Insiemi infiniti

Definizione (2.36)**.** Un insieme X si dice *equipotente* a un insieme Y se esiste una funzione biiettiva $f : X \to Y$.

La Definizione definisce una relazione tra insiemi, che denotiamo in questo capitolo con il simbolo $\sim$: mostriamo che si tratta in effetti di una relazione di equivalenza:

- La relazione è riflessiva: infatti, dato un qualunque insieme X, la funzione identica $id_X : X \to X$ che manda ogni elemento di X in se stesso è una funzione biiettiva (è chiaramente iniettiva in quanto due elementi x, x' diversi hanno come immagini x, x' stessi, quindi immmagini diverse; e chiaramente suriettiva in quanto ogni elemento x del codominio è immagine di se stesso nel dominio.

- La relazione è simmetrica: infatti, supponiamo che sia $X \sim Y$, ovvero per definizione che esista una funzione biiettiva $f : X \to Y$: per mostrare che $Y \sim X$ e quindi la simmetria ci basta trovare una funzione biiettiva da Y a X. A questo scopo, basta ricordare che le funzioni biiettive sono caratterizzate dal fatto di essere invertibili e prendere la funzione $f^{-1} : Y \to X$ inversa di f: essendo f^{-1} l'inversa di f, si ha $f \circ f^{-1} = id_Y$ e $f^{-1} \circ f = id_X$. Ma queste due uguaglianze ci dicono che a sua f è l'inversa (sia destra che sinistra) di f^{-1}, quindi f^{-1} è invertibile e quindi, per quanto appena ricordato, biiettiva. Abbiamo dunque trovato una funzione biiettiva da Y a X, cioè $Y \sim X$, e possiamo concludere che la relazione è simmetrica.

- La relazione è transitiva: infatti, supponiamo che sia $X \sim Y$ e $Y \sim Z$, ovvero che esista una funzione $f : X \to Y$ biiettiva da X a Y e una funzione $g : Y \to Z$ biiettiva da Y a Z. Se riusciamo a mostrare che la composizione $g \circ f : X \to Z$ è anch'essa biiettiva avremo dimostrato che esiste una funzione biiettiva da X a Z e quindi che $X \sim Z$, da cui la transitività. A questo scopo, dimostriamo separatamente che $g \circ f : X \to Z$ è iniettiva e che è suriettiva. Per quello che riguarda l'iniettività, siano $x, x' \in X$, con $x \neq x'$: dobbiamo arrivare a dimostrare che $(g \circ f)(x) \neq (g \circ f)(x')$. Iniziamo con l'osservare che, dal momento che f è biiettiva e quindi in particolare iniettiva, abbiamo $f(x) \neq f(x')$. Essendo $f(x)$ e $f(x')$ elementi diversi di Y, che è il codominio di f ma anche il dominio di $g : Y \to Z$, possiamo applicare loro la g e, essendo anche quest'ultima biiettiva e in particolare iniettiva, si avrà $g(f(x)) \neq g(f(x'))$. Ma per definizione di composta questo significa proprio $(g \circ f)(x) \neq (g \circ f)(x')$, che è quell oche volevamo.

Per quello che riguarda la suriettività di $g \circ f : X \to Z$, dobbiamo dimostrare che per ogni $z \in Z$ esiste un $x \in X$ tale che $(g \circ f)(x) = z$. Iniziamo con l'osservare che, dal momento che $g : Y \to Z$ è biiettiva e in particolare suriettiva, esiste (almeno) un $y \in Y$ tale che $g(y) = z$. Ma dal momento che $f : X \to Y$ è biiettiva e in particolare suriettiva, a sua volta esiste un $x \in X$ tale che $f(x) = y$. Ma allora possiamo riscrivere la $g(y) = z$ come $g(f(x)) = z$. Ma per definizione di composizione questo significa proprio $(g \circ f)(x) = z$, che è quello che volevamo dimostrare.

Osservazione (2.37)**.** Si noti che per dimostrare che la composizione $g \circ f$ è iniettiva abbiamo usato solo il fatto che g e f sono entrambe iniettive, e analogamente per dimostrare che la composizione $g \circ f$ è suriettiva abbiamo usato solo il fatto che g e f sono entrambe suriettiva. La dimostrazione appena fatta mostra quindi il risultato, interessante e utile di per sé, che la composizione di funzioni iniettive è iniettiva e la composizione di funzioni suriettive è suriettiva.

Essendo allora l'equipotenza una relazione di equivalenza, possiamo parlare delle sue classi di equivalenza. Ebbene, i numeri naturali, che ci accingiamo a definire in modo rigoroso tra poco, sono esattamente il modo in cui noi indentifichiamo le classi di equivalenza degli insiemi finiti: infatti, quando diciamo per esempio che l'insieme $X = \{a, b, c, d\}$ ha 4 elementi, lo possiamo dire dopo aver *contato* i suoi elementi, ovvero dopo averli messi in corrispondenza con gli elementi dell'insieme $\{1, 2, 3, 4\}$ mediante una funzione biettiva (ad esempio, a 1 associamo a, a 2 associamo b, a 3 associamo c, a 4 associamo d). Chiaramente avremmo contato male se avessimo contato a due volte, associando sia a 1 che a 2 l'elemento a, e anche se dimenticassimo di contare qualche elemento di X, ad esempio d: ma il primo errore significherebbe che abbiamo costruito una corrispondenza $\{1, 2, 3, 4\} \to \{a, b, c, d\}$ non iniettiva (in cui gli elementi diversi 1 e 2 del dominio hanno la stessa immagine, a, nel codominio); il secondo errore significherebbe aver costruito una corrispondenza non suriettiva (in cui l'elemento d, non essendo stato contato, non è immagine di nessuno degli elementi $1, 2, 3, 4$ del dominio).
In generale, *contare* gli elementi di un insieme e concludere che questo ha n elementi significa costruire una funzione biiettiva dall'insieme dei numeri naturali che vanno da 1 a n a X.

Osservazione (2.38)**.** La (**??**) ci dice che se esiste una funzione biiettiva tra due insiemi *finiti*, allora essi hanno lo stesso numero di elementi, e non è difficile verificare anche il viceversa: se il numero di elementi di X e Y è lo stesso, allora non è difficile costruire una funzione biiettiva $X \to Y$.

Nel caso in cui X e Y siano insiemi infiniti, parlare di numero di elementi sembra non avere più senso, o al più verrebbe spontaneo dire che due insiemi infiniti hanno lo stesso numero di elementi (infinito, appunto). Tuttavia, se decidiamo, procedendo per analogia con gli insiemi finiti, di dire anche per due insiemi infiniti X e Y che essi hanno lo stesso numero di elementi se esiste una funzione biiettiva $X \to Y$, allora scopriremo che *non tutti gli insiemi infiniti hanno lo stesso numero di elementi* (detto anche *cardinalità*).
Per illustrare tale affermazione, usiamo come esempi gli insiemi numerici $\mathbb{N}$ (i numeri naturali), $\mathbb{Z}$ (i numeri interi), $\mathbb{Q}$ (i numeri razionali), $\mathbb{R}$ (i numeri reali), che sono inclusi uno nel successivo:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Iniziamo con il chiederci se esiste una funzione biettiva $\mathbb{N} \to \mathbb{Z}$: questo significherebbe che è possibile associare a ogni naturale un intero in modo da non lasciare scoperto nessun intero e da non ripetere due volte lo stesso intero, o in altre parole mettere gli interi in una successione infinita $a_0, a_1, a_2 \ldots$.
La risposta è affermativa, ad esempio gli interi possono essere messi in sequenza come segue:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \ldots \end{array}$$

Dunque esiste una corrispondenza biunivoca tra $\mathbb{N}$ e $\mathbb{Z}$, ovvero possiamo dire che i naturali e gli interi hanno lo stesso numero di elementi.
Mentre da una parte questo può risultare banale (si potrebbe pensare che avendo entrambi infiniti elementi, necessariamente questi debbano poter essere messi in corrispondenza biunivoca), dall'altra il risultato ha un aspetto sorprendente: dal momento che $\mathbb{N}$ si identifica con un sottoinsieme di $\mathbb{Z}$ (quello degli interi non negativi), stiamo dicendo che $\mathbb{Z}$ ha lo stesso numero di elementi di un suo sottoinsieme proprio[1] Questo fatto non è possibile per insiemi finiti: esso caratterizza gli insiemi infiniti ed è spesso assunto come definizione di insieme infinito (ovvero, un insieme si dice infinito se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio).
Anche i razionali $\mathbb{Q}$ possono essere messi in corrispondenza biunivoca con i naturali. Per mostrare come, consideriamo per facilità solo i razionali positivi (il ragionamento si riesce ad aggiustare poi per tutti i razionali), che si scrivono come quoziente n/m di due naturali n, m (con $m \neq 0$).

[1] Si dice sottoinsieme proprio di un insieme X un sottoinsieme che non sia X stesso (in base alla definizione di sottoinsieme, vale sempre l'inclusione $X \subseteq X$, ovvero ogni insieme è sottoinsieme di se stesso).

Consideriamo la seguente tabella infinita di frazioni dove, nella riga n-esima, scriviamo le frazioni con numeratore uguale a n:

$$\begin{array}{cccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \dots \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \dots \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \dots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \dots \\ & & \dots & & & \end{array}$$

Chiaramente in questa tabella alcune frazioni rappresentano lo stesso razionale (1/2 e 2/4, oppure 1/1 e 2/2)) ma se riusciamo a mostrare che è possibile realizzare una corrispondenza biunivoca tra le entrate della tabella e i naturali, a maggior ragione questo sarà vero per i razionali che corrispondono alle entrate della tabella senza ripetizioni.
La corrispondenza cercata con le frazioni della tabella si può per esempio realizzare scrivendo in sequenza tutte le diagonali della tabella a partire dall'angolo in alto a sinistra: prima 1/1, poi la diagonale adiacente $1/2, 2/1$, poi continuando a scendere verso destra la terza diagonale $1/3, 2/2, 3/1$ e così via.

$$1/1, 1/2, 2/1, 1/3, 2/2, 3/1, 1/4, 2/3, 3/2, 4/1, \dots$$

In questo modo, si riesce a mettere in una sequenza (ovvero in corrispondenza con i numeri naturali) tutti i razionali, e realizzare una funzione biiettiva $\mathbb{N} \to \mathbb{Q}$ che ci dice che anche $\mathbb{N}$ e $\mathbb{Q}$ hanno lo stesso numero di elementi.

Questi esempi potrebbero generare l'idea che qualunque insieme infinito possa essere messo in corrispondenza biunivoca con l'insieme dei naturali. In realtà questo è falso: si dimostra che per l'insieme $\mathbb{R}$ dei numeri reali questa corrispondenza non esiste.
Un'idea della dimostrazione è la seguente: supponiamo per assurdo di poter mettere in una sequenza in corrispondenza biunivoca con i numeri naturali tutti i numeri reali: $x_0, x_1, x_2, x_3, \dots$.
Rappresentando ogni reale con la sua rappresentazione decimale, possiamo riscrivere tale sequenza come

$$x_0 = a_0, b_0c_0d_0\dots$$

$$x_1 = a_1, b_1c_1d_1\dots$$

$$x_2 = a_2, b_2c_2d_2\dots$$

$$x_3 = a_3, b_3c_3d_3\dots$$

$$\dots$$

Ora, mostreremo che in realtà una tale sequenza non può mai contenere tutti i numeri reali, e lo faremo costruendo esplicitamente un numero reale che non è contenuto nella sequenza, il numero

$$x = 0, bcd \dots$$

in cui $b, c, d, \dots$ sono definiti come segue: $b = 1$ se $b_0 = 0$ e $b = 0$ se $b_0 \neq 0$ (questo garantisce già che x non sia il primo numero della sequenza x_0); $c = 1$ se $c_1 = 0$ e $c = 0$ se $c_1 \neq 0$ (questo garantisce che x non sia il secondo numero della sequenza x_1); $d = 1$ se $d_2 = 0$ e $d = 0$ se $d_2 \neq 0$ (questo garantisce che x non sia il terzo numero della sequenza x_2) e così via.

Dunque, $\mathbb{R}$ non ha lo stesso numero di elementi di $\mathbb{N}$ (pur essendo entrambi gli insiemi infiniti), e poichè $\mathbb{R}$ contiene $\mathbb{N}$ possiamo dire che $\mathbb{R}$ ha una cardinalità strettamente maggiore di quella di $\mathbb{N}$.

Non esiste dunque un unico "infinito", ma infiniti di tipo diverso. È lecito chiedersi se $\mathbb{R}$ sia il maggiore infinito possibile: la risposta è no, infatti, dato un qualunque insieme infinito, ne esiste sicuramente sempre uno di cardinalità più grande. Più precisamente, Cantor (al quale si deve la teoria degli insiemi infiniti che stiamo illustrando) mostrò che dato un insieme X, l'insieme costituito dai sottoinsiemi di X (detto *insieme potenza* e denotato $P(X)$) ha sempre cardinalità maggiore di X. Quindi, ad esempio, se vogliamo un insieme che abbia cardinalità maggiore di $\mathbb{R}$, basta prendere l'insieme potenza $P(\mathbb{R})$ di $\mathbb{R}$.

Concludiamo dicendo che si dimostra che la cardinalità di $\mathbb{R}$ coincide con quella dell'insieme potenza di $\mathbb{N}$.

L'affermazione che non esistono insiemi di cardinalità compresa tra quella di $\mathbb{N}$ e quella di $\mathbb{R}$ si chiama *ipotesi del continuo*: si dimostra che tale affermazione non è né dimostrabile né confutabile nella teoria assiomatica degli insiemi.

Teorema (2.39)**.** Dato un qualunque insieme X, il suo insieme potenza $P(X)$ ha cardinalità maggiore di quella di X.

Proof. Dobbiamo mostrare che esiste una funzione iniettiva $X \to P(X)$ ma non esiste una funzione biiettiva $X \to P(X)$. Per quello che riguarda la prima affermazione, un esempio di funzione iniettiva da X a $P(X)$ è dato dalla funzione che manda ogni $x \in X$ nel sottoinsieme $\{x\}$ che contiene solamente x: l'iniettività di tale funzione è immediata in quanto è chiaro che se $x \neq x'$ allora i due sottoinsiemi $\{x\}$ e $\{x'\}$ sono necessariamente diversi.

Dimostriamo ora la seconda affermazione per assurdo, ovvero supponiamo che esista una funzione $f : X \to P(X)$ biiettiva e mostriamo che questo porta a una contraddizione. Tale funzione associa a ogni $x \in X$ un sottoinsieme $f(x)$ di X. Questo sottoinsieme $f(x)$ potrebbe contenere o meno x. Consideriamo allora il sottoinsieme

$$A = \{x \in X \mid x \notin f(x)\}$$

costituito da tutti gli elementi di X che non appartengono al sottoinsieme $f(x)$ che viene loro associato mediante la f.
Dal momento che A è un sottoinsieme di X, ovvero appartiene a $P(X)$, e la funzione $f : X \to P(X)$ è biiettiva e in particolare suriettiva, deve esistere un elemento $a \in X$ che ha come immagine proprio A, ovvero $f(a) = A$.
Ma a questo punto otteniamo la contraddizione cercata chiedendoci se a appartiene a A: infatti, se $a \in A$, allora essendo A l'insieme degli elementi x caratterizzati dalla proprietà $x \notin f(x)$, sarebbe $a \notin f(a)$, che essendo $f(a) = A$ significa $a \notin A$. Viceversa, se $a \notin A$ questo significa che $a \notin f(a)$ e quindi a gode della proprietà $x \notin f(x)$ che definisce gli elementi di A ovvero $a \in A$. Vediamo quindi che $a \in A$ se e solo se $a \notin A$, contraddizione.
Deduciamo quindi che l'ipotesi che $f : X \to P(X)$ fosse biiettiva era assurda, ovvero non esiste nessuna funzione biiettiva da X a $P(X)$. $\square$