Lezione 6 ottobre 22

giovedì 6 ottobre 2022 10:02

Visto: campo (5 assiomi)

Def.: Sia V insieme non vuoto, e sia $\mathbb{K}$ un campo. Allora V si dice SPAZIO VETTORIALE su $\mathbb{K}$, opp. $\mathbb{K}$-spazio vettoriale se su V sono definite 2 operazioni $+$ e $\cdot$ per un elemento di $\mathbb{K}$, che verificano gli assiomi (V1), ..., (V8) con $\mathbb{K}$ sostituito a $\mathbb{R}$.

Esempi:

① (visto: $\mathbb{R}$ è sp. vett. reale)

$\mathbb{K}$ esso stesso è uno SV su $\mathbb{K}$

(in $\mathbb{K}$ ci sono $+$ e $\cdot$)

② $(\mathbb{R} \times \mathbb{R} = \mathbb{R}^2)$

$\mathbb{K} \times \mathbb{K} = \mathbb{K}^2 = \{$coppie ordinate di elementi di $\mathbb{K}\}$

$\downarrow$ prodotto cartesiano di insiemi

Def.: $\begin{pmatrix}a\\b\end{pmatrix}, \begin{pmatrix}c\\d\end{pmatrix} \in \mathbb{K}^2$

$$\underset{\in\mathbb{K}}{\begin{pmatrix}\overset{\in\mathbb{K}}{a}\\ b\end{pmatrix}} \underset{\text{in } \mathbb{K}^2}{\underset{\downarrow}{+}} \begin{pmatrix}\overset{\in\mathbb{K}}{c}\\ \underset{\in\mathbb{K}}{d}\end{pmatrix} := \begin{pmatrix}\overset{\text{in } \mathbb{K}}{a+c}\\ \underset{\text{in } \mathbb{K}}{b+d}\end{pmatrix}$$

Sia ora $k\in\mathbb{K}$;

$$\underset{\in\mathbb{K}}{\underset{\downarrow}{k\cdot}} \underbrace{\begin{pmatrix}a\\b\end{pmatrix}}_{\in\mathbb{K}^2} := \begin{pmatrix}k\cdot a\\ k\cdot b\end{pmatrix} \begin{matrix}\cdot \text{ in } \mathbb{K}\\ \cdot \text{ in } \mathbb{K}\end{matrix}$$

Si verifica con $+$ e $\cdot$ l'insieme $\mathbb{K}^2$ verifica (V1), ..., (V8)

③ Sia $n\in\mathbb{N}$, $n>0$

e cons. $\mathbb{K}^n := \underbrace{\mathbb{K}\times\mathbb{K}\times\cdots\times\mathbb{K}}_{n \text{ volte}}$

$$= \left\{ \begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix} : a_i\in\mathbb{K} \right\}$$

$=$ {stringhe ordinate di n elementi di $\mathbb{K}$}

Def. $+$ e $\cdot$ come prima:

$$\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix} + \begin{pmatrix}b_1\\\vdots\\b_n\end{pmatrix} := \begin{pmatrix}a_1+b_1\\\vdots\\a_n+b_n\end{pmatrix}$$

$k \in \mathbb{K}$, $\quad k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} k \cdot a_1 \\ \vdots \\ k\, a_n \end{pmatrix}$

verifica (V1), ..., (V8)

Esempi di campi :

② CAMPI CON 2 ELEMENTI :

Prop. Se K è un campo con almeno 2 elementi, allora neutro 0 per + e neutro 1 per · sono elementi DIVERSI.

Dim.: Per assurdo
Supp. che i 2 neutri (per + e ·) siano uguali: N

$$\mathbb{K} \supseteq \{N, *\},$$

$$\boxed{* \neq N}$$

OSS.: In ogni campo, se 0 è il neutro per +, vale

$$0 \cdot a = 0 \qquad \forall\, a \in \mathbb{K}$$

Infatti: $0\cdot a = (0+0)\cdot a \overset{\substack{K5\\ \uparrow}}{=} 0\cdot a + 0\cdot a$

somma $-0\cdot a$ a entrambi i membri

$$\underbrace{-0\cdot a + 0\cdot a}_{=0} = \underbrace{-0\cdot a + 0\cdot a}_{=0} + 0\cdot a$$

$$0 = 0\cdot a$$

* * *

Torniamo alla dimostrazione:

$N\cdot * = *$ perché N neutro per $\cdot$

$N\cdot * = N$ perché N neutro per $+$

$\Rightarrow * = N$ assurdo

(ho supp. $* \neq N$).

* * *

② Campo con 2 elementi:

$K = \{0, 1\}$ con 0 neutro per $+$

con 1 neutro per $\cdot$

oss.: In ogni campo, i neutri sono unici. (non lo dimostriamo)

In $\{0,1\}$ voglio def. $+$ e $\cdot$:

$+$	0	1
0	0	1
1	1	0

$1+1=$

- 1 no, perché 1 sarebbe neutro per $+$
- 0 sì

$\Rightarrow$ l'opposto di 1 è 1

$-1 = 1$

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

$1\cdot 1 =$

- 0 NO perché 1 è neutro per $\cdot$
- 1

$1\cdot 1 = 1$

OSS: $0\cdot a = 0 \quad \forall a \in \mathbb{K}$

Esercizio: verificare che (K1), ..., (K5) sono verificati

OSS.: Su un insieme con 2 elementi, c'è un UNICO MODO di

def. 2 operaz. + e · in modo da avere un campo: $\mathbb{Z}_2 = \mathbb{K}$

* * *

Esempi di SV su $\mathbb{Z}_2$:

$$\mathbb{K}^2 = \mathbb{Z}_2 \times \mathbb{Z}_2 = (\mathbb{Z}_2)^2$$

$$= \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$\mathbb{K}^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$= \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ldots \right.$$

$$\left. \ldots \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

* * *

③ Campo con 3 elementi:

$$\mathbb{K} = \{0, 1, 2\}$$

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

2 + 1 =

- 1 NO, perché sennò 2 neutro per +
- 2 NO, perché sennò 1 neutro per +
- 0

= 1 + 2

⇒ 2 è l'opposto di 1 e 1 è l'opposto di 2

$-1 = 2$, $-2 = 1$

1 + 1 =

- 1 , NO perché sennò 1 neutro
- 0 , NO , perché altrimenti 1 sarebbe opposto di se stesso, e in un campo l'opp. è UNICO
- 2 ok

2 + 2 =

- 0 NO, perché altrimenti 2 opposto di 2

2 No perché 2 neutro per +

1 sì

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

$2 \cdot 2 = 1$

perché 2 ($\neq 0$)
deve avere inverso

Anche in questo caso, astrattamente c'è 1 unico modo di definire + e · su insieme di 3 elementi: $\mathbb{Z}_3$

Oss. Le operazioni in $\mathbb{Z}_2$ e $\mathbb{Z}_3$ possono essere ottenute nel modo seguente: $a, b \in \mathbb{Z}_2$ (opp. $\in \mathbb{Z}_3$) e li penso come elementi di $\mathbb{Z}$

li sommiamo o moltiplichiamo in $\mathbb{Z}$, facciamo la divisione per 2 (opp. per 3) e ne cons. il resto

Def. Sia $n \in \mathbb{N}$, e poniamo

$\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$

def. $+$ e $\cdot$ in questo modo:

$a, b \in \mathbb{Z}_n$, li cons. $a, b \in \mathbb{Z}$

$a +_{\mathbb{Z}} b$ in $\mathbb{Z}$, $a +_{\mathbb{Z}_n} b :=$ resto nella divisione per n di $a +_{\mathbb{Z}} b$

$a \cdot_{\mathbb{Z}_n} b :=$ resto nella divisione per n di $a \cdot_{\mathbb{Z}} b$

Es.: $\mathbb{Z}_4$

+	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

2 non ha inverso $\Longrightarrow$ $\mathbb{Z}_4$ non è un campo

Teorema: $\mathbb{Z}_n$ è un campo $\Longleftrightarrow$ n è un numero primo.

oss.: in un campo, se $a \neq 0$ e $b \neq 0$ $\Longrightarrow$ $a \cdot b \neq 0$

infatti: se per assurdo $a \cdot b = 0$

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

$$\underbrace{(a^{-1} \cdot a)}_{=1} \cdot b = 0$$

$$b = 0$$