Una relazione su un insieme A è un sottoinsieme $R \subseteq A \times A$. Quando una coppia $(x, y) \in A \times A$ è in R, allora xRy (x è in relazione con y).

ESEMPIO

Se abbiamo $f : A \to A$, allora *Graf(f)* è una relazione, perché $Graf(f) \stackrel{\text{def}}{=} \{(x, y): x, y \in A, y = f(x)\}$ e $xRy \Leftrightarrow y = f(x)$

RELAZIONI DI EQUIVALENZA

Diciamo che una relazione $R \subseteq A \times A$ è una RELAZIONE DI EQUIVALENZA quando gode di tre proprietà:

- Riflessività: $xRx, \forall x \in A$
- Simmetria: $xRy \Rightarrow yRx$
- Transitività: $(xRy\ e\ yRz) \Rightarrow xRz$

Le relazioni d'ordine per esempio non sono relazioni di equivalenza, perché sono asimmetriche.

Preso l'insieme A e una relazione di equivalenza R su A, $\forall x \in A$ denotiamo $[x]_R \stackrel{\text{def}}{=} \{y \in A: xRy\}$ la classe di equivalenza di x.

TEOREMA FONDAMENTALE SULLE RELAZIONI DI EQUIVALENZA

Sia R una relazione di equivalenza su A. Allora:

1) $\boldsymbol{xRy \Leftrightarrow [x] = [y]}$
2) $\boldsymbol{x\not Ry \Leftrightarrow [x] \cap [y] = \emptyset}$
3) $\boldsymbol{\cup_{x \in A}^{d} [x] = A}$

Il terzo punto implica che ogni relazione di equivalenza induce una partizione.

DIMOSTRAZIONE:

1) Sia [x]=[y], allora $z \in [x] \Leftrightarrow z \in [y] \Rightarrow zRy \Leftrightarrow zRy$. Sappiamo che $xRx \Leftrightarrow xRy$. Viceversa, sia xRy. Vogliamo mostrare che $[x] = [y]$, cioè che $[x] \subseteq [y]$ e $[y] \subseteq [x]$. Sia dunque $z \in [x]$, dobbiamo mostrare che $z \in [y]$: infatti $z \in [x] \Leftrightarrow zRx$, inoltre per ipotesi $xRy \Rightarrow zRy \Rightarrow yRz$, cioè $z \in [y]$. Che $[y] \subseteq [x]$ si dimostra allo stesso modo: infatti $z \in [y] \Leftrightarrow zRy$, inoltre per ipotesi $xRy \Rightarrow yRx \Rightarrow zRx$, cioè $z \in [x]$. C.v.d.
2) Supponiamo che $x\not Ry$ e proviamo che $[x] \cap [y] = \emptyset$. Sappiamo che $x\ \not R\ y$. Se fosse $[x] \cap [y] \neq \emptyset$ allora $\exists z \in [x] \cap [y]$ e quindi $z \in [x]$ e $z \in [y]$, cioè zRx e zRy, cioè xRz e zRy, dunque xRy, ma questa è una contraddizione. Dunque $[x] \cap [y] = \emptyset$.
   Se viceversa sappiamo che $[x] \cap [y] = \emptyset$, vogliamo vedere che $x\not Ry$. Infatti se fosse xRy allora [x]=[y], contraddicendo che $[x] \cap [y] = \emptyset$. C.v.d.
3) Questa deriva dalle 2 dimostrazioni precedenti. L'unione disgiunta delle classi di equivalenza è uguale all'intero insieme■

L'insieme delle classi di equivalenza di A, detto **Insieme Quoziente** si denoterà con: $A/_R \stackrel{\text{def}}{=} \{[x]: x \in A\}$.

RELAZIONE DI EQUIPOTENZA

Sia U un insieme universo e A, B, C, … ⊆ U. Diciamo che due insiemi A e B sono **EQUIPOTENTI** quando $\exists f: A \to B$ biunivoca, e scriviamo $A \sim B$.

PROPOSIZIONE: La relazione di equipotenza è una relazione di equivalenza.

DIMOSTRAZIONE:

1) $A \sim A, \forall A \in U$? Si, perché $i: A \to A,\ a \mapsto i(a) = a$
2) $A \sim B \Longrightarrow B \sim A$? Si, perché se $f: A \to B$ è biunivoca, allora $f^{-1}: B \to A$ è biunivoca e dunque $B \sim A$.
3) $(A \sim B, B \sim C) \Rightarrow A \sim C$? Cioè, se $f: A \to B$ è biunivoca e $g: B \to C$ è biunivoca, allora $h = g \circ f$ è biunivoca?. Sappiamo di si■

Se A e B sono insiemi finiti, quand'è che sono equipotenti? Ossia, quando è possibile trovare una $f: A \to B$ biunivoca? **Naturalmente quando hanno lo stesso numero di elementi: #[A]=#[B]. In tal caso ogni classe di equivalenza individua un numero naturale.**■

CLASSI DI EQUIPOTENZA

A è il rappresentante della classe di equipotenza $[A]_{\sim}$, ma la classe di equipotenza non dipende da esso. Denotiamo con ${}^{U}/_{\sim} = \{[A]_{\sim} : A \subset U\}$ l'insieme delle classi di equipotenza dell'insieme universo.

Quando $\#(A) = n, possiamo\ identificare\ [A]_{\sim}\ con\ n$, dove n indica il numero degli elementi della classe.

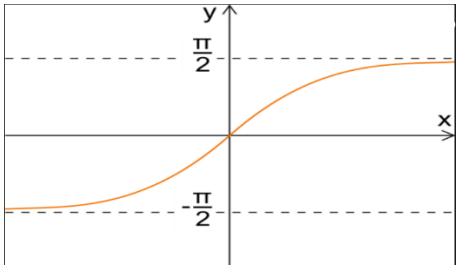
E se A non è finito? $\forall A, B\ insiemi\ infiniti\ \exists f: A \to B$ biunivoca? **Non sempre esiste**.

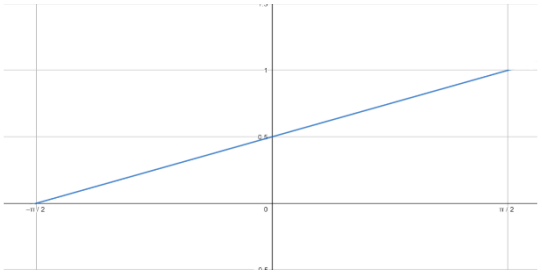
TEOREMA (METODO DELLA DIAGONALE DI CANTOR)

Non esiste nessuna funzione suriettiva da $\mathbb{N} \to [0, 1]$ e dunque nemmeno fra $\mathbb{N}$ *ed* $\mathbb{R}$.

DIMOSTRAZIONE

Prima di tutto, $]0,1[$ è equipotente a $\mathbb{R}$. Infatti, consideriamo $arctg : \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ ed $r : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to]0,1[$, definita da $r(x) = \frac{2}{\pi}x$. Allora $r \circ (arctg) : \mathbb{R} \to]0,1[$ è biunivoca e dunque l'intervallo $]0,1[\equiv \mathbb{R}$.





Supponiamo che $\mathbb{N} \equiv]0,1[$ e mostriamo che otteniamo una contraddizione.

Supponiamo che esista una funzione $\mathbb{N} \to]0,1[$ suriettiva e mostriamo che otteniamo una contraddizione. Sia *f* una funzione qualunque $f : \mathbb{N} \to]0,1[$. Sarà necessariamente

$f(1) = 0, x_1^1 x_2^1 x_3^1 x_4^1 \ldots$

$f(2) = 0, x_1^2 x_2^2 x_3^2 x_4^2 \ldots$

$f(3) = 0, x_1^3 x_2^3 x_3^3 x_4^3 \ldots$

$\vdots$

$f(k) = 0, x_1^k x_2^k x_3^k x_4^k \ldots$

$\vdots$

Ogni numero avrà il suo sviluppo decimale. Ora consideriamo $b \overset{\text{def}}{=} \{0, b_1 b_2 b_3 b_4 \ldots b_k \ldots\}$, dove

$$b_k = \begin{cases} 5\ se\ x_k^k \neq 5 \\ 7\ se\ x_k^k = 5 \end{cases}$$

Allora $b \in]0,1[$ e se f fosse suriettiva dovrebbe esistere $n \in \mathbb{N}: f(n) = b$, ma questo non è possibile per come è costruito b, perché $\forall k \in \mathbb{N}$, b ha la k-esima cifra decimale diversa da quella di f(k). Questo numero non ha una controimmagine, dunque f non può essere mai suriettiva ■

Ne segue che l'infinità di $\mathbb{R}$ è diversa da quella di $\mathbb{N}$.

$U/_{\sim} = \{[A]_{\sim}: A \subset U\}$ dove $[A]_{\sim}$ indica i numeri cardinali, cioè le classi di equipotenza.

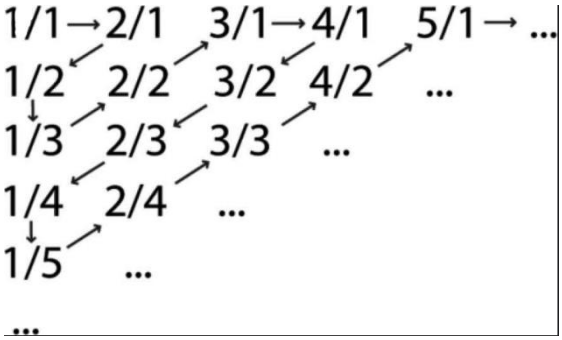
$[\mathbb{N}]_{\sim} = \aleph_0$, la lettera ebraica "Aleph" sta ad indicare la cardinalità degli insiemi numerabili

$[\mathbb{R}]_{\sim} = C$ cardinalità del continuo

Queste sono due cardinalità diverse infinite.

ESMPI DI INSIEMI NUMERABILI.

1. $\mathbb{P}$, insieme dei numeri naturali pari, è numerabile, cioè $\exists f: \mathbb{N} \to \mathbb{P}$ biunivoca. Possiamo prendere ad esempio$f(n) = 2n$, in tal modo $f^{-1}(2n) = n$.
2. $\mathbb{D}$, insieme dei numeri naturali dispari è numerabile, perché $f: \mathbb{N} \to \mathbb{D}$, $f(n) = 2n + 1$ è biunivoca.
3. $\mathbb{Z}$ è numerabile, ad esempio una biezione $f: \mathbb{N} \to \mathbb{Z}$, è $data\ da\ \ f(n) = \begin{cases} -\frac{n}{2}\ se\ n \text{ è } pari \\ \frac{n-1}{2}\ se\ n \text{ è } dispari \end{cases}$
4. Anche $\mathbb{Q}$ è numerabile:



Eliminando i numeri che si ripetono, si ottiene una funzione iniettiva e suriettiva.

$[\mathbb{P}]_{\equiv} = [\mathbb{N}]_{\equiv} = [\mathbb{D}]_{\equiv} = [\mathbb{Z}]_{\equiv} = [\mathbb{Q}]_{\equiv}$

Un insieme $A \in [A]_{\equiv}$ ha la cardinalità della sua classe.

In $U/_{\equiv}$ possiamo cercare di definire una relazione d'ordine: $[A]_{\equiv} \leq [B]_{\equiv} \Leftrightarrow \exists f: A \to B$ iniettiva, cioè:

1) Dati [A] e [B] risulta $[A] \leq [B] o\ [B] \leq [A]$ (Ordine totale)
2) $[A]_{\sim} \leq [A]_{\sim}$ (Riflessività)
3) $([A]_{\sim} \leq [B]_{\sim}\ e\ [B]_{\sim} \leq [A]_{\sim}) \Leftrightarrow [A]_{\sim} = [B]_{\sim}$ (Antisimmetria)
4) $([A]_{\sim} \leq \sim\ e\ [B]_{\sim} \leq [C]_{\sim}) \Leftrightarrow [A]_{\sim} \leq [C]_{\sim}$ (Transitività)

DIMOSTRAZIONE

1) Il primo si dimostra attraverso l'impiego dell'ASSIOMA DELLA SCELTA.
2) La riflessività è ovvia.
3) L'antisimmetria deriva dal teorema di Cantor, Shröeder, Bernstein:

$\begin{pmatrix}\exists f: A \to B\ iniettiva \\ \exists g: B \to A\ iniettiva\end{pmatrix} \Leftrightarrow (\exists k: A \to B\ biunivoca)$

Esporremo la dimostrazione di questo Teorema dopo ave esaminato il Lemma della Concordia.

4) La transitività è ovvia■

Indicheremo d'ora in avanti con $\mathfrak{P}(A) = \{C \leq U: C \subset A\}$ l'insieme delle parti di A .

La cardinalità di A si indica con |A|.

ESEMPIO

Se |A|=3, quanto vale $|\mathfrak{P}(A)|$?

$A = \{1,2,3\}$; $\mathfrak{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, quindi $|\mathfrak{P}(A)| = 8$

Esercizio: Dimostrare per induzione che Se $A < +\infty$ allora $|\mathfrak{P}(A)| = 2^{|A|}$.

LEMMA DELLA CONCORDIA

Siano X, Y due insiemi, $f: X \to Y, g: Y \to X$, allora $\exists\{X_1, X_2\}$ partizione di X, $\exists\{Y_1, Y_2\}$ partizione di Y, t.c. $f(X_1) = Y_1, g(Y_2) = X_2$

DIMOSTRAZIONE LEMMA DELLA CONCORDIA

Consideriamo la funzione $h: \mathfrak{P}(X) \to \mathfrak{P}(X),\ definita\ da\ h(E) \stackrel{\text{def}}{=} [g([f(E)]^c)]^c$, $\forall\ E \in \mathfrak{P}(X)$,

Allora:

1) $E_1, E_2 \in \mathfrak{P}(X), E_1 \subseteq E_2 \Rightarrow f(E_1) \subseteq f(E_2) \Rightarrow \big(f(E_2)\big)^c \subseteq \big(f(E_1)\big)^c \Rightarrow g[\big(f(E_2)\big)^c] \subseteq g[(f(E_1))^c] \Rightarrow (g[(f(E_1)^c)])^c \subseteq g[(f(E_2)^c)]^c$, cioè $h(E_1) \subseteq h(E_2)$. Riassumendo, se $E_1 \subseteq E_2, allora\ h(E_1) \subseteq h(E_2)$, vale a dire **La funzione h è crescente rispetto all'ordine dell'inclusione.**

2) Consideriamo l'insieme A:= $\{E \subseteq X : h(E) \subseteq E\}$ e prendiamo $\bigcap_{M \in A} M := X_1$

3) Vogliamo vedere ora che $h(X_1) = X_1$. Mostriamo prima che $h(X_1) \subseteq X_1$.

4) Infatti $\forall M \in A, h(M) \subseteq M \Rightarrow h(X_1) = h(\bigcap_{M \in A} M) = \bigcap_{M \in A} h(M) \subseteq \bigcap_{M \in A} M = X_1$.

5) Rimane da vedere che $X_1 \subseteq h(X_1)$. $Abbiamo\ già\ provato\ che\ h(X_1) \subseteq X_1$. Applicando $h\ avremo\ h\big(h(X_1)\big) \subseteq h(X_1) \Rightarrow h(X_1) \in A \Rightarrow h(X_1) \supseteq X_1$.

6) A questo punto consideriamo la partizione di X, data da X_1 e $X_2 \stackrel{\text{def}}{=} X_1^c$ e la partizione di Y data da $Y_1 = f(X_1)$ e $Y_2 \stackrel{\text{def}}{=} [f(X_1)]^c$.

Rimane da provare che $g(Y_2) = X_2, cio$è $g(Y_1^c) = X_2$.

Infatti $g(Y_1^c) = g\Big[\big(f(X_1)\big)^c\Big] = [g(f(X_1)^c)^c]^c = [h(X_1)]^c = X_1^c = X_2$.■

TEOREMA DI CANTOR, BERNSTEIN, SCHRÖEDER,

Se X e Y sono due insiemi ed $\exists f: X \to Y$ iniettiva e $\exists g: Y \to X$ iniettiva, allora $\exists k: X \to Y$ biunivoca.

$([X]_{\equiv} \leq [Y]_{\equiv}\ e\ [Y]_{\equiv} \leq [X]_{\equiv}) \Rightarrow [X]_{\equiv} = [Y]_{\equiv}$

DIMOSTRAZIONE

Per il lemma della concordia, $\exists\{X_1, X_2\}$ **partizione di X,** $\exists\{Y_1, Y_2\}$ **partizione di Y, t.c.** $f(X_1) = Y_1, g(Y_2) = X_2$.

Definiamo allora $k: X \to Y$ in questo modo: $k(x) = \begin{cases} f(x)\ se\ x \in X_1 \\ g^{-1}(x)\ se\ x \in X_2 \end{cases}$.

E' ovvio verificare che k è biunivoca ■

TEOREMA DI CANTOR-BERNSTEIN

Non esiste nessuna applicazione suriettiva da X a $\mathfrak{P}(X)$, qualunque sia l'insieme X.

DIMOSTRAZIONE

Sia $f: X \to \mathfrak{P}(X)$ una qualunque funzione. Consideriamo il sottoinsieme di X definito da

$$\boldsymbol{C \overset{\text{def}}{=} \{x \in X: x \notin f(x)\}}$$

Allora se f fosse suriettiva, **dovrebbe esistere $x_0 \in X$ $t.c.$ $f(x_0) = C$**

$Ora\ chiediamoci: x_0 \in C?$

- Se si, $x_0 \in C \Leftrightarrow x_0 \in \{x \in X: x \in f(x)\} \Rightarrow x_0 \notin f(x_0) \Rightarrow x_0 \notin C$
- Se no, $x_0 \notin C = f(x_0) \Rightarrow x_0 \in C$, di nuovo contraddizione.

Così un tale x_0 non può esistere e dunque f non può essere suriettiva. ■

Ne segue

$$|X| < |\mathfrak{P}(X)| < |\mathfrak{P}(\mathfrak{P}(X))| < \left|\mathfrak{P}\left(\mathfrak{P}\left(\mathfrak{P}(X)\right)\right)\right| < \cdots$$

Esistono infiniti tipi di infinito, i cui elementi sono detti NUMERI TRANSFINITI

$|\mathfrak{P}(\mathbb{N})| = C$ cardinalità del continuo

$|\mathfrak{P}(\mathbb{N})| = C < 2^C < 2^{2^C} < \cdots$■

Finiamo questa breve introduzione della relazione di equipotenza dando una caratterizzazione degli insiemi infiniti la cui dimostrazione è lasciata per esercizio:

Teorema: Un insieme è infinito sse è equipotente ad una sua parte propria.■

Esaminiamo infine una seconda relazione di equivalenza particolarmente significativa, la

RELAZIONE DI CONGRUENZA MODULO p IN Z

Fissiamo un $p \in \mathbb{N}$, numero primo. Definiamo $x, y \in \mathbb{Z}, x \equiv_p y \overset{def}{\Longleftrightarrow} \exists k \in \mathbb{Z}: x - y = kp$

PROPOSIZIONE: $\equiv_p$ è una relazione di equivalenza su $\mathbb{Z}$

DIMOSTRAZIONE

- Riflessività: $x \equiv_p x, \forall x? \, Si \; perch\grave{e} \; 0 = 0p$
- Simmetria: $x \equiv_p y \Rightarrow y \equiv_p x? \, Si \; perch\grave{e} \; x - y = kp \Leftrightarrow y - x = -kp$
- Transitività: $\left(x \equiv_p y \; e y \equiv_p z\right) \Rightarrow x \equiv_p z? \, Si \; perch\grave{e} \; x - y = kp \; e \; y - z = hp \Rightarrow x - z = x - y + y - z = kp + hp = (k + h)p$ ■

Dunque $\equiv_p$ è una relazione di equivalenza che chiameremo **relazione di congruenza mod. p.**

Chiameremo insieme quoziente

$$\mathbb{Z}/_{\equiv_p} = \left\{[x]_{\equiv_p}, x \in \mathbb{Z}\right\}$$

PROPOSIZIONE (caratterizzazione della congruenza modulo p come classi di resti modulo p)

$$x \equiv_p y \Leftrightarrow \text{x e y hanno lo stesso resto nella divisione per p}$$

$x, y \in \mathbb{Z}, x \equiv_p y \Rightarrow x - y = kp \Rightarrow q_1 p + r_1 - q_2 p - r_2 = (q_1 - q_2)p + r_1 - r_2 = kp \Rightarrow q_1 - q_2 = k,$
$r_1 - r_2 = 0$

Dunque $r_1 = r_2$.

Sia ora $\begin{matrix} x = q_1 p + r \\ y = q_1 p + r \end{matrix} \Rightarrow x - y = q_1 p + r - q_2 p - r = (q_1 - q_2)p \Leftrightarrow x \equiv_p y$ ■

$[x]_{\equiv_p} = \{y \in \mathbb{Z}: x - y = kp, k \in \mathbb{Z}\} = \{y = x + kp, k \in \mathbb{Z}\}$ Questa classe è fatta da infiniti elementi.

$[x]_{\equiv_p} \cap [y]_{\equiv_p} = \emptyset \; \boldsymbol{oppure} \; [x]_{\equiv_p} = [y]_{\equiv_p}$

$[0] = [0] \;\; [0] = \{0, p, -p - 2p, -2p, 3p, -3p, \dots\}$

$[1] = \{1, 1 + p, 1 - p, 1 + 2p, 1 - 2p, \dots\}$

$[2] = \{2, 2 + p, 2 - p, 2 + 2p, 2 - 2p, \dots\}$

$[p - 1] = \{p - 1, 2p - 1, -1, 3p - 1, -p - 1, \dots\}$

$[p] = [0] \;\; [p + 1] = [1]$

Ci sono esattamente p classi diverse, $\left|\mathbb{Z}/_{\equiv_p}\right| = p$

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

$[x] + [y] \overset{\text{def}}{=} [x + y]$ È ben posta? Ha senso?

TEOREMA

La definizione di somma tra classi di congruenza è ben posta, ossia $x \equiv_p y \; e \; z \equiv_p t, allora \; [x] + [y] \overset{\text{def}}{=} [x + z] = [y + t]$

DIMOSTRAZIONE

Sotto le ipotesi date bisogna provare che $[x + z] = [y + t]$. Sia dunque $w \in [x + z]$ e mostriamo che $w \in [y + t]$. Ora, $x \equiv_p y \Leftrightarrow y - x = hp, \; z \equiv_p t \Leftrightarrow \; t - z = lp,$ così

$w \in [x+z] \Leftrightarrow w - x - z = kp$ e dunque $w - y - t = w - x - hp - z - lp = (k - h - l)p$. Pertanto **La somma delle classi è uguale alla classe della somma.**■

TEOREMA

Se definiamo

$$[\boldsymbol{x}] \cdot [\boldsymbol{y}] \stackrel{\text{def}}{=} [\boldsymbol{xy}],$$

allora la definizione è ben posta, cioè $(\boldsymbol{x \equiv z\ e\ y \equiv t}) \Rightarrow [\boldsymbol{xy}] = [\boldsymbol{zt}]$

DIMOSTRAZIONE

Stessa idea della dimostrazione per la somma■

Dalla relazione di congruenza mod p si ricavano i consueti criteri di divisibilità per 3 e per 11.