ALGEBRA I: CARDINALITÀ DI INSIEMI

1. CONFRONTO DI CARDINALITÀ

E' chiaro a tutti che esistono insiemi finiti (cioè con un numero finito di elementi) ed insiemi infiniti. E' anche chiaro che ogni insieme infinito è *più grande* di ogni insieme finito; ma esiste una maniera di confrontare la *taglia* di insiemi infiniti? E' possibile cioè dire se un dato insieme infinito possegga più elementi di un altro?

La situazione è delicata, perché ogni tentativo di definire la grandezza di insiemi infiniti produce una gran quantità di fenomeni antiintuitivi, che si scontrano con l'impossibilità di garantire che *il tutto sia più grande della parte*.

Se viene data una corrispondenza biunivoca (cioè un'applicazione invertibile) tra gli elementi di un insieme X e quelli di un insieme Y, possiamo ben dire che gli insiemi X e Y posseggano la stessa quantità di elementi. In questo caso diciamo anche che X e Y hanno *la stessa cardinalità*. Due insiemi finiti hanno la stessa cardinalità se e solo se hanno lo stesso numero di elementi (che nel caso di insiemi finiti può certamente essere contato). Senza indugi, passo a dare le definizioni che saranno oggetto del nostro studio.

Definizione 1.1. Due insiemi X e Y *hanno la stessa cardinalità* se esiste un'applicazione invertibile $f : X \to Y$. Il fatto che X e Y hanno la stessa cardinalità si esprime in simboli in uno dei modi seguenti: $c(X) = c(Y)$, $|X| = |Y|$, $X \simeq Y$. Due insiemi che hanno la stessa cardinalità si dicono anche *equipotenti*.

Osservazione 1.2. In ogni famiglia di insiemi — che è come dire insieme di insiemi, ma meno cacofonico — la relazione di avere la stessa cardinalità è di equivalenza: in effetti, $\mathrm{id}_X : X \to X$ è sempre un'applicazione invertibile, e quindi ogni insieme ha la propria stessa cardinalità; inoltre se $f : X \to Y$ è un'applicazione invertibile, allora anche $f^{-1} : Y \to X$ è invertibile, e quindi avere la stessa cardinalità è una relazione simmetrica; la transitività segue dal fatto che se $f : X \to Y$ e $g : Y \to Z$ sono applicazioni invertibili, allora anche $g \circ f : X \to Z$ è un'applicazione invertibile.

Esempio 1.3. Gli insiemi $\mathbb{N}$ e $\mathbb{N} \setminus \{0\}$ hanno la stessa cardinalità. In effetti l'applicazione $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ data da $f(n) = n + 1$ è iniettiva e suriettiva, quindi invertibile. Pertanto, rimuovendo un elemento da $\mathbb{N}$ si ottiene un insieme con la stessa cardinalità, e quindi $\mathbb{N}$ possiede sottoinsiemi propri che hanno la sua stessa cardinalità: questo è un esempio del fatto che *la parte può essere grande quanto il tutto*, se "grande" vuol dire avere la stessa cardinalità. Vedremo in seguito che ogni insieme infinito possiede sottoinsiemi della sua stessa cardinalità.

Il fenomeno più interessante è quello di insiemi infiniti che non hanno la stessa cardinalità: che non possono cioè essere messi in corrispondenza biunivoca l'uno con l'altro. Se vogliamo confrontare le cardinalità di insiemi infiniti — per confrontare quelle di insiemi finiti basta contare! — è necessario fornire una definizione naturale del concetto di *avere meno elementi*.

Definizione 1.4. L'insieme X *ha cardinalità minore o uguale* a quella dell'insieme Y se esiste un'applicazione iniettiva $f : X \to Y$. Il fatto che la cardinalità di X sia minore o uguale a quella di Y si esprime in simboli in uno dei modi seguenti: $c(X) \leq c(Y), |X| \leq |Y|, X \preceq Y$.

Osservazione 1.5. Se $X \subset Y$, allora $|X| \leq |Y|$. In effetti l'inclusione $\iota : X \to Y$ è sempre un'applicazione iniettiva.

Osservazione 1.6. In ogni famiglia di insiemi, la relazione $|X| \leq |Y|$ è transitiva. In effetti, se $f : X \to Y$ e $g : Y \to Z$ sono applicazioni iniettive, anche $g \circ f : X \to Z$ è iniettiva. Inoltre, se $|X| = |Y|$, allora $|X| \leq |Y|$ e $|Y| \leq |X|$: infatti, ogni applicazione invertibile è in particolare iniettiva. Nessuno ci garantisce — per ora, almeno — che sia vero il viceversa: va dimostrato che se esiste un'applicazione iniettiva da X a Y ed un'altra, sempre iniettiva, da Y in X, allora esiste un'applicazione invertibile tra X e Y. Vedremo presto come convincercene.

Non si può dire che la relazione $|X| \leq |Y|$ sia d'ordine, perché esistono sicuramente insiemi diversi con la stessa cardinalità, e quindi $|X| \leq |Y|, |Y| \leq |X|$ non assicura che $X = Y$ — tutt'al più garantisce che $|X| = |Y|$, come abbiamo appena detto.

Si definisce il concetto di cardinalità minore o uguale, invece di quello di cardinalità minore, per due validi motivi. Innanzitutto un'applicazione iniettiva può ben essere anche suriettiva, nel qual caso le cardinalità dei due insiemi sono uguali. Tuttavia, anche nel caso di applicazioni iniettive che non sono suriettive, esiste la possibilità che X e Y abbiano la stessa cardinalità! In effetti, abbiamo visto che $\mathbb{N}$ possiede sottoinsiemi propri della sua stessa cardinalità: l'inclusione un tale sottoinsieme in $\mathbb{N}$ fornisce un'applicazione iniettiva e non suriettiva tra insieme che possiedono tuttavia la stessa cardinalità.

Abbiamo definito il concetto di cardinalità minore o uguale tramite le applicazioni iniettive, ma avremmo potuto farlo anche per mezzo di quelle suriettive.

Proposizione 1.7. *Siano X, Y insiemi non vuoti. Allora $|X| \leq |Y|$ se e solo se esiste un'applicazione suriettiva $f : Y \to X$.*

Dimostrazione. Per definizione, se $|X| \leq |Y|$, allora esiste un'applicazione iniettiva $g : X \to Y$. Se quest'applicazione è anche suriettiva, abbiamo finito. Se non è suriettiva, g definisce un'applicazione invertibile $X \to g(X) \subsetneq Y$, dalla quale possiamo ricavare un'inversa $g^{-1} : g(X) \to X$. Possiamo estendere tale applicazione ad una $f : Y \to X$ scegliendo in modo qualsiasi — qui è necessario che X sia non vuoto!!! — le immagini degli elementi in $Y \setminus g(X)$. L'applicazione f ottenuta sarà necessariamente suriettiva.

Viceversa, supponiamo sia data $f : Y \to X$ suriettiva, e definiamo una funzione $g : X \to Y$ che per ogni $x \in X$ sceglie una controimmagine, cioè un elemento $y \in Y$ tale che $f(y) = x$ — tale elemento esiste sempre, dal momento che f è suriettiva. L'applicazione g così ottenuta sarà iniettiva, dal momento che per costruzione $f \circ g = \mathrm{id}_X$. □

Osservazione 1.8. Avete sicuramente osservato che mi sto appoggiando, nelle dimostrazioni, ad enunciati fatti a lezione. In questo caso ho utilizzato il fatto che se $f \circ g$ è invertibile, allora g è iniettiva ed f è suriettiva.

Un fatto che non abbiamo visto a lezione, e che mi accingo a dimostrare, è il seguente:

Teorema 1.9. *Se $|X| \leq |Y|$ e $|Y| \leq |X|$ allora $|X| = |Y|$.*

Prima di procedere, però, ho bisogno di un risultato tecnico preliminare. Rubo questa tecnica dimostrativa a Marco Manetti[1].

Lemma 1.10. *Siano X e Y insiemi qualsiasi. Allora, per ogni scelta di applicazioni $f : X \to Y$, $g : Y \to X$ esiste un sottoinsieme $A \subset X$ tale che $g(Y \setminus f(A)) = X \setminus A$.*

Dimostrazione. Sicuramente esiste un sottoinsieme $B \subset X$ tale che $g(Y \setminus f(B)) \cap B = \emptyset$ — ad esempio, $B = \emptyset$ soddisfa questa proprietà. Sia F la famiglia di tutti tali sottoinsiemi.

Se $A = \bigcup_{B \in F} B$, allora $A \in F$: in effetti, sia $x \in g(Y \setminus f(A)) \cap A$. Allora $x \in A$, e quindi $x \in B$ per almeno un $B \in F$. Inoltre

$$Y \setminus f(A) = Y \setminus f\left(\bigcup_{B \in F} B\right) = Y \setminus \bigcup_{B \in F} f(B) = \bigcap_{B \in F} Y \setminus f(B).$$

Ricordando che

$$g\left(\bigcap_{B \in F} Y \setminus f(B)\right) \subset \bigcap_{B \in F} g\left(Y \setminus f(B)\right),$$

concludiamo che se $x \in g(Y \setminus f(A))$ allora $x \in g(Y \setminus f(B))$ per ogni $B \in F$. Ma allora, per almeno un $B \in F$, vale $x \in g(Y \setminus f(B)) \cap B = \emptyset$, il che è assurdo. A è quindi l'elemento massimo in F.

Abbiamo dimostrato che $g(Y \setminus f(A)) \subset X \setminus A$. Per mostrare che vale l'uguaglianza, supponiamo che esista $x \in X$, con $x \notin g(Y \setminus f(A)) \cup A$. Allora $A' = A \cup \{x\}$ è tale che $g(Y \setminus f(A')) \cap A' = \emptyset$, contro la massimalità di A in F. (verificatelo!) □

Dimostrazione del Teorema1.9. Siano $f : X \to Y$ e $g : Y \to X$ applicazioni iniettive. Il Lemma 1.10 ci assicura l'esistenza di $A \subset X$ tale che $g(Y \setminus f(A)) = X \setminus A$.

Ma allora la restrizione $f|_A$ è una corrispondenza biunivoca tra A e $f(A)$ e la restrizione $g|_{Y \setminus f(A)}$ è una corrispondenza biunivoca tra $Y \setminus f(A)$ e $X \setminus A$. Pertanto, l'applicazione

$$\phi(x) = \begin{cases} f(x) & \text{se } x \in A \\ g^{-1}(x) & \text{se } x \in X \setminus A \end{cases}$$

è un'applicazione invertibile da X a Y. □

Osservazione 1.11. Si può rimanere confusi di fronte alla necessità di dimostrare che se $|X| \leq |Y|$ e $|Y| \leq |X|$, allora $|X| = |Y|$. Tuttavia bisogna comprendere che non esistono dei numeri $|X|$ e $|Y|$, appartenenti ad un insieme parzialmente ordinato, che sono ciascuno minore o uguale dell'altro: $|X| \leq |Y|$ è semplicemente una notazione psicologicamente efficace per indicare l'esistenza di un'applicazione iniettiva da X a Y. Il Teorema 1.9 permette di giustificare questa scelta notazionale.

E' comune indicare con la notazione $|X| < |Y|$ il fatto che la cardinalità di X sia minore o uguale di quella di Y, e che X e Y non hanno la stessa cardinalità. In questo caso, si dice anche che la cardinalità di X è strettamente inferiore a quella di Y. Ad esempio, tra gli insiemi finiti, avere cardinalità strettamente inferiore vuol dire che il numero di elementi (che può essere contato) del primo insieme è strettamente inferiore a quello del secondo insieme.

Rimane da mostrare, per il momento, soltanto il fatto intuitivo che due insiemi infiniti hanno la stessa grandezza, oppure uno dei due è più grande dell'altro.

Proposizione 1.12. *Siano X e Y insiemi. Allora $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

Dimostrazione. Sull'insieme $F = \{(A, f) \,|\, A \subset X, f : A \to Y \text{ iniettiva}\}$ definiamo una relazione d'ordine ponendo $(A, f) \leq (B, g)$ se e solo se $A \subseteq B$ e $g|_A = f$. Per applicare il Lemma di Zorn, e mostrare che F possiede elementi massimali, dobbiamo mostrare che ogni catena in F possiede un maggiorante.

Sia $C = \{(A_i, f_i), i \in I\}$ una catena in F. Questo vuol dire che se $i, j \in I$, allora $A_i \subset A_j$ oppure $A_j \subset A_i$; inoltre, delle due applicazioni f_i e f_j, quella definita sul sottoinsieme più grande estende quella definita sul sottoinsieme più piccolo. E' utile osservare che se $a \in A_i$ e $b \in A_j$, allora a e b appartengono entrambi al più grande tra A_i e A_j.

Poniamo $A = \bigcup_{i \in I} A_i$, e definiamo $f : A \to Y$ tale che $f(a) = f_i(a)$ se $a \in A_i$. L'applicazione f è ben definita, poiché le f_i si estendono l'una l'altra, e quindi coincidono sulle intersezioni comuni. Inoltre f è iniettiva: siano

[1]che tra l'altro scrive le dimostrazioni meglio di me...

$a, b \in A$ tali che $f(a) = f(b)$. Per quanto detto prima, a, b appartengono allo stesso A_i per qualche i, e allora $f_i(a) = f(a) = f(b) = f_i(b)$. Ma f_i è iniettiva, quindi $a = b$.

Abbiamo mostrato che $(A, f) \in F$: per come è stato costruito, tale elemento è un maggiorante di C. Il Lemma di Zorn ci garantisce quindi l'esistenza di elementi massimali in F.

Sia $(A, f) \in F$ tale che $A \neq X, f(A) \neq Y$. Scegliendo $x_0 \in X \setminus A$ e $y_0 \in Y \setminus f(A)$, si può estendere f a $A \cup \{x_0\}$ definendo $f(x_0) = y_0$. Pertanto, se (A, f) è massimale in F, allora $A = X$ oppure $f(A) = Y$. Nel primo caso, f è un'applicazione iniettiva da X in Y. Nel secondo, $f : A \to Y$ è un'applicazione invertibile, e la sua inversa $f^{-1} : Y \to A \subset X$ definisce un'applicazione iniettiva da Y in X. □

2. Insiemi numerabili

La più piccola cardinalità infinita è quella dell'insieme $\mathbb{N}$: ogni insieme infinito con la stessa cardinalità di $\mathbb{N}$ è detto *numerabile*.

Osservazione 2.1. Chiaramente, due insiemi numerabili hanno la stessa cardinalità, perché la relazione di avere la stessa cardinalità è transitiva. Se X e Y sono insiemi numerabili, esiste quindi sempre almeno un'applicazione invertibile $f : X \to Y$.

Abbiamo già visto come $\mathbb{N}$ contenga sottoinsiemi propri numerabili. Il seguente enunciato mostra che i sottoinsiemi di $\mathbb{N}$ sono finiti oppure numerabili.

Lemma 2.2. *Ogni sottoinsieme infinito di* $\mathbb{N}$ *è numerabile.*

Dimostrazione. Se $X \subset \mathbb{N}$ è un sottoinsieme infinito, si tratta di stabilire un'applicazione invertibile $\phi : \mathbb{N} \to X$. Ricordando la proprietà di buon ordinamento di $\mathbb{N}$ — cioè che ogni sottoinsieme non vuoto di $\mathbb{N}$ possiede un elemento minimo — definiamo per ricorrenza ϕ come segue:

- $\phi(0) = \min X$;
- $\phi(n+1) = \min X \setminus \{\phi(0), \phi(1), \dots, \phi(n)\}$.

Allora ϕ è iniettiva, poiché per costruzione $\phi(n) < \phi(n+1)$. Inoltre è facile dimostrare che $\phi(n) \geq n$ — fatelo per induzione! — e quindi $n \in \phi(\{0, 1, \dots, n\})$, che garantisce la suriettività. □

Lemma 2.3. *Sia X un insieme e x_0 un suo elemento. Allora X è numerabile se e solo se $X \setminus \{x_0\}$ è numerabile.*

Dimostrazione. E' una semplice riformulazione dell'Esempio 1.3. Se $X \setminus \{x_0\}$ è numerabile, sia $f : X \setminus \{x_0\} \to \mathbb{N}$ un'applicazione invertibile. Allora

$$g(x) = \begin{cases} 0 & \text{se } x = x_0 \\ f(x) + 1 & \text{se } x \neq x_0 \end{cases}$$

è un'applicazione invertibile da X a $\mathbb{N}$.

Viceversa, se X è numerabile, sia $f : X \to \mathbb{N}$ un'applicazione invertibile. Allora

$$g(x) = \begin{cases} f(x) & \text{se } f(x) < f(x_0) \\ f(x) - 1 & \text{se } f(x) > f(x_0) \end{cases}$$

è un'applicazione invertibile da $X \setminus \{x_0\}$ a $\mathbb{N}$. □

Corollario 2.4. *Aggiungendo a, o togliendo da, un insieme numerabile una quantità finita di elementi, si ottiene un insieme numerabile.*

Dimostrazione. Il caso di un elemento è trattato nel Lemma 2.3. Il caso generale segue da una semplice induzione. (Fatela!) □

Lemma 2.5. $\mathbb{N} \times \{0, 1\}$ *è numerabile.*

Dimostrazione. L'applicazione $\phi : \mathbb{N} \times \{0, 1\} \to \mathbb{N}$ definita da $\phi(n, 0) = 2n, \phi(n, 1) = 2n + 1$ è invertibile. □

Corollario 2.6. *L'unione di due insiemi numerabili è numerabile.*

Dimostrazione. Siano $\phi_X : \mathbb{N} \to X, \phi_Y : \mathbb{N} \to Y$ applicazioni invertibili. Allora l'applicazione $\phi : \mathbb{N} \times \{0, 1\} \to X \cup Y$ definita da $\phi(n, 0) = \phi_X(n), \phi(n, 1) = \phi_Y(n)$ è suriettiva, e dalla Proposizione 1.7 si ha $|X \cup Y| \leq |\mathbb{N} \times \{0, 1\}| = |\mathbb{N}|$. Inoltre, l'inclusione di X in $X \cup Y$ è un'applicazione iniettiva, quindi $|X| \leq |X \cup Y|$. Concludendo, abbiamo

$$|\mathbb{N}| = |X| \leq |X \cup Y| \leq |\mathbb{N} \times \{0, 1\}| = |\mathbb{N}|,$$

e di conseguenza $|X \cup Y| = |\mathbb{N}|$. □

Corollario 2.7. *L'unione di un numero finito (non nullo) di insiemi numerabili è numerabile.*

Dimostrazione. Per induzione sul numero $n \geq 1$ di insiemi, la base $n = 1$ dell'induzione essendo ovvia. Per quanto riguarda il passo induttivo, basta notare che grazie al Corollario 2.6 l'unione di $n + 1$ insiemi numerabili

$$X_1 \cup \dots \cup X_n \cup X_{n+1} = X_1 \cup \dots \cup X_{n-1} \cup (X_n \cup X_{n+1})$$

è anche unione di n insiemi numerabili. □

Lemma 2.8. *L'insieme* $\mathbb{N} \times \mathbb{N}$ *è numerabile.*

Dimostrazione. L'applicazione definita da

$$\phi(m,n) = \binom{m+n+1}{2} + m$$

è biunivoca[2]. □

Corollario 2.9. *Il prodotto cartesiano di due insiemi numerabili è numerabile.*

Dimostrazione. Se $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$ sono invertibili, l'applicazione $X \times Y \ni (x,y) \mapsto (f(x), g(y)) \in \mathbb{N} \times \mathbb{N}$ è anch'essa invertibile. □

Corollario 2.10. *L'unione di un'infinità numerabile di insiemi numerabili è numerabile.*

Dimostrazione. Indichiamo con X l'unione degli insiemi numerabili $X_i, i \in \mathbb{N}$, e siano $\phi_i : \mathbb{N} \to X_i$ applicazioni invertibili. Allora $\phi(m,n) = \phi_m(n)$ definisce un'applicazione suriettiva $\phi : \mathbb{N} \times \mathbb{N} \to X$. Per la Proposizione 1.7, abbiamo $|X| \le |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, e quindi

$$|\mathbb{N}| = |X_0| \le |X| \le |\mathbb{N}|,$$

e per il Teorema 1.9, si ha $|X| = |\mathbb{N}|$. □

Lemma 2.11. *Il prodotto cartesiano $\mathbb{N}^n$ di $n > 0$ copie di $\mathbb{N}$ è numerabile.*

Dimostrazione. Per induzione su n, la base $n = 1$ essendo ovvia. Per quanto riguarda il passo induttivo si noti che $\mathbb{N}^{n+1} = \mathbb{N}^{n-1} \times (\mathbb{N} \times \mathbb{N})$ ammette una corrispondenza biunivoca con $\mathbb{N}^{n-1} \times \mathbb{N} = \mathbb{N}^n$ grazie al Lemma 2.8. □

Corollario 2.12. *Sia $n > 0$. I sottoinsiemi di $\mathbb{N}$ di cardinalità minore o uguale ad n sono un'infinità numerabile.*

Dimostrazione. E' sufficiente mostrare la numerabilità della famiglia $P_n(\mathbb{N})$ dei sottoinsiemi *non vuoti* di $\mathbb{N}$ di cardinalità $\le n$. La maggiorazione $|\mathbb{N}| \le |P_n(\mathbb{N})|$ è ovvia: basta ad esempio considerare l'applicazione iniettiva che associa ad ogni n il suo singoletto $\{n\}$. Esiste inoltre un'applicazione suriettiva $\mathbb{N}^n \to P_n(\mathbb{N})$ che associa ad $(a_1, \dots, a_n)$ il sottoinsieme $\{a_1, \dots, a_n\}$. Pertanto $|P_n(\mathbb{N})| \le |\mathbb{N}^n| = |\mathbb{N}|$. □

Proposizione 2.13. *L'insieme $P'(\mathbb{N})$ dei sottoinsiemi* finiti *di $\mathbb{N}$ è numerabile.*

Dimostrazione. Ogni insieme i cui elementi sono i sottoinsiemi di $\mathbb{N}$ di cardinalità $\le n$ è numerabile per il corollario precedente, e $P'(\mathbb{N})$ è la loro unione, che è numerabile per il Corollario 3.8. □

Vedremo in seguito che l'insieme delle parti di $\mathbb{N}$ non è numerabile.

3. Insiemi più che numerabili

Abbiamo finora avuto a che fare solo con insiemi numerabili; esistono tuttavia insiemi infiniti i cui elementi non possono essere messi in corrispondenza biunivoca con i numeri naturali. In questo paragrafo fornirò alcune informazioni sugli insiemi infiniti qualsiasi, mentre nel successivo esibirò una costruzione di Cantor per esibire, a partire da un insieme infinito X, un insieme di cardinalità strettamente superiore. La mia trattazione segue molto da vicino quella di Serge Lang in *Algebra*.

3.1. **Generalità sulla cardinalità degli insiemi finiti.**

Lemma 3.1. *Ogni insieme infinito contiene un sottoinsieme numerabile.*

Dimostrazione. Se X è il nostro insieme infinito, dobbiamo costruire un'applicazione iniettiva $f : \mathbb{N} \to X$: l'immagine $f(X)$ di tale applicazione sarà in corrispondenza biunivoca con $\mathbb{N}$.

Consideriamo una funzione di scelta ϕ che per ogni sottoinsieme $Y \subsetneq X$ sceglie un elemento nel suo complementare $X \setminus Y$ — stiamo di fatto indicizzando i sottoinsiemi non vuoti di X per mezzo dei loro complementari, che sono i sottoinsiemi propri di X, ed utilizzando l'assioma della scelta per costruire ϕ.

Allora definendo per ricorrenza

$$f(n) = \begin{cases} \phi(\emptyset) & \text{se } n = 0 \\ \phi(\{f(0), f(1), \dots, f(n-1)\}) & \text{se } n > 0 \end{cases}$$

si ottiene l'applicazione iniettiva desiderata[3]. □

Lemma 3.2. *Ogni insieme infinito possiede una partizione in sottoinsiemi tutti numerabili.*

Dimostrazione. Ho dato la dimostrazione nella dispensa sul Lemma di Zorn. □

Corollario 3.3. *Aggiungendo a, o togliendo da, un insieme infinito una quantità finita di elementi, si ottiene un insieme della stessa cardinalità. In particolare, ogni insieme infinito contiene un sottoinsieme proprio della sua stessa cardinalità.*

---

[2]convincetevi che è la stessa che ho descritto a lezione!

[3]Questa dimostrazione si volgarizza dicendo: *scelgo un elemento $f(0) \in X$, poi scelgo un elemento $f(1) \in X$ diverso da $f(0)$, ed in generale un elemento $f(n+1)$ diverso da tutti quelli scelti in precedenza. Posso fare queste scelte perché l'insieme X è infinito, e quindi il complementare di un sottoinsieme finito è sempre non vuoto*

Dimostrazione. Sia X il nostro insieme, e $\{U_i, i \in I\}$ una sua partizione in sottoinsiemi U_i tutti numerabili[4]. Per il Corollario 2.4, aggiungendo o togliendo a ciascun sottoinsieme U_i un numero finito di elementi si ottiene ancora un sottoinsieme numerabile.

Se X' è ottenuto da X aggiungendo o togliendo un numero finito di elementi, possiamo ottenere una partizione $\{U'_i, i \in I\}$ di X' aggiungendo o togliendo a ciascun U_i un numero finito di elementi. Per il Corollario 2.4, U'_i è numerabile per ogni $i \in I$, ed esistono quindi applicazioni invertibili $f_i : U_i \to U'_i$. L'applicazione $f : X \to X'$ che *incolla* tutte le f_i, cioè la cui restrizione ad U_i coincide con f_i per ogni $i \in I$, è allora un'applicazione invertibile tra X e X'. □

Proposizione 3.4. *Se X è un insieme infinito, allora $X \times \{0, 1\}$ e $X \times \mathbb{N}$ hanno la stessa cardinalità di X.*

Dimostrazione. Stessa dimostrazione del corollario precedente. Se $Y = \{0, 1\}$ oppure $Y = \mathbb{N}$, si utilizza la numerabilità del prodotto cartesiano di un insieme numerabile con Y (Lemmi 2.5 e 2.8), e si incollano le applicazioni invertibili $f_i : U_i \to U_i \times Y$. □

Corollario 3.5. *Se X, Y sono insiemi tali che $|X| \leq |Y|$, allora $X \cup Y$ ha la stessa cardinalità di Y.*

Dimostrazione. Dal momento che $|X| \leq |Y|$, esiste un'applicazione suriettiva $f : Y \to X$. Ma allora possiamo definire un'applicazione $g : Y \times \{0, 1\} \to X \cup Y$ tale che $g(y, 0) = y, g(y, 1) = f(y)$, che è evidentemente suriettiva. Di conseguenza $|X \cup Y| \leq |Y \times \{0, 1\}| = |Y|$. Ma Y è un sottoinsieme di $X \cup Y$ e quindi $|Y| \leq |X \cup Y|$. In conclusione $|Y| \leq |X \cup Y| \leq |Y|$, e quindi Y e $X \cup Y$ hanno la stessa cardinalità. □

Corollario 3.6. *Se $X \subset Y$ è tale che $|X| < |Y|$, allora Y e $Y \setminus X$ hanno la stessa cardinalità.*

Dimostrazione. Per il corollario precedente, la cardinalità di $Y = X \cup (Y \setminus X)$ è la maggiore tra la cardinalità di X e quella di $Y \setminus X$. Poiché $|X| < |Y|$, deve essere $|Y \setminus X| = |Y|$. □

Osservazione 3.7. Gli ultimi due corollari generalizzano il Corollario 2.4 al caso di cardinalità qualsiasi: aggiungendo a, o togliendo da, un insieme infinito Y un insieme di cardinalità strettamente inferiore, si ottiene un insieme della stessa cardinalità di Y.

Corollario 3.8. *Siano $X_n, n \in \mathbb{N}$ insiemi di cui almeno uno infinito, e supponiamo che $|X_n| \leq |X_0|$ per ogni $i \in \mathbb{N}$. Allora l'unione $X = \bigcup_{i \in \mathbb{N}} X_i$ ha la stessa cardinalità di X_0.*

Dimostrazione. Se alcuni X_n sono vuoti, possiamo sostituirli con X_0 senza cambiare l'unione X: possiamo quindi supporre che gli X_n siano tutti non vuoti. Esistono allora applicazioni suriettive $f_n : X_0 \to X_n$, che possiamo utilizzare per definire l'applicazione suriettiva $f : X_0 \times \mathbb{N} \to X$ tale che $f(x, n) = f_n(x)$. Allora $|X| \leq |X_0 \times \mathbb{N}| = |X_0|$. D'altronde, X_0 è un sottoinsieme di X e quindi $|X_0| \leq |X|$, da cui l'uguaglianza $|X| = |X_0|$. □

Osservazione 3.9. E' importante sottolineare che il Corollario 3.8 mostra implicitamente — e in realtà anche abbastanza esplicitamente — che la cardinalità dell'unione di un numero finito di insiemi è uguale alla massima tra le cardinalità degli insiemi. Questo fatto segue immediatamente scegliendo l'insieme di cardinalità massima come X_0, e tutti gli insiemi X_n tranne un numero finito uguali a $\emptyset$.

3.2. **Cardinalità del quadrato cartesiano di un insieme infinito.** Abbiamo già visto che se X è un insieme numerabile, allora $X \times X$ è anch'esso numerabile, ed ha quindi la stessa cardinalità di X. Questo è vero per ogni insieme infinito, anche se la dimostrazione è più complessa, e richiede l'utilizzo del Lemma di Zorn — e potete quindi saltarne la dimostrazione ad una prima lettura.

Teorema 3.10. *Se X è un insieme infinito, allora $|X \times X| = |X|$.*

Dimostrazione. E' sufficiente dimostrare l'enunciato per un insieme Y della stessa cardinalità di X.

Sull'insieme $F = \{(A, f) \,|\, A \subset X, f : A \to A \times A$ è un'applicazione invertibile$\}$ — che è non vuoto perché ogni sottoinsieme numerabile di X possiede una corrispondenza biunivoca con il suo quadrato cartesiano — definiamo una relazione d'ordine[5] tale che $(A, f) \leq (B, g)$ se e solo se A è un sottoinsieme di B e la restrizione di g ad A coincide con f. L'insieme parzialmente ordinato $(F, \leq)$ soddisfa le ipotesi del Lemma di Zorn: in effetti se $C = \{(A_i, f_i), i \in I\}$ è una catena in F, allora si ottiene un maggiorante di C scegliendo $A = \bigcup_{i \in I} A_i$ e definendo $f(a) = f_i(a)$ se $a \in A_i$.

Esistono quindi elementi massimali in F. Voglio adesso mostrare che se (A, f) è un elemento massimale di F, la cardinalità di A *non può* essere strettamente inferiore a quella di X. In effetti, se $|A| < |X|$, allora $|X \setminus A| = |X|$ e quindi $|A| < |X \setminus A|$. Questo mostra che $X \setminus A$ contiene un sottoinsieme A' della stessa cardinalità di A (ad esempio, l'immagine di un'applicazione iniettiva da A in $X \setminus A$). Il mio obiettivo è quello di costruire un elemento $(B, g) \in F$ tale che $B = A \cup A'$ e $(A, f) \leq (B, g)$: vediamo come fare.

Dal momento che $B = A \cup A'$ e $A \cap A' = \emptyset$, abbiamo una decomposizione di $B \times B$ nell'unione disgiunta:

$$B \times B = (A \times A) \cup (A \times A') \cup (A' \times A) \cup (A' \times A').$$

I tre insiemi $A \times A'$, $A' \times A$, $A' \times A'$ hanno tutti la stessa cardinalità di $A \times A$, e quindi di A, e quindi la cardinalità della loro unione $(B \times B) \setminus (A \times A)$ è uguale a quella di A, grazie al Corollario 3.8 e all'Osservazione 3.9.

---

[4] L'insieme I degli indici non sarà generalmente numerabile, e vedremo più avanti che esso ha in effetti la stessa cardinalità di X.

[5] lascio a voi la facile dimostrazione che $\leq$ è effettivamente riflessiva, antisimmetrica e transitiva.

Ma allora la cardinalità di $(B \times B) \setminus (A \times A)$ è uguale a quella di $B \setminus A = A'$; se $f' : A' \to (B \times B) \setminus (A \times A)$ è un'applicazione invertibile, allora

$$g(b) = \begin{cases} f(b) & \text{se } b \in A \\ g(b) & \text{se } b \in A' \end{cases}$$

definisce un'applicazione invertibile $g : B \to B \times B$ che estende f. Pertanto $(A, f) \leq (B, g)$, contro la massimalità di (A, f).

Ricapitolando, ogni elemento massimale $(A, f) \in F$ fornisce un sottoinsieme $A \subset X$ della stessa cardinalità di X, dotato di una corrispondenza biunivoca $f : A \to A \times A$; di conseguenza anche X ammette una corrispondenza biunivoca col suo quadrato simmetrico $X \times X$. □

Corollario 3.11. *Se X e Y sono insiemi non vuoti, con $|X| \leq |Y|$ ed Y infinito, allora $|X \times Y| = |Y|$.*

Dimostrazione. Sia x_0 un elemento di X. Allora $\{x_0\} \times Y$ è un sottoinsieme di $X \times Y$ biunivoco con Y, quindi $|Y| = |\{x_0\} \times Y| \leq |X \times Y|$.

D'altronde, $|X| \leq |Y|$ e quindi esiste un'applicazione suriettiva $\phi : Y \to X$, che può essere utilizzata per costruire un'applicazione suriettiva $(\phi, \mathrm{id}_Y) : Y \times Y \to X \times Y$. Pertanto, $|X \times Y| \leq |Y \times Y| = |Y|$. Utilizzando le due disuguaglianze si ottiene $|X \times Y| = |Y|$. □

Corollario 3.12. *Sia $\{X_i\}$ una famiglia finita di insiemi non vuoti, almeno uno dei quali infinito. Allora la cardinalità del prodotto cartesiano degli insiemi X_i è uguale alla massima tra le cardinalità dei fattori.*

Dimostrazione. Segue facilmente per induzione, utilizzando il corollario precedente. □

4. Il Teorema di Cantor

Abbiamo ricavato finora molte proprietà degli insiemi infiniti, anche quando questi non sono numerabili. Tuttavia, non abbhiamo ancora visto un singolo esempio di insieme più che numerabile. Il Teorema di Cantor garantisce che l'insieme delle parti $P(X)$ di un insieme infinito X ha sempre cardinalità strettamente superiore a quella di X; come conseguenza indiretta, dimostra che non esiste un insieme di cardinalità maggiore di ogni altro insieme.

Teorema 4.1 (Cantor)**.** *Sia un X un insieme, e $P(X)$ l'insieme delle parti di X. Allora non esistono applicazioni suriettive $f : X \to P(X)$.*

Dimostrazione. Se $f : X \to P(X)$ è un'applicazione, definiamo $F = \{x \in X \mid x \notin f(x)\}$.

Comunque si scelga $a \in X$, il sottoinsieme $F \subset X$ non è uguale a $f(a)$. In effetti, se $a \in F$, allora $a \notin f(a)$ per la definizione di F. Allo stesso modo, se $a \notin F$, allora $a \in f(a)$. Pertanto a appartiene solo ad uno dei due insiemi F ed $f(a)$, ma non all'altro.

Abbiamo dimostrato che $F \neq f(a)$ per ogni $a \in X$, e quindi che F non appartiene all'immagine di f. In altre parole, f non è suriettiva. □

Corollario 4.2. *La cardinalità di $P(X)$ è strettamente superiore a quella di X.*

Dimostrazione. Se $P(X) \leq X$, allora esisterebbe un'applicazione suriettiva $X \to P(X)$. Il teorema precedente mostra che questo è impossibile. Allora $P(X) \not\leq X$, cioè $X < P(X)$. □

Una variante del Teorema 4.1 mostra che l'insieme $\mathbb{R}$ dei numeri reali non è numerabile.

Teorema 4.3. *Non esistono applicazioni suriettive da $\mathbb{N}$ a $\mathbb{R}$.*

Dimostrazione. Data un'applicazione $F : \mathbb{N} \to \mathbb{R}$, costruiamo un numero reale $0 \leq \alpha < 1$ la cui $n+1$.esima cifra dopo la virgola è 1 se la $n+1$.esima cifra di $F(n)$ dopo la virgola è ≥ 5, ed è 6 se la $n+1$.esima cifra di $F(n)$ dopo la virgola è < 5. Allora α differisce da $F(n)$ in almeno una cifra, e non appartiene quindi all'immagine di F. □

Ogni insieme con la stessa cardinalità di $\mathbb{R}$ è detto avere *la potenza del continuo*, o semplicemente *possedere un'infinità continua di elementi*.

5. La cardinalità del continuo

In quest'ultimo paragrafo mostrerò che l'insieme $P(\mathbb{N})$ delle parti di $\mathbb{N}$ ha la stessa cardinalità di $\mathbb{R}$. Come passo preliminare, fornisco una descrizione di $P(X)$ in termini più maneggevoli.

Lemma 5.1. *Esiste una corrispondenza biunivoca tra $P(X)$ e l'insieme $\{0,1\}^X = \{f : X \to \{0,1\}\}$ delle funzioni su X a valori in $\{0,1\}$.*

Dimostrazione. Ad ogni sottoinsieme $Y \subset X$, possiamo associare l'applicazione $\phi_Y : X \to \{0,1\}$ tale che $\phi_Y(x) = 1$ se $x \in Y$, $\phi_Y(x) = 0$ se $x \notin Y$. Viceversa, ad ogni $f : X \to \{0,1\}$ possiamo associare $f^{-1}(1) \in P(X)$. Le due applicazioni $Y \mapsto \phi_Y$ e $f \mapsto f^{-1}(1)$ sono una l'inversa dell'altra. Ciascuna delle due costituisce quindi una corrispondenza biunivoca tra $P(X)$ e $\{0,1\}^X$. □

L'insieme $\mathbb{R}$ è equipotente a qualsiasi suo intervallo limitato

Lemma 5.2. *$\mathbb{R}$ ha la stessa cardinalità degli intervalli $(0,1)$, $[0,1)$, $[0,1]$.*

Dimostrazione. Basta dimostrare che $|\mathbb{R}| = |(0,1)|$, dal momento che gli altri intervalli differiscono da $(0,1)$ per un numero finito di elementi. Per quanto riguarda $(0,1)$, basta esibire un'applicazione $(0,1) \to \mathbb{R}$ invertibile, ad esempio

$$(0,1) \ni x \mapsto \frac{1}{x} + \frac{1}{x-1} \in \mathbb{R}$$

è invertibile[6]. □

Proposizione 5.3. *L'applicazione* $\phi : \{0,1\}^{\mathbb{N}} \to [0,1]$ *definita da*

$$\{0,1\}^{\mathbb{N}} \ni f \mapsto \phi(f) = \sum_{n \in N} \frac{f(n)}{2^{n+1}}$$

è suriettiva, e $\phi^{-1}(\alpha)$ *contiene al più due elementi per ogni* $\alpha \in [0,1]$.

Dimostrazione. Gli elementi di $\{0,1\}^{\mathbb{N}}$ sono applicazioni da $\mathbb{N}$ in $\{0,1\}$, o equivalentemente successioni di cifre 0 e 1. In quest'ottica, l'applicazione ϕ associa ad ogni successione $(f(n), n \in \mathbb{N})$ di cifre 0 e 1 il numero reale compreso tra 0 e 1 la cui espansione in cifre binarie dopo la virgola è data esattamente dalla successione $(f(n), n \in \mathbb{N})$ — convincetevi di questo, prima di andare avanti.

Contrariamente a quello che viene solitamente raccontato, esistono espansioni binarie[7] distinte che danno origine allo stesso numero reale. Tuttavia nessun numero reale è associato a più di due espansioni binarie. Supponiamo infatti che $f \neq g \in \{0,1\}^{\mathbb{N}}$ siano tali che $\phi(f) = \phi(g)$. Allora

$$\sum_{n \in \mathbb{N}} \frac{f(n) - g(n)}{2^{n+1}} = 0.$$

Se $f \neq g$, allora esiste almeno un $n \in \mathbb{N}$ tale che $f(n) \neq g(n)$. Sia N il minimo tra questi numeri naturali. A meno di scambiare f e g tra loro, possiamo supporre che $f(N) - g(N) = 1$. Allora abbiamo

$$\sum_{n=N}^{\infty} \frac{f(n) - g(n)}{2^{n+1}} = 0, \quad \text{cioè} \quad \frac{1}{2^{N+1}} = \sum_{n=N+1}^{\infty} \frac{g(n) - f(n)}{2^{n+1}}.$$

Il secondo membro è facile da stimare:

$$\sum_{n=N+1}^{\infty} \frac{g(n) - f(n)}{2^{n+1}} \leq \sum_{n=N+1}^{\infty} \frac{1}{2^{n+1}} = \frac{1}{2^{N+1}},$$

e la disuguaglianza non è stretta se e solo se le differenze $g(n) - f(n)$ sono tutte uguali ad 1. Ricordando che $f(n), g(n) \in \{0,1\}$, si ricava immediatamente che $g(n) = 1, f(n) = 0$ per ogni $n > N$, mentre sapevamo già che $g(N) = 0$ e $f(N) = 1$.

Pertanto se $\phi^{-1}(\alpha)$ non contiene un solo elemento, tra gli elementi contenuti in $\phi^{-1}(\alpha)$ vi è sicuramente f per il quale esiste $N \in \mathbb{N}$ tale che $f(N) = 1$ e $f(n) = 0$ per ogni $n > N$. Inoltre, ogni altro elemento $g \in \phi^{-1}(\alpha), g \neq f$ è tale che $g(n) = f(n)$ per $n < N$, $g(N) = 0$ e $g(n) = 1$ per ogni $n > N$. In particolare, $\phi^{-1}(\alpha)$ contiene soltanto questi due elementi. □

Lemma 5.4. *Siano* X, Y *insiemi infiniti, e* $f : X \to Y$ *un'applicazione suriettiva tale che* $f^{-1}(y)$ *è un insieme finito o numerabile per ogni* $y \in Y$. *Allora* $|X| = |Y|$.

Dimostrazione. f è suriettiva, quindi $|Y| \leq |X|$. Poiché sappiamo che $|f^{-1}(\{y\})| \leq |\mathbb{N}|$, esiste per ogni $y \in Y$ un'applicazione iniettiva $\phi_y : f^{-1}(\{y\}) \to \mathbb{N}$. Ma allora l'applicazione $X \ni x \mapsto (f(x), \phi_{f(x)}(x)) \in Y \times \mathbb{N}$ è iniettiva, e quindi $|X| \leq |Y \times \mathbb{N}| = |Y|$. Di conseguenza, $|X| = |Y|$. □

Corollario 5.5. *L'insieme delle parti di* $\mathbb{N}$ *ha la potenza del continuo.*

Dimostrazione. Abbiamo già visto come $|P(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}|$ e $|\mathbb{R}| = |[0,1]|$. L'applicazione $\phi : \{0,1\}^{\mathbb{N}} \to [0,1]$ considerata nella Proposizione 5.3 è suriettiva, e $\phi^{-1}(\alpha)$ consiste al più di due elementi. Per il lemma precedente, abbiamo allora $|\mathbb{R}| = |[0,1]| = |\{0,1\}^{\mathbb{N}}| = |P(\mathbb{N})|$. □

Esercizi:

- $\mathbb{R}$ e $\mathbb{C}$ hanno la stessa cardinalità.
- Mostrate che se X è un insieme finito con almeno due elementi, $X^{\mathbb{N}}$ ha la stessa cardinalità di $\mathbb{R}$.
- Mostrate che il prodotto cartesiano di un'infinità numerabile di insiemi finiti, tutti con almeno due elementi, ha la stessa cardinalità di $\mathbb{R}$.
- Mostrate che $\mathbb{R}^{\mathbb{N}}$ ha la stessa cardinalità di $\mathbb{R}$.
  [Sugg.: Sapete che $\mathbb{R} \simeq \{0,1\}^{\mathbb{N}}$, *quindi* $\mathbb{R}^{\mathbb{N}} \simeq (\{0,1\}^{\mathbb{N}})^{\mathbb{N}} \simeq \{0,1\}^{\mathbb{N}\times\mathbb{N}} \simeq \{0,1\}^{\mathbb{N}}$*...]*
- Mostrate che $\mathbb{N}^{\mathbb{N}}$ ha la stessa cardinalità di $\mathbb{R}$.
- L'insieme delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$ ha la stessa cardinalità di $\mathbb{R}$.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it

---

[6] Questa funzione non ha nulla di magico: qualsiasi funzione suriettiva sull'intervallo $(0,1)$, come ad esempio $x \mapsto \cot(\pi x)$ sarebbe stata ugualmente valida.

[7] ma anche decimali! Ad esempio $0,99999\ldots$ e 1 individuano lo stesso numero reale.