CONTE - PICCO BOTTA - ROMAGNOLI

__Def:__ X, Y insiemi

Una CORRISPONDENZA F di dominio X e codominio Y è un sottoinsieme di $X \times Y$.

$\{(x,y) \mid x \in X, y \in Y\}$

Se $(x,y) \in F$ diremo che x è in corrispondenza con y $(x F y)$

__es:__
- $\emptyset$ e $X \times Y$ corrispondenze banali
- $X = \{\text{studenti PoliTo}\}$
  $Y = \{\text{docenti PoliTo}\}$

$F = \{(x,y) \mid x \text{ segue un corso di } y\} \subseteq X \times Y$

__Def:__ X, Y insiemi. Una corrispondenza F di dominio X e codominio Y è detta FUNZIONE da X a Y $(F: X \longrightarrow Y)$ se

$$\forall x \in X \quad \exists!\, y \in Y \text{ t.c. } x F y$$

$$y = F(x)$$

Y^X = insieme di tutte le funzioni da X a Y

<u>es:</u> • la corrispondenza dell'esempio precedente <u>non</u> è una funzione.

• $F = \{(x,y) \mid x + 2y = 5\} \subseteq \mathbb{R} \times \mathbb{R}$

$$y = \frac{5-x}{2}$$

<u>Def:</u> X insieme.
Una RELAZIONE R è una corrispondenza di X in X (cioè un sottoinsieme di $X \times X$)

R si dice
- RIFLESSIVA se $xRx \ \forall x \in X$
- TRANSITIVA se $xRy,\ yRz \Longrightarrow xRz \ \forall x,y,z \in X$
- SIMMETRICA: $xRy \Longleftrightarrow yRx \ \forall x,y \in X$
- ANTISIMMETRICA: $xRy,\ yRx \Longrightarrow x = y \ \forall x,y \in X$

<u>es:</u> • $X = \{$spazi vett. di dim. finita su $\mathbb{R}\}$

R = relazione di isomorfismo

isomorfo

$R = \{(V,W) \mid V \cong W\} \subseteq X \times X$

R è una relazione di equivalenza.

Def: Una relazione che gode delle proprietà riflessiva, transitiva, simmetrica è detta RELAZIONE DI EQUIVALENZA.

Notazione: xRy $\quad x \sim y$

es: In $\mathbb{Z} \times \mathbb{Z}$ prendiamo

$R = \{(a,b) \mid a \leq b\}$

se $a \leq b$ e $b \leq a \Longrightarrow a = b$

antisimmetria

$\leq$ è una relazione d'ordine.

Def: Una relazione riflessiva, transitiva e antisimmetrica è detta RELAZIONE D'ORDINE.

Ordine totale = ordine + $\forall$ coppia $(x,y) \in X \times X$ o xRy oppure yRx

Ordine parziale = non totale

es: • la relazione d'ordine $\leq$ dell'esempio precedente è totale.

- X insieme con almeno 2 elementi

L'insieme di tutti i sottoinsiemi di X è detto INSIEME DELLE PARTI di X

$$\mathcal{P}(X) = \{ Y \mid Y \subseteq X \}$$

Su $\mathcal{P}(X)$ definiamo la relazione

$$Y_1 R Y_2 \iff Y_1 \subseteq Y_2$$

$$R = \{ (Y_1, Y_2) \mid Y_1, Y_2 \subseteq X \text{ e } Y_1 \subseteq Y_2 \}$$

Relazione d'ordine <u>parziale</u>

$X = \{a, b\}$ $\quad$ $Y_1 = \{a\}$ $\quad$ $Y_2 = \{b\}$

<u>Def</u>: Sia X un insieme, e sia $\sim$ una relazione di equivalenza su X. L'insieme

$$\bar{x} = \{ y \in X \mid x \sim y \} \qquad [x]$$

è detto CLASSE DI EQUIVALENZA dell'elemento $x \in X$.

<u>es:</u> se $X = \{\text{sp. vett.}\}$ e $\sim \; = \; \cong$ come prima, allora

$$\bar{V} = \{ W \in X \mid W \cong V \}$$
$$= \{ W \in X \mid \dim(W) = \dim(V) \}$$

vedi ALG LiN

es: $X = \mathbb{Z}$

Fissiamo $n \in \mathbb{N}$ e definiamo

$$a \sim b \iff a-b \text{ é un multiplo di } n,$$
cioé se $\exists\, c \in \mathbb{Z}$ t.c. $a-b = cn$

notazione: $a \equiv_n b$ $\qquad a = b \pmod{n}$

"a é congruo modulo n a b"

- $a \equiv_n a$ perché $a-a = 0 = 0 \cdot n$
- $\alpha \equiv_n \beta$, $\beta \equiv_n \gamma \overset{?}{\Longrightarrow} \alpha \equiv_n \gamma$

$\alpha \equiv_n \beta$: $\exists\, c$ t.c. $\alpha - \beta = cn$

$\beta \equiv_n \gamma$: $\exists\, d$ t.c. $\beta - \gamma = dn$

$$\alpha - \gamma = \underbrace{\alpha - \beta}_{cn} + \underbrace{\beta - \gamma}_{dn} = cn + dn = (c+d)n$$

$\Longrightarrow \alpha \equiv_n \gamma$

- $\alpha \equiv_n \beta \qquad \alpha - \beta = cn$

$\Longrightarrow \beta - \alpha = -cn$, cioé $\beta \equiv_n \alpha$

Sia $a \in \mathbb{Z}$, chi é $\bar{a}$ / $[a]$?

$$\bar{a} = \{ b \in \mathbb{Z} \mid a \equiv_n b \} = \{ b \in \mathbb{Z} \mid a-b = cn \text{ per qualche } c \in \mathbb{Z} \}$$
$$= \{ b \in \mathbb{Z} \mid b = a - cn, \text{ per qualche } c \in \mathbb{Z} \}$$
$b = a + dn$

es: $n=2$

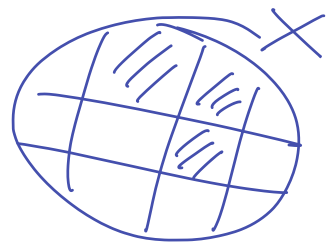
$$\bar{a} = \{ b \in \mathbb{Z} \mid a-b = 2n \}$$

$$\mathbb{Z} = \bar{0} \cup \bar{1}$$

numeri pari — numeri dispari

$$\overline{14} = \{ 2, \dots \}$$

classe di equiv. modulo 12



Def: Sia X un insieme. Una PARTIZIONE di X è una famiglia $\{X_i\}_{i\in I} \subseteq \mathcal{P}(X)$ di insiemi non vuoti

t.c.: ① $X_i \cap X_j = \emptyset$ se $i \neq j$

(o equivalentemente: se $X_i \cap X_j \neq \emptyset \Longrightarrow X_i = X_j$)

② $\bigcup_{i \in I} X_i = X$

Prop.
Proposizione Sia X un insieme, e $\sim$ una relazione di equivalenza su X. Allora l'insieme delle classi di equivalenza $\{\bar{x}\}_{x\in X}$ è una partizione di X.

dim: $x \in \bar{x} \quad \forall x \in X$

$$X = \bigcup_{x\in X} \{x\} \subseteq \bigcup_{x\in X} \bar{x} \implies X = \bigcup_{x\in X} \bar{x}$$

Sia $z \in \bar{x} \cap \bar{y} \implies z \sim x$ e $z \sim y$

$$\implies x \sim y$$

$$\begin{rcases} x \in \bar{y} \implies \bar{x} \subseteq \bar{y} \\ y \in \bar{x} \implies \bar{y} \subseteq \bar{x} \end{rcases} \implies \bar{x} = \bar{y} \quad \#$$

CVD

Def: X insieme, $\sim$ relazione di equivalenza su X _ L'INSIEME QUOZIENTE $X/\sim$ "X modulo $\sim$" è l'insieme delle classi di equivalenza:

$$X/\sim = \{\bar{x}\}_{x\in X}$$

es: $\sim \; = \; \equiv_2 \qquad \mathbb{Z} = \bar{0} \cup \bar{1}$

$$\mathbb{Z}/\sim = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

NOTAZIONE $\mathbb{Z}/\equiv_n = \mathbb{Z}_n$

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

multipli di 3 $= \{0, 3, 6, -3, \dots\}$

multipli di 3 + 1 $\{4, 7, -2 \dots\}$

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

$n \in \mathbb{N}$

$\mathbb{N} = \{1, 2, 3, \dots\}$

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

$\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \dots, \overline{11}\}$

$\mathbb{Z}_{24}$

<u>oss:</u> L'insieme quoziente $\mathbb{Z}_n$ contiene n elementi

<u>es:</u> $\mathbb{R}$ su $\mathbb{R}$ definiamo $\sim$

$\forall x, y \in \mathbb{R}: \quad x \sim y \iff x - y \in \mathbb{Z}$

- $\sim$ è una relazione di equiv.
- $\mathbb{R}/_\sim = [0, 1)$

Se $x \in \mathbb{R} \qquad x = a, a_0 a_1 a_2 a_3 \dots$

$x \sim 0, a_0 a_1 a_2 \dots$

Sia $\mathbb{N}$ = numeri naturali

NOTAZIONE: $I_n = \{1, 2, 3, \dots, n\} \subseteq \mathbb{N}$

PRINCIPIO DI INDUZIONE

Se $P(k)$ è una proprietà che dipende da $k \in \mathbb{N}$ e vale che: ① $P(1)$ è vera
② $\forall n \geq 1$ se $P(n)$ è vera $\Longrightarrow$ $P(n+1)$ è vera,

allora $P(k)$ è vera $\forall k \in \mathbb{N}$.

es: usiamo l'induzione per mostrare che

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

dim: $n=1$:

$$\sum_{i=1}^{1} i \stackrel{?}{=} \frac{1(1+1)}{2}$$

$$1 = 1 \quad \checkmark$$

$n \geq 1$, supponiamo che la tesi sia vera per n

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) \xleftarrow{\text{ipotesi induttiva}} \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1)+2(n+1)}{2} = \frac{n^2+n+2n+2}{2} = \frac{(n+1)(n+2)}{2} \quad \checkmark$$

esercizio per casa: dimostrare che per ogni $z \in \mathbb{Z}$, $z^3 - z$ è divisibile per 6.

PRINCIPIO DEL BUON ORDINAMENTO

<u>Prop:</u> Ogni sottoinsieme non vuoto $S \subseteq \mathbb{N}$ ha un primo elemento.

<u>dim:</u> dimostriamo che se S non ha un primo elt., allora $S = \emptyset$ (cioè $\mathbb{N} \setminus S = \mathbb{N}$)

osserviamo che $1 \notin S$, altrimenti S avrebbe un primo elt. ($\Longrightarrow 1 \in \mathbb{N} \setminus S$)

Supponiamo che $I_n = \{1, 2, 3, \dots, n\} \subseteq \mathbb{N} \setminus S$:
se $n+1 \notin \mathbb{N} \setminus S \Longrightarrow n+1 \in S$, ma non può essere, perché sarebbe un primo elemento!

In altre parole:
se $I_n \subseteq \mathbb{N} \setminus S \Longrightarrow I_{n+1} \subseteq \mathbb{N} \setminus S$
$\Longrightarrow$ per induzione, tutto $\mathbb{N} \subseteq \mathbb{N} \setminus S$ #

Abbiamo dimostrato:
INDUZIONE $\Longrightarrow$ BUON ORDINAMENTO

Ora dimostriamo il viceversa:

<u>dim:</u> $S \subseteq \mathbb{N}$ sottoinsieme definito così:

- $1 \in S$
- S ha la proprietà che se $n \in S \Longrightarrow n+1 \in S$

Vogliamo dimostrare che $S = \mathbb{N}$, cioè $\mathbb{N} \setminus S = \emptyset$:

Se per assurdo $\mathbb{N} \setminus S \neq \emptyset$, siccome vale il buon ordinamento per ipotesi, $\mathbb{N} \setminus S$ deve avere un primo elt, chiamiamolo m.

Osserviamo che $m > 1$, perché $1 \in S$ $1 \notin \mathbb{N} \setminus S$.

$m-1$ non può appartenere a $\mathbb{N} \setminus S$ (altrimenti sarebbe lui il 1° elt, non m!)

quindi $m-1 \in S \Longrightarrow (m-1)+1 \in S$ m

ASSURDO

ALGORITMO EUCLIDEO DI DIVISIONE

$\forall a \in \mathbb{N}_0$ e $b \in \mathbb{N}$ $\exists!$ $q, r \in \mathbb{N}_0$, con $0 \leq r < b$ tali che:

$$a = qb + r$$

q = quoziente

r = resto