Lezione 02 - 30/09/2022

Relazione

Sia X insieme, $X \times X = \{(a,b) | a, b \in X\}$

Esempio:

$$X = \{1,2\}$$
$$X \times X = \{(1,1),(1,2),(2,1),(2,2)\}$$

Definizione

Una relazione su X è un sottoinsieme R di $X \times X$. Diremo che $x \in X$ è in relazione con $g \in X$ se $(x,g) \in R$

Esempio:

$$X = \{1,2,3\}$$
$$R = \{(1,2),(1,3),(3,3)\}$$

- 1 è in relazione con 2
- 2 non è in relazione con 1

Notazione

Se R è una relazione e x è in relazione con y, scriveremo $x \sim y$.

Definizione - Relazione di equivalenza

Una relazione R su X si dice di **equivalenza** se valgono le 3 seguenti proprietà:

1. **Riflessiva**: $x \sim x, \forall x \in X$
2. **Simmetrica**: $x \sim y \Rightarrow y \sim x$
3. **Transitiva**: $x \sim y, y \sim z \Rightarrow x \sim z$

Esempi:

- R è la relazione di eguaglianza
- X = rette nel piano, R = relazione di parallelismo
- Congruenza modulo n, $n \in \mathbb{N}$

Osservazione

$\mathbb{Z}$ non è una campo in quanto non si può fare la divisione, ma si può comunque fare la divisione con resto. Verrà dimostrato che dati

$$a, b \in \mathbb{Z}, b \neq 0\ \exists! q, r \in \mathbb{Z} \text{ t.c.} \\ a = bq + r,\ 0 \leq r < |b|$$

Esempio: $17 = 4 * 4 + 1$

Fissato n, si pone

$$a \equiv_n b \\ \text{oppure} \\ a \equiv b \mod n$$

se a, b hanno lo stesso resto nella divisione per n. Quindi $a \equiv_n b$ se

$$a = q_1 n + r \\ b = q_2 n + r$$

e varrà la seguente regola

$$b - a = q_2 n + r - (q_1 n + r) = (q_2 - q_1)n$$

ovvero che $b - a$ è un multiplo di n, quindi

$$b \equiv_n a \Leftrightarrow \text{b-a è multiplo di n}$$

Verifichiamo che $\equiv_n$ è una **relazione di equivalenza**

- **Riflessiva**: $a \equiv_n a,\ a - a = 0 = 0 \cdot n$ ✓
- **Simmetrica**: $a \equiv_n b \Rightarrow b \equiv_n a$
  - Ipotesi: $b - a = kn$
  - Tesi: $\exists h$: $a - b = hn$, cioè $a - b = (-k)n$, quindi $h = -k$ ✓
- **Transitiva**: $a \equiv_n b, b \equiv_n c \Rightarrow a \equiv_n c$
  - Ipotesi:
    1. $b - a = hn$
    2. $c - b = kn$
  - Tesi: $\exists s$: $c - a = sn$. Sommando 1. con 2. si ottiene

$$c - a = c - b + b - a = hn + kn = (h + k)n \checkmark$$

Classi di equivalenza

Se R è un'equivalenza su X, poniamo per $x \in X$

$$[x] = \{y \in X | y \sim x\}$$

e la chiamiamo **classe di equivalenza di x.**

Osservazione

$$x \sim y \Leftrightarrow [x] = [y]$$

<u>Dimostrazione</u>:

- $\Rightarrow$

  Supponiamo $x \sim y$ e facciamo vedere che $[x] = [y]$, ovvero $[x] \subseteq [y]$ e $[y] \subseteq [x]$.

  1. $z \in [x]$

$$z \sim x, \overbrace{x \sim y}^{\text{ipotesi}} \overset{\text{TRA.}}{\Rightarrow} z \sim y \Rightarrow z \in [y]$$

  2. $t \in [y]$

$$t \sim y, \overbrace{x \sim y}^{\text{ipotesi}} \overset{SIM.}{\Rightarrow} y \sim x \overset{TRA.}{\Rightarrow} t \sim x \Rightarrow t \in [x]$$

- $\Leftarrow$

  Supponiamo $[x] = [y]$, allora $x \in [y]$, quindi $x \sim y$.

Costruzione dell'insieme quoziente

Siano X inseme e $\sim$ relazione di equivalenza

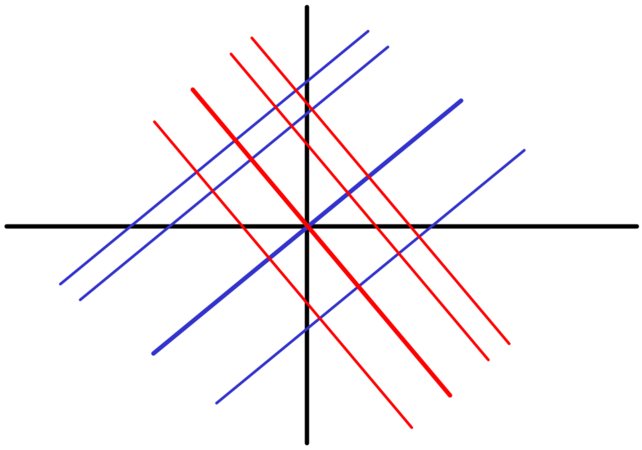
$$X/ \sim= \{[x] | x \in X\}$$

e si chiama **insieme quoziente di x modulo $\sim$.**

Esempi:

- $[x] = [y] \Leftrightarrow x = y$

  $X/_= = X$
- $X/_\sim = \text{direzioni nel piano} \leftrightarrow \text{rette che passano per l'origine}$



  Vengono scelte come rappresentanti solo quelle che passano per l'origine.
- $a \equiv_n b \Leftrightarrow a, b \text{ hanno lo stesso resto nella divisione per } n \leftrightarrow$
  $\text{un insieme di rappresentanti è dato dai resti della divisione per } n$

$$\mathbb{Z}/ \equiv_n = \{[0], [1], ..., [n-1]\}$$

  Esempi:

- $\mathbb{Z}/\equiv_2 = \{[0],[1]\}$ che stanno ad indicare rispettivamente i **numeri pari** e i **numeri dispari**.
- $\mathbb{Z}/\equiv_3 = \{[0],[1],[2]\}$

> Di solito si scrive $\mathbb{Z}_n$ per indicare $\mathbb{Z}/\equiv_n$.

Definizione di anello su Zn

Si vuole definire una struttura di anello su $\mathbb{Z}_n$:

- $+\ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [a+b]$
- $\cdot\ \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

  $([a],[b]) \mapsto [ab]$

Esempio: $n = 4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$
$[2]$	$[2]$	$[0]$	$[2]$
$[3]$	$[3]$	$[2]$	$[1]$

> ⚠️ Negli anelli si toglie lo 0 per l'operazione $\cdot$

> ⚠️ 2 non ha inversi quindi non è un campo. In quanto non ha inversi si dice che 2 è un **divisore dello 0**.

Spiegazione: a differenza di 2, tutti gli altri hanno inverso:

- $[1] \cdot [1] = [1]$
- $[3] \cdot [3] = [1]$

Mentre per $[2]$ non c'è nessuna classe $[b]$ tale che $[2] \cdot [b] = [1]$.

Problema teorico

Quando si definisce una funzione su un insieme quoziente, bisogna assicurarsi che la definizione sia **ben posta**, ovvero non dipenda dal **rappresentante scelto**.

Esempio: $\mathbb{Z}_{21}$

$$[18] + [8] = [26] = [5]$$

Ma in $\mathbb{Z}_{21}$ si ha anche $[18] = [-3]$ e $[8] = [50]$, quindi analogamente

$$[-3] + [50] = [47] = [5]$$

I risultati sono gli stessi, ma andrebbe dimostrato!

Verifichiamo che la $+$ in $\mathbb{Z}_n$ non dipenda dai rappresentanti. Bisogna vedere che:

$$[a] = [a'], [b] = [b'] \Rightarrow [a+b] = [a'+b']$$

Ipotesi:

1. $a' - a = kn$, ovvero è un multiplo di n
2. $b' - b = hn$

Verifichiamo che $(a' + b') - (a+b)$ è un multiplo di n:

$$a' + b' - a - b = \underbrace{(a' - a)}_{1.} + \underbrace{(b' - b)}_{2.} = kn + hn = (k+h)n \checkmark$$

Facciamo la stessa cosa per il prodotto:

$$[a] = [a'], [b] = [b'] \Rightarrow [ab] = [a'b']$$

Ipotesi:

1. $a' - a = hn$
2. $b' - b = kn$

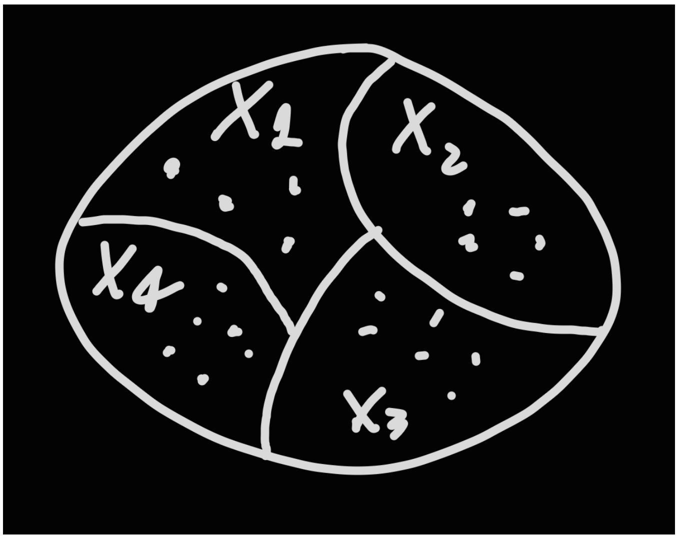
$$a'b' - ab = (a+hn)(b+kn) - ab = ab + hnb + akn + hkn^2 - ab =$$
$$= (hb + ak + hkn)n \checkmark$$

Entrambe le operazioni son **ben poste**.

Partizione

Sia X un insieme. Una famiglia $\{X_\alpha\}_{\alpha \in I}$ sottoinsiemi non vuoti di X si dice **partizione** di X se:

1. $X = \bigcup_{\alpha \in I} X_\alpha$
2. $X_\alpha \cap X_\beta = \emptyset \text{ se } \alpha \neq \beta$



$$X = X_1 \cup X_2 \cup X_3 \cup X_4$$
$$X_i \cap X_j = \emptyset \text{ se } i \neq j$$

Proposizione

Esiste una corrispondenza biunivoca tra paritzioni di X e relazioni di equivalenza su X.

<u>Dimostrazione</u>: sia $\sim$ una relazione di equivalenza. Poniamo

$$X_\alpha = \{x \in X | x \sim \alpha\} \alpha \in X$$

Dico che $\{X_\alpha\}_{\alpha \in X}$ è una partizione di X.

Dato $\alpha \in X$, allora $\alpha \in X_\alpha$ poichè $\alpha \sim \alpha$ per la **relazione riflessiva**. Quindi $X = \bigcup X_\alpha$.

Devo ora vedere che se X_α e X_β si intersecano, allora $\alpha = \beta$:
Sia $z \in X_\alpha \cap X_\beta$

$$
\begin{aligned}
& z \in X_\alpha, z \sim \alpha \overset{SIM.}{\Longrightarrow} \alpha \sim z \\
& z \in X_\beta, z \sim \beta \\
& \overset{TRA.}{\Longrightarrow} \alpha \sim \beta \Rightarrow X_\alpha = X_\beta
\end{aligned}
$$

<u>Viceversa</u>: sia $X = \bigcup_{\alpha \in I} X_\alpha$ una partizione. Definisco la relazione

$$x \sim y \Leftrightarrow \exists \delta \in I : x, y \in X_\delta$$

Verifico che $\sim$ è di **equivalenza**:

- **Riflessiva**: $x \sim x$, devo vedere che esiste

  $$\alpha \in I \text{ t.c. } x \in X_\alpha$$

  Ma questo segue dall'ipotesi che $X = \bigcup_{\alpha \in I} X_\alpha$.
- **Simmetrica**:

  $$
  \begin{aligned}
  & x \sim y \Rightarrow \exists \alpha \in I \text{ t.c. } x, y \in X_\alpha \\
  & \Rightarrow y \sim x \text{ (poichè entrambe appartengono a } X_\alpha)
  \end{aligned}
  $$

- **Transitiva**:

  $$x \sim y, y \sim z \Rightarrow x \sim z$$

  Ipotesi:

  $$
  \begin{aligned}
  & \exists \alpha_1 \in I : x, y \in X_{\alpha_1} \\
  & \exists \alpha_2 \in I : x, y \in X_{\alpha_2}
  \end{aligned}
  $$

  quindi $y \in X_{\alpha_1} \cap X_{\alpha_2} \Rightarrow \alpha_1 = \alpha_2$ e di conseguenza $x, z \in X_{\alpha_1} \Rightarrow x \sim z$.

  Si verifica facilmente che le corrispondenze costruite sono una l'inversa dell'altra.