Alcune informazioni. Ci sono due canali per il trasferimento di informazioni e materiali relative a corso di Geo1-20-21:

• La pagina dedicata nella home-page di Benedetti: http://people.dm.unipi.it/benedett/dida.html

• La pagina del corso di Geo1-20-21 in e-learning: https://elearning.dm.unipi.it

Attenzione: Ogni studente deve iscriversi nella pagina e-learning del corso, fatelo al più presto.

Relazioni di equivalenza

Dato un insieme non vuoto X, una *relazione* su X è un sottoinsieme non vuoto

$$R \subset X \times X \ .$$

Dati due elementi $x, y \in X$, diciamo che x è in R-relazione con y se la coppia *ordinata* $(x, y) \in R$. In tal caso, scriviamo $x \sim_R y$ o anche semplicemente $x \sim y$ sottointendendo R.

Attenzione, può darsi che x non sia in relazione con se stesso ($(x, x) \notin R$), oppure che $x \sim y$ ma y non sia in relazione con x, cioè $(x, y) \in R$ ma $(y, x) \notin R$.

R è una **relazione di equivalenza** se soddisfa le seguenti proprietà:

1. (Riflessiva) Per ogni $x \in X$, $x \sim x$. In altre parole, la diagonale

$$\Delta_X := \{(x, y) \in X \times X; x = y\} \subset R \ .$$

2. (Simmetrica) Per ogni $x, y \in X$, $x \sim y$ se e solo se $y \sim x$. In altre parole, R è un insieme *invariante* per la riflessione

$$\tau : X \times X \to X \times X, \ \tau(x, y) = (y, x)$$

cioè, $\tau(R) \subset R$. La diagonale è l'insieme dei punti fissi di τ

3. (Transitiva) Per ogni $x, y, z \in X$, se $x \sim y$ e $y \sim z$, allora $x \sim z$.

Un esempio di relazione che non è di equivalenza.

Y un insieme, $X = \mathcal{P}(Y)$ l'insieme delle parti (sottoinsiemi) di Y.

"$A, B \in X$, $A \sim B$ se $A \subset B$"

È riflessiva e transitiva, ma $A \subset B$ e $B \subset A$ se e solo se $A = B$, quindi non è simmetrica.

Una relazione riflessiva, transitiva, tale che

$x \sim y$ e $y \sim x$ se e solo se $x = y$

è detta una **relazione di ordine**. Ad esempio $\leq$ su $\mathbb{Z}$ è una relazione d' ordine.

Ogni insieme X porta due relazioni di equivalenza "estreme" .

$R = \Delta_X$, cioè R è la relazione di *uguaglianza*; R è la relazione di equivalenza minima, rispetto all'ordinamento su $\mathcal{P}(X \times X)$ dato dall'inclusione $\subset$.

$R = X \times X$, gli elementi di X sono tutti equivalenti tra loro . Questa è la relazione di equivalenza massima.

Le relazioni di equivalenza "interessanti" sono quelle relazioni "intermedie" che emergono soprattutto quando X è munito di strutture addizionali.

Dati R e $x \in X$, la *classe di equivalenza* di x è per definizione

$$[x]_R = [x] = \{y \in X; y \sim x\} \subset X$$

L' *insieme quoziente* di X (rispetto a R) è l'insieme delle classi di equivalenza.

$$X/R = X/\sim := \{[x]; x \in X\}$$

Quindi $[x] \subset X$ e $[x] \in X/R$.

$$\pi : X \to X/R,\ \pi(x) = [x]$$

è detta la *proiezione sul quoziente*, è surgettiva, $x \sim y$ se e solo se $\pi(x) = \pi(y)$,

$$[x] = \pi^{-1}([x]) := \{y \in X; \pi(y) = [x]\}$$

Sia $f : X \to Y$ un'applicazione. Supponiamo che f sia surgettiva, $Y = \mathrm{Im}(f)$. La relazione

"$x \sim_f y$ se e solo se $f(x) = f(y)$"

è una relazione di equivalenza. Per ogni $x \in X$,

$$[x]_f = f^{-1}(f(x))$$

L'applicazione

$$\widehat{f} : X/f \to Y,\ \widehat{f}([x]) = f(x)$$

è *ben definita* ed è bigettiva (iniettiva e surgettiva). L'applicazione inversa è

$$\widehat{f}^{-1} : Y \to X/f,\ \widehat{f}^{-1}(y) = f^{-1}(y)$$

intendendo che $f^{-1}(y) = [x]_f$, per ogni x tale che $f(x) = y$.

Sia X insieme non vuoto.

$$S(X) = \{\sigma : X \to X;\ \sigma\ bigettiva\}$$

munito dell'operazione data dalla *composizione*

$$\circ : S(X) \times S(X) \to S(X),\ (\sigma, \tau) \to \sigma \circ \tau$$

è un gruppo detto *gruppo delle* **simmetrie**, *equivalentemente, delle* **trasformazioni** *dello insieme* X.

[L' operazione $\circ : S(X) \times S(X) \to S(X)$ è associativa, $\mathrm{id}_X \in S(X)$ è l'elemento neutro, ogni $\sigma \in S(X)$ ammette l'elemento inverso σ^{-1}.]

$G \subset S(X)$ tale che $\mathrm{id}_X \in G$, e tale che

$G \times G \subset S(X) \times S(X)$ è chiuso per l' operazione $\circ$,

G è invariante per l'applicazione $S(X) \to S(X)$, $\sigma \to \sigma^{-1}$

è un *gruppo di trasformazioni* di X.

Gruppi di trasformazioni "interessanti" emergono quando X è munito di strutture addizionali e si considerano trasformazioni di X che preservano tali strutture.

Dato un gruppo di trasformazioni G di X,

"$x \sim_G y$ se e solo se esiste $\sigma \in G$ tale che $y = \sigma(x)$"

è una relazione di equivalenza su X.

Verifica: $x = \mathrm{Id}_X(x)$;

$y = \sigma(x)$ se e solo se $x = \sigma^{-1}(y)$;

$y = \sigma(x)$, $z = \tau(y) \Rightarrow z = (\tau \circ \sigma)(x)$.

$$[x]_G = Gx := \{\sigma(x);\ \sigma \in G\}$$

è anche detta la *G-orbita di x*.

Una *partizione* P di X è un insieme di sottoinsiemi di X ($P \subset \mathcal{P}(X)$) che soddisfa le seguenti proprietà.

1. Ogni $U \in P$ è non vuoto;

2. P *ricopre* X cioè, per ogni $x \in X$ esiste $U \in P$ tale che $x \in U$; in altre parole, X è l'unione dei sottoinsiemi che appartengono a P.

3. Se $U, U' \in P$ e $U \neq U'$, allora $U \cap U' = \emptyset$. In altre parole, se $U \cap U' \neq \emptyset$, allora $U = U'$; ne segue che per ogni $x \in X$ esiste un *unico* $U \in P$ tale che $x \in U$.

Proposizione *Se R è una relazione di equivalenza su X, allora $\{[x]_R \subset X;\ x \in X\}$ è una partizione di X.*

Dim. $x \in [x]$, quindi ogni $[x]$ è non vuota e le classi di equivalenza ricoprono X.

Se $[x] \cap [y] \neq \emptyset$, sia z in tale intersezione. Se $u \sim x$, allora $u \sim z \sim y$ (qui si usano le proprietà simmetrica e transitiva), da cui $[x] \subset [y]$. Per simmetria, anche $[y] \subset [x]$, quindi $[x] = [y]$.

■

Proposizione *Sia P una partizione di X. Allora*

" $x \sim_P y$ se esiste $U \in P$ tale che x e $y \in U$ "

definisce una relazione di equivalenza su X. Inoltre, per ogni $x \in X$, $[x]_P$ è l'unico $U \in P$ tale che $x \in U$.

Dim. $x \sim x$ perché P ricopre X. È evidentemente simmetrica. Se $x, y \in U$ e $y, z \in U'$, allora $y \in U \cap U'$, quindi $U = U'$, $x, z \in U$.

■

Relazioni di equivalenza e partizioni su X sono sostanzialmente la stessa struttura (formulata in due modi diversi).

Esempio. Sia $\mathbb{Z} \subset \mathbb{R}$. Poniamo

"$x \sim_{\mathbb{Z}} y$ se $x - y \in \mathbb{Z}$" .

È una relazione di equivalenza: $x - x = 0 \in \mathbb{Z}$;

$x - y \in \mathbb{Z} \Rightarrow y - x \in \mathbb{Z}$;

$x - y, y - z \in \mathbb{Z} \Rightarrow x - z = (x - y) + (y - z) \in \mathbb{Z}$.

Per ogni $x \in \mathbb{R}$,

$$[x]_{\mathbb{Z}} = x + \mathbb{Z} := \{y = x + m \in \mathbb{R};\ m \in \mathbb{Z}\}$$

Per ogni $m \in \mathbb{Z}$, $\sigma_m : \mathbb{R} \to \mathbb{R}$, $\sigma_m(x) := x + m$ è una traformazione di $\mathbb{R}$ (con inversa σ_{-m}).

$\sigma_{m+n}(x) = x + (m + n) = (x + m) + n =$

$\sigma_n \circ \sigma_m(x) = \sigma_m \circ \sigma_n(x)$

Possiamo quindi identificare $\mathbb{Z}$ con un gruppo G di trasformazioni di $\mathbb{R}$,

$x \sim_{\mathbb{Z}} y$ se e solo se $x \sim_G y$.

Sia $f : \mathbb{R} \to \mathbb{R}^2,\ f(x) = (\cos(2\pi x), \sin(2\pi x))$.

f è periodica di periodo minimo uguale a 1. Cioè

$x \sim_f y$ se e solo se esiste $m \in \mathbb{Z}$ tale che $y = x + m$. Quindi $x \sim_f y$ se e solo se $x \sim_{\mathbb{Z}} y$.

L'immagine di f è la circonferenza unitaria

$$C = \{(a, b) \in \mathbb{R}^2; a^2 + b^2 = 1\}$$

quindi l'insieme quoziente $X/\mathbb{Z}$ si identifica con C.

L'operazione di somma su $(\mathbb{R}, +)$ "passa al quoziente": poniamo

$$[x]_{\mathbb{Z}} \oplus [y]_{\mathbb{Z}} := [x + y]_{\mathbb{Z}}$$

è ben definita:

$$[x + n] \oplus [y + m] = [x + y + (n + m)] = [x + y]$$

La proiezione

$$\pi : (\mathbb{R}, +) \to (\mathbb{R}/\mathbb{Z}, \oplus), x \to [x]_{\mathbb{Z}}$$

verifica (tautologicamente):

$$\pi(x + y) = \pi(x) \oplus \pi(y)$$

cioè è un "omomorfismo di gruppi".

Domanda: *Cosa diventa l'operazione $\oplus$ quando la "trasportiamo" sulla circonferenza C?*

Esempio.

Per ogni $m \in \mathbb{N}$, $m > 1$, si consideri la seguente relazione su $\mathbb{Z}$:

"$x \sim_m y$ se $x - y \in m\mathbb{Z}$" .

È una relazione di equivalenza. Per ogni $x \in \mathbb{Z}$, $[x]_m = x + m\mathbb{Z}$.

Ponendo per ogni $z \in m\mathbb{Z}$,

$\sigma_z : \mathbb{Z} \to \mathbb{Z}$, $\sigma_z(n) = n + z$

identifichiamo $m\mathbb{Z}$ con un gruppo di trasformazioni G di $\mathbb{Z}$, tale che

$x \sim_m y$ se e solo se $x \sim_G y$.

Ricordiamo che su $\mathbb{Z}$ è definita la (fondamentale) **divisione con il resto**.

Per ogni $m \neq 0 \in \mathbb{Z}$, per ogni $a \in \mathbb{Z}$, esistono unici $q, r \in \mathbb{Z}$, tali che

$$a = qm + r,\ 0 \leq r < |m|$$

Definiamo

$r = r_m : \mathbb{Z} \to \{0, 1, \ldots, m-1\}$ dove $r(a)$ è il resto della divisione di a per m.

$x \sim_m y$ se e solo se $x \sim_r y$:

$x = q(x)m + r(x), y = x + ms \Rightarrow$

$y = q(x) + r(x) + ms = (q(x) + s)m + r(x)$

$r(y) = r(x)$.

Viceversa:

$x = q(x)m + r, y = q(y)m + r, \Rightarrow$

$x - y = (q(x) - q(y))m, x \sim_m y$.

L'insieme quoziente $\mathbb{Z}/m\mathbb{Z}$ è **finito** in corrispondenza biunivoca con l'insieme dei possibili resti della divisione per m.

Le operazioni somma e prodotto su $\mathbb{Z}$ passano al quoziente $\mathbb{Z}/m\mathbb{Z}$ con tutte le solite prorietà aritmetiche:

$$[x]_m + [y_m] = [x+y]_m,\ [x]_m[y]_m = [xy]_m$$

$0 = [0]_m$, $-[x]_m = [-x]_m$, $1 = [1]_m$, ...

Sappiamo che solo $\pm 1 \in \mathbb{Z}$ ammettono inverso rispetto alla moltiplicazione su $\mathbb{Z}$. Cosa possiamo dire in proposito per il prodotto su $\mathbb{Z}/m\mathbb{Z}$?

Se $m = pq$, $1 < p, q < m$, non è primo, allora $[p]_m, [q]_m \neq 0 \in \mathbb{Z}/m\mathbb{Z}$, ma non ammettono inverso rispetto al prodotto. Per assurdo, supponiamo, per esempio, che esista $[d]_m$ tale che $[d]_m[p]_m = [dp]_m = 1 \in \mathbb{Z}/m\mathbb{Z}$. Allora

$$0 = [d]_m[m]_m =$$

$$[d]_m[pq]_m = [dp]_m[q]_m = [q]_m \neq 0$$

che è assurdo.

Si può dimostrare che

Esiste l'inverso per ogni $[x]_m \neq 0$ *se e solo se* m *è primo.*

Costruzione di $(\mathbb{Z}, +)$ a partire da $(\mathbb{N}, +)$

Sull 'insieme $\mathbb{N} \times \mathbb{N}$, poniamo formalmente

$$(x, y) = x - y$$

Definiamo la relazione

"$(x, y) \sim (a, b)$, cioè, formalmente, $x - y \sim a - b$, se $x + b = a + y$" .

È una relazione di equivalenza:

$x + y = x + y$;

se $x + b = a + y$ allora $a + y = x + b$;

se $x+b = a+y$ e $a+d = c+b$, allora, sommando e usando le proprietà associativa e commutativa di $(\mathbb{N}, +)$, abbiamo

$$x + d + (b + a) = c + y + (a + b)$$

da cui

$$x + d = c + y$$

perché $(\mathbb{N}, +)$ ha la *proprietà di cancellazione*.

Indichiamo con $\mathbb{Z}$ l'insieme quoziente; $[a-b] \in \mathbb{Z}$ la classe di equivalenza di (a, b).

Poniamo

$$[a-b]+[x-y]=[(a+x)-(b+y)]$$

È ben definita.

$0=[0-0]$, $-[a-b]=[b-a]$.

$j:(\mathbb{N},+)\to(\mathbb{Z},+)$, $j(n)=[n-0]$ è una inclusione che rispetta l'operazione.

Facciamo l'abuso di scrivere

$n=[n-0]$, $-n=-[n-0]=[0-n]$.

Allora $[a-b]=[a-0]+[0-b]=a+(-b)$. Quindi ogni $z\in\mathbb{Z}$ si scrive in modo unico come

$z=\pm n$, per qualche $n\in\mathbb{N}$.

Si può estendere anche la moltiplicazione ponendo

$$(a-b)(x-y)=(ax+by)-(bx+ay)\ .$$

Costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$.

$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Su $\mathbb{Z} \times \mathbb{Z}^*$ definiamo la relazione

" $(a, b) \sim (x, y)$ se $ay = bx$" .

È una relazione di equivalenza. Chiamiamo $\mathbb{Q}$ l'insieme quoziente e poniamo $[(a, b)] := \frac{a}{b}$. Definiamo le operazioni $+$ e $\cdot$ su $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + cb}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Sono ben definite. $0 = \frac{0}{1}$, $1 = \frac{1}{1}$. $\mathbb{Z}$ si include in $\mathbb{Q}$ via $m = \frac{m}{1}$ così che le operazioni su $\mathbb{Q}$ estendono quelle di $\mathbb{Z}$. Se $\frac{a}{b} \neq 0$, allora

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = 1$$

Esempio. Il gruppo moltiplicativo

$\mathbb{R}^* := \mathbb{R} \setminus \{0\}$

agisce come un gruppo di trasformazioni di

$X := \mathbb{R}^2 \setminus \{(0,0)\}$;

$\lambda \neq 0$ corrisponde a $\sigma_\lambda : X \to X$,

$\sigma_\lambda(a,b) := (\lambda a, \lambda b)$

Indichiamo con $\mathbf{P}$ l'insieme quoziente.

$$[v] = \{\lambda v \in \mathbb{R}^2 \setminus \{0,0\}; \lambda \in \mathbb{R} \setminus \{0\}\}$$

è la retta passante per l'origine e il punto $v \neq (0,0) \in \mathbb{R}^2$, privata dell'origine. C'è una corrispondenza biunivoca naturale tra $\mathbf{P}$ e l'insieme delle rette passanti per l'origine.

Sia C come sopra la circonferenza unitaria. Per ogni $v = (a, b) \neq (0, 0)$,

$$w = v/||v||, ||v|| = \sqrt{a^2 + b^2}; [v] \cap C = \pm w \ .$$

Restringendo la relazione su C, questa diventa $(a, b) \sim (c, d)$ se e solo se $(c, d) = \pm(a, b)$. Essa è indotta dal gruppo moltiplicativo $\{\pm 1\} \subset \mathbb{R}^*$ considerato come gruppo di trasformazioni di C. $\mathbf{P} = C/\pm 1$.