mathbb{K}^n}_{\text{vettore}}$

#

x^2+1 diviso x^2+x+1

$\exists\, p(x) \in \mathbb{K}[x]$ e $r(x) \in \mathbb{K}[x]$ con $\deg r(x) < 2$

tali che

$$(x^2+1) = (x^2+x+1)\,p(x) + r(x)$$

$$p(x)=1 \Rightarrow (x^2+1) = (x^2+x+1)\cdot 1 + r(x)$$

$\mathbb{K} = \mathbb{Z}_2 \quad -1 = +1$

$$\underbrace{(x^2+1)+(x^2+x+1)}_{=\,x} = r(x)$$

Esempi di sp. vettoriali.

1) $(\mathbb{K}^n, +)$ s. vettoriale su $\mathbb{K}$.

$\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$, $\mathbb{K} = \mathbb{Z}_2$

$\mathbb{Z}_2^8 = \{(a_1, \dots a_8) : a_i \in \{0,1\}\}$.

$\cancel{\mathbb{K}[x] = \{\sum_{i=0}^{n} x_i \mid x_i \in}$

$$\mathbb{K}[x] = \{a_0 + a_1 x + \dots + a_n x^n + \dots \mid a_i \in \mathbb{K} \ n \in \mathbb{N}\}$$

$$= \{\sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{K}, n \in \mathbb{N}\}.$$

$\mathbb{K}[x]$ è detto anello dei polinomi in x a coeff. sul campo $\mathbb{K}$.

$$p(x) = \sum_i p_i x^i \qquad q(x) = \sum_j q_j x^j$$

$$(p+q)(x) := \sum_i (p_i + q_i) x^i$$

$$\alpha \cdot p(x) := \sum_i (\alpha p_i) x^i$$

$(\mathbb{K}[x], +)$ è uno sp. vettoriale su $\mathbb{K}$.

$\mathbb{K}[x]_{\leq d} := \left\{ \sum_{i=0}^{d} a_i x^i \mid a_i \in \mathbb{K} \right\}$. polinomi di grado al più d.

$$\mathbb{R}[x]_{\leq 2} := \{ a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in \mathbb{R} \}$$

$$(\underline{\underline{a_0}} + a_1x + a_2x^2) + (\underline{\underline{b_0}} + b_1x + b_2x^2) =$$

$$= (\underline{a_0 + b_0}) + (a_1 + b_1)x + (a_2 + b_2)x^2$$

$$\alpha \cdot (\underline{\underline{a_0}} + a_1x + a_2x^2) = (\underline{\underline{\alpha a_0}}) + (\alpha a_1)x + (\alpha a_2)x^2$$

$$\mathbb{R}^3 := \{ (a_0\ a_1\ a_2) \mid a_0\ a_1\ a_2 \in \mathbb{R} \}.$$

$$(\underline{\underline{a_0}}\ a_1\ a_2) + (\underline{\underline{b_0}}\ b_1\ b_2) =$$

$$= (\underline{a_0 + b_0}\ \ a_1 + b_1\ \ a_2 + b_2)$$

$$\alpha (\underline{\underline{a_0}}\ a_1\ a_2) = (\underline{\underline{\alpha a_0}}\ \alpha a_1\ \alpha a_2)$$

Def: Siano $V(\mathbb{K})$ e $W(\mathbb{K})$ due sp. vettoriali sul medesimo campo $\mathbb{K}$.

Si dice omomorfismo di spazi vettoriali (APPLICAZIONE LINEARE $V \to W$) una funzione

$$f: V \longrightarrow W$$

tale che

$$\forall \bar{a}, \bar{b} \in V: \ f(\bar{a}+\bar{b}) = f(\bar{a}) + f(\bar{b})$$

$$\forall \alpha \in \mathbb{K}, \forall \bar{v} \in V: \ f(\alpha \bar{v}) = \alpha f(\bar{v})$$

Un omomorfismo biettivo è detto isomorfismo

$\Updownarrow$

invertibile

$$\mathbb{R}^3 \to \mathbb{R}^2$$
$$(a,b,c) \to (a,b)$$

OMOMORFISMO
MA NON ISOMORFISMO

$$\varphi[(a,b,c)+(d,e,f)] = \varphi[(a+d,b+e,c+f)] =$$

$$= (a+d,\ b+e) =$$

$$= \varphi((a,b,c)) + \varphi((d,e,f)) = (a,b)+(d,e)$$

$$= (a+d, b+e)$$

$$\mathbb{R}^{m,n} := \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} : a_{ij} \in \mathbb{R} \right\}.$$

$$\varphi : \mathbb{R}^{m,n} \longrightarrow \mathbb{R}^{m \cdot n}$$

$$\mathbb{R}^{2,2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}.$$

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = (a, b, c, d)$$

Un isomorfismo è sempre relativo ad un certo tipo di struttura algebrica

$$\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) \neq (a, b\ c\ d) \overset{??}{\cdot\cdot} (e\ f\ g\ h)$$