Seminario

Cardinalità infinite

Ester Dalvit

25 gennaio 2005

prof. Sisto Baldo

Definire un insieme significa stabilire una regola secondo la quale per ogni oggetto dato si possa decidere se esso appartiene o meno all'insieme.

Prendiamo un insieme finito, cioè contenente un numero finito di elementi: possiamo dire quanti elementi esso contiene, cioè possiamo contarli. Contare significa stabilire una corrispondenza biunivoca tra oggetti (elementi dell'insieme) e simboli $1, 2, \ldots, n$. Questi simboli sono ciò che chiamiamo numeri: ogni numero naturale n è l'astrazione degli insiemi contenenti n oggetti.

Ma se consideriamo gli insiemi infiniti, non possiamo più *contarne* gli elementi, perchè, essendo infiniti, non finiremmo mai! Potremmo allora chiederci: gli insiemi infiniti sono tutti "grandi uguali"? Se non è così, dovremo trovare un altro modo per stabilire "quanto è grande" un insieme infinito.

Diamo una definizione rigorosa di insiemi finiti ed infiniti.

Definizione 1. *Sia $I_n := \{0, 1, 2, \ldots, n-1\}$ un segmento iniziale dei naturali. Un insieme X si dice finito se esiste un numero naturale n tale che gli elementi di X possono essere posti in corrispondenza biunivoca con gli elementi di I_n. Se non esiste un tale n, diremo che X è infinito.*

La seguente definizione vale sia per gli insiemi finiti che per quelli infiniti.

Definizione 2. *Due insiemi A e B hanno la stessa cardinalità (si dice anche che hanno lo stesso numero cardinale o che sono equivalenti o equipotenti) se esiste una corrispondenza biunivoca tra gli elementi di A e gli elementi di B. Ovvero se esiste una funzione $f : A \to B$ biiettiva.*

Diremo che un insieme finito ha cardinalità n se esiste una corrispondenza biunivoca tra i suoi elementi e gli elementi di I_n, ovvero se il nostro insieme contiene n elementi.

Sarà utile introdurre una relazione per confrontare gli insiemi.

Definizione 3. *Diremo che l'insieme A ha cardinalità minore dell'insieme B e scriveremo $\#(A) \leq \#(B)$ se esiste una funzione iniettiva $f : A \to B$.*

Dimostriamo prima di tutto che esiste un insieme con un numero infinito di elementi.

Teorema 1. *L'insieme $\mathbb{N}$ dei numeri naturali è infinito.*

Dimostrazione. Sia $I_n := \{1, 2, 3, \ldots, n\}$ l'insieme dei primi n numeri interi positivi.
Supponiamo per assurdo che $\mathbb{N}$ sia finito, cioè che per qualche n esista una funzione $f : \mathbb{N} \to I_n$ biiettiva.
Allora $f|_{I_n}$ è iniettiva e ha per immagine un sottoinsieme proprio di I_n. Quindi possiamo porre in corrispondenza biunivoca I_n con il suo sottoinsieme proprio

$f(I_n)$. Ma ciò è impossibile perchè I_n è un insieme finito, dunque ogni sottoinsieme proprio di I_n ha un numero di elementi strettamente minore del numero di elementi di I_n. $\square$

Ora, poichè i numeri naturali possono essere considerati un sottoinsieme degli interi, dei razionali, o dei reali, anche questi insiemi sono infiniti.

Insiemi numerabili

Vediamo alcune proprietà del più semplice insieme infinito che possiamo considerare, quello dei numeri naturali.

Definizione 4. *Un insieme si dice numerabile se ha la stessa cardinalità di* $\mathbb{N}$. *Indicheremo la cardinalità di* $\mathbb{N}$ *con il simbolo* $\aleph_0$.

Può essere utile rappresentare graficamente la corrispondenza biunivoca tra gli elementi di un insieme numerabile A e i numeri naturali.

Siano $a_0, a_1, a_2, \ldots, a_n, \ldots$ gli elementi dell'insieme A.

$$\begin{array}{cccccc} 0 & 1 & 2 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ a_0 & a_1 & a_2 & \cdots & a_n & \cdots \end{array}$$

Si vede banalmente che un insieme finito non può mai essere posto in corrispondenza biunivoca con una sua parte propria, perchè ha sempre un numero di elementi strettamente maggiore di ogni suo sottoinsieme proprio.

Questa proprietà non vale però per gli insiemi infiniti.

Un semplice esempio: possiamo vedere che l'insieme dei numeri naturali può essere posto in corrispondenza biunivoca con l'insieme dei numeri naturali positivi.

$$\begin{array}{cccccc} 0 & 1 & 2 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ 1 & 2 & 3 & \cdots & n+1 & \cdots \end{array}$$

Vediamo un esempio più interessante: l'insieme dei numeri pari, che è un sottoinsieme proprio dei naturali, è numerabile!

Per dimostrarlo basta porre la corrispondenza biunivoca $n \mapsto 2n$.

$$\begin{array}{cccccc} 0 & 1 & 2 & \cdots & n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ 0 & 2 & 4 & \cdots & 2n & \cdots \end{array}$$

Anche l'insieme $\mathbb{Z}$ dei numeri interi è numerabile. Basta considerare questa corrispondenza biunivoca tra i naturali e gli interi:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & \cdots & 2n-1 & 2n & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \\ 0 & 1 & -1 & 2 & -2 & \cdots & n & -n & \cdots \end{array}$$

Ricordiamo ora l'assioma della scelta, che utilizzeremo per dimostrare il prossimo teorema.

Assioma (della scelta). *Data una partizione $\mathcal{F}$ di un insieme E, esiste un sottoinsieme di E che ha uno e uno solo elemento in comune con ciascuno degli insiemi $F \in \mathcal{F}$.*
Una formulazione equivalente: dato un insieme E, chiamiamo $\mathcal{P}(E)$ l'insieme delle parti di E; allora esiste una funzione $\varphi : \mathcal{P}(E) \to E$, detta funzione di scelta, tale che per ogni $X \in \mathcal{P}(E)$ si ha $\varphi(X) \in X$.

Teorema 2. *Ogni insieme infinito contiene un sottoinsieme numerabile.*

Dimostrazione. Sia X un insieme infinito e sia $\varphi : \mathcal{P}(X) \to X$ una funzione di scelta per X.
Definiamo una successione di elementi di X:

$$\begin{aligned} a_0 &= \varphi(X) \\ a_n &= \varphi(X \setminus \{a_0, a_1, ..., a_{n-1}\}) \end{aligned}$$

Gli a_n sono distinti. L'insieme $X \setminus \{a_0, a_1, \dots, a_{n-1}\}$ non è vuoto per alcun n, poichè X è infinito. L'insieme $A = \{a_n : n \in \mathbb{N}\}$ è contenuto in X ed è numerabile. $\square$

Teorema 3. *Ogni insieme infinito può essere posto in corrispondenza biunivoca con una sua parte propria.*

Dimostrazione. Come abbiamo visto nell'esempio precedente, $\mathbb{N}$, e dunque ogni insieme numerabile, può essere posto in corrispondenza biunivoca con una sua parte propria.
Ora, sia X un insieme infinito qualsiasi; per il teorema 2 possiamo scrivere $X = A \cup \overline{A}$ dove A è un sottoinsieme numerabile di X e $\overline{A}$ è il complementare di A in X.
Definiamo una funzione iniettiva $f : X \to X$, data dall'identità su $\overline{A}$ e che mandi A in una sua parte propria. Allora f stabilisce una corrispondenza biunivoca tra X e una sua parte propria. $\square$

Teorema 4. *L'unione di una famiglia finita non vuota di insiemi numerabili* $A_0, A_1, \ldots, A_k$ *è un insieme numerabile.*

Dimostrazione. Sia $0 \leq s \leq k$ e $t \in \mathbb{N}$. Chiamiamo a_s^t l'elemento t-esimo dell'insieme A_s. Scriviamo gli elementi di ogni insieme in questo modo:

$$\begin{array}{ccccc} a_0^0 & a_0^1 & \cdots & a_0^n & \cdots \\ a_1^0 & a_1^1 & \cdots & a_1^n & \cdots \\ \vdots & \vdots & & \vdots & \\ a_k^0 & a_k^1 & \cdots & a_k^n & \cdots \end{array}$$

Si può stabilire una corrispondenza biunivoca tra gli elementi degli insiemi $A_0, A_1, \ldots, A_k$ e l'insieme $\mathbb{N}$, partendo da a_0^0 e leggendo in ordine la prima colonna, quindi la seconda, e così via. Questo vale se supponiamo che gli insiemi $A_0, A_1, \ldots, A_k$ siano a due a due disgiunti; in caso contrario è sufficiente saltare gli elementi già presenti. $\square$

Teorema 5. *L'unione di una famiglia numerabile di insiemi* $A_0, A_1, \ldots, A_n, \ldots$ *finiti e non vuoti, a due a due disgiunti, è un insieme numerabile.*

Dimostrazione. Sia k_s il numero di elementi dell'insieme A_s, dove s e k_s sono numeri naturali. Per numerare questa unione è sufficiente leggere gli elementi di ogni insieme uno dopo l'altro, cioè leggendo riga per riga:

$$\begin{array}{cccccc} a_0^0 & a_0^1 & \cdots & a_0^{k_0} & & \\ a_1^0 & a_1^1 & \cdots & \cdots & \cdots & a_1^{k_1} \\ \vdots & \vdots & & & & \\ a_n^0 & a_n^1 & \cdots & \cdots & a_n^{k_n} & \\ \vdots & \vdots & & & & \end{array}$$

In questo modo si può anche mostrare che togliendo l'ipotesi che gli insiemi $A_0, A_1, \ldots, A_n, \ldots$ siano a due a due disgiunti, la loro unione è al più numerabile. $\square$

Teorema 6. *Un sottoinsieme* B *di un insieme numerabile* A *è finito o numerabile.*

Dimostrazione. Supponiamo che B non sia finito; è sufficiente mostrare che B è numerabile. Ma questo è banale, in quanto B ha al massimo la stessa cardinalità di A essendo un suo sottoinsieme. $\square$

Teorema 7. *Una partizione* P *di un insieme numerabile* A *è finita o numerabile.*

Dimostrazione. Ogni insieme X della partizione contiene almeno un elemento di A. Dunque la cardinalità della partizione è al più uguale alla cardinalità di A, cioè P è al più numerabile, ovvero finito o numerabile. $\square$

Teorema 8. *L'insieme* $\mathbb{N} \times \mathbb{N}$ *è numerabile.*

Dimostrazione. Per ogni elemento (a, b) di $\mathbb{N} \times \mathbb{N}$, definiamo il "peso" $a + b = r$. Fissato un $r \in \mathbb{N}$, gli elementi di peso r sono in numero finito, esattamente $r + 1$. Possiamo ora vedere l'insieme $\mathbb{N} \times \mathbb{N}$ come unione di insiemi, ciascuno dei quali contiene tutti gli elementi (a, b) che hanno lo stesso peso $r \in \mathbb{N}$.

Questi insiemi sono finiti, non vuoti e a due a due disgiunti; inoltre si possono numerare, grazie all'indice r. Dunque per il Teorema 5 l'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile. $\square$

Teorema 9. *L'insieme* $\mathbb{Q}$ *dei numeri razionali è numerabile.*

Dimostrazione. Consideriamo l'insieme

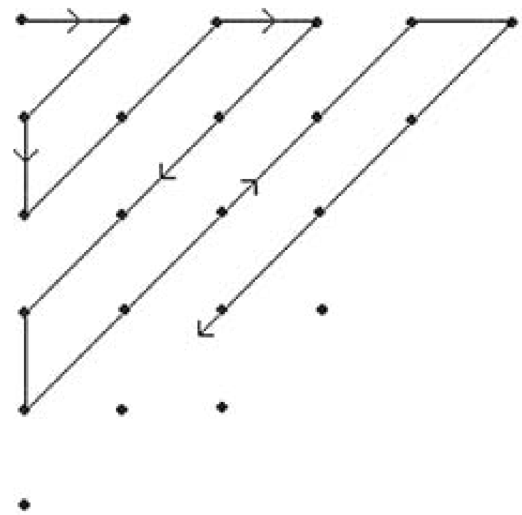
$$\mathbb{Z} \times \mathbb{Z}^* := \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$$

e introduciamo una relazione di equivalenza $\sim$ definita in questo modo: siano $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, si dice che (a, b) e (c, d) sono equivalenti, e si scrive $(a, b) \sim (c, d)$, se $(a, b) = p\ (c, d)$, dove $p \in \mathbb{Z}$.
Ogni numero razionale q si può identificare con una classe di equivalenza dell'insieme $\mathbb{Z} \times \mathbb{Z}^*$: possiamo infatti scrivere $q = \frac{a}{b}$, dove la frazione è ridotta ai minimi termini. Poichè l'insieme $\mathbb{Z}$ è numerabile, lo è anche l'insieme prodotto $\mathbb{Z} \times \mathbb{Z}^*$. Allora, per il teorema 7 l'insieme $\mathbb{Q}$ è finito o numerabile. Ma non è finito, poichè "contiene" tutti i numeri naturali, che sono infiniti; dunque l'insieme $\mathbb{Q}$ è numerabile. $\square$

Vediamo un modo per numerare i razionali. Ogni numero razionale positivo può essere scritto come $\frac{a}{b}$, dove a e b sono interi positivi. Possiamo scrivere questi numeri in una tabella, in modo che il numero $\frac{a}{b}$ si trovi nella riga a e nella colonna b, come in figura.

$$\begin{array}{cccccc}
1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \dots \\[1em]
2 & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \dots \\[1em]
3 & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \dots \\[1em]
4 & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \dots \\[1em]
\dots & \dots & \dots & \dots & \dots & \dots
\end{array}$$

Tracciamo ora una spezzata che tocchi tutti i numeri che abbiamo scritto, come in figura: partendo da 1 procediamo orizzontalmente fino ad incontrare $\frac{1}{2}$, quindi in diagonale fino a 2; ora scendiamo verticalmente fino a 3 e tracciamo la diagonale ascendente fino a $\frac{1}{3}$. Ora di nuovo tracciamo la linea orizzontale finchè incontriamo il prossimo numero, quindi scendiamo per la diagonale verso sinistra fino alla prima colonna, scendiamo verticalmente di un numero e torniamo a salire per la diagonale verso destra finchè raggiungiamo la prima riga. Ripetendo il procedimento riusciamo a coprire tutti i numeri scritti.



Percorrendo la spezzata che abbiamo tracciato otteniamo una successione

$$1, \frac{1}{2}, 2, 3, \frac{2}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, 4, 5, \frac{4}{2}, \frac{3}{3}, \ldots$$

In questa successione cancelliamo tutti i numeri $\frac{a}{b}$ in cui a e b hanno un fattore in comune. In questo modo otteniamo una successione in cui ogni razionale positivo appare una e una sola volta, ridotto ai minimi termini.

Per numerare i razionali, positivi e negativi, è sufficiente considerare la successione sopra ottenuta e, dopo ogni termine, inserire il suo opposto. Resta ancora lo zero, che non abbiamo considerato, ma basta aggiungerlo come termine iniziale.

Teorema 10. *L'unione di una famiglia numerabile di insiemi numerabili è numerabile.*

Dimostrazione. Siano B_k, per $k \in \mathbb{N}$, insiemi numerabili, e sia

$$A = \bigcup_{k=0}^{\infty} B_k$$

Si può scrivere $B_k = \{x_{k,n} : n \in \mathbb{N}\}$. Dunque $A = \{x_{k,n} : k, n \in \mathbb{N}\}$.
L'applicazione

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \rightarrow & A \\ (k, n) & \mapsto & x_{k,n} \end{array}$$

è suriettiva. Poichè l'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile, l'insieme A è finito o numerabile. Ma evidentemente A non può essere finito, dunque è numerabile. $\square$

La retta reale

Spostiamo ora la nostra attenzione sui numeri reali.

Dimostriamo che la retta reale è equipotente a un qualunque intervallo aperto sulla retta. La funzione

$$(-\tfrac{\pi}{2}, \tfrac{\pi}{2}) \to \mathbb{R}$$

$$x \mapsto \tan(x)$$

è invertibile. Dunque l'intervallo $(-\frac{\pi}{2}, \frac{\pi}{2})$ ha la stessa cardinalità di $\mathbb{R}$.

È facilissimo mostrare che intervalli aperti e limitati sono equipotenti: è sufficiente un "cambio di variabile", ovvero dati (a, b) e (c, d) con $a < b$ e $c < d$, consideriamo la funzione

$$x \quad \mapsto \quad \frac{d-c}{b-a}\, x + \frac{bc-ad}{b-a}$$

che è biiettiva.

Componendo le due funzioni, si ottiene che la retta reale è equipotente a un qualunque intervallo aperto e limitato.

Ora, una qualsiasi semiretta ha la stessa cardinalità di $\mathbb{R}$: infatti la funzione esponenziale $x \to e^x$ è biiettiva e manda la retta nella semiretta $(0, +\infty)$. Inoltre le semirette sono tutte equipotenti tra loro; infatti date due semirette, con un cambio di variabile si mettono in corrispondenza biunivoca i loro punti.

Allora la retta reale è equipotente a un qualunque intervallo aperto.

Lemma 1. *Se un insieme A si può porre in corrispondenza biunivoca con un suo sottoinsieme X, allora esso può essere posto in corrispondenza biunivoca con un qualunque sottoinsieme Y tale che $X \subset Y \subset A$.*

Dimostrazione. Per ipotesi, esiste un'applicazione biiettiva $f : A \to X$. Siano

$$E := Y \setminus X \qquad \text{e} \qquad F := A \setminus Y.$$

Poichè gli insiemi X, E ed F sono a due a due disgiunti, si ha

$$A = X \cup E \cup F \qquad Y = X \cup E$$

Poniamo:

$$f(X) = X_1 \quad f(E) = E_1 \quad f(F) = F_1$$

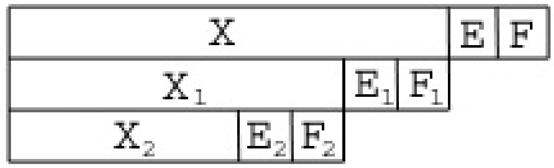
Allora $X = f(A) = X_1 \cup E_1 \cup F_1$ e, poichè f è biiettiva, gli insiemi X_1, E_1, F_1 sono disgiunti.

Ponendo, per ogni n intero positivo,

$$f^n(X) = X_n \quad f^n(E) = E_n \quad f^n(F) = F_n$$

si ha:

$$f^n(A) = f^{n-1}(f(A)) = f^{n-1}(X) = X_{n-1} = X_n \cup E_n \cup F_n$$



Indichiamo con M l'insieme $\bigcap_{k=1}^{\infty} X_k$. Sia $x \in X \setminus M$. Per come l'abbiamo preso, x non appartiene a tutti gli insiemi X_k, dunque esiste un indice $\overline{k}$ tale che $x \in Z_{\overline{k}}$ e $x \notin Z_{\overline{k}+1}$. Poichè $Z_{\overline{k}} = Z_{\overline{k}+1} \cup E_{\overline{k}+1} \cup F_{\overline{k}+1}$, x deve appartenere a $E_{\overline{k}+1}$ oppure a $F_{\overline{k}+1}$.

Dunque possiamo scrivere:

$$A = M \cup E \cup F \cup E_1 \cup F_1 \cup \cdots \cup E_n \cup F_n \cup \ldots$$

$$Y = M \cup E \cup F_1 \cup E_1 \cup F_2 \cup \cdots \cup E_n \cup F_{n+1} \cup \ldots$$

Ora, con questa scomposizione è facile costruire una applicazione biiettiva $g : A \to Y$. Sia $a \in A$; definiamo g nel modo seguente:

$$g(a) := \begin{cases} a & \text{se } a \in M \text{ o } a \in E_k \\ f(a) & \text{se } a \in F_n \end{cases}$$

Tenendo presente che $F_{n+1} = g(F_n)$, si vede facilmente che g è biiettiva. □

Teorema 11 (Bernstein). *Se è $\#(A) \leq \#(B)$ e $\#(B) \leq \#(A)$, allora vale $\#(A) = \#(B)$*

Di questo teorema diamo due dimostrazioni.

Dimostrazione. Per ipotesi, esistono due applicazioni iniettive

$$f : A \to B \quad \text{e} \quad g : B \to A.$$

Evidentemente si ha:

$$g \circ f(A) \subset g(B) \subset A.$$

Gli insiemi A e $g \circ f(A)$ sono posti in corrispondenza biunivoca. Allora, per il lemma 1, si può stabilire una corrispondenza biunivoca tra A e $g(B)$. Ma allora anche A e B si possono porre in corrispondenza biunivoca. □

Vediamo un'altra dimostrazione del teorema di Bernstein, più intuitiva.

Dimostrazione. Per ipotesi, esistono due applicazioni iniettive

$$f : A \to B \quad \text{e} \quad g : B \to A.$$

Vogliamo costruire una funzione invertibile $h : A \to B$.

Se $a \in A$, diremo che $b \in B$ è un genitore di a se $g(b) = a$. Analogamente, se $b \in B$, diremo che $a \in A$ è un genitore di b se $f(a) = b$. Poichè f e g sono iniettive, ogni elemento ha al più un genitore; inoltre ci possono essere elementi "orfani".

In questo modo, partendo da un elemento, possiamo risalire al genitore, quindi al genitore del genitore, e via dicendo. Possiamo avere tre casi diversi:

- arriviamo a un elemento in A senza genitore.
- arriviamo a un elemento in B senza genitore.
- ogni elemento possiede un genitore: risaliamo all'infinito.

Suddividiamo ciascuno dei due insiemi A e B in tre parti disgiunte:

$A_1 := \{a \in A : a \text{ è orfano o possiede un progenitore orfano in } A\}$
$A_2 := \{a \in A : a \text{ possiede un progenitore orfano in } B\}$
$A_3 := \{a \in A : a \text{ possiede una stirpe infinita di progenitori}\}$
$B_1 := \{b \in B : b \text{ possiede un progenitore orfano in } A\}$
$B_2 := \{b \in B : b \text{ è orfano o possiede un progenitore orfano in } B\}$
$B_3 := \{b \in B : b \text{ possiede una stirpe infinita di progenitori}\}$

Ora, la restrizione di f ad A_1 è una biiezione di A_1 in B_1, la restrizione di f ad A_3 è una biiezione di A_3 in B_3 e la restrizione di g ad A_2 è una biiezione di A_2 in B_2.

Per costruire la funzione biiettiva h cercata, basta porre:

$$h(a) = \begin{cases} f(a) & \text{se } a \in A_1 \cup A_3 \\ g^{-1}(a) & \text{se } a \in A_2 \end{cases}$$

dove con g^{-1} si intende l'inversa di g ristretta ad A_2. □

Una facile conseguenza del teorema di Bernstein: la retta reale $\mathbb{R}$ è equipotente a un qualsiasi intervallo chiuso $[a, b]$.

Sono sufficienti queste due funzioni: una funzione iniettiva di $[-\pi, \pi]$ in $\mathbb{R}$ è l'inclusione, mentre una funzione iniettiva di $\mathbb{R}$ in $[-\pi, \pi]$ è $x \mapsto \arctan x$.

Senza utilizzare il teorema di Bernstein, questa dimostrazione non è così immediata: infatti non è facile costruire una funzione invertibile tra un intervallo chiuso $[a, b]$ e $\mathbb{R}$ (vedi esercizi).

Veniamo ora ad un risultato importante: il seguente teorema, di cui verranno illustrate due dimostrazioni, afferma che esistono diverse cardinalità tra gli insiemi infiniti.

Teorema 12. *$\mathbb{R}$, l'insieme dei numeri reali, è non numerabile.*

Dimostrazione. (Dimostrazione data da Cantor) Per evitare la doppia scrittura di alcuni numeri, scriviamo i numeri reali che terminano con un infinito numero di cifre 9, in modo che terminino con infinite cifre 0, ovvero che abbiano un numero finito di cifre decimali. Ad esempio non scriviamo $0,1569999\ldots$, ma $0,157$.

Supponiamo per assurdo che $\mathbb{R}$ sia numerabile. Allora possiamo costruire una funzione biiettiva da $\mathbb{N}$ in $\mathbb{R}$, e dunque una funzione suriettiva da $\mathbb{N}$ in $(0,1)$. Otterremo una successione che contiene tutti i reali compresi tra 0 e 1:

$$\begin{array}{lll} 0 & \mapsto & 0,a_1a_2a_3a_4\ldots \\ 1 & \mapsto & 0,b_1b_2b_3b_4\ldots \\ 2 & \mapsto & 0,c_1c_2c_3c_4\ldots \\ 3 & \mapsto & 0,d_1d_2d_3d_4\ldots \\ \ldots & & \end{array}$$

Ora, se troviamo un numero α compreso tra 0 e 1 che non faccia parte dell'elenco, la funzione che supponevamo suriettiva non lo potrà essere, dunque $\mathbb{R}$ non sarà numerabile.

Sia $\alpha = 0,\alpha_1\alpha_2\alpha_3\alpha_4\ldots$ dove ogni cifra $\alpha_k \neq 9$ per $k \in \mathbb{N}$ e:

α_1 è diversa dalla prima cifra del primo numero	$\alpha_1 \neq a_1$
α_2 è diversa dalla seconda cifra del secondo numero	$\alpha_2 \neq b_2$
α_3 è diversa dalla terza cifra del terzo numero	$\alpha_3 \neq c_3$
$\ldots$	
α_k è diversa dalla k-esima cifra del k-esimo numero	

Il numero così costruito differisce da ogni numero nell'elenco per almeno una cifra. □

Dimostrazione. Anche questa dimostrazione è per assurdo. Supponiamo che l'insieme di tutti i punti del segmento reale $(0,1)$ possa essere posto in corrispondenza biunivoca con $\mathbb{N}$, cioè si possa scrivere una successione di punti $a_1, a_2, a_3, \ldots$ che contenga tutti i punti del segmento.

Ora racchiudiamo il punto di ascissa a_1 in un intervallo di ampiezza $\frac{1}{10}$, il punto di ascissa a_2 in un intervallo di ampiezza $\frac{1}{10^2}$, il punto di ascissa a_k in un intervallo di ampiezza $\frac{1}{10^k}$.

Poichè la successione $a_1, a_2, a_3, \ldots$ contiene tutti i punti compresi tra 0 e 1, l'intervallo unitario sarà interamente coperto dalla successione di sottointervalli, eventualmente sovrapposti, di ampiezza $\frac{1}{10}, \frac{1}{10^2}, \ldots$. L'unione di questi intervalli avrà ampiezza minore o uguale a

$$\frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots = \sum_{i=1}^{\infty} \frac{1}{10^i} = \frac{1}{10}\left(\frac{1}{1-\frac{1}{10}}\right) = \frac{1}{9}$$

Possiamo dunque coprire l'intervallo $(0,1)$ di lunghezza 1 con una successione di intervalli la cui unione ha al massimo lunghezza $\frac{1}{9}$, che è assurdo. □

Nello stesso modo possiamo dimostrare che un insieme numerabile di punti sulla retta ha misura nulla. Racchiudiamo il punto x_n in un intervallo di lunghezza $\frac{\epsilon}{10^n}$, per $n \in \mathbb{N}$ e con $\epsilon > 0$ piccolo a piacere. L'insieme dei punti può dunque essere contenuto in un'unione di intervalli di lunghezza totale al più

$$\frac{\epsilon}{10} + \frac{\epsilon}{10^2} + \frac{\epsilon}{10^3} + \cdots = \frac{\epsilon}{9}$$

che si può rendere arbitrariamente piccolo.

Analogamente si può dimostrare che un insieme numerabile di punti nel piano (in $\mathbb{R}^n$) ha misura nulla.

Definizione 5. *Si dice che B ha numero cardinale maggiore di A e si scrive $\#(A) < \#(B)$ se è $\#(A) \leq \#(B)$ e $\#(A) \neq \#(B)$.*

Finora abbiamo visto due "tipi" di infinito: gli insiemi numerabili e quelli con cardinalità pari alla cardinalità dei reali. È naturale chiedersi se vi siano altri "gradi" di infinito. Il seguente teorema risponde a questa domanda.

Teorema 13. *Per ogni insieme X, ne esiste uno di cardinalità maggiore: $\#(\mathcal{P}(X)) > \#(X)$.*

Dimostrazione. L'applicazione $x \mapsto \{x\}$ è iniettiva; dunque $\#(X) \leq \#(\mathcal{P}(X))$.

Ora è sufficiente dimostrare che non è $\#(X) = \#(\mathcal{P}(X))$. Per fare questo, mostreremo che non esistono applicazioni suriettive $X \to \mathcal{P}(X)$.

Ciò è evidente se X è vuoto.

Sia X non vuoto; sia ϕ un'applicazione $X \to \mathcal{P}(X)$. Consideriamo il sottoinsieme di X:

$$H := \{x : x \in X \text{ e } x \notin \phi(x)\} .$$

Affermo che H differisce da ciascuno degli insiemi $\phi(x)$; infatti, preso un $\overline{x} \in X$, se è $\overline{x} \in \phi(\overline{x})$ si ha $\overline{x} \notin H$ e viceversa, se $\overline{x} \in H$ si ha $\overline{x} \notin \phi(\overline{x})$. □

Un'immediata conseguenza: se X è un insieme numerabile, $\#(\mathcal{P}(X))$ non è numerabile.

Abbiamo visto che la cardinalità dei reali è maggiore di $\aleph_0$; a questo punto potremmo chiederci se esistano cardinalità intermedie.

Ipotesi (del continuo). *Non esiste alcuna cardinalità intermedia tra $\mathbb{N}$ e $\mathbb{R}$.*

In realtà, l'ipotesi del continuo è indecidibile: la sua verità dipende da quali assiomi si scelgono per la teoria degli insiemi.

Esercizi

Esercizio 1. Sia $\#(A) = \aleph_0$ e $\#(B) = \#(\mathbb{R})$. Si dimostri che

$$\#(A \cup B) = \#(\mathbb{R}).$$

Poichè $B \subset A \cup B$, vale $\#(A \cup B) \geq \#(B)$.

Ora è sufficiente dimostrare che $\#(A \cup B) \leq \#(B)$ e applicare il teorema di Bernstein. Cerchiamo dunque una funzione iniettiva

$$A \cup B \to B.$$

Ciò equivale a trovare una funzione iniettiva

$$\mathbb{N} \cup \mathbb{R} \to \mathbb{R},$$

ovvero

$$\mathbb{N} \cup (0, 1) \to \mathbb{R},$$

per cui basta considerare l'identità.

Esercizio 2. Come conseguenza del risultato precedente, dimostrare che

$$\#(\mathcal{P}(\mathbb{N})) = \#([0, 1]) = \#(\mathbb{R}).$$

Scriviamo ogni elemento X di $\mathcal{P}(\mathbb{N})$ in questo modo:

$$0, a_0 a_1 a_2 a_3 \dots$$

dove le cifre a_k assumono il valore 1 se $k \in X$, 0 altrimenti.

Ora scriviamo l'insieme $\mathcal{P}(\mathbb{N})$ come unione di due insiemi disgiunti:

- A, l'insieme degli elementi che terminano con infinite cifre 1, cioè l'insieme di quegli insiemi che contengono tutti i naturali maggiori di un certo valore;
- B, l'insieme degli altri insiemi: $B = \mathcal{P}(\mathbb{N}) \smallsetminus A$.

Si può porre una corrispondenza biunivoca tra l'intervallo $[0, 1)$ e l'insieme B, leggendo ogni elemento di B come un numero reale compreso tra 0 e 1, scritto in base binaria. Inoltre all'elemento $a = 0, 11111 \dots \in A$ si può far corrispondere il numero 1. In questo modo abbiamo stabilito una corrispondenza biunivoca tra l'intervallo $[0, 1]$ e l'insieme $B' := B \cup \{a\}$.

Sia $A' := A \smallsetminus \{a\}$. Consideriamo gli elementi di A' la cui ultima cifra diversa da 1 è la k-esima dopo la virgola, con $k \in \mathbb{N}^*$. Per ogni k, avremo un numero finito di questi elementi (precisamente 2^{k-1}, cioè tutte le permutazioni di due elementi, 0 e 1, su $k-1$). Allora possiamo scrivere A' come unione disgiunta di una famiglia numerabile di insiemi finiti e non vuoti; dunque, per il teorema 5, l'insieme A' è numerabile.

Ora, $\mathcal{P}(\mathbb{N}) = A' \cup B'$, dove $\#(A') = \aleph_0$ e $\#(B') = \#([0,1]) = \#(\mathbb{R})$. Dunque, per il risultato visto nell'esercizio precedente, si ha

$$\#(\mathcal{P}(\mathbb{N})) = \#(A' \cup B') = \#(\mathbb{R}).$$

Esercizio 3. Senza usare il teorema di Bernstein, costruendo esplicitamente una funzione biiettiva, dimostrare che

$$\#([a,b]) = \#((a,b)) = \#((a,b]) = \#([a,b)) = \#(\mathbb{R}).$$

Senza perdere di generalità, possiamo considerare l'intervallo $(0,1)$. Infatti un cambiamento di coordinate è dato dalla funzione biiettiva

$$\begin{array}{ccc} (0,1) & \to & (a,b) \\ x & \mapsto & a + x(b-a) \end{array}$$

Ovviamente $(0,1]$ e $[0,1)$ hanno la stessa cardinalità: infatti una funzione biiettiva $(0,1] \to [0,1)$ è l'applicazione identica su $(0,1)$ e che manda $1 \mapsto 0$.

Costruiamo una funzione biiettiva $f : (0,1] \to (0,1)$, suddividendo i due intervalli in una quantità numerabile di intervalli e punti.

$$f(x) = \begin{cases} \frac{1}{2^{i-1}} & \text{se } x = \frac{1}{2^i} \text{ per qualche } i \in \mathbb{N} \\ x & \text{altrimenti} \end{cases}$$

Abbiamo così dimostrato che $(0,1]$ e $(0,1)$ sono equipotenti.

Ora il gioco è fatto! Infatti "aggiungendo" un punto ad ognuno dei due intervalli precedenti, è immediato vedere che anche $[0,1]$ e $[0,1)$ hanno la stessa cardinalità.

Abbiamo già dimostrato che $\mathbb{R}$ ha la stessa cardinalità di ogni intervallo aperto: infatti la funzione

$$\left(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\right) \to \mathbb{R}$$

$$x \mapsto \tan(x)$$

è biiettiva. Con un intervallo aperto generico, basta considerare un cambio di variabile.

Allora vale

$$\#(\mathbb{R}) = \#((0,1)) = \#((0,1]) = \#([0,1)) = \#([0,1])$$

Esercizio 4. Dimostrare che le successioni a valori in $\mathbb{N}$ hanno la stessa cardinalità dell'intervallo $[0,1]$, ovvero $\#(\mathbb{N}^{\mathbb{N}}) = \#([0,1])$.

Vogliamo utilizzare il teorema di Bernstein. Per fare ciò, cerchiamo due funzioni iniettive $f : \mathbb{N}^{\mathbb{N}} \to [0,1]$ e $g : [0,1] \to \mathbb{N}^{\mathbb{N}}$.

Prendiamo una successione $\{a_i\}_{i \in \mathbb{N}}$ e scriviamo in notazione binaria i numeri $a_1, a_2, a_3, \ldots$ che la compongono. Definiamo f in questo modo:

$$f(a_1, a_2, a_3, \ldots) = 0, a_1\ 2\ a_2\ 2\ a_3\ 2\ \ldots.$$

Questa applicazione manda distinte successioni a valori naturali in distinti numeri reali decimali compresi tra 0 e 1; dunque è un'applicazione iniettiva.

Sia $x \in [0,1]$; allora si può scrivere $x = 0, a_1 a_2 a_3 \ldots$. Sia g definita come segue:

$$x = 0, a_1 a_2 a_3 \ldots \mapsto \{a_1, a_2, a_3, \ldots\};$$

è una funzione iniettiva.

Notiamo che questa funzione non è biiettiva, perchè ad esempio le successioni $0, 9, 9, 9, 9, 9, 9, \ldots$ e $1, 0, 0, 0, 0, 0, 0, \ldots$, che sono distinte, definiscono lo stesso numero reale $0, 1$.

Esercizio 5. Dimostrare che $\#(\mathbb{R}^2) = \#(\mathbb{R})$.

Poichè hanno la stessa cardinalità, possiamo considerare l'intervallo $(0,1)$ invece dell'insieme dei numeri reali.
Decidiamo che i numeri che finiscono con infinite cifre 9 si scrivano in modo unico come numeri con un numero finito di cifre decimali. Quindi il numero $0, a_1 a_2 \ldots a_k 9999 \ldots$ con $a_k \neq 9$, si scrive in questo modo: $0, a_1 a_2 \ldots a_k (a_k + 1)$.

Siano $0, a_1 a_2 a_3 \ldots,\ 0, b_1 b_2 b_3 \ldots \in (0,1)$. Definiamo la funzione biiettiva

$$\begin{gathered} \mathbb{R}^2 \to \mathbb{R} \\ (0, a_1 a_2 a_3 \ldots,\ 0, b_1 b_2 b_3 \ldots) \mapsto 0, a_1 b_1 a_2 b_2 \ldots a_k b_k \ldots \end{gathered}$$

Questo dimostra la tesi.

Esercizio 6. Sia $f : [a,b] \to \mathbb{R}$ una funzione monotona. Dimostrare che f ha al massimo una quantità numerabile di punti di discontinuità.
Trovare una funzione monotona che abbia esattamente una quantità numerabile di punti di discontinuità.

In ogni punto di discontinuità $\tilde{x}$ è definito il "salto" di f, ovvero

$$\left| \lim_{x \to \tilde{x}^+} f(x) - \lim_{x \to \tilde{x}^-} f(x) \right|$$

che è non nullo. Dunque, per la densità dei razionali nei reali, esiste un $q \in \mathbb{Q}$ che appartiene all'intervallo

$$\left(\lim_{x \to \tilde{x}^-} f(x), \lim_{x \to \tilde{x}^+} f(x) \right)$$

se f è crescente, mentre l'intervallo ha gli estremi scambiati se f è decrescente.

Ogni razionale identifica l'intervallo a cui appartiene, e dunque anche il punto di discontinuità corrispondente.

Allora il numero dei punti di discontinuità di f può avere al massimo la cardinalità dei razionali, ovvero essere numerabile.

Cerchiamo ora una funzione $f : [a, b] \to \mathbb{R}$ monotona che abbia esattamente una quantità numerabile di punti di discontinuità.

Sia $n \in \mathbb{N}$. Definiamo la funzione f nel modo seguente:

$$f(x) = \begin{cases} 2 & \text{se } \frac{b+a}{2} < x \leq b \\ 1 & \text{se } a + \frac{b-a}{4} < x \leq \frac{b+a}{2} \\ \vdots & \vdots \\ \frac{1}{n} & \text{se } a + \frac{b-a}{2^{n+1}} < x \leq \frac{b+a}{2^n} \\ \vdots & \vdots \\ 0 & \text{se } x = a \end{cases}$$

La funzione f è monotona decrescente, ed ha una quantità numerabile di punti di discontinuità; infatti per ogni $n \in \mathbb{N}$, f è discontinua in $\frac{1}{n}$.

Esercizio 7. L'insieme di Cantor C è un insieme compatto totalmente sconnesso, con $\#(C) = \#(\mathbb{R})$, ma la sua misura di Lebesgue è nulla $|C| = 0$.

Vediamo innanzitutto come si costruisce l'insieme di Cantor.

Prendiamo l'intervallo $[0, 1]$ e dividiamolo in tre sottointervalli uguali mediante i punti $\frac{1}{3}$ e $\frac{2}{3}$. Cancelliamo l'intervallo $(\frac{1}{3}, \frac{2}{3})$. Ora consideriamo ciascuno dei due intervalli $[0, \frac{1}{3}]$ e $[\frac{2}{3}, 1]$ e dividiamoli ciascuno in tre sottointervalli uguali, quindi cancelliamo il sottointervallo centrale.

Iterando il procedimento all'infinito, otteniamo quello che viene detto insieme di Cantor e denotato con C.

È facile vedere che C non è vuoto: infatti alcuni punti non vengono mai cancellati: ad esempio, restano 0, 1, $\frac{1}{3}$, ...

L'insieme di Cantor è limitato, poichè è contenuto nell'intervallo $[0,1]$; inoltre è chiuso perchè complementare di unione di aperti (gli intervalli che vengono "cancellati" nella costruzione). Dunque è compatto.

Valutiamo la sua misura di Lebesgue.

Nei successivi passaggi della costruzione, si toglie prima un intervallo lungo $\frac{1}{3}$, poi due intervalli lunghi $\frac{1}{9}$, quindi quattro intervalli lunghi $\frac{1}{27}$, e così via.

Dunque in totale si tolgono degli intervalli aperti per una lunghezza totale di

$$\sum_{i=0}^{\infty} \frac{2^i}{3^{i+1}} = \frac{1}{3}\frac{1}{1-\frac{2}{3}} = 1$$

Dunque ciò che resta misura 0, ovvero ha misura nulla!

Un altro modo di dimostrarlo è il seguente.

Diamo un nome all'insieme ottenuto dopo ogni passo: sia C_1 l'insieme che resta dopo la cancellazione dell'intervallo di lunghezza $\frac{1}{3}$, C_2 l'insieme che resta dopo la cancellazione degli intervalli di lunghezza $\frac{1}{9}$, ..., C_n l'insieme che resta dopo la cancellazione degli intervalli di lunghezza $\frac{1}{3^n}$.

La misura di questi insiemi sarà $|C_n| = \left(\frac{2}{3}\right)^n$.

Evidentemente, per ogni $n \in \mathbb{N}$, si ha $C \subset C_n$. Dunque vale $|C| \leq |C_n|$

Allora

$$0 \leq |C| \leq \lim_{n\to+\infty} |C_n| = \lim_{n\to+\infty} \left(\frac{2}{3}\right)^n = 0$$

cioè la misura di Lebesgue di C è nulla.

L'insieme di Cantor non contiene intervalli, ma solo punti isolati: per questo è totalmente sconnesso.

Dimostriamo ora che $\#(C) = \#(\mathbb{R})$.

Ovviamente, si ha $\#(C) \leq \#(\mathbb{R})$, perchè $C \subset \mathbb{R}$.

Prendiamo un punto dell'insieme C e scriviamolo come un numero reale in base 3 come $0, a_1a_2a_3\dots$, dove:

$$a_1 = \begin{cases} 0 & \text{se il punto è nell'intervallo a sinistra, ovvero in } [0, \frac{1}{3}] \\ 2 & \text{se il punto è nell'intervallo a destra, ovvero in } [\frac{2}{3}, 1] \end{cases}$$

$$a_2 = \begin{cases} 0 & \text{se il punto è nell'intervallo a sinistra, ovvero in } [0, \frac{1}{9}] \text{ o in } [\frac{2}{3}, \frac{7}{9}] \\ 2 & \text{se il punto è nell'intervallo a destra, ovvero in } [\frac{2}{9}, \frac{1}{3}] \text{ o in } [\frac{8}{9}, 1] \end{cases}$$

Procediamo così fino a scrivere tutte le infinite cifre decimali dei numeri reali associati ai punti dell'insieme di Cantor.

In altre parole, l'n-esima cifra decimale è 0 se il punto appartiene all'intervallo a sinistra nell'n-esima suddivisione, 2 se appartiene all'intervallo a destra.

Otteniamo un insieme di numeri reali in base ternaria, che identificano tutti i punti di C. Ovvero, ogni numero così trovato è un punto dell'insieme di Cantor e ogni punto di questo insieme viene rappresentato con uno dei numeri trovati.

Nessuno dei punti di C scritti in questo modo può contenere la cifra 1, a meno che non sia l'ultima cifra del numero. Infatti nessun punto può essere nell'intervallo centrale, che viene di volta in volta cancellato, però può trovarsi negli estremi dell'intervallo. Ad esempio $0,1$ appartiene a C perchè $0,1 = 0,0222222\ldots$.

Vogliamo ora trovare una funzione iniettiva $f : (0,1) \to C$.

Scriviamo i numeri reali nell'intervallo $(0,1)$ in base binaria. Ovviamente non consideriamo le scritture di numeri che terminano con infinite cifre 1.

Per ogni numero $b = 0, b_1 b_2 b_3 \ldots$, sia $f(b) = a = 0, a_1 a_2 a_3 \ldots$, dove per ogni $n \in \mathbb{N}$:

$$a_n = \begin{cases} 0 & \text{se } b_n = 0 \\ 2 & \text{se } b_n = 1 \end{cases}$$

Interpretando il numero a in base 3, esso definisce un punto dell'insieme di Cantor. f è iniettiva, dunque $\#(C) \geq \#((0,1)) = \#(\mathbb{R})$.

Allora, per il teorema di Bernstein, $\#(C) = \#(\mathbb{R})$.

Esercizio 8. Sia I un insieme di indici, non necessariamente numerabile. Sia $\{a_i\}_{i \in I}$ una successione generalizzata (funzione da I in $\mathbb{R}$) e $a_i \geq 0$ per ogni $i \in I$. Definiamo

$$S := \sum_{i \in I} a_i := \sup \left\{ \sum_{i \in I'} a_i : I' \subset I, I' \text{ finito} \right\}$$

Supponiamo inoltre che $S < +\infty$.
Dimostrare che $A := \{i \in I : a_i \neq 0\}$ è al più numerabile.

Fissiamo $n \in \mathbb{N}$. Supponiamo che esistano infiniti indici $i \in I$ per cui $a_i \geq \frac{1}{n}$. Allora $S = \sup \left\{ \sum_{i \in I'} a_i : I' \subset I, I' \text{ finito} \right\} = +\infty$.

Poichè nelle ipotesi S è finito, per ogni $n \in \mathbb{N}$ esiste solo un numero finito di indici $i \in I$ per cui $a_i \geq \frac{1}{n}$.

Duqnue per ogni $n \in \mathbb{N}$ gli indici i tali che $\frac{1}{n} \geq a_i \geq \frac{1}{n-1}$ sono in numero finito.

Allora A è formato da un numero finito di indici per ogni $n \in \mathbb{N}$, cioè è un'unione numerabile di insiemi finiti. Dunque è numerabile.

Riferimenti bibliografici

[1] R. Courant, H. Robbins, *Che cos'è la matematica?*, seconda edizione, Bollati Boringhieri, 2000. (pagg.122-129)

[2] G. Prodi, *Analisi Matematica 1*, Bollati Boringhieri (pagg. 61-67 e 82)

[3] Una lezione sulle cardinalità infinite *http://www-math.science.unitn.it/~baldo/aa2002/Diariossis/node4.html*

[4] Insieme di Cantor *http://en.wikipedia.org/wiki/Cantor_set*