Insiemi infiniti

1. Introduzione

Finché gli insiemi che si considerano sono finiti (cioè si può contare quanti sono i loro elementi mettendoli in corrispondenza biiettiva con i numeri che precedono un certo numero naturale) la nozione di insieme può fornire un comodo modo di esprimersi, ma non è indispensabile. Di fatto Cantor per primo elaborò la nozione di insieme per risolvere problemi di quantità di elementi in insiemi infiniti (cioè non finiti).

Definizione. Si dice che due classi *hanno la stessa cardinalità* quando c'è una biiettività tra le due classi. In tal caso si dirà anche che le due classi sono *equinumerose*.

Definizione. Si dice che un insieme A è *finito* se esistono un numero naturale n e una biiettività da A sull'insieme dei numeri naturali che precedono n; in questo caso diremo che A ha n elementi. Se ciò non succede, si dice che l'insieme è infinito.

Se un insieme A è finito e un altro insieme B è contenuto propriamente (contenuto ma non uguale) in A allora A e B non sono equinumerosi, cioè non c'è alcuna biiettività tra i due.

Questo risultato dipende dal fatto che per nessun numero naturale ci può essere una biiettività tra l'insieme dei numeri che lo precedono e l'insieme di quelli che precedono un diverso numero naturale.

L'ultima affermazione non si estende agli insiemi infiniti; lo giustifichiamo con un controesempio già considerato da Galileo Galilei nel suo *Dialogo sopra i due massimi sistemi del mondo*. I numeri pari sono un sottinsieme proprio dei numeri naturali, ed entrambi gli insiemi non sono finiti; inoltre la funzione che a un numero naturale associa il suo doppio è una biiettività dai numeri naturali sui numeri pari. Così si deve dire che i numeri naturali sono tanti quanti i numeri pari pur costituendo questi un sottinsieme proprio dell'insieme dei naturali.

Per gli insiemi finiti non solo si può dire se hanno lo stesso numero di elementi, ma anche se uno ha più elementi di un altro o meno. Per fare ciò ci si rifà alla relazione d'ordine naturale tra i numeri naturali che contano gli elementi di ciascuno dei due insiemi. Per gli insiemi infiniti non si può utilizzare lo stesso metodo. Come decidere allora quando un insieme ha più o meno elementi di un altro?

Ci si potrebbe limitare a dire che un insieme è finito o infinito. Tuttavia l'esperienza di vari insiemi infiniti porta naturalmente a domandarci se si può stabilire una gerarchia simile a quella fra gli insiemi finiti.

Prenderemo a modello le stesse proprietà degli insiemi finiti.

2. Cardinalità

Definizione 1. Siano A e B due insiemi. Diremo che la cardinalità dell'insieme A è minore o uguale a quella dell'insieme B, e scriveremo $|A| \leq |B|$ quando esiste una *funzione totale iniettiva* di A in B.

Questa relazione fra insiemi non è un ordine, né stretto né largo. Non è stretto perché $|A| \leq |A|$, per motivi ovvi (basta considerare la funzione identità). Non è un ordine largo, perché può accadere che $|A| \leq |B|$ e anche $|B| \leq |A|$, con $A \neq B$. Un esempio è proprio quello in cui A è l'insieme dei numeri naturali e B quello dei numeri naturali pari.

Scopo di queste note è di studiare le proprietà di questa relazione. Attraverso essa potremo arrivare al concetto di "uguale cardinalità", che è ciò che ci interessa.

Esempi. (1) Se A è un insieme e $B \subseteq A$, allora $|B| \leq |A|$.

(2) Se $\mathbb{Z}$ è l'insieme dei numeri interi e $\mathbb{N}$ quello dei numeri naturali, allora $|\mathbb{Z}| \leq |\mathbb{N}|$. Ciò può apparire paradossale, ma vedremo che non lo è.

Consideriamo infatti la seguente funzione:

$$f(x) = \begin{cases} 2x & \text{se } x \geq 0, \\ -2x-1 & \text{se } x < 0. \end{cases}$$

Si può facilmente verificare che $f\colon \mathbb{Z} \to \mathbb{N}$ è non solo iniettiva, ma anche suriettiva.

(3) Se X è un insieme finito e Y è un insieme infinito, allora $|X| \leq |Y|$.

Supponiamo che X abbia n elementi. Faremo induzione su n.

Se $n = 0$, la funzione vuota è quella che cerchiamo.

Supponiamo la tesi vera per insiemi con n elementi e supponiamo che X abbia $n+1$ elementi: $X = \{x_1, \dots, x_n, x_{n+1}\}$. Per ipotesi induttiva esiste una funzione totale iniettiva $f\colon \{x_1, \dots, x_n\} \to Y$. Siccome Y è infinito, esiste un elemento $y \notin \operatorname{Im}(f)$ (altrimenti Y avrebbe n elementi). Possiamo allora definire una funzione totale iniettiva $g\colon X \to Y$ che estende f ponendo $g(x_{n+1}) = y$.

Diamo subito la definizione che ci interessa maggiormente.

Definizione 2. Siano A e B due insiemi. Diremo che A e B *hanno la stessa cardinalità*, e scriveremo $|A| = |B|$, quando esiste una funzione biiettiva (totale) di A su B.

Non daremo la definizione di cardinalità, per la quale occorrerebbe molta più teoria e che non ci servirà. Sarà più rilevante per noi scoprire le connessioni fra le due relazioni introdotte.

3. Proprietà della cardinalità di insiemi infiniti

(C1) Se A è un insieme, allora $|A| = |A|$.
(C2) Se A e B sono insiemi e $|A| = |B|$, allora $|B| = |A|$.
(C3) Se A, B e C sono insiemi, $|A| = |B|$ e $|B| = |C|$, allora $|A| = |C|$.

Queste tre proprietà sono quasi ovvie: basta, nel primo caso, considerare la funzione identità; nel secondo si prende la funzione inversa della biiettività $A \to B$; nel terzo si prende la composizione fra la biiettività $A \to B$ e la biiettività $B \to C$.

(M1) Se A è un insieme, allora $|A| \leq |A|$.
(M2) Se A, B e C sono insiemi, $|A| \leq |B|$ e $|B| \leq |C|$, allora $|A| \leq |C|$.

La dimostrazione di queste due è facile (esercizio).

C'è un legame fra le due relazioni? La risposta è sì e sta proprio nella "proprietà antisimmetrica" che sappiamo non valere per $\leq$.

Il risultato che enunceremo ora è uno fra i più importanti della teoria degli insiemi e risale allo stesso Cantor, poi perfezionato da altri studiosi.

Teorema 1 (Cantor, Schröder, Bernstein). *Siano A e B insiemi tali che $|A| \leq |B|$ e $|B| \leq |A|$, allora*

$$|A| = |B|.$$

Dimostrazione. L'ipotesi dice che esistono una funzione $f\colon A \to B$ iniettiva totale e una funzione $g\colon B \to A$ iniettiva totale.

Per completare la dimostrazione dobbiamo trovare una funzione biiettiva $h\colon A \to B$.

Un elemento $a \in A$ ha un *genitore* se esiste un elemento $b \in B$ tale che $g(b) = a$. Analogamente diremo che un elemento $b \in B$ ha un genitore se esiste $a \in A$ tale che $f(a) = b$.

Siccome f e g sono iniettive, il genitore di un elemento, se esiste, è unico.

Dato un elemento $a \in A$ oppure $b \in B$, possiamo avviare una procedura:

(a) poniamo $x_0 = a$ o, rispettivamente $x_0 = b$ e $i = 0$;
(b) se x_i non ha genitore, ci fermiamo;
(c) se x_i ha genitore, lo chiamiamo x_{i+1}, aumentiamo di uno il valore di i e torniamo al passo (b).

Partendo da un elemento $a \in A$, possono accadere tre casi:

- la procedura non termina; scriveremo che $a \in A_0$;

- la procedura termina in un elemento di A; scriveremo che $a \in A_A$;
- la procedura termina in un elemento di B; scriveremo che $a \in A_B$.

Analogamente, partendo da un elemento $b \in B$, possono accadere tre casi:

- la procedura non termina; scriveremo che $b \in B_0$;
- la procedura termina in un elemento di A; scriveremo che $b \in B_A$;
- la procedura termina in un elemento di B; scriveremo che $b \in B_B$.

Abbiamo diviso ciascuno degli insiemi A e B in tre sottoinsiemi a due a due disgiunti: $A = A_0 \cup A_A \cup A_B$, $B = B_0 \cup B_A \cup B_B$.

Se prendiamo un elemento $a \in A_0$, è evidente che $f(a) \in B_0$, perché, per definizione, a è genitore di $f(a)$. Dunque f induce una funzione $h_0 \colon A_0 \to B_0$, dove $h_0(a) = f(a)$. Questa funzione, essendo una restrizione di f, è iniettiva e anche totale. È suriettiva, perché, se $b \in B_0$, esso ha un genitore a che deve appartenere ad A_0.

Se prendiamo un elemento $a \in A_A$, allora $f(a) \in B_A$: infatti a è genitore di $f(a)$ e la procedura, a partire da $b = f(a)$ termina in A. Dunque f induce una funzione $h_A \colon A_A \to B_A$ che è iniettiva e totale. Essa è anche suriettiva, perché ogni elemento di B_A ha genitore che deve appartenere ad A_A.

Analogamente, se partiamo da un elemento $b \in B_B$, allora $g(b) \in A_B$ e g induce una funzione iniettiva e totale $h_B \colon B_B \to A_B$ che è suriettiva, esattamente per lo stesso motivo di prima.

Ci resta da porre $h = h_0 \cup h_A \cup h_B^{-1}$. Allora h è una funzione $h \colon A \to B$ che è totale, iniettiva e suriettiva (lo si verifichi). $\square$

Esempio. Illustriamo la dimostrazione precedente con la seguente situazione: sia $f \colon \mathbb{N} \to \mathbb{Z}$ la funzione inclusione; consideriamo poi la funzione $g \colon \mathbb{Z} \to \mathbb{N}$

$$g(z) = \begin{cases} 4z & \text{se } z \geq 0, \\ -4z - 2 & \text{se } z < 0. \end{cases}$$

Quali sono gli elementi di $\mathbb{N}$ che hanno un genitore? Esattamente quelli che appartengono all'immagine di g, cioè i numeri pari. I numeri dispari, quindi, appartengono a $\mathbb{N}_{\mathbb{N}}$, perché la procedura si ferma a loro stessi.

Consideriamo $x_0 = 2 \in \mathbb{N}$; siccome $g(-1) = 2$, abbiamo $x_1 = -1$; poiché $-1 \notin \operatorname{Im}(f)$, la procedura si ferma e $2 \in \mathbb{N}_{\mathbb{Z}}$.

Consideriamo invece $x_0 = 4 \in \mathbb{N}$; siccome $g(1) = 4$, abbiamo $x_1 = 1$ e possiamo andare avanti, perché $1 = f(1)$, dunque $x_2 = 1 \in \mathbb{N}$. Poiché $1 \notin \operatorname{Im}(g)$, abbiamo che $4 \in \mathbb{N}_{\mathbb{N}}$.

Studiamo ora $x_0 = 16 \in \mathbb{N}$; siccome $g(4) = 16$, abbiamo $x_1 = 4$; siccome $f(4) = 4$, abbiamo $x_2 = 4 \in \mathbb{N}$; siccome $4 = g(1)$, abbiamo $x_3 = 1 \in \mathbb{Z}$; siccome $1 = f(1)$, abbiamo $x_4 = 1 \in \mathbb{N}$. La procedura si ferma qui, dunque $16 \in \mathbb{N}_{\mathbb{N}}$.

Si lascia al lettore l'esame di altri elementi di $\mathbb{N}$ o di $\mathbb{Z}$.

La relazione $\leq$ si può allora vedere non come una relazione d'ordine largo fra insiemi, ma piuttosto come un ordine largo fra le "cardinalità" degli insiemi. Non vogliamo però definire il concetto di cardinalità; ci limiteremo a confrontarle usando le relazioni introdotte.

Il teorema seguente dice, in sostanza, che la cardinalità dell'insieme dei numeri naturali è la più piccola cardinalità infinita.

Teorema 2. *Sia A un insieme infinito. Allora* $|\mathbb{N}| \leq |A|$.

Dimostrazione. Costruiremo un sottoinsieme di A per induzione.

Siccome A è infinito, esso non è vuoto; sia $x_0 \in A$. Evidentemente $\{x_0\} \neq A$, quindi esiste $x_1 \in A \setminus \{x_0\}$. Ancora $\{x_0, x_1\} \neq A$, quindi esiste $x_2 \in A \setminus \{x_0, x_1, x_2\}$.

Proseguiamo allo stesso modo: supponiamo di avere scelto gli elementi $x_0, x_1, \dots, x_n \in A$, a due a due distinti. Siccome $\{x_0, \dots, x_n\} \neq A$, esiste

$$x_{n+1} \in A \setminus \{x_0, \dots, x_n\}.$$

Dunque la procedura associa a ogni numero naturale un elemento di A e la funzione $n \mapsto x_n$ è iniettiva. $\square$

Questo risultato ha una conseguenza immediata.

Corollario 3. *Sia $A \subseteq \mathbb{N}$. Allora A è finito oppure $|A| = |\mathbb{N}|$.*

Dimostrazione. Se A non è finito, allora è infinito. Per il teorema, $|\mathbb{N}| \leq |A|$. Ma $|A| \leq |\mathbb{N}|$ perché $A \subseteq \mathbb{N}$. Per il teorema di Cantor-Schröder-Bernstein, $|A| = |\mathbb{N}|$. □

Un altro corollario è la caratterizzazione che Dedekind prese come definizione di insieme infinito.

Corollario 4. *Un insieme A è infinito se e solo se esiste un sottoinsieme proprio $B \subset A$ tale che $|B| = |A|$.*

Dimostrazione. Se A è finito, è evidente che un suo sottoinsieme proprio non può avere tanti elementi quanti A.

Supponiamo ora che A sia infinito. Per il corollario precedente, esiste una funzione iniettiva totale $f\colon \mathbb{N} \to A$. Definiamo ora una funzione $g\colon A \to A$ ponendo:

$$g(x) = \begin{cases} f(n+1) & \text{se esiste } n \in \mathbb{N} \text{ tale che } x = f(n), \\ x & \text{se } x \notin \operatorname{Im}(f). \end{cases}$$

La condizione "esiste $n \in \mathbb{N}$ tale che $x = f(n)$" equivale alla condizione "$x \in \operatorname{Im}(f)$".

La funzione g è ben definita, perché f è iniettiva; dunque, se $x = f(n)$ per qualche n, questo n è unico. Osserviamo anche che $x \in \operatorname{Im}(f)$ se e solo se $g(x) \in \operatorname{Im}(f)$.

Verifichiamo che g è totale e iniettiva. Il fatto che sia totale è ovvio. Supponiamo che $g(x) = g(y)$.

- Se $x \notin \operatorname{Im}(f)$, allora $g(x) = x$; dunque non può essere $y \in \operatorname{Im}(f)$ e perciò $g(y) = y$, da cui $x = y$.
- Se $x \in \operatorname{Im}(f)$, è $x = f(n)$ per un unico $n \in \mathbb{N}$. Allora $g(x) = f(n+1) \in \operatorname{Im}(f)$. Perciò $g(y) = g(x) = f(n+1) \in \operatorname{Im}(f)$ e quindi, per quanto osservato prima, $y \in \operatorname{Im}(f)$. Ne segue che $y = f(m)$ per un unico $m \in \mathbb{N}$ e $g(y) = f(m+1)$.

  Abbiamo allora $f(n+1) = f(m+1)$ e, siccome f è iniettiva, $n+1 = m+1$; perciò $n = m$ e $x = f(n) = f(m) = y$.

Qual è l'immagine di g? È chiaro che $f(0) \notin \operatorname{Im}(g)$. Viceversa, ogni elemento di $A \setminus \{f(0)\}$ appartiene all'immagine di g, cioè $\operatorname{Im}(g) = A \setminus \{f(0)\}$. Se allora consideriamo la funzione g come una funzione $g\colon A \to A \setminus \{f(0)\}$, questa è una biiettività.

In definitiva $|A| = |A \setminus \{f(0)\}|$; se poniamo $B = A \setminus \{f(0)\}$, abbiamo il sottoinsieme cercato. □

Notiamo che, nella dimostrazione precedente, $A \setminus B = \{f(0)\}$ è finito. Come esercizio si trovi in modo analogo al precedente un sottoinsieme $C \subset A$ tale che $|C| = |A|$ e $A \setminus C$ sia infinito.

4. Insiemi numerabili

Il teorema secondo il quale per ogni insieme infinito A si ha $|\mathbb{N}| \leq |A|$ ci porta ad attribuire un ruolo speciale a $\mathbb{N}$ (più precisamente alla sua cardinalità).

Definizione 3. Un insieme A si dice *numerabile* se $|A| = |\mathbb{N}|$.

Un sottoinsieme di $\mathbb{N}$ è allora finito o numerabile. Abbiamo già visto in precedenza che anche $\mathbb{Z}$ (insieme dei numeri interi) è numerabile.

Più in generale possiamo enunciare alcune proprietà degli insiemi numerabili.

Teorema 5. *Se A è finito e B è numerabile, allora $A \cup B$ è numerabile.*

Dimostrazione. Se $A \subseteq B$, l'affermazione è ovvia. Siccome

$$A \cup B = (A \setminus B) \cup B$$

possiamo supporre che A e B siano disgiunti, sostituendo A con $A \setminus B$ che è finito.

Possiamo allora scrivere $A = \{a_0, \dots, a_{m-1}\}$ e considerare una biiettività $g\colon \mathbb{N} \to B$. Definiamo una funzione $f\colon \mathbb{N} \to A \cup B$ ponendo

$$f(n) = \begin{cases} a_n & \text{se } 0 \leq n < m, \\ g(n-m) & \text{se } n \geq m. \end{cases}$$

È facile verificare che f è una biiettività. □

TEOREMA 6. *Se A e B sono numerabili, allora $A \cup B$ è numerabile.*
Se A_1, A_2,..., A_n sono insiemi numerabili, allora $A_1 \cup A_2 \cup \dots \cup A_n$ è un insieme numerabile.

DIMOSTRAZIONE. La seconda affermazione segue dalla prima per induzione (esercizio).
Vediamo la prima. Supponiamo dapprima che $A \cap B = \emptyset$. Abbiamo due biiettività $f \colon \mathbb{N} \to A$ e $g \colon \mathbb{N} \to B$. Definiamo una funzione $h \colon \mathbb{N} \to A \cup B$ ponendo:

$$h(n) = \begin{cases} f\left(\dfrac{n}{2}\right) & \text{se } n \text{ è pari,} \\ g\left(\dfrac{n-1}{2}\right) & \text{se } n \text{ è dispari.} \end{cases}$$

Si verifichi che h è una biiettività.
In generale, possiamo porre

$$A' = A \setminus (A \cap B), \qquad B' = B \setminus (A \cap B)$$

e abbiamo $A \cup B = A' \cup (A \cap B) \cup B'$; questi tre insiemi sono a due a due disgiunti. I casi possibili sono i seguenti:
(1) A', $A \cap B$ e B' sono infiniti;
(2) A' è finito, $A \cap B$ è infinito, B' è infinito;
(3) A' è finito, $A \cap B$ è infinito, B' è finito;
(4) A' è infinito, $A \cap B$ è infinito, B' è finito;
(5) A' è infinito, $A \cap B$ è finito, B' è infinito;
(6) A' è infinito, $A \cap B$ è finito, B' è finito.
Ci basta applicare quanto appena dimostrato e il teorema precedente.
Si concluda la dimostrazione per induzione della seconda affermazione. □

Il prossimo teorema può essere sorprendente. Un modo breve per enunciarlo è dire: *L'unione di un insieme numerabile di insiemi numerabili è numerabile.*

TEOREMA 7. *Per ogni $n \in \mathbb{N}$, sia A_n un insieme numerabile e supponiamo che, per $m \neq n$, $A_m \cap A_n = \emptyset$. Allora*

$$A = \bigcup \{\, A_n : n \in \mathbb{N} \,\}$$

è numerabile.

DIMOSTRAZIONE. Per questa dimostrazione ci serve sapere che la successione dei numeri primi $p_0 = 2$, $p_1 = 3$, $p_2 = 5$,..., è infinita.
Sia, per ogni $n \in \mathbb{N}$, $g_n \colon A_n \to \mathbb{N}$ una funzione biiettiva. Se $x \in A$, esiste un unico $n \in \mathbb{N}$ tale che $x \in A_n$; poniamo $j(x) = n$. Definiamo allora

$$f(x) = p_{j(x)}^{g_{j(x)}(x)}.$$

Per esempio, se $x \in A_2$, sarà $f(x) = 5^{g_2(x)}$. La funzione $f \colon A \to \mathbb{N}$ è iniettiva; quindi $|A| \leq |\mathbb{N}|$. Ma $A_0 \subseteq A$ e quindi

$$|\mathbb{N}| = |A_0| \leq |A| \leq |\mathbb{N}|.$$

Per il teorema di Cantor-Schröder-Bernstein, $|A| = |\mathbb{N}|$. □

Il teorema si può estendere anche al caso in cui gli insiemi A_n non sono a due a due disgiunti; si provi a delinearne una dimostrazione.
Questo teorema ha una conseguenza sorprendente.

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

DIMOSTRAZIONE. Poniamo $A_n = \{\, (m, n) : m \in \mathbb{N} \,\}$. Gli insiemi A_n sono a due a due disgiunti e ciascuno è numerabile. È evidente che $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N} \times \mathbb{N}$. □

Ancora più sorprendente è forse quest'altro fatto.

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

Dimostrazione. Un numero razionale positivo si scrive in uno e un solo modo come m/n, con $m, n \in \mathbb{N}$ primi fra loro (cioè aventi massimo comune divisore uguale a 1). Ne segue che l'insieme $\mathbb{Q}'$ dei numeri razionali positivi è numerabile, perché a m/n (con m e n primi fra loro) possiamo associare la coppia $(m, n) \in \mathbb{N} \times \mathbb{N}$ e la funzione così ottenuta è iniettiva. Dunque

$$|\mathbb{N}| \leq |\mathbb{Q}'| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$

L'insieme $\mathbb{Q}''$ dei numeri razionali negativi è numerabile, perché la funzione $f\colon \mathbb{Q}' \to \mathbb{Q}''$ definita da $f(x) = -x$ è chiaramente biiettiva. Per concludere, possiamo applicare altri teoremi precedenti, tenendo conto che

$$\mathbb{Q} = \mathbb{Q}' \cup \{0\} \cup \mathbb{Q}''. \qquad \square$$

C'è un altro modo per convincersi che $\mathbb{Q}'$ è numerabile, illustrato nella figura 1. Si

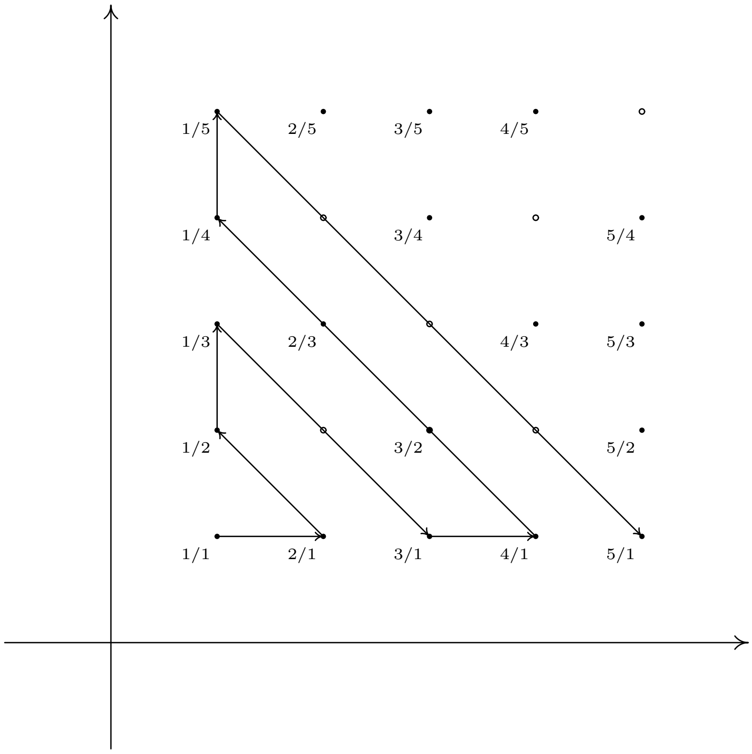

Figura 1. Enumerazione dei razionali positivi

immagina una griglia dove segniamo tutte le coppie con coordinate intere positive. Possiamo percorrere tutta la griglia secondo il percorso indicato e associare in questo modo a ogni numero naturale un numero razionale, incontrandoli tutti. Trascuriamo naturalmente i punti in cui il quoziente fra ascissa e ordinata è un numero razionale già incontrato precedentemente (per esempio, nella prima diagonale si trascura il punto $(2, 2)$ che corrisponderebbe al numero razionale $2/2 = 1$, già incontrato come $1/1$; nella terza diagonale si trascurano $(2, 4)$, $(3, 3)$ e $(4, 2)$).

5. Esistenza di cardinalità

A questo punto sorge naturale la domanda se ci sono insiemi infiniti di un'infinità diversa da quella dei numeri naturali. Non ci siamo riusciti nemmeno considerando l'insieme dei razionali che, intuitivamente, dovrebbe avere più elementi dei numeri naturali.

C'è una costruzione che produce cardinalità maggiori. Prima però definiamo con precisione ciò che intendiamo.

Definizione 4. Se A e B sono insiemi, diciamo che *A ha cardinalità minore della cardinalità di B*, e scriviamo $|A| < |B|$, se $|A| \leq |B|$, ma non è vero che $|A| = |B|$.

Il modo corretto per verificare che $|A| < |B|$ è questo:

- *esiste* una funzione totale iniettiva di A in B;
- *non esiste* una biiettività di A su B.

Notiamo che non basta verificare che una funzione iniettiva totale di A in B non è suriettiva. Per esempio, esiste certamente una funzione totale iniettiva di $\mathbb{N}$ in $\mathbb{Q}$ che non è suriettiva; tuttavia, come abbiamo visto, $|\mathbb{N}| = |\mathbb{Q}|$. Un altro esempio: l'insieme $\mathbb{N} \cup \{-2\}$ è numerabile, anche se la funzione di inclusione $\mathbb{N} \to \mathbb{N} \cup \{-2\}$ non è suriettiva. Infatti la funzione $f\colon \mathbb{N} \to \mathbb{N} \cup \{-2\}$ definita da $f(0) = -2$ e $f(n) = n - 1$ per $n > 0$ è una biiettività.

L'idea per trovare un insieme di cardinalità maggiore partendo da un insieme X è dovuta a Cantor.

Teorema 10 (Cantor). *Se X è un insieme, allora $|X| < |P(X)|$.*

Dimostrazione. Dimostriamo che esiste una funzione totale iniettiva $X \to P(X)$; essa è, per esempio,

$$\{\, (x, \{x\}) : x \in X \,\}$$

cioè la funzione che all'elemento $x \in X$ associa il sottoinsieme $\{x\} \in P(X)$.

Dobbiamo ora dimostrare che non esistono funzioni biiettive di X su $P(X)$. Lo faremo per assurdo, supponendo che $g\colon X \to P(X)$ sia biiettiva. Consideriamo

$$C = \{\, x \in X : x \notin g(x) \,\}.$$

La definizione di C ha senso, perché $g(x)$ è un sottoinsieme di X, dunque si hanno sempre due casi: $x \in g(x)$ oppure $x \notin g(x)$.

Siccome, per ipotesi, g è suriettiva, deve esistere un elemento $c \in X$ tale che $C = g(c)$.

Dunque si ha $c \in C$ oppure $c \notin C$.

Supponiamo $c \in C$; allora $c \in g(c)$ e quindi, per definizione di C, $c \notin C$: questo è assurdo.

Supponiamo $c \notin C$; allora $c \notin g(c)$ e quindi, per definizione di C, $c \in C$: assurdo.

Ne concludiamo che l'ipotesi che g sia suriettiva porta a una contraddizione. Perciò nessuna funzione di X in $P(X)$ è suriettiva. □

L'insieme $P(X)$ ha la stessa cardinalità di un altro importante insieme. Indichiamo con 2^X l'insieme delle funzioni totali di X in $\{0, 1\}$.

Definizione 5. Se A è un sottoinsieme di X, la *funzione caratteristica di A* è la funzione $\chi_A\colon X \to \{0, 1\}$ definita da

$$\chi_A(x) = \begin{cases} 1 & \text{se } x \in A, \\ 0 & \text{se } x \notin A. \end{cases}$$

Possiamo definire due funzioni, $f\colon P(X) \to 2^X$ e $g\colon 2^X \to P(X)$ nel modo seguente: per $A \in P(X)$ si pone $f(A) = \chi_A$; per $\varphi \in 2^X$ si pone

$$g(\varphi) = \{\, x \in X : \varphi(x) = 1 \,\}.$$

Teorema 11. *Per ogni insieme X si ha $|P(X)| = |2^X|$.*

Dimostrazione. Proveremo che $g \circ f$ e $f \circ g$ sono funzioni identità.

Sia $A \in P(X)$; dobbiamo calcolare $g(f(A)) = g(\chi_A)$: abbiamo

$$g(\chi_A) = \{\, x \in X : \chi_A(x) = 1 \,\} = A,$$

per definizione di χ_A.

Sia $\varphi \in 2^X$; dobbiamo calcolare $f(g(\varphi))$. Poniamo $B = g(\varphi) = \{\, x \in X : \varphi(x) = 1 \,\}$. Occorre verificare che $\varphi = \chi_B$. Sia $x \in X$; se $\varphi(x) = 1$, allora $x \in B$ e quindi $\chi_B(x) = 1$; se $\varphi(x) = 0$, allora $x \notin B$ e quindi $\chi_B(x) = 0$. Non essendoci altri casi, concludiamo che $\varphi = \chi_B$.

Ora, siccome per ogni $A \in P(X)$ si ha $A = g(f(A))$, g è suriettiva e f è iniettiva. Analogamente, per $\varphi \in 2^X$, $\varphi = f(g(\varphi))$ e dunque f è suriettiva e g è iniettiva. □

6. La cardinalità dell'insieme dei numeri reali

Con il teorema di Cantor a disposizione, si può affrontare il problema di determinare la cardinalità dei numeri reali.

Intanto dimostriamo un risultato preliminare; consideriamo l'intervallo aperto

$$I = \{\, x \in \mathbb{R} : 0 < x < 1 \,\}$$

e dimostriamo che $|I| = |\mathbb{R}|$. Consideriamo la funzione $f\colon \mathbb{R} \to \mathbb{R}$,

$$f(x) = \begin{cases} \dfrac{\sqrt{1+x^2}-1}{x} & \text{se } x \neq 0, \\ 0 & \text{se } x = 0. \end{cases}$$

Un facile studio di funzione mostra che f è iniettiva e che $\operatorname{Im}(f) = I$.

Allo stesso risultato si arriva considerando la funzione

$$g(x) = \frac{2}{\pi} \arctan x.$$

La considerazione di I ci permetterà di semplificare i ragionamenti.

Sappiamo che ogni numero reale in I si può scrivere come allineamento decimale:

$$\begin{aligned} \frac{1}{2} &= 0{,}500000000000\dots \\ \frac{1}{3} &= 0{,}333333333333\dots \\ \frac{1}{7} &= 0{,}142857142857\dots \\ \frac{\sqrt{2}}{2} &= 0{,}707106781187\dots \\ \frac{\pi}{4} &= 0{,}785398163397\dots \end{aligned}$$

dove i puntini indicano altre cifre decimali. Prevedibili in base a uno schema periodico nei primi tre casi, non prevedibili negli ultimi due che sono numeri irrazionali.

Il numero dieci non ha nulla di particolare. Si può allo stesso modo sviluppare un numero reale come allineamento binario. Gli stessi numeri, scritti a destra dell'uguale come allineamenti binari, sono:

$$\begin{aligned} \frac{1}{2} &= 0{,}10000000000000000000000000\dots \\ \frac{1}{3} &= 0{,}01010101010101010101010101\dots \\ \frac{1}{7} &= 0{,}00100100100100100100100100\dots \\ \frac{\sqrt{2}}{2} &= 0{,}10110101000001001111001100\dots \\ \frac{\pi}{4} &= 0{,}11001001000011111101101010\dots \end{aligned}$$

e le cifre si ripetono ancora periodicamente nei primi tre casi.

In generale un numero $r \in I$ si scrive come

$$r = 0{,}a_0 a_1 a_2 \dots,$$

dove $a_i = 0$ oppure $a_i = 1$; in modo unico, se escludiamo tutte le successioni che, da un certo momento in poi, valgono 1. Questo è analogo ai numeri di periodo 9 nel caso decimale.

Dunque abbiamo in modo naturale una funzione $f\colon I \to 2^{\mathbb{N}}$: $f(r)$ è la funzione $\varphi\colon \mathbb{N} \to \{0,1\}$ definita da

$$\varphi(n) = a_n$$

dove $a_0, a_1, \cdots$ sono le cifre di r nello sviluppo binario di r.

La funzione f è totale e iniettiva, quindi concludiamo che $|I| \leq |2^{\mathbb{N}}|$.

Vogliamo ora definire una funzione $g\colon 2^{\mathbb{N}} \to I$. Prendiamo $\varphi \in 2^{\mathbb{N}}$; la tentazione sarebbe di definire $g(\varphi)$ come quel numero reale il cui sviluppo binario è

$$0{,}\varphi(0)\ \varphi(1)\ \varphi(2)\ \dots$$

ma questo non funziona, perché, se per esempio la funzione φ è la costante 1, il numero

$$0{,}111111\dots$$

è $1 \notin I$. Se anche escludessimo questa funzione, avremmo il problema del "periodo 1". Dunque agiamo in un altro modo. Alla funzione φ associamo il numero reale il cui sviluppo binario è

$$g(\varphi) = 0{,}0\ \varphi(0)\ 0\ \varphi(1)\ 0\ \varphi(2)\ \dots$$

cioè intercaliamo uno zero fra ogni termine. È chiaro che, se $\varphi \neq \psi$, allora $g(\varphi) \neq g(\psi)$, dunque g è iniettiva e totale.

Teorema 12 (Cantor). $|\mathbb{R}| = |P(\mathbb{N})|$.

Dimostrazione. Abbiamo già a disposizione le funzioni $f\colon I \to 2^{\mathbb{N}}$ e $g\colon 2^{\mathbb{N}} \to I$, entrambe iniettive. In particolare,

$$|I| \leq |2^{\mathbb{N}} \qquad \text{e} \qquad |2^{\mathbb{N}}| \leq |I|;$$

per il teorema di Cantor-Schröder-Bernstein, $|I| = |2^{\mathbb{N}}|$.

Sappiamo poi che $|I| = |\mathbb{R}|$ e che $|2^{\mathbb{N}}| = |P(\mathbb{N})|$. Dunque

$$|\mathbb{R}| = |I| = |2^{\mathbb{N}}| = |P(\mathbb{N})|,$$

come voluto. □

Occorre commentare questo risultato. Per dimostrarlo abbiamo usato il teorema di Cantor-Schröder-Bernstein, quindi non abbiamo potuto scrivere esplicitamente una biiettività di $\mathbb{R}$ su $P(\mathbb{N})$. Ma non è questo il punto più importante. La conseguenza più rilevante del teorema è che non è possibile descrivere *ogni* numero reale, perché, come vedremo in seguito, i numeri reali che possono essere espressi con una formula sono un insieme numerabile.

7. Il paradiso di Cantor

Un'altra applicazione del teorema di Cantor porta alla costruzione del cosiddetto "paradiso di Cantor". Questa espressione vuole indicare l'esistenza di una successione di cardinalità infinite ciascuna strettamente maggiore della precedente. Allo scopo basta iterare il passaggio all'insieme dei sottinsiemi, per esempio a partire dall'insieme dei numeri naturali, per ottenere una successione di insiemi la cui cardinalità, per il teorema di Cantor, continua a crescere strettamente:

$$|\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < |P(P(P(\mathbb{N})))| < \dots < |P(\dots P(P(P(\mathbb{N})))\dots)| < \cdots$$

Si potrebbe ancora andare avanti; definiamo, per induzione,

$$P^0(X) = X, \qquad P^{n+1}(X) = P(P^n(X)).$$

Allora possiamo considerare l'insieme

$$Y_1 = \bigcup_{n\in\mathbb{N}} P^n(\mathbb{N}),$$

e si può dimostrare che $|P^n(\mathbb{N})| < |Y_1|$, per ogni $n \in \mathbb{N}$. Dunque abbiamo trovato una cardinalità ancora maggiore di tutte quelle trovate in precedenza e il gioco può continuare: consideriamo

$$Y_2 = \bigcup_{n\in\mathbb{N}} P^n(Y_1)$$

e ancora $|P^n(Y_1)| < |Y_2|$. E così via, costruendo una gerarchia infinita di cardinalità sempre maggiori.

Oltre a interrogarci sul prolungarsi della successione delle cardinalità infinite sempre maggiori, è del tutto naturale domandarsi se tra $|\mathbb{N}|$ e $|P(\mathbb{N})|$ c'è o no una cardinalità strettamente compresa tra le due. Più in generale, ci si può chiedere se, dato un insieme infinito X, esiste un insieme Y tale che $|X| < |Y| < |P(X)|$.

Cantor ipotizzò che non ci siano insiemi Z tali che $|\mathbb{N}| < |Z| < |P(\mathbb{N})|$, e questa ipotesi ha preso il nome di *ipotesi del continuo*. Non è questo il luogo dove discutere questa questione, risolta brillantemente da P. J. Cohen nel 1963: *l'ipotesi del continuo è indecidibile* rispetto agli assiomi della teoria degli insiemi, nel senso che è altrettanto coerente prenderla come vera che prenderla come falsa. Non si tratta di argomenti semplici, tanto che per i suoi studi Cohen fu insignito della *Fields Medal* che, per i matematici, è l'analogo del Premio Nobel.

Esercizi

Si ricordi che $k\mathbb{N}$ indica l'insieme dei numeri naturali multipli di k, $\mathbb{N}_{\geq k}$ l'insieme dei numeri naturali maggiori o uguali a k, e $\mathbb{N}_{>k}$ l'insieme dei numeri naturali strettamente maggiori di k.

Esercizio 1. Si dica, motivando la risposta, se gli insiemi $3\mathbb{N} \cup \{2, 5\}$ e $2\mathbb{N} \setminus \{10, 8\}$ hanno la stessa cardinalità.

Esercizio 2. Si costruisca una funzione biiettiva tra gli insiemi $4\mathbb{N} \cup \{\frac{3}{2}, 7, \sqrt{2}\}$ e $\mathbb{N}_{>9}$.

Esercizio 3. Si dimostri che per ogni insieme finito X, se $f : X \to X$ è totale e iniettiva, allora è biiettiva. Si dia un esempio di un insieme infinito in cui l'analoga proprietà non sussiste.

Esercizio 4. Si dimostri che per ogni insieme finito X, se $f : X \to X$ è totale e suriettiva, allora è biiettiva. Si dia un esempio di un insieme infinito in cui l'analoga proprietà non sussiste.

Esercizio 5. Si costruisca una funzione biiettiva tra gli insiemi $\mathbb{Z} \cup \{\frac{3}{2}, \sqrt[3]{2}\}$ e $3\mathbb{N}$.

Esercizio 6. Si dica, motivando la risposta, se gli insiemi $(5\mathbb{N} \setminus \{5, 15\}) \cup \{\sqrt{3}, \frac{5}{2}\}$ e $2\mathbb{N} \cup \{11, 17\}$ hanno la stessa cardinalità.

Esercizio 7. Si dica, motivando la risposta, se gli insiemi $\mathbb{N}_{\geq 50} \cup 5\mathbb{N}$ e $3\mathbb{N} \cap 2\mathbb{N}$ hanno la stessa cardinalità.

Esercizio 8. Sia A un insieme numerabile e sia $a \notin A$. Si costruisca una biiezione tra gli insiemi A e $A \cup \{a\}$.

Esercizio 9. Sia A un insieme numerabile e sia $a \in A$. Si costruisca una biiezione tra gli insiemi A e $A \setminus \{a\}$.

Esercizio 10. Sia Π l'insieme dei numeri reali irrazionali. L'insieme Π è numerabile?

Esercizio 11. L'insieme di tutte le funzioni da $\mathbb{Q}$ all'insieme $\{0, 1, 2, 3\}$ è numerabile?

Esercizio 12. Sia $P = \{I \mid I \subseteq \mathbb{N} \text{ e } I \text{ è un insieme finito}\}$ l'insieme delle *parti finite* di $\mathbb{N}$. Qual è la cardinalità di P?

Esercizio 13. Si dica, motivando la risposta, se l'insieme $P(3\mathbb{N})$ è numerabile.