ALGEBRA I: CARDINALITÀ DI INSIEMI

1. Processi e costruzioni infinite

Molte volte, in matematica, c'è la necessità di ripetere una data costruzione infinite volte. In tale situazione è spesso necessario compiere delle scelte arbitrarie, anch'esse in quantità infinita. La liceità dell'atto di compiere un'infinità di scelte arbitrarie è un argomento dibattuto: dal punto di vista puramente logico è stato mostrato che supporre di poterlo fare non porta a (nuove) contraddizioni — in altre parole, l'*assioma della scelta*, che garantisce la possibilità di compiere infinite scelte, è indipendente dagli altri assiomi generalmente usati in matematica.

L'assioma della scelta, insieme alle sue molteplici riformulazioni equivalenti, permette di mostrare molte proprietà interessanti in molte strutture algebriche; allo stesso modo permette di esibire comportamenti profondamente antiintuitivi: l'assioma della scelta consente di dimostrare l'esistenza di sottoinsiemi di $\mathbb{R}$ non misurabili secondo Lebesgue; un'altra delle sue conseguenze è il cosiddetto *paradosso di Banach-Tarski*[1], che garantisce la possibilità di ripartire la palla tridimensionale in un numero finito di pezzi, che possono poi essere ruotati e traslati in modo da ricomporre due palle tridimensionali delle stesse dimensioni di quella iniziale!

Il lemma di Zorn è forse la riformulazione più duttile dell'assioma della scelta, anche se a primo impatto è un po' dura da digerire. Prima di enunciarlo, vi ricordo che una *relazione d'ordine* su un insieme X è una relazione riflessiva, antisimmetrica e transitiva. Se su X è data una relazione d'ordine $\leq$, l'insieme X, o meglio la coppia $(X, \leq)$, si dice allora *insieme parzialmente ordinato*.

Una relazione d'ordine su X può essere *totale* quando, per ogni scelta di $x, y \in X$, almeno una tra $x \leq y$ e $y \leq x$ è vera — chiaramente sono entrambe vere se e solo se $x = y$; tuttavia la maggior parte delle relazioni d'ordine che ci interesseranno non saranno totali. Può accadere invece che un sottoinsieme C di X sia totalmente ordinato rispetto all'ordine parziale $\leq$ posseduto da X: in tal caso, C è detto *catena*. E' importante comprendere come le catene non debbano essere necessariamente sottoinsiemi finiti, né tantomeno numerabili. Una catena è semplicemente un sottoinsieme nel quale tutti gli elementi sono confrontabili, e può essere grande quanto vogliamo, compatibilmente con l'insieme che la ospita.

Esempio: Sia $A = \{a, b, c, 1, 2\}$, e sia X il suo insieme delle parti. La relazione di inclusione $\subseteq$ è di ordine parziale, ma non totale, in X. Ad esempio, nessuno tra i due sottoinsiemi $\{a, b\}, \{b, 1, 2\}$ è incluso nell'altro, sebbene non siano uguali. Tuttavia X contiene sottoinsiemi (di X) totalmente ordinati. Ad esempio:

$$C = \{\emptyset, \{a\}, \{a, b, 1\}, \{a, b, 1, 2\}\}$$

è totalmente ordinato, poiché comunque presi due suoi elementi (che sono sottoinsiemi di A) uno dei due è contenuto nell'altro. C è una di quelle che abbiamo definito catene: X non è totalmente ordinato da $\subseteq$, ma $C \subset X$ sì.

Vi ricordo ancora che, in un insieme parzialmente ordinato $(X, \leq)$, si chiama *maggiorante* di $Y \subset X$ ogni elemento $m \in X$ tale che $y \leq m$ per ogni $y \in Y$. Ad esempio 2 è un maggiorante di $Y = (0, 1)$ in $X = (\mathbb{R}, \leq)$ — a dire il vero ogni $m \geq 1$ è un maggiorante di Y. Un elemento $x \in X$ è invece *massimale* in X se non ci sono in X elementi più grandi, cioè se $x \leq y \Rightarrow x = y$. Ogni insieme parzialmente ordinato non vuoto *finito* ammette elementi massimali: se così non fosse, sarebbe possibile costruire una catena infinita di elementi distinti ognuno $\leq$ del successivo. Siamo pronti ad enunciare il

Lemma di Zorn: Sia $(X, \leq)$ un insieme parzialmente ordinato non vuoto nel quale ogni catena ha (almeno) un maggiorante. Allora X possiede elementi massimali.

Se credete che ogni insieme parzialmente ordinato debba contenere elementi massimali, pensate all'insieme X i cui elementi sono i sottoinsiemi finiti di $\mathbb{N}$, ordinato rispetto all'inclusione. Chiaramente nessun elemento di X è massimale, perché a ogni sottoinsieme finito di $\mathbb{N}$ posso aggiungere un elemento, ottenendo così un sottoinsieme più grande, ma ancora finito.

Questo insieme X non contiene elementi massimali, e non può quindi soddisfare le ipotesi del Lemma di Zorn: deve ammettere catene senza maggioranti. Ad esempio, se C è il sottoinsieme di X i cui elementi sono tutti i sottoinsiemi della forma $\{0, 1, \dots, n\}$:

$$C = \{\{0\}, \{0, 1\}, \{0, 1, 2\}, \{0, 1, 2, 3\}, \dots\},$$

allora C è chiaramente una catena che non ammette alcun maggiorante in X. In effetti, un sottoinsieme di $\mathbb{N}$ che contenga tutti tali sottoinsiemi (che sono tutti finiti) dovrebbe essere $\mathbb{N}$ stesso, che non è un insieme finito, e quindi non è un elemento di X.

Nonostante il nome del Lemma di Zorn, noi lo prenderemo come principio da non dimostrare, cioè come assioma. In effetti può essere dimostrato a partire dall'Assioma della scelta, ma l'Assioma della scelta stesso segue a partire

[1] che in realtà paradosso non è, essendo una costruzione totalmente lecita che non fornisce alcuna contraddizione, se non con la nostra logica geometrica intuitiva.

dal Lemma di Zorn: in altre parole, l'uno vale l'altro! Dal momento che la dimostrazione dell'Assioma della scelta a partire dal Lemma di Zorn è facile, mentre il viceversa è un po' più complicato, noi diamo per buono il Lemma di Zorn, e lo utilizziamo ogni volta che ci serve. Se siete interessati alla dimostrazione del Lemma di Zorn a partire dall'assioma della scelta, ne trovate una sul libro di *Topologia* di Marco Manetti.

2. Il Lemma di Zorn e l'Assioma della scelta

Ho fatto un gran parlare, finora, dell'Assioma della scelta, ma non ho ancora detto che cosa sia:

Assioma della scelta: Sia I un insieme (di indici), ed $\mathcal{X} = \{X_i, i \in I\}$ una famiglia di insiemi non vuoti (indicizzati da I); indichiamo inoltre con X l'unione di tutti gli X_i. Allora esiste una *funzione di scelta*, cioè un'applicazione $f : I \to X$ tale che $f(i) \in X_i$ per ogni $i \in I$.

Per i pignoli, avrei potuto utilizzare come insieme di indici $\mathcal{X}$ stesso, ed indicare l'unione di tutti gli elementi di $\mathcal{X}$ con $\bigcup \mathcal{X}$. Però garantire l'esistenza di $f : \mathcal{X} \to \bigcup \mathcal{X}$ tale che $f(x) \in x$ per ogni $x \in \mathcal{X}$ mi sembrava davvero troppo criptico! Quella data sopra non è l'unica formulazione dell'assioma della scelta, ma una delle più naturali — e in ogni caso, sono tutte equivalenti.

Perché l'Assioma della scelta dovrebbe essere intuitivamente valido? Dal mio punto di vista[2], questo è chiaro: devo scegliere un elemento da uno degli X_i, un altro elemento da un altro degli X_i, e così via. E' chiaro che se le scelte le devo fare io, non termino mai; ma è altrettanto chiaro che una scelta di un elemento da ogni insieme è possibile — almeno a me è chiaro e intuitivo: non so a voi!

Il Lemma di Zorn è lo strumento creato appositamente per trasformare le parole "e così via" in un argomento stringente. Descrivo la dimostrazione con estrema attenzione ai dettagli, perché è il prototipo di ogni utilizzo del Lemma di Zorn. Le dimostrazioni che fanno uso del Lemma di Zorn diverranno sempre più asciutte, man mano che diventeremo familiari con tale strumento.

Dimostrazione dell'Assioma della scelta a partire dal Lemma di Zorn: Definiamo un insieme $\mathcal{F}$ come segue

$$\mathcal{F} = \{(J, f) \mid \quad J \subset I, \quad f : J \to X \text{ è tale che } f(i) \in X_i \text{ per ogni } i \in J\}.$$

In altre parole, $\mathcal{F}$ è l'insieme delle funzioni di scelta *parziali*, cioè di quelle funzioni che scelgono un elemento da ciascun X_i non per tutti gli $i \in I$, ma solo per quegli i che appartengono ad un sottoinsieme $J \subset I$.

Innanzitutto, l'insieme $\mathcal{F}$ è non vuoto: sia perché esiste una funzione di scelta parziale definita su $J = \emptyset$, sia perché compiere una quantità finita di scelte non crea problemi a nessuno, e quindi esistono anche funzioni di scelta parziali definite su sottoinsiemi finiti di I. Possiamo inoltre definire una relazione di ordine parziale su $\mathcal{F}$ come segue: $(J, f) \leq (J', f')$ se e solo se $J \subset J'$ e la restrizione di f' a J coincide con f. In altri termini $(J, f) \leq (J', f')$ se f' è sicuramente definita su tutti gli indici sui quali è definita anche la f (ma possibilmente anche su altri indici), e su tali indici sceglie gli stessi elementi che sceglie f: in parole povere $(J, f) \leq (J', f')$ se f' *estende* f.

Ora, se un elemento (J, f) in $\mathcal{F}$ non è definito su tutto I, cioè $J \neq I$, è facile estenderlo ad un insieme un po' più grande: si sceglie $i \notin J$, e si sceglie $f(i) \in X_i$. Queste sono solo due scelte da fare, e non rappresentano una difficoltà psicologica insormontabile neanche per chi nega l'assioma di scelta. Ci siamo quindi convinti che (J, f) non possa essere massimale in $\mathcal{F}$, a meno che $J = I$. Ma se $(I, f) \in \mathcal{F}$, allora $f : I \to X$ è una funzione di scelta! Quindi per mostrare l'esistenza di una funzione di scelta è sufficiente mostrare l'esistenza di elementi massimali in $\mathcal{F}$. E' qui che entra in gioco il Lemma di Zorn.

Il Lemma di Zorn garantisce l'esistenza di elementi massimali in $\mathcal{F}$ non appena siamo in grado di mostrare che ogni catena in $\mathcal{F}$ ammette un maggiorante. Sia quindi $\mathcal{C}$ una catena in $\mathcal{F}$: gli elementi di $\mathcal{C}$ sono coppie (J, f) tutte confrontabili tra loro; le funzioni di scelta parziali corrispondenti si estendono l'una con l'altra. Ogni maggiorante di $\mathcal{C}$ deve essere una coppia $(\overline{J}, \overline{f})$ con la proprietà che $J \subset \overline{J}$ per ogni $(J, f) \in \mathcal{C}$ e tale che $\overline{f}$ estende tutte le f contemporaneamente. Ma costruire un tale maggiorante è facile!

Si prende come $\overline{J}$ l'unione di tutti i J degli elementi di $\mathcal{C}$, e si definisce $f : \overline{J} \to X$ come $\overline{f}(j) = f(j)$ se $(f, J) \in \mathcal{C}$ e $j \in J$. Questa definizione non dipende dalla scelta di $(f, J) \in \mathcal{C}$ perché le funzioni descritte da elementi di $\mathcal{C}$ si estendono l'una con l'altra. Inoltre $\overline{J}$ è l'unione di tutti i J degli elementi di $\mathcal{C}$, e quindi se $j \in \overline{J}$, allora j appartiene ad almeno uno dei sottoinsiemi J.

Abbiamo mostrato che ogni catena in $\mathcal{F}$ ammette un maggiorante; grazie al Lemma di Zorn, $\mathcal{F}$ possiede elementi massimali, cioè funzioni di scelta per la famiglia $\mathcal{X} = \{X_i, i \in I\}$. □

L'utilizzo del Lemma di Zorn si fa sempre in questo modo: si inventa un insieme parzialmente ordinato i cui elementi massimali diano risposta positiva al nostro problema; quindi si costruisce un maggiorante per ogni catena. Nel caso dell'Assioma della scelta, le funzioni di scelta sono funzioni di scelta parziali massimali (va mostrato, e noi lo abbiamo mostrato), e l'esistenza di maggioranti delle catene si fa semplicemente considerando la funzione di scelta definita sull'unione dei domini delle funzioni di scelta parziali appartenenti alla catena.

Notate che la dimostrazione di sopra traduce perfettamente la dimostrazione data a lezione, che era: *scelgo un indice, e scelgo un elemento dall'insieme che indicizza, poi scelgo un altro indice, e scelgo un elemento dall'insieme che indicizza... Quando non posso più andare avanti, vuol dire che l'insieme di indici per i quali ho operato la scelta coincide con tutto* I.

Il Lemma di Zorn è quel che c'è dietro i puntini di sospensione: nel procedimento di scegliere ogni volta un nuovo indice, ed un elemento dall'insieme che indicizza, sto costruendo una catena di funzioni di scelta parziali. Come

[2]Ma come vi ho detto, la percezione di che cosa sia *intuitivo* varia da persona a persona..

esseri umani, possiamo operare soltanto una famiglia finita, arbitrariamente grande, di scelte (quindi costruire una catena numerabile), ma allora il Lemma di Zorn ci garantisce l'esistenza di un maggiorante, cioè di una scelta fatta sull'insieme numerabile (grande almeno quanto quello) dato dall'unione di tutti gli indici che abbiamo considerato finora. Ma allora possiamo scegliere un altro indice fuori, ed un altro elemento nell'insieme che indicizza, e continuare la nostra catena oltre l'infinità numerabile di scelte fatta inizialmente. Anche in questo caso, il Lemma di Zorn ci garantisce l'esistenza di una funzione di scelta definita sull'unione dei due insiemi numerabili, e di poter andare avanti.

La cosa stupefacente è che il Lemma di Zorn incorpora al suo interno la possibilità, procedendo di scelte numerabili in scelte numerabili, di raggiungere sottoinsiemi di cardinalità qualsivoglia elevata: l'importante è essere in grado, ad ogni passo, di costruire un maggiorante (cioè una estensione collettiva di tutte le funzioni di scelta compatibili fino a quel momento considerate) di qualsiasi catena, qualsiasi sia la sua cardinalità.

3. Due applicazioni del Lemma di Zorn

Avete già visto nel corso di algebra lineare che ogni spazio vettoriale di dimensione finita possiede una base. L'assioma della scelta permette di dimostrare l'esistenza di basi in spazi vettoriali qualsiasi, anche non di dimensione finita.

Prima di procedere, è il caso di chiarire cosa intendiamo per base quando lo spazio non ha dimensione finita. Se V è uno spazio vettoriale sul campo $\mathbb{K}$, un sottoinsieme $X = \{v_i, i \in I\} \subset V$ si dice *linearmente indipendente* se ogni sottoinsieme finito di X è linearmente indipendente. Si dice che X genera V se ogni elemento di V si può esprimere come combinazione lineare di un numero finito di elementi di X. X è una base di V se è linearmente indipendente e genera V. In altre parole, generalizziamo il concetto di dipendenza lineare e base imponendo che le combinazioni lineari siano tutte finite.

Ricordiamo che, nel caso di spazi vettoriali di dimensione finita, è sufficiente scegliere un vettore non nullo v_1; poi un vettore v_2 non appartenente alla retta generata da v_1; poi un vettore v_3 non appartenente al piano generato da v_1, v_2 e così continuando. L'ipotesi di dimensione finita ci garantisce che dopo un numero finito di passi, i vettori scelti, che costituiscono un insieme linearmente indipendente per il modo in cui sono stati selezionati, dovranno generare l'intero spazio vettoriale. Questo non accade per spazi vettoriali di dimensione infinita.

Proposizione 3.1. *Ogni spazio vettoriale possiede almeno una base.*

Dimostrazione. Se V è uno spazio vettoriale sul campo $\mathbb{K}$, poniamo $\mathcal{F} = \{X \subset V \,|\, V \text{ è linearmente indipendente}\}$. L'insieme $\mathcal{F}$ è non vuoto, poiché $\emptyset \in \mathcal{F}$. Inoltre, $\mathcal{F}$ è parzialmente ordinato dalla relazione di inclusione. E' importante mostrare l'esistenza di elementi massimali in $\mathcal{F}$ poiché questi sono le basi di V!

In effetti, se X non è una base di V, allora X non genera V. Detto $U_X \subset V$ l'insieme degli elementi di V che si possono esprimere come combinazioni lineari di un numero finito di elementi di X, se $v \in V \backslash U_X$, allora $X' = X \cup \{v\}$ è ancora linearmente indipendente: ogni sottoinsieme finito di X' che non contiene v è linearmente indipendente in quanto sottoinsieme di X; ma questo è vero anche dei sottoinsiemi finiti che contengono v. Ogni relazione lineare non banale $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n + \beta v = 0$ permette di esprimere v come combinazione lineare dei v_i se $\beta \neq 0$, ed è una relazione lineare tra elementi di X se $\beta = 0$. Questo mostra che se X non genera V, non può allora essere massimale.

L'esistenza di elementi massimali in $\mathcal{F}$ sarà immediata se possiamo mostrare che $\mathcal{F}$ soddisfa le ipotesi del Lemma di Zorn. Sappiamo già che è un'insieme parzialmente ordinato non vuoto; mostriamo ora che ogni catena $\mathcal{C} \subset \mathcal{F}$ possiede un maggiorante. Se abbiamo $\mathcal{C} = \{X_j, j \in J\}$, consideriamo l'insieme $X = \bigcup_{j \in J} X_j$. Per come è definito, X contiene tutti i sottoinsiemi $X_j, j \in J$; se mostriamo che X è linearmente indipendente, allora $X \in \mathcal{F}$ è un maggiorante di $\mathcal{C}$.

Per convincerci che X è linearmente indipendente dobbiamo far vedere che ogni sottoinsieme finito di X è linearmente indipendente. In effetti, se $\{x_1, \ldots, x_n\}$ è un sottoinsieme di X, allora ciascun $x_i, i = 1, \ldots, n$ appartiene ad un elemento di $\mathcal{C}$, diciamo a X_{j_i}. Dal momento che $\mathcal{C}$ è una catena, uno tra tali insiemi (sono in numero finito!) contiene tutti gli altri: in altre parole, possiamo trovare $j \in J$ tale che $x_1, \ldots, x_n$ siano tutti elementi di X_j. Ma a questo punto è facile concludere: poiché $X_j \in \mathcal{C} \subset \mathcal{F}$, sappiamo che X_j è linearmente indipendente; pertanto il suo sottoinsieme finito $\{x_1, \ldots, x_n\}$ deve essere anch'esso linearmente indipendente. □

Questa è un'altra applicazione del Lemma di Zorn, che ho fatto a lezione.

Proposizione 3.2. *Per ogni scelta di X, Y insiemi, esiste un'applicazione iniettiva di X in Y oppure di Y in X.*

Dimostrazione. La dimostrazione rigorosa è una riformulazione della seguente osservazione: è sufficiente mettere in corrispondenza biunivoca tra loro gli elementi di X con quelli di Y una coppia alla volta; il processo si interrompe quando non rimangono più elementi in X, nel qual caso è stata costruita un'applicazione iniettiva da X in Y, o non ne restano più in Y, ed abbiamo costruito un'applicazione iniettiva da Y in X.

Sia $\mathcal{F} = \{(U, V, \phi) \,|\, U \subset X, V \subset Y, \, \phi : U \to V \text{ è invertibile}\}$, e poniamo $(U, V, \phi) \leq (U', V', \phi')$ se $U \subset U', V \subset V'$ e $\phi'|_U = \phi$. Si vede subito che $\leq$ è una relazione d'ordine: la riflessività e la transitività sono ovvie, e la simmetria non presenta grandi difficoltà. Pertanto, $(\mathcal{F}, \leq)$ è un insieme parzialmente ordinato, ed è non vuoto in quanto $(\emptyset, \emptyset, \mathrm{id})$ appartiene ad $\mathcal{F}$.

Vogliamo mostrare che $(\mathcal{F}, \leq)$ soddisfa le ipotesi del Lemma di Zorn, e cioè che ogni catena in $\mathcal{F}$ ammette un maggiorante. Se $\mathcal{C} = \{(A_i, B_i, f_i), i \in I\}\mathcal{F}$ è una catena, poniamo $A = \bigcup_{i \in I} A_i, B = \bigcup_{i \in I} B_i$ e $f(a) = f_i(a)$ se $a \in A_i$: f definisce effettivamente un'applicazione $A \to B$, poiché ogni elemento di A appartiene ad A_i per qualche i. Inoltre, se a appartiene sia ad A_i che ad A_j, allora, a meno di scambiare i con j, deve valere l'inclusione $A_i \subset A_j$

e $f_j|A_i = f_i$. In altre parole, f_i ed f_j coincidono su A_i, e pertanto restituiscono lo stesso risultato se calcolate su $a \in A_i \cap A_j$. L'iniettività e la suriettività di f seguono dall'invertibilità di ciascuna delle f_i (controllatelo!). L'elemento (A, B, f) è allora un maggiorante di $\mathcal{C}$.

Poiché $\mathcal{F}$ soddisfa le ipotesi del Lemma di Zorn, deve possedere elementi massimali. Si vede facilmente che se $A \neq X, B \neq Y$, l'elemento $(A, B, f) \in \mathcal{F}$ non può essere massimale. Ma allora $A = X$ oppure $B = Y$, e in entrambi i casi abbiamo concluso. □

L'importanza del risultato appena dimostrato diventerà evidente una volta introdotto il concetto di cardinalità di un insieme.

4. 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 4.1. 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 4.2. 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 4.3. 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 4.4. 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 4.5. Se $X \subset Y$, allora $|X| \leq |Y|$. In effetti l'inclusione $\iota : X \to Y$ è sempre un'applicazione iniettiva.

Osservazione 4.6. 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 4.7. *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 4.8. 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.

Il teorema che segue è il cosiddetto Teorema di Cantor-Schröder-Bernstein.

Teorema 4.9. *Se $|X| \leq |Y|$ e $|Y| \leq |X|$ allora $|X| = |Y|$.*

Dimostrazione. Siano $f : X \to Y$ e $g : Y \to X$ applicazioni iniettive. Poniamo

$$N_X = \{x \in X \mid x \in \mathrm{Im}(gf)^n \text{ per ogni } n \in \mathbb{N}\},$$
$$V_X = \{x \in X \mid \text{ esiste } n \in \mathbb{N} \text{ tale che } x \in \mathrm{Im}(gf)^n \text{ ma } x \notin \mathrm{Im}((gf)^n g)\},$$
$$R_X = \{x \in X \mid \text{ esiste } n \in \mathbb{N} \text{ tale che } x \in \mathrm{Im}((gf)^n g) \text{ ma } x \notin \mathrm{Im}(gf)^{n+1}\}.$$

Allo stesso modo, poniamo

$$N_Y = \{y \in Y \mid y \in \mathrm{Im}(fg)^n \text{ per ogni } n \in \mathbb{N}\},$$
$$V_Y = \{y \in Y \mid \text{ esiste } n \in \mathbb{N} \text{ tale che } x \in \mathrm{Im}((fg)^n f) \text{ ma } y \notin \mathrm{Im}(fg)^{n+1}\},$$
$$R_Y = \{y \in Y \mid \text{ esiste } n \in \mathbb{N} \text{ tale che } x \in \mathrm{Im}(fg)^n \text{ ma } x \notin \mathrm{Im}((fg)^n f)\}.$$

E' facile verificare che N_X, V_X, R_X costituiscono una partizione di X: in altre parole, sono a due a due disgiunti e la loro unione è tutto X. Allo stesso modo, N_Y, V_Y, R_Y costituiscono una partizione di Y. Inoltre $f(N_X) = N_Y, f(V_X) = V_Y$ e $g(R_Y) = R_X$. Pertanto $f|_{N_X}, f|_{V_X}$ e $g|_{R_Y}$ sono tutte invertibili, e ponendo

$$h(x) = \begin{cases} f(x) & \text{se } x \in N_X \cup V_X \\ g^{-1}(x) & \text{se } x \in R_X \end{cases}$$

si ottiene un'applicazione invertibile da X a Y. □

Osservazione 4.10. 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 4.9 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.

Il fatto intuitivo che due insiemi infiniti hanno la stessa grandezza, oppure uno dei due è più grande dell'altro, è una semplice riformulazione di un risultato già mostrato

Proposizione 4.11. *Siano X e Y insiemi. Allora $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

Dimostrazione. Per la Proposizione 3.2, esiste un'applicazione iniettiva da X in Y, oppure un'applicazione iniettiva da Y in X. □

5. 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 5.1. Chiaramente, due insiemi numerabili hanno la stessa cardinalità, perché la proprietà 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 5.2. *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:

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

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 5.3. *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 4.3. 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 5.4. *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 5.3. Il caso generale segue da una semplice induzione. (Fatela!) □

Lemma 5.5. *$\mathbb{N} \times \{0, 1\}$ 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 5.6. *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 4.7 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 5.7. *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 5.6 l'unione di $n + 1$ insiemi numerabili

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

è anche unione di n insiemi numerabili. □

Lemma 5.8. *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[3]. □

Corollario 5.9. *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 5.10. *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 4.7, abbiamo $|X| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, e quindi

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

e per il Teorema 4.9, si ha $|X| = |\mathbb{N}|$. □

Lemma 5.11. *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 $\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N}$ ammette una corrispondenza biunivoca con $\mathbb{N} \times \mathbb{N}$ per ipotesi induttiva, e quindi anche con $\mathbb{N}$ grazie al Lemma 5.8. □

Corollario 5.12. *Sia $n > 0$. I sottoinsiemi di $\mathbb{N}$ di cardinalità minore o uguale ad n sono un'infinità numerabile.*

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

Dimostrazione. E' sufficiente mostrare la numerabilità della famiglia $P_n(\mathbb{N})$ dei sottoinsiemi *non vuoti* di $\mathbb{N}$ di cardinalità $\leq n$. La maggiorazione $|\mathbb{N}| \leq |P_n(\mathbb{N})|$ 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 $(a_1, \ldots, a_n)$ il sottoinsieme $\{a_1, \ldots, a_n\}$. Pertanto $|P_n(\mathbb{N})| \leq |\mathbb{N}^n| = |\mathbb{N}|$. □

Proposizione 5.13. *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 $\leq n$ è numerabile per il corollario precedente, e $P'(\mathbb{N})$ è la loro unione, che è numerabile per il Corollario 6.7. □

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

6. 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.

6.1. Generalità sulla cardinalità degli insiemi finiti.

Lemma 6.1. *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

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

si ottiene l'applicazione iniettiva desiderata[4]. □

Corollario 6.2. *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.*

Dimostrazione. Se X è il nostro insieme, abbiamo appena visto che possiede un sottoinsieme numerabile U. Per il Corollario 5.4, aggiungendo o togliendo ad U un numero finito di elementi si ottiene ancora un sottoinsieme numerabile.

Se X' è ottenuto da X togliendo un sottoinsieme finito F, non è quindi restrittivo supporre che $F \subset U$. Sia $f : U \to U \setminus F$ un'applicazione invertibile. Allora

$$h(x) = \begin{cases} f(x) & \text{se } x \in U \\ x & \text{se } x \notin U \end{cases}$$

è un'applicazione invertibile $X \to X' = X \setminus F$, e quindi $|X| = |X \setminus F|$.

Se X' è ottenuto da X aggiungendo un sottoinsieme finito, è sufficiente scambiare il ruolo di X e X'. □

Proposizione 6.3. *Se X è un insieme infinito, allora $X \times \{0, 1\}$ ha la stessa cardinalità di X.*

Dimostrazione. Se X è numerabile, l'enunciato segue dal Lemma 5.5. Se X è più che numerabile, consideriamo l'insieme $\mathcal{F} = \{(U, \phi) \,|\, U \subset X \text{ è infinito, e } \phi : U \to U \times \{0, 1\} \text{ è invertibile}\}$. $\mathcal{F}$ è certamente non vuoto, poiché X contiene sottoinsiemi numerabili, che possono essere messi in corrispondenza biunivoca col loro doppio.

Se poniamo $(U, \phi) \leq (V, \psi)$ quando $U \subset V$ e $\psi|_U = \phi$, è facile verificare, come al solito, come $\leq$ definisca una relazione d'ordine parziale su $\mathcal{F}$.

Sia ora $\mathcal{C} \subset \mathcal{F}$ una catena. Se $\mathcal{C} = \{(A_i, f_i) \,|\, i \in I\}$, poniamo $A = \bigcup_{i \in I} A_i$, e definiamo un'applicazione $f : A \to A \times \{0, 1\}$ data da $f(a) = f_i(a)$ se $a \in A_i$; poiché $\mathcal{C}$ è una catena, le f_i si estendono l'una l'altra, e quindi se a appartiene sia ad A_i che ad A_j, si ha $f_i(a) = f_j(a)$; pertanto $f(a)$ non dipende dalla scelta di $i, a \in A_i$. L'invertibilità di f segue dall'invertibilità di ciascuna delle f_i (mostratelo!).

Possiamo concludere che $(A, f) \in \mathcal{F}$ maggiora ciascun (A_i, f_i), ed è quindi un maggiorante della catena $\mathcal{C}$. In conclusione, $\mathcal{F}$ soddisfa le ipotesi del Lemma di Zorn, e possiede quindi almeno un elemento massimale (M, μ). Se $X \setminus M$ è finito, abbiamo concluso: si avrebbe infatti $|X| = |M|, |X \times \{0, 1\}| = |M \times \{0, 1\}|$ per il Corollario 6.2, e sappiamo che $|M| = |M \times \{0, 1\}|$ grazie all'applicazione invertibile μ.

Se invece $X \setminus M$ è infinito, arriviamo facilmente ad un assurdo: possiamo trovare un sottoinsieme numerabile $U \subset X \setminus M$ che può essere messo in corrispondenza biunivoca con $U \times \{0, 1\}$. Ma allora anche $M \cup U$ possiede una corrispondenza biunivoca con $(M \cup U) \times \{0, 1\}$ — basta incollare quella per M con quella per U — contro la massimalità di (M, μ). □

[4]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*

Corollario 6.4. *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 6.5. *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 6.6. Gli ultimi due corollari generalizzano il Corollario 5.4 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 6.7. *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 6.8. E' importante sottolineare che il Corollario 6.7 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 $\emptyset$.

6.2. **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 6.9. *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 $\mathcal{F} = \{(U, \phi) \,|\, U \subset X$ è infinito, e $\phi : U \to U \times U$ 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 $(U, \phi) \leq (V, \psi)$ se e solo se U è un sottoinsieme di V e la restrizione di ψ ad U coincide con ϕ. L'insieme parzialmente ordinato $(\mathcal{F}, \leq)$ soddisfa le ipotesi del Lemma di Zorn: in effetti se $\mathcal{C} = \{(A_i, f_i), i \in I\}$ è una catena in $\mathcal{F}$, allora si ottiene un maggiorante di $\mathcal{C}$ 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 $\mathcal{F}$. Voglio adesso mostrare che se (M, μ) è un elemento massimale di $\mathcal{F}$, la cardinalità di M *non può* essere strettamente inferiore a quella di X. In effetti, se $|M| < |X|$, allora $|X \setminus M| = |X|$ e quindi $|M| < |X \setminus M|$. Questo mostra che $X \setminus M$ contiene un sottoinsieme U della stessa cardinalità di M (ad esempio, l'immagine di un'applicazione iniettiva da M in $X \setminus M$). Il mio obiettivo è quello di costruire un elemento $(N, \nu) \in \mathcal{F}$ tale che $N = M \cup U$ e $(M, \mu) \leq (N, \nu)$: vediamo come fare.

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

$$N \times N = (M \times M) \cup (M \times U) \cup (U \times M) \cup (U \times U).$$

I tre insiemi $M \times U, U \times M, U \times U$ hanno tutti la stessa cardinalità di $M \times M$, e quindi di M, e quindi la cardinalità della loro unione $(N \times N) \setminus (M \times M)$ è uguale a quella di M, grazie al Corollario 6.7 e all'Osservazione 6.8.

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

$$\nu(n) = \begin{cases} \mu(n) & \text{se } n \in M \\ f(n) & \text{se } n \in U \end{cases}$$

definisce un'applicazione invertibile $\nu : N \to N \times N$ che estende μ. Pertanto $(M, \mu) \leq (N, \nu)$, contro la massimalità di (M, μ).

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

Corollario 6.10. *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 $|X \times Y| = |Y|$. □

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

Corollario 6.11. *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. □

7. 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 7.1 (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 7.2. *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 7.1 mostra che l'insieme $\mathbb{R}$ dei numeri reali non è numerabile.

Teorema 7.3. *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*.

8. 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 8.1. *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 8.2. *$\mathbb{R}$ 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 8.3. *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 $\alpha \in [0,1]$.

[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.

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 8.4. *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 8.5. *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 8.3 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 $\mathbb{R}$.
- (Difficile) Mostrate, utilizzando il Lemma di Zorn, che ogni insieme X può essere dotato di un buon ordinamento. *[Considerate l'insieme F i cui elementi sono coppie $(Y, \preceq)$ dove Y è un sottoinsieme di X e $\preceq$ è un buon ordinamento su Y, e definite su F una relazione d'ordine data da $(Y, \preceq) \leq (Y', \preceq')$ se e solo se: $Y \subseteq Y'$, la relazione $\preceq'$ coincide con $\preceq$ sugli elementi di Y, e $y \preceq' y'$ per ogni $y \in Y$, $y' \in Y' \setminus Y$.]*

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

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