Lezione 5 ottobre 2023

giovedì 5 ottobre 2023 11:08

Teorema: $(\mathbb{Z}_n, +, \cdot)$ è un campo $\Leftrightarrow$ n è un numero primo

(n primo se è divisibile solo per 1 e per n)
$n \geq 2$
1 non è un numero primo.

Dim.: Dimostriamo prima $\mathbb{Z}_n$ campo $\Rightarrow$ n primo

Facciamo per contrapposizione, cioè dimostro

n non primo $\Rightarrow$ $\mathbb{Z}_n$ non è campo.

n non primo $\Rightarrow$ $\exists\, a, b \in \mathbb{N}$ tali che $n = a \cdot b$
$\boxed{1 < a < n}$
$1 < b < n$

$\Rightarrow$ $\bar{n} = \overline{a \cdot b}$ in $\mathbb{Z}_n$
$\|$ $\quad$ $\|$ per definiz. di $\cdot$ in $\mathbb{Z}_n$
$\bar{0} = \bar{a} \cdot \bar{b}$

oss. infine che $\bar{a} \neq \bar{0}$
infatti: $a = 0 \cdot n + a$ perché $1 < a \leq n-1$

anche $\bar{b} \neq \bar{0}$, perché $b = 0 \cdot n + b$
$1 < b \leq n-1$

$\Rightarrow$ in $\mathbb{Z}_n$ ci sono 2 elementi non nulli il cui prodotto è nullo $\Rightarrow$ $\mathbb{Z}_n$ non è un campo per la Proposizione di ieri, punto ②.

Es: $\mathbb{Z}_6$ non è campo: $\bar{2} \cdot \bar{3} = \bar{0}$

Dimostriamo ora n numero primo $\Rightarrow$ $\mathbb{Z}_n$ è campo

Abbiamo bisogno di:

LEMMA 1 : p primo, $a, b \in \mathbb{Z}$

Se $p \underset{\text{divide}}{|} (a \cdot b)$ p divide $a \cdot b$

$\Longrightarrow p | a$ oppure $p | b$

Dim. È una conseguenza del Teorema Fondamentale dell'Aritmetica (Gauss 1798)

Ogni numero intero si può scrivere in modo unico, a meno dell'ordine dei fattori, come prodotto di numeri primi

$a = p_1 \cdots p_k$ p_i numeri primi, con eventuali ripetizioni

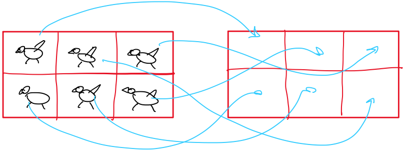
$b = q_1 \cdots q_r$ q_j numeri primi

$p | (a \cdot b) \Longrightarrow a \cdot b = p \cdot c$, $c = s_1 \cdots s_h$

$$p \cdot c = \boxed{p \cdot s_1 \cdots s_h = p_1 \cdots p_k \cdot q_1 \cdots q_r}$$

LEMMA 2 (PRINCIPIO DELLA PICCIONAIA)

Se X è finito, e $f : X \to X$ funzione iniettiva $\Longrightarrow f$ è anche suriettiva.



Dim. $f : X \to X$ iniettiva

allora X e $f(X) = \{ y \in X : \exists x \in X, f(x) = y \} \subseteq X$

sono in biiezione

$$\tilde{f} : X \longrightarrow f(X) \subseteq X$$
$$x \longrightarrow f(x)$$

$$\Rightarrow \boxed{\underbrace{\# X} = \# f(X)}$$

cardinalità di X
cioè il numero di elementi

$$f(X) \subseteq X \quad \Rightarrow \quad f(X) = X$$

$\Rightarrow$ f è suriettiva.

Torniamo alla Dim. di n numero primo $\Rightarrow \mathbb{Z}_n$ campo.

Osservo: $\mathbb{Z}_n$ ha quasi tutte le proprietà richieste, l'unica non sempre garantita è $\exists$ dell'inverso per elementi $\neq \bar{0}$.

Sia $\bar{a} \in \mathbb{Z}_n$, $\quad \bar{a} \neq \bar{0}$

e cons. la funzione $\quad f_{\bar{a}} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$$f_{\bar{a}}(\bar{x}) = \bar{a} \cdot \bar{x}$$

è la MOLTIPLICAZIONE PER $\bar{a}$.

Affermo che $\forall\, \bar{a} \neq \bar{0}$, la $f_{\bar{a}}$ è INIETTIVA.

Supp. $\quad f_{\bar{a}}(\bar{x}) = f_{\bar{a}}(\bar{y})$

$$\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$$

$$\overline{a\cdot x} = \overline{a\cdot y} \quad , \qquad \overline{ax - ay} = \overline{0}$$

$$\overline{a\cdot(x-y)} = \overline{0}$$

$$a\cdot(x-y) = kn \quad , \quad \text{per } k\in\mathbb{Z}$$

$$\downarrow$$

n primo , $\quad n \mid a\cdot(x-y)$

per Lemma 1: $\underbrace{n\mid a}_{\text{MAI}}$ opp. $n\mid(x-y)$

$\bar{a} \neq \bar{0} \Rightarrow$ a non è un multiplo di n

$\Rightarrow n \mid (x-y)$, cioè $x - y = h\cdot n$

$$x = y + hn$$

$$x \equiv_n y$$

$\Rightarrow \quad \bar{x} = \bar{y}$

$\Rightarrow f_{\bar{a}}$ è iniettiva

$\xrightarrow[\text{Piccionaia}]{} \quad f_{\bar{a}}$ è suriettiva

$\Rightarrow$ in particolare per $\bar{1}\in\mathbb{Z}_n$, $\exists\, \bar{b}\in\mathbb{Z}_n$

tale che $\quad f_{\bar{a}}(\bar{b}) = \bar{1}$

$\quad\quad \bar{a}\cdot\bar{b} = \bar{1} \quad (= \bar{b}\cdot\bar{a}$ perché $\cdot$ è commutativo$)$

* * *

SPAZI VETTORIALI

Introduzione: Geometria Euclidea

Fondata da Euclide ~ 300 a.C.

Teor. assiomatica : • elementi primitivi
punto, retta, piano
• assiomi : 5

David Hilbert : 5 assiomi non sufficienti

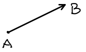
+ 20 assiomi

fino circa 1850
Poi è nata la ALGEBRA LINEARE

Per definire SPAZI VETTORIALI useremo come modello la teoria dei VETTORI LIBERI nel piano e nello spazio.

Def. Cons. un piano reale "fisico"
un VETTORE APPLICATO è un SEGMENTO ORIENTATO, determinato da:

- un punto iniziale A
- una direzione (la retta su cui giace)
- il suo modulo (lunghezza del segmento)
- il suo verso

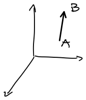


Un vett. applicato è assegnato dalla coppia $\vec{AB}$, B punto finale

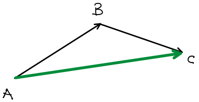
Tra i vettori appl. ci sono $\vec{AA}$, $\vec{BB}$

VETTORI NULLI

Analogamente: cons. vettori nello spazio "fisico"



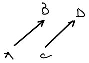
Operazioni:



$\vec{AB} + \vec{BC} := \vec{AC}$

Sia $c \in \mathbb{R}$, $c \cdot \vec{AB} = \begin{cases} & c > 0 \\ & c = 0 \\ & c < 0 \end{cases}$

Def.: Dati 2 vettori applicati $\vec{AB}$ e $\vec{CD}$, si dicono EQUIPOLLENTI se hanno stessa direzione stesso verso e stesso modulo (in altre, si posso sovrapporre spostandoli in modo parallelo)



PROP. La relaz. di equipollenza è rel. di equivalenza.

Def.: Un VETTORE LIBERO (o GEOMETRICO) del piano o dello spazio è UNA CLASSE DI EQUIPOLLENZA.

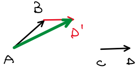
Def: Insieme dei vettori liberi piani $\mathcal{V}^2$

dello spazio $\mathcal{V}^3$.

Def.: Introduco $+$ e $\cdot$ per un numero:

$$+ : \mathcal{V}^2 \times \mathcal{V}^2 \longrightarrow \mathcal{V}^2$$

$$[\vec{AB}] + \underbrace{[\vec{CD}]} = [\vec{AB}] + \underbrace{[\vec{BD'}]} =: [\vec{AD'}]$$



OSS.: $+$ è BEN DEFINITA.