

$\mathbb{R}, \mathbb{C}, \mathbb{Q}$: campi infiniti

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

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

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

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

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}$ insieme dei numeri interi $(\mathbb{Z}, +, \cdot)$ è un anello

p numero primo in $\mathbb{Z}$

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

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

possibili resti della divisione per p

$a \% p :=$ resto di a diviso p

cioè l'unico numero r

≥ 0 e $< p$ tale che

$$a = kp + r$$

$$\forall a, b \in \mathbb{Z}_p : (a + b) := (a + b) \% p$$

$$(a \cdot b) := (a b) \% p$$

Teorema $(\mathbb{Z}_p, +, \cdot)$ è un campo se e solo se p è un numero primo.

$$p=2 \Rightarrow \mathbb{Z}_2 = \mathbb{F}_2$$

$$p=3 \Rightarrow \mathbb{Z}_3 = \mathbb{F}_3$$

$$(\mathbb{Z}_4, +, \cdot) \quad \text{In } \mathbb{Z}_4 \quad 2 \cdot 2 = 4 \equiv 0$$

$\mathbb{Z}_4$ NON È UN CAMPO!

Relazioni in un insieme A

Una relazione R in A è un sottoinsieme $R \subseteq A \times A$

$$\bullet (a, b) \in R \equiv a R b.$$

- 1) $\rightarrow R$ è riflessiva se $\forall a \in A : (a, a) \in R$
- 2) $\rightarrow R$ è simmetrica se $\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R$
- 3) $\rightarrow R$ è transitiva se $\forall a, b, c \in A : (a, b) \in R \& (b, c) \in R \Rightarrow (a, c) \in R$
- 4) $\rightarrow R$ è antisimmetrica se $\forall a, b \in A : (a, b) \in R \& (b, a) \in R \Rightarrow a = b$

Se R soddisfa 1, 2, 3 $\Rightarrow R$ è detta di equivalenza

Se R soddisfa 1, 3, 4 $\Rightarrow R$ è detta di ordine (largo)

Le relazioni di equivalenza servono ad
 avere le proprietà di un ente

oss: Sia A un insieme e R una relazione di
 equivalenza su $A \Rightarrow$ si dice $\forall a \in A$
 classe di equivalenza di A

$$[a]_R = \{ b \in A \mid (a, b) \in R \}$$

Teorema: le classi di equivalenza rispetto R
 formano una partizione di A

cioè $\forall a \in A \exists !$ classe di equivalenza
 x tale che $a \in x$

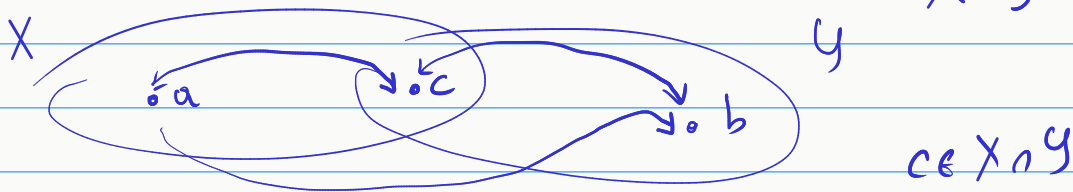
equivalentemente: l'unione di tutte le classi di equivalenza di R è tutto A e due classi distinte sono disgiunte.

→ L'insieme di tutte le classi di equivalenza di R su A è detto insieme quoziente A/R ("A su R")

DIM: Iniziamo tutto per la proprietà riflessiva
 $\forall a \in A: a \in [a]_R$

quindi $\bigcup_{x \in A/R} x = A$

Mostriamo che se $X, Y \in A/R$ e $X \cap Y \neq \emptyset \Rightarrow X = Y$



$a \in X, b \in Y$

$(a, c) \in R$
 $(c, b) \in R$

per la p. transitiva

→ $(a, b) \in R \Rightarrow$

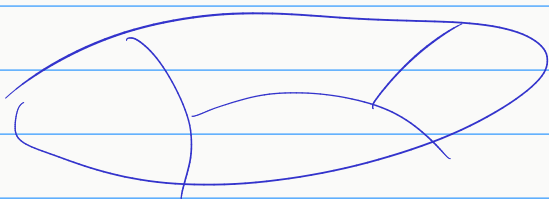
Questo vale $\forall b \in Y \Rightarrow Y \subseteq X$

$\forall a \in X \Rightarrow X \subseteq Y$

$b \in X$
 $a \in Y$

$\Rightarrow X = Y$

□

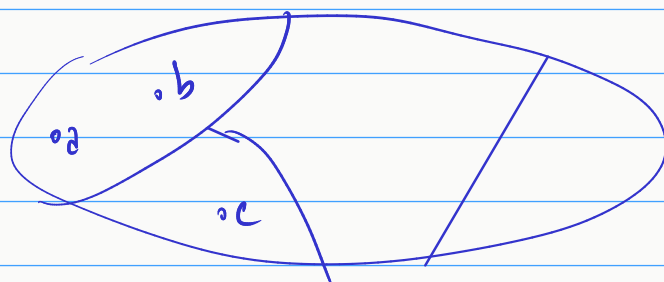


OGNI RELAZIONE DI EQUIVALENZA DETERMINA UNA PARTIZIONE DI A

VICEVERSA: DATA UNA PARTIZIONE DI A ABBIAMO UNA

RELAZIONE DI EQUIVALENZA

QUALE? LA RELAZIONE "ESSERE NELLA STESSA CLASSE"



$(\mathbb{Z}, +, \cdot)$ relazione "essere congruenti modulo n "

$$a \equiv_n b \Leftrightarrow n \mid (a-b)$$

$\uparrow$
divide

$\equiv_n$ è di equivalenza

Dim: $(a-a)=0$ in particolare $n \mid (a-a) \Rightarrow a \equiv_n a$

$$(a \equiv_n b) \Rightarrow n \mid (a-b) \Rightarrow n \mid (b-a) \Rightarrow b \equiv_n a$$

$$(a \equiv_n b) \& (b \equiv_n c) \Rightarrow n \mid a-b \& n \mid b-c \Rightarrow$$

$$\exists k, k' \in \mathbb{Z}: (a-b)=kn, (b-c)=k'n$$

$$\Rightarrow (a-c) = (a-b) + (b-c) = kn + k'n = (k+k')n \Rightarrow n \mid (a-c)$$

□

OSSERVAZIONE: LE CLASSI DI EQUIVALENZA

di $\equiv_n$ SONO CORRISPONDENTI

AI RESTI DELLA DIVISIONE PER n

$$(a-b)=kn \Leftrightarrow a \% n = b \% n$$

OGNI CLASSE DI EQUIVALENZA CORRISPONDE AD UN

RESTO $\rightarrow$ "PASSARE AL QUOZIENTE" È LA STESSA COSA DI
 DIRE "PER OGNI $n \in \mathbb{Z}$ " considero SOLO il suo resto
 diviso per n .

$(K, +, \cdot)$ campo

ambiente per studiare le equazioni
 lineari (di primo grado)

$$(*) \quad \boxed{ax + b = 0}$$

si dice $\bar{x}$ soluzione di $(*)$ se $a\bar{x} + b = 0$
 $\in K$

$(*)$ vediamo quando si può risolvere

$$a = 0 \begin{cases} 0x + b = 0 \text{ con } b = 0 \Rightarrow 0x = 0 \quad \forall x \in K \text{ è soluzione} \\ 0x + b = 0 \text{ con } b \neq 0 \quad 0x = -b \neq 0 \quad \nexists \text{ soluzione.} \end{cases}$$

$$a \neq 0 \rightarrow ax = (-b) \text{ perché } a \neq 0 \exists a^{-1} \in K$$

$$\Rightarrow x = a^{-1}(-b) \text{ è}$$

soluzione ed è l'unica
 soluzione possibile.

pensate a

$$\begin{array}{c} 2x = 4 \\ 2x = 5 \end{array} \text{ in } \mathbb{Z}$$

oss. $2x = 5$ non è
 risolvibile in $\mathbb{Z}$
 ma lo è in $\mathbb{Q}$.

$$\boxed{ax + b = 0}$$

$$\boxed{ax = (-b)}$$

$$ax = b \quad x = a^{-1}b$$

CAPITOLO 1 DEL LIBRO "ALGEBRA LINEARE E GEOM. ANALITICA".

CAPITOLO 2 NOTIZIE E TEORIA DEGLI SPAZI VETTORIALI

Spazio vettoriale V su di un campo K .

Sia K un campo e $(V, \tilde{+})$ un gruppo abeliano
 $(K, +, \cdot)$

Si dice che V è spazio vettoriale sul campo K
(e scriverò $V(K)$) se $\exists$ una funzione

$\tilde{\cdot} : K \times V \rightarrow V$ tale che.

$$1) 1 \tilde{\cdot} \tilde{v} = \tilde{v} \quad \forall \tilde{v} \in V$$

$$2) \forall \alpha, \beta \in K, \forall \tilde{v} \in V : (\alpha \cdot \beta) \tilde{\cdot} \tilde{v} = \alpha \tilde{\cdot} (\beta \tilde{\cdot} \tilde{v})$$

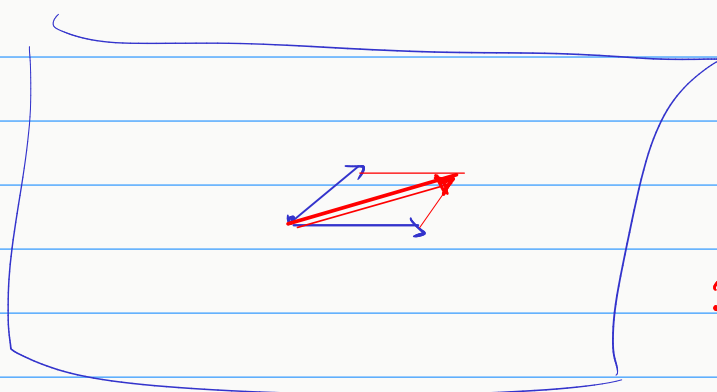
$$3) \forall \alpha, \beta \in K, \forall \tilde{v} \in V : (\alpha + \beta) \tilde{\cdot} \tilde{v} = \alpha \tilde{\cdot} \tilde{v} \tilde{+} \beta \tilde{\cdot} \tilde{v}$$

$$4) \forall \alpha \in K, \forall \tilde{v}, \tilde{w} \in V : \alpha \tilde{\cdot} (\tilde{v} \tilde{+} \tilde{w}) = \alpha \tilde{\cdot} \tilde{v} \tilde{+} \alpha \tilde{\cdot} \tilde{w}$$

$\tilde{\cdot}$ è detto
prodotto per
scalare o
prodotto esterno

GLI ELEMENTI DI K si dicono scalari

GLI ELEMENTI DI $V(K)$ si dicono vettori



Procedi per
l'origine 5
vettori

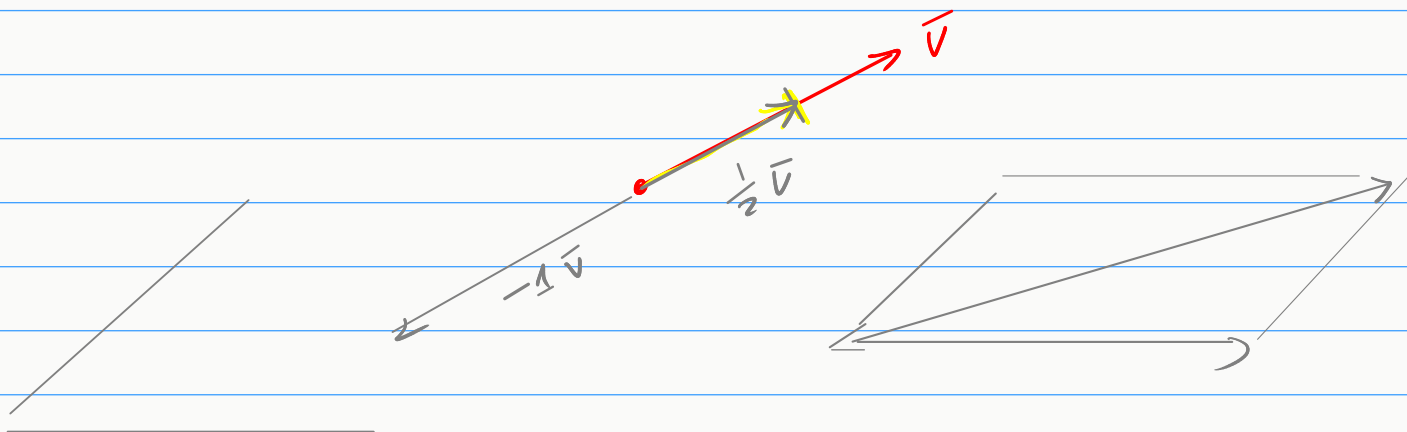
$\tilde{+}$ = legge del
parallelogramma

$(V, \tilde{+})$

Il prodotto di un $\alpha \in K$ con $\alpha > 0$ per un vettore $\nearrow$

è un vettore con la stessa direzione e verso del vettore di partenza e a volte la sua lunghezza

Se $\alpha < 0$ è un vettore con la stessa direzione e verso opposto del vettore di partenza e $-\alpha$ la sua lunghezza



$$|K \text{ campo} \quad V := |K^2 = \{(a, b) \mid a, b \in |K\}.$$

$$(a, b) \tilde{+} (c, d) := (a+c, b+d) \quad (|K^2, \tilde{+}) \text{ è un gruppo abeliano}$$

$$\tilde{\cdot}: |K \times |K^2 \rightarrow |K^2$$

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

somma e prodotto
componente per
componente

$|K^2$ con le operazioni indicate è uno spazio vettoriale.

1) $(|K^2, \tilde{+})$ è gruppo abeliano, infatti

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

$$(a, b) \tilde{+} (0, 0) = (a, b) \quad \forall (a, b) \in \mathbb{K}^2$$

$$(a, b) \tilde{+} (-a, -b) = (a-a, b-b) = (0, 0) \quad \forall (a, b) \in \mathbb{K}^2$$

$$\begin{aligned} ((a, b) \tilde{+} (c, d)) \tilde{+} (e, f) &= (a+c, b+d) \tilde{+} (e, f) = \\ &= ((a+c)+e, (b+d)+f) = (a+(c+e), b+(d+f)) = \\ &= (a, b) \tilde{+} ((c, d) \tilde{+} (e, f)) \end{aligned}$$

$(\mathbb{K}^2, +)$ è un gruppo abeliano

$$1) \quad 1 \circ (a, b) = (1 \cdot a, 1 \cdot b) = (a, b) \quad \checkmark$$

$$\begin{aligned} 2) \quad \alpha, \beta \in \mathbb{K} \quad (\alpha \cdot \beta) \circ (a, b) &= ((\alpha \beta)a, (\alpha \beta)b) = (\alpha(\beta a), \alpha(\beta b)) = \\ &= \alpha \circ (\beta a, \beta b) = \alpha \circ (\beta \circ (a, b)) \quad \checkmark \end{aligned}$$

$$\begin{aligned} 3) \quad \alpha, \beta \in \mathbb{K} \quad (\alpha + \beta) \circ (a, b) &= ((\alpha + \beta)a, (\alpha + \beta)b) = \\ &= (\alpha a + \beta a, \alpha b + \beta b) = \\ &= (\alpha a, \alpha b) \tilde{+} (\beta a, \beta b) = \\ &= \alpha \circ (a, b) \tilde{+} \beta \circ (a, b) \quad \checkmark \end{aligned}$$

$$4) \quad \forall \alpha \in \mathbb{K}, (a, b), (c, d) \in \mathbb{K}^2$$

$$\begin{aligned} \alpha \circ ((a, b) \tilde{+} (c, d)) &= \\ &= \alpha \circ (a+c, b+d) = (\alpha(a+c), \alpha(b+d)) = \\ &= \dots \alpha \circ (a, b) \tilde{+} \alpha \circ (c, d). \quad \checkmark \end{aligned}$$

$$\mathbb{R} \rightarrow \mathbb{R}^2$$

