Lezione 29 settembre 2023

venerdì 29 settembre 2023 11:18

beorchia@units.it

Visto: relaz. di equivalenza $\sim$

classe di equiv. $[x]$

insieme quoziente $X/\sim$

Def: Sia $X \neq \emptyset$ insieme. Una PARTIZIONE di X è un sottoinsieme $\mathcal{T} \subseteq \mathcal{P}(X)$ tale che:

(P1) nessun elemento di $\mathcal{T}$ è $\emptyset$

(P2) l'unione dei sottoinsiemi che corrispondo a tutti gli elementi di $\mathcal{T}$ è uguale a X

$\bigcup_{T \in \mathcal{T}} T = X$; più precisamente: $\forall\, t \in \mathcal{T}$, sia $T_t \subseteq X$ il corrispondente sottoinsieme

(unione dei sottoinsiemi T, al variare di T in $\mathcal{T}$)

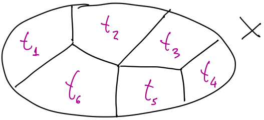
(P2) $\bigcup_{t \in \mathcal{T}} T_t = X$

(notazione simile: $\sum_{i=1}^{100} a_i$, $\sum_{n \in \mathbb{N}} a_n$

$\prod_{i=1}^{n} b_i$, $\prod_{n \in \mathbb{N}} b_n$, $\bigcup_{i=1}^{k} A_i$, $\bigcup_{A \in \mathcal{A}} A$,

$\bigcap_{i=1}^{h} B_i$, $\bigcap_{A \in \mathcal{A}} A$)

(P3) se $S, T \in \mathcal{T}$ e $S \neq T \Rightarrow S \cap T = \emptyset$



$\mathcal{E} = \{t_1, t_2, t_3, t_4, t_5, t_6\}$

PROPOSIZIONE: X insieme, $\sim$ relazione di equivalenza. Allora $X/_\sim$ è una partizione di X.

Dim.: **P1** sia $[x] \in X/_\sim$

per **RE1** riflessività : $x \sim x$

$\Rightarrow x \in [x] \Rightarrow [x] \neq \emptyset$

P2 $\bigcup_{[x]\in X/_\sim} [x] \overset{?}{=} X$

cioè: è vero che ogni elemento di X appartiene ad almeno una classe di equiv. ?

Sì : sia $y \in X$ qualunque

$y \in [y]$

P3 è vero che se $[x] \neq [y]$ allora

$[x] \cap [y] = \emptyset$?

Facciamo dim. per contrapposizione, e

precisamente che se

$$\underbrace{[x]\cap[y]\neq\emptyset}_{\text{ipotesi}} \Rightarrow \underbrace{[x]=[y]}_{\text{tesi}}$$

sia $z\in[x]\cap[y]$

$$\left.\begin{array}{l} z\in[x] \Longleftrightarrow x\sim z \\ z\in[y] \Longleftrightarrow z\sim y \end{array}\right\} \xRightarrow[\text{transitività}]{\boxed{\text{RE3}}} x\sim y$$

adesso dimostro che $[y]\subseteq[x]$ e

che $[x]\subseteq[y]$

$$\underbrace{\forall u\in[y],\quad \left.\begin{array}{l} y\sim u \\ \text{ma } x\sim y \end{array}\right\} \Rightarrow x\sim u \Rightarrow u\in[x]}$$

$$\Rightarrow [y]\subseteq[x]$$

L'altra inclusione:

$$\underbrace{\forall v\in[x] \Rightarrow \left.\begin{array}{l} x\sim v \\ y\sim x \end{array}\right\} \Rightarrow y\sim v \Rightarrow v\in[y]}$$

$$\Rightarrow [x]\subseteq[y]$$

Esempio fondamentale:

CONGRUENZA MODULO n

Sia $n \in \mathbb{N}$, $n \geq 2$

sia $X = \mathbb{Z}$

Def.: $x, y \in \mathbb{Z}$ sono congrui modulo n

$x \equiv_n y$, o anche $x \equiv y \mod n$

se $\exists\, k \in \mathbb{Z}$ tale che $x - y = kn$

Es. $n = 3$, $x = 10$

$10 \equiv_3 4$, $10 \equiv_3 7$, $10 \equiv_3 1$

$10 - 4 = 2 \cdot 3$ $\quad$ $10 - 7 = 1 \cdot 3$ $\quad$ $10 - 1 = 3 \cdot 3$

$10 \equiv_3 -2$

$10 - (-2) = 12 = 4 \cdot 3$

$x = 5$; $\quad 5 \equiv_3 2$ $\qquad 5 \equiv_3 -10$

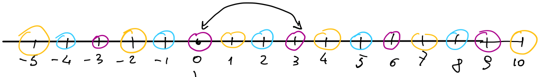
$5 - 2 = 1 \cdot 3$ $\qquad 5 - (-10) = 15 = 5 \cdot 3$

$5 \equiv_3 -1$

$5 - (-1) = 6 = 2 \cdot 3$

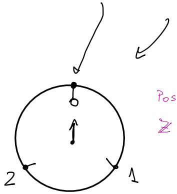
$x = 3$, $\quad 3 \equiv_3 0$, $\quad 3 \equiv_3 -9$, $\quad 3 \equiv_3 6$

$3 - 6 = -3 = (-1) \cdot 3$



$2 = 0\cdot 3 + 2$

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



Possiamo pensare di "arrotolare" l'insieme $\mathbb{Z}$ attorno a un orologio con sole 3 ore.

PROP. La relazione $\equiv_n$ è una relazione di equivalenza.

Dim. $\boxed{RE1}$ $x \in \mathbb{Z}$, $x - x = 0 = 0\cdot n$

$\Rightarrow x \equiv_n x$

$\boxed{RE2}$ Supp. $x \equiv_n y$, quindi $x - y = k n$

calcolo $y - x = \underbrace{-k}_{\in \mathbb{Z}} \cdot n \Rightarrow y \equiv_n x$

$\boxed{RE3}$ Supp. $x \equiv_n y$, $y \equiv_n z$

$\Downarrow$ $\Downarrow$

$x - y = kn$ $y - z = h\cdot n$

$x - z = x - y + y - z = kn + hn = (k+h)\cdot n$

$\Rightarrow x \equiv_n z$

PROP.: $x \equiv_n y \iff$ x e y hanno lo stesso resto nella divisione per n.

PARENTESI: $\mathbb{Z}$ è un DOMINIO EUCLIDEO, cioè

in $\mathbb{Z}$ è definita la divisione euclidea,

cioè: $\forall n \in \mathbb{N}, n \geq 1, \forall x \in \mathbb{Z}$, $\exists! \, q \in \mathbb{Z}$ e $\exists! \, r$: $\boxed{0 \leq r \leq n-1}$

tale che $x = q \cdot n + r$

es: $5 = 1 \cdot 3 + 2$, $r = 2$

$n = 3$

$\cancel{5 = 0 \cdot 3 + 5}$ $0 \leq r \leq 2$

$-7 = -3 \cdot 3 + 2$

Dim. della Proposizione:

$\Rightarrow$: Supponiamo $x \equiv_n y \Rightarrow x - y = k \cdot n$, $x = y + kn$

$\underbrace{y = q \cdot n + r}$ $= q \cdot n + r + kn$

$0 \leq r \leq n-1$ $= (q+k) \cdot n + r$

$0 \leq r \leq n-1$

$\Rightarrow$ i due resti sono uguali

$\Leftarrow$: Supponiamo $x = qn + r$ $y = q'n + r$

$=$

$$\Rightarrow \; x - y = qn + r - q'n - r = \underbrace{(q - q')}_{=k} n$$

$$\Rightarrow \quad x \equiv_n y$$

COROLLARIO : $$\underbrace{\mathbb{Z}/_{\equiv_n}}_{=:\,\mathbb{Z}_n} = \{[0], [1], \dots, [n-1]\}$$

$$\overset{\|}{=} \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

Infatti: i numeri interi $0, 1, \dots, n-1 \in \mathbb{Z}$ rappresentano classi diverse in $\mathbb{Z}_n$, perché hanno resti diversi nella divisione per n:

$0 = 0 \cdot n + 0$

$1 = 0 \cdot n + 1$

$\vdots$

$n-1 = 0 \cdot n + (n-1)$

Se ora fisso un qualunque $x \in \mathbb{Z}$, si avrà $x = q \cdot n + r$, con $0 \le r \le n-1$

$\Rightarrow \quad x - r = q \cdot n \quad \Rightarrow \quad x \sim r \quad \Rightarrow \quad [x] = [r]$

$\Rightarrow \quad [x] \in \{[0], [1], \dots, [n-1]\}$

FATTO IMPORTANTE : in $\mathbb{Z}_n$ possiamo introdurre $+$ e $\cdot$ ereditate da $\mathbb{Z}$:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$\bar{x} + \bar{y} := \overline{x+y}$$

$$\left([x] + [y] := [x+y] \right)$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$\bar{x} \cdot \bar{y} := \overline{x \cdot y}$$

$$\left([x] \cdot [y] := [x \cdot y] \right)$$