ALGEBRA I: CARDINALITÀ DI INSIEMI E ASSIOMA DELLA SCELTA

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: $|X| = |Y|$, $X \simeq Y$. Due insiemi che hanno la stessa cardinalità si dicono anche *equipotenti*.

Osservazione 1.2. In ogni famiglia di insiemi[1] 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. Un modo di verificare che due insiemi X, Y abbiano la stessa cardinalità è quindi quello di metterli in corrispondenza biunivoca con uno stesso terzo insieme Z.

Osservazione 1.3. Se $f : A \to X$ e $g : B \to Y$ sono applicazioni invertibili, allora l'*applicazione prodotto*

$$f \times g : A \times B \ni (a, b) \mapsto (f(a), g(b)) \in X \times Y$$

è anch'essa invertibile. Di conseguenza, se $|A| = |X|$ e $|B| = |Y|$, allora $|A \times B| = |X \times Y|$. In altre parole, la cardinalità di un prodotto cartesiano non cambia se sostituiamo ciascun insieme fattore con uno equipotente.

Esempio 1.4. 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 1.5. 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: $|X| \leq |Y|, X \preceq Y$.

Osservazione 1.6. Se $X \subset Y$, allora $|X| \leq |Y|$. In effetti l'inclusione $\iota : X \to Y$ è sempre un'applicazione iniettiva.

Osservazione 1.7. 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 nella dimostrazione del Teorema 1.11 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.

Osservazione 1.8. Dire che $|X| \leq |Y|$ è equivalente a dire che X è in corrispondenza biunivoca con un sottoinsieme di Y. In effetti, se $f : X \to Y$ è iniettiva, allora f stabilisce una corrispondenza biunivoca tra X e l'immagine $f(X) \subset Y$. Viceversa, se $|X| = |U|$, dove $U \subset Y$, allora $|U| \leq |Y|$ per l'Osservazione 1.6 e quindi $|X| \leq |Y|$.

[1] In questi appunti, *famiglia di insiemi* vuol dire esattamente *insieme di insiemi*, ma è meno cacofonico.

Osservazione 1.9. Poiché un'applicazione invertibile è automaticamente iniettiva, se $|A| = |X|, |B| = |Y|$ e $|A| \leq |B|$, allora si ha anche $|X| \leq |Y|$. In altre parole, in un confronto tra cardinalità si può sostituire ciascun insieme con uno equipotente.

Inoltre, analogamente a quanto visto nell'Osservazione 1.3, da $|A| \leq |X|, |B| \leq |Y|$ segue $|A \times B| \leq |X \times Y|$.

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 insiemi che possiedono tuttavia la stessa cardinalità.

Osservazione 1.10. Prima di andare avanti, devo fare un commento importante. Supponiamo di avere applicazioni $f : A \to X$ e $g : B \to Y$, dove A, B sono insiemi disgiunti e X, Y sono insiemi disgiunti. Allora abbiamo un'applicazione $\phi : A \cup B \to X \cup Y$ definita da

$$\phi(c) = \begin{cases} f(c) & \text{se } c \in A \\ g(c) & \text{se } c \in B. \end{cases}$$

Quest'applicazione è iniettiva (risp. suriettiva, invertibile) non appena f, g sono entrambe iniettive (risp. suriettive, invertibili) come si verifica facilmente.[2]

Ad esempio, si può costruire una corrispondenza biunivoca tra due insiemi ripartendo ciascuno degli insiemi in più sottoinsiemi (non serve neanche che si tratti di un numero **finito** di pezzi) e mettendo ordinatamente in corrispondenza biunivoca ciascun sottoinsieme del primo insieme con ciascun sottoinsieme del secondo insieme. Questa è una strategia che adotteremo frequentemente, senza ulteriori commenti.

Teorema 1.11 (Bernstein-Schröder, Cantor, Dedekind)**.** *Se* $|X| \leq |Y|$ *e* $|Y| \leq |X|$ *allora* $|X| = |Y|$.

Dimostrazione. Dobbiamo mostrare che se $f : X \to Y$ e $g : Y \to X$ sono applicazioni iniettive, possiamo costruire una corrispondenza biunivoca tra X e Y.

Inizio con una premessa pignola che non ho fatto a lezione: possiamo supporre senza perdere di generalità che X e Y siano insiemi disgiunti. In effetti, se $A = X \cup Y$, possiamo mettere X in corrispondenza biunivoca con $X' = X \times \{0\} \subset A \times \{0, 1\}$ e Y con $Y' = Y \times \{1\} \subset A \times \{0, 1\}$. I sottoinsiemi X', Y' sono disgiunti per costruzione, e l'enunciato del teorema è equivalente a quello che si ottiene sostituendo X con X' e Y con Y'.

Come detto a lezione, per ogni scelta di $x \in X$ possiamo costruire una successione di elementi

$$x \mapsto f(x) \mapsto g(f(x)) \mapsto f(g(f(x))) \mapsto \dots$$

che appartengono alternativamente agli insiemi X, Y. Ogni elemento in una tale successione determina tutti quelli successivi. Allo stesso modo, se $x \in X$ appartiene all'immagine di g (e solo in tal caso!) possiamo prolungare verso sinistra tale successione:

$$g^{-1}(x) \mapsto x \mapsto f(x) \mapsto g(f(x)) \mapsto f(g(f(x))) \mapsto \dots$$

in un unico modo, poiché g è iniettiva. Allo stesso modo, se $g^{-1}(x) \in Y$ sta nell'immagine di f, possiamo estendere ancora la successione verso sinistra

$$f^{-1}(g^{-1}(x)) \mapsto g^{-1}(x) \mapsto x \mapsto f(x) \mapsto g(f(x)) \mapsto f(g(f(x))) \mapsto \dots$$

In ciascuna di tali successioni, ogni elemento di X si ottiene da quello alla sua sinistra applicando g e ogni elemento di Y si ottiene da quello alla sua sinistra applicando f.[3]

Diremo che $x \in X$ è di tipo 1 se la successione appena descritta si può estendere indefinitamente (= tante volte quante si voglia) verso sinistra[4]; di tipo 2 se si arriva ad un elemento di X che non appartiene all'immagine di g; di tipo 3 se si giunge ad un elemento di Y che non appartiene all'immagine di f. Si definiscono allo stesso modo elementi di tipo 1, 2, 3 nell'insieme Y. E' evidente che $f : X \to Y$ manda elementi di X di tipo 1 (rispettivamente 2, 3) in elementi di Y di tipo 1 (risp. 2, 3), e analogamente si può dire di g.

Più precisamente, f stabilisce una corrispondenza biunivoca tra elementi di X di tipo 2 e elementi di Y di tipo 2; l'iniettività segue dall'iniettività di f, mentre la suriettività dipende dal fatto che ogni elemento $y \in Y$ di tipo 2 si trova alla destra di un elemento di X di tipo 2 e quindi appartiene all'immagine di f. In maniera analoga si vede che g definisce una corrispondenza biunivoca tra elementi di Y di tipo 3 e elementi di X di tipo 3. Nel caso degli elementi di tipo 1, sia f che g forniscono corrispondenze biunivoche. Ma allora l'applicazione $\phi : X \to Y$ definita da

$$\phi(x) = \begin{cases} f(x) & \text{se } x \text{ è di tipo 1, 2} \\ g^{-1}(x) & \text{se } x \text{ è di tipo 3} \end{cases}$$

è una corrispondenza biunivoca. □

[2] Fatelo!!!

[3] E' in questa frase e nelle successive che ho bisogno di poter dire che X, Y sono disgiunti, se voglio evitare confusione.

[4] Volendo essere estremamente formali, $x \in X$ è di tipo 1 se x appartiene all'immagine dell'applicazione $(g \circ f)^n$ per ogni n.

Osservazione 1.12. 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 1.11 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.

2. Insiemi numerabili

La prima cardinalità infinita che incontriamo è quella dell'insieme $\mathbb{N}$: ogni insieme infinito con la stessa cardinalità di $\mathbb{N}$ è detto *numerabile*. Per quanto già detto, due insiemi numerabili hanno quindi necessariamente la stessa cardinalità.

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 2.1. *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, se $x \in X$, sia n la cardinalità del sottoinsieme (finito!) $\{a \in \mathbb{N} \mid a < x\}$. Allora $x = \phi(n)$, il che garantisce la suriettività.[5] □

Lemma 2.2. *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 1.4. 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 2.3. *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 2.2. Il caso generale segue da una semplice induzione. (Fatela!) □

Lemma 2.4. *$\mathbb{N} \times \{0, 1\}$ 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 2.5. *L'unione di due insiemi numerabili è numerabile.*

Dimostrazione. Siano $\phi_X : X \to \mathbb{N}$, $\phi_Y : Y \to \mathbb{N}$ applicazioni invertibili. Allora l'applicazione $\phi : X \cup Y \to \mathbb{N} \times \{0, 1\}$ definita da

$$\phi(a) = \begin{cases} (\phi_X(a), 0) & \text{se } a \in X \\ (\phi_Y(a), 1) & \text{altrimenti} \end{cases}$$

è iniettiva, da cui $|X \cup Y| \leq |\mathbb{N} \times \{0, 1\}| = |\mathbb{N}|$. Allora $X \cup Y$ è in corrispondenza biunivoca con un sottoinsieme infinito di $\mathbb{N}$, ed è quindi numerabile per il Lemma 2.1. □

Corollario 2.6. *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 2.5 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 2.7. *L'insieme $\mathbb{N} \times \mathbb{N}$ è numerabile.*

[5] Dimostrate bene per induzione l'affermazione *"Se $x \in X$ ha n predecessori, allora $x = \phi(n)$"*.

Dimostrazione. L'applicazione definita da

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

è biunivoca[6]. □

Corollario 2.8. *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 2.9. *Se per ogni $i \in \mathbb{N}$ è data un'applicazione $\phi_i : X_i \to \mathbb{N}$ invertibile, allora l'unione $\bigcup_{i\in\mathbb{N}} X_i$ è un insieme numerabile.*

Dimostrazione. Indichiamo con X l'unione degli insiemi numerabili $X_i, i \in \mathbb{N}$. Allora possiamo definire un'applicazione $\phi : X \to \mathbb{N} \times \mathbb{N}$ data da

$$\phi(x) = (\phi_k(x), k) \qquad \text{se } k \text{ è il più piccolo indice tale che } x \in X_k.$$

L'applicazione ϕ è iniettiva, e quindi $|X| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, da cui la numerabilità di $\mathbb{N}$. □

Osservazione 2.10. E' irresistibile la tentazione di modificare l'enunciato nella formulazione *"L'unione numerabile di insiemi numerabili è numerabile"*. Come vi ho detto a lezione, questo richiede di nascondere un po' di polvere sotto il tappeto, il che non farò ancora per un po'.[7]

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 2.7. □

Corollario 2.12. *Sia $n > 0$. L'insieme $P_n(\mathbb{N})$, i cui elementi sono tutti e soli i sottoinsiemi di $\mathbb{N}$ di cardinalità uguale ad n, è numerabile.*

Dimostrazione. E' facile costruire un'applicazione iniettiva $P_n(\mathbb{N}) \to \mathbb{N}^n$, ad esempio associando al sottoinsieme $\{a_1, \ldots, a_n\}$ la n-upla $(a_1, \ldots, a_n)$ **una volta deciso** che $a_1 < a_2 < \ldots a_n$. $\{a_1, \ldots, a_n\}$. Pertanto $|P_n(\mathbb{N})| \leq |\mathbb{N}^n|$.

Abbiamo già dato una concreta biiezione (implicita ma può essere esplicitata) $\mathbb{N}^n \to \mathbb{N}$ e il Lemma 2.1 ci fornisce ora una corrispondenza biunivoca esplicita tra $P_n(\mathbb{N})$ e $\mathbb{N}$. □

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

Dimostrazione. $P'(\mathbb{N}) \setminus \{\emptyset\}$ è unione numerabile degli insiemi $P_n(\mathbb{N}), n > 0$, per ciascuno dei quali abbiamo una esplicita biiezione con $\mathbb{N}$. Possiamo allora utilizzare il Corollario 2.9. □

2.1. **Cardinalità di $\mathbb{Z}$ e $\mathbb{Q}$.**

Proposizione 2.14. *L'insieme $\mathbb{Z}$ è numerabile.*

Dimostrazione. L'applicazione $f : \mathbb{N} \to \mathbb{Z}$ definita da

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ è pari} \\ -(n+1)/2 & \text{se } n \text{ è dispari} \end{cases}$$

è invertibile. □

Proposizione 2.15. *L'insieme $\mathbb{Q}$ è numerabile.*

Dimostrazione. Se $n > 0$ è un numero naturale, indichiamo con X_n l'insieme dei numeri razionali della forma $a/n, a \in \mathbb{Z}$. Allora $X_n \ni a/n \mapsto f(a) \in \mathbb{N}$ è invertibile se f è l'applicazione della proposizione precedente.

Poiché $\mathbb{Q}$ è unione degli insiemi X_n, deve essere necessariamente numerabile. □

E' il momento di fare conoscenza con insiemi infiniti non numerabili.

---

[6] Convincetevi che è la stessa che ho descritto a lezione!

[7] Anche parecchia polvere: esistono *modelli* della teoria degli insiemi nei quali $\mathbb{R}$ è unione numerabile di insiemi numerabili. Come vedremo tra poco, $\mathbb{R}$ è però sicuramente non numerabile.

3. Il Teorema di Cantor

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 conseguenze indirette, permette di costruire un insieme infinito non numerabile e dimostra che non esiste un insieme di cardinalità massima.

Teorema 3.1 (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 $\Omega = \{x \in X \mid x \notin f(x)\}$.

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

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

Corollario 3.2. *Per ogni insieme X, si ha $|X| < |P(X)|$.*

Dimostrazione. L'applicazione $X \ni x \mapsto \{x\} \in P(X)$ è iniettiva, quindi $|X| \leq |P(X)|$. Tuttavia non esistono applicazioni suriettive $X \to P(X)$ e quindi nemmeno invertibili. □

Scopriamo quindi che l'insieme $P(\mathbb{N})$ delle parti di $\mathbb{N}$ non è numerabile. Una variante della dimostrazione del Teorema 3.1 mostra che nemmeno l'insieme $\mathbb{R}$ dei numeri reali è numerabile.

Teorema 3.3. *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*.

Osservazione 3.4. Abbiamo finora utilizzato un'idea molto confusa e imprecisa del concetto di insieme, che corrisponde più o meno a *"mucchio di elementi"*. Il Teorema di Cantor ci mette in guardia dal fatto che questa concezione informale di insieme è pericolosa: ad esempio *"l'unione di tutti gli insiemi"* non è un'espressione valida in matematica, o almeno non va interpretata come insieme, poiché conterrebbe (e avrebbe quindi cardinalità maggiore o uguale a) qualsiasi altro insieme.

Allo stesso modo, *"l'insieme di tutti gli insiemi"* è un concetto pericoloso, perché per ogni insieme A dovrebbe avere tra i suoi elementi tutti i sottoinsiemi di A e avere quindi cardinalità strettamente superiore a quella di A.

In generale, se si vogliono evitare contraddizioni bisogna avere un approccio un po' più formale della cosiddetta *Teoria ingenua degli insiemi*. Una buona regola approssimativa consiste nell'utilizzare, come insiemi, esclusivamente quelli che si costruiscono ricorsivamente a partire da altri insiemi attraverso prodotto cartesiano, insieme delle parti, unione e intersezione di una famiglia di insiemi che sia essa stessa un insieme, oppure scegliendo dentro un insieme dato quegli elementi che soddisfano una fissata proprietà. Alcune costruzioni sono inevitabili per fare matematica (che l'insieme vuoto, così come anche $\mathbb{N}$, siano insiemi, ad esempio), ma in generale, quando è possibile, bisogna essere cauti con il significato della parola "insieme".

4. La cardinalità del continuo

In questo 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 4.1. *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 $\{0,1\}^X$. □

Lemma 4.2. *$\mathbb{R}$ ha la stessa cardinalità dell'intervallo aperto $(0,1)$.*

Dimostrazione. E' sufficiente esibire un'applicazione $(0,1) \to \mathbb{R}$ invertibile, ad esempio

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

□

Lemma 4.3. *Aggiungere o togliere a $\mathbb{R}$ una quantità finita di elementi non ne modifica la cardinalità.*

Dimostrazione. Innanzitutto, $\mathbb{R}$ contiene il sottoinsieme numerabile $\mathbb{N}$. Se X è un insieme finito (diciamo disgiunto da $\mathbb{R}$) possiamo trovare una corrispondenza biunivoca tra $X \cup \mathbb{N}$ e $\mathbb{N}$ ed estenderla ad una biiezione $X \cup \mathbb{R} \to \mathbb{R}$ mandando ogni altro numero reale in se stesso.

Analogamente, se $X \subset \mathbb{R}$ è un sottoinsieme finito, sia $Y \subset \mathbb{R}$ un sottoinsieme numerabile che contiene X, come ad esempio $Y = X \cup \mathbb{N}$. Possiamo allora estendere una corrispondenza biunivoca $Y \to Y \setminus X$ a una biiezione $\mathbb{R} \to \mathbb{R} \setminus X$ mandando ogni elemento di $\mathbb{R} \setminus X$ in se stesso. □

Osservazione 4.4. Chiaramente, l'enunciato del Lemma 4.3 è valido anche per ogni insieme con la stessa cardinalità di $\mathbb{R}$.

Corollario 4.5. *$\mathbb{R}$ ha la stessa cardinalità di $[0, 1]$ e $[0, 1)$.*

Dimostrazione. I due intervalli differiscono da $(0, 1)$ per un numero finito di elementi. □

Lemma 4.6. *L'applicazione $\phi : \{0, 1\}^{\mathbb{N}} \to \mathbb{R}$ definita da*

$$\{0, 1\}^{\mathbb{N}} \ni f \mapsto \phi(f) = \sum_{n \in \mathbb{N}} \frac{f(n)}{10^{n+1}}$$

è iniettiva.

Dimostrazione. Due espansioni decimali diverse, le cui cifre siano solo 0 e 1, forniscono numeri reali distinti. □

Lemma 4.7. *L'applicazione $\psi : [0, 1) \to P(\mathbb{N})$ definita da*

$$\psi(\alpha) = \{n \in \mathbb{N} \mid \textit{l'n-esima cifra dopo la virgola nell'espansione binaria di } \alpha \textit{ è } 1\}$$

è iniettiva.

Dimostrazione. La parte dopo la virgola dell'espansione binaria di $\alpha \in [0, 1)$ è univocamente individuata da α.[8] □

Proposizione 4.8. *Gli insiemi $\mathbb{R}$ e $P(\mathbb{N})$ hanno la stessa cardinalità.*

Dimostrazione. Abbiamo mostrato finora che

$$|\mathbb{R}| = |[0, 1)| \leq |P(\mathbb{N})| = |\{0, 1\}^{\mathbb{N}}| \leq |\mathbb{R}|,$$

da cui segue l'affermazione fatta. □

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 $\mathbb{R}$.
- Mostrate che l'insieme delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$ ha la stessa cardinalità di $\mathbb{R}$.

5. L'ASSIOMA DELLA SCELTA

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 contraddizioni ulteriori rispetto a quelle già insite nella teoria degli insiemi — 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; consente tuttavia di esibire anche comportamenti profondamente antiintuitivi: attraverso l'assioma della scelta si costruiscono[9] sottoinsiemi non misurabili di $\mathbb{R}$; si decompone[10] la palla unitaria di $\mathbb{R}^3$ in un numero finito di pezzi che possono essere risistemati, attraverso movimenti rigidi, per ricomporre due palle unitarie distinte.

L'enunciato più economico dell'assioma della scelta è il seguente:

Assioma della scelta: prima forma. Se A, B sono insiemi e A è non vuoto, allora per ogni applicazione suriettiva $f : A \to B$ esiste un'applicazione $g : B \to A$ tale che $f \circ g = \mathrm{id}_B$.

Una dimostrazione informale di tale affermazione è la seguente: $f \circ g = \mathrm{id}_B$ si traduce in $f(g(b)) = b$ per ogni $b \in B$. Allora $g(b) \in A$ è un elemento che viene mandato da f in b. In altre parole, $g(b)$ è una controimmagine di b attraverso l'applicazione f.

[8] Qui ci mettiamo d'accordo che terminare una rappresentazione binaria con tutti 1 da un certo punto in poi non è ammissibile, come ci siamo detti a lezione.

[9] Cercate "Insieme di Vitali" in rete.

[10] Keyword: paradosso di Banack-Tarski.

Costruire un'inversa destra $g : B \to A$ alla suriezione $f : A \to B$ consiste nel fornire un modo di scegliere, per ogni $b \in B$, un elemento dell'insieme non vuoto $f^{-1}(b)$. Se B è finito, dobbiamo operare solo un numero finito di scelte, e questo non crea difficoltà concettuali. Quando invece B è infinito, a meno di dare una ricetta uniforme per procedere, la possibilità di costruire l'applicazione g è molto dibattuta nella comunità matematica. Per quanto ci riguarda, da questo momento in poi utilizzeremo l'assioma della scelta liberamente.

Proposizione 5.1. *Siano A, B insiemi non vuoti. Allora $|B| \leq |A|$ se e solo se esiste un'applicazione suriettiva $f : A \to B$.*

Dimostrazione. Un'inversa destra $g : B \to A$ di f è necessariamente iniettiva. □

Una conseguenza immediata di questo fatto è che se $\sim$ è una relazione di equivalenza sull'insieme X allora, detto $X/\sim$ il corrispondente insieme quoziente, si ha $|X/\sim| \leq |X|$. In effetti, la proiezione al quoziente $\pi : X \to X/\sim$ è suriettiva per definizione.

La prima forma dell'assioma della scelta che abbiamo dato è poco malleabile. Possiamo però dimostrarne un'altra versione, che segue immediatamente dalla prima.

Assioma della scelta: seconda forma. Sia I un insieme e $\{X_i\}_{i\in I}$ una famiglia di insiemi non vuoti. Allora esiste un'applicazione $\varphi : I \to \bigcup_{i\in I} X_i$ tale che $\varphi(i) \in X_i$.

Dimostrazione. Se $X = \bigcup_{i\in I} X_i$ indichiamo con $\pi_1 : X \times I \to X$, $\pi_2 : X \times I \to I$ le proiezioni sulla prima e sulla seconda coordinata. Poniamo $A = \{(x, i) \in X \times I \,|\, x \in X_i\}$.

La restrizione $\pi_2|_A : A \to I$ è suriettiva poiché ogni X_i è non vuoto. Se $g : I \to A$ è la sua inversa destra, la composizione $\varphi = \pi_1|_A \circ g : I \to X$ è la funzione di scelta cercata.[11] □

La funzione φ è detta *funzione di scelta* perché sceglie, effettivamente, un elemento da ciascuno degli insiemi.

Il lemma di Zorn è forse la riformulazione più duttile dell'assioma della scelta, anche se a primo impatto è un po' duro 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 a $\leq$: 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. Per convenzione, il sottoinsieme vuoto è una catena.

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 magari 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 $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato non vuoto[12] nel quale ogni catena ha (almeno) un maggiorante. Allora $\mathcal{F}$ possiede (almeno) un elemento massimale.

Se credete che ogni insieme parzialmente ordinato debba contenere elementi massimali, pensate all'insieme $\mathcal{F}$ i cui elementi sono i sottoinsiemi finiti di $\mathbb{N}$, ordinato rispetto all'inclusione. Chiaramente nessun elemento di $\mathcal{F}$ 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 $\mathcal{F}$ 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 $\mathcal{F}$ i cui elementi sono tutti i sottoinsiemi della forma $\{0, 1, \ldots, n\}$:

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

[11] A lezione ho spiegato tutto meglio, ma verificate che questa dimostrazione è la stessa!

[12] A dirla tutta, che $\mathcal{F}$ sia non vuoto segue dal fatto che la catena vuota deve possedere un maggiorante in $\mathcal{F}$.

allora C è chiaramente una catena che non ammette alcun maggiorante in $\mathcal{F}$. 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 $\mathcal{F}$.

Nonostante il nome del Lemma di Zorn, noi lo prenderemo come principio da non dimostrare, cioè come assioma. In effetti, come vedremo in seguito, può essere dimostrato a partire dall'Assioma della scelta, ma l'Assioma della scelta stesso segue a partire dal Lemma di Zorn: in altre parole, l'uno vale l'altro! Prima di mostrare l'equivalenza tra le due affermazioni, abbiamo però bisogno di sviluppare un po' di linguaggio.

6. Buoni ordinamenti

6.1. **Gergo.** Ricapitoliamo ora per comodità tutte le definizioni già date. Una relazione $\leq$ sull'insieme X si dice *ordinamento parziale* se soddisfa:

- $x \leq x$ per ogni $x \in X$ — *Riflessività*
- $x \leq y, y \leq x \implies x \leq z$ — *Transitività*
- $x \leq y, y \leq x \implies x = y$ — *Antisimmetria*

Ad esempio, l'inclusione $\subseteq$ è un'ordinamento parziale sull'insieme $X = P(\Omega)$ delle parti di un insieme Ω dato. E' importante notare come, dati $x, x' \in X$, non si richiede che $x \leq x'$ oppure $x' \leq x$: se questo accade, x, x' si dicono *confrontabili*. Un ordinamento parziale per il quale ogni coppia di elementi sia confrontabile si dice *ordinamento totale*. Se $x \leq x'$, si scrive anche $x' \geq x$; se $x \leq x'$ e $x \neq x'$, si scrive anche $x < x'$ o equivalentemente $x' > x$. Attenzione! Un ordinamento totale **è** un ordinamento parziale. Un insieme dotato di un ordinamento parziale/totale si dice, ovviamente, *insieme parzialmente/totalmente ordinato*.

Esempio 6.1. Le naturali relazioni d'ordine su $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono tutte ordinamenti totali.

Esempio 6.2. Se X possiede al più un elemento, ogni ordinamento parziale su X è totale.

Se $U \subset X$, un *maggiorante* (risp. *minorante*) di U è ogni elemento $m \in X$ tale che $m \geq u$ (risp. $m \leq u$) per ogni $u \in U$: in generale, $U \subset X$ può avere più di un maggiorante in X, ma può anche non averne alcuno.

Un elemento $m \in X$ si dice *massimale* (risp. *minimale*) se $m \leq m'$ (risp. $m \geq m'$) implica $m = m'$. Si dice *massimo* (risp. *minimo*) se $m \geq x$ (risp. $m \leq x$) per ogni $x \in X$. Un massimo (minimo) di X è sempre unico; ogni massimo (minimo) di X è sempre massimale (minimale) in X, ma il contrario non è necessariamente vero; inoltre, un insieme parzialmente ordinato può avere più di un elemento massimale (minimale) o può anche non averne nessuno.

Esempio 6.3. L'unico elemento minimale di $(\mathbb{N}, \leq)$ è 0, che è anche il suo elemento minimo. Al contrario, $(\mathbb{N}, \leq)$ non ha elementi massimali (e quindi neanche massimi).

Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, rispetto alla naturale relazione d'ordine, non hanno elementi massimali né minimali.

Se $(X, \leq)$ è un insieme parzialmente ordinato e $Y \subset X$, allora la restrizione a Y di $\leq$ è ancora una relazione d'ordine parziale: questo ci permette di interpretare, cosa che faremo sempre, i sottoinsiemi di un insieme parzialmente ordinato come insiemi parzialmente ordinati.

Può capitare che un sottoinsieme Y di $(X, \leq)$ sia totalmente ordinato rispetto all'ordinamento ereditato da X, anche se X non lo è necessariamente. In tal caso, diremo che Y è una *catena* in X.

6.2. **Insiemi bene ordinati.** Ogni sottoinsieme non vuoto di $\mathbb{N}$, rispetto alla naturale relazione d'ordine, possiede un minimo elemento: questo fatto è noto come *principio di buon ordinamento* ed è essenzialmente equivalente al principio di induzione.

Definizione 6.4. Un ordinamento parziale $\leq$ su un insieme X si dice *buon ordinamento* se ogni sottoinsieme non vuoto di X possiede minimo.

Un insieme dotato di un buon ordinamento si dice *bene ordinato*. Se x', x'' sono elementi distinti di un insieme bene ordinato $(X, \leq)$, allora il minimo del sottoinsieme non vuoto $\{x', x''\} \subset X$ è minore o uguale dell'altro elemento. Pertanto ogni buon ordinamento è un ordinamento totale. Il viceversa è però falso.

Esempio 6.5. Il sottoinsieme $(0, 1) \subset \mathbb{R}$ non ha minimo rispetto alla naturale relazione d'ordine. Pertanto $(\mathbb{R}, \leq)$ è un insieme totalmente ordinato ma non bene ordinato.

Esempio 6.6. L'intervallo chiuso $[0, 1]$ ha minimo rispetto alla naturale relazione d'ordine ed è totalmente ordinato. Non è però bene ordinato in quanto, ad esempio, il suo sottoinsieme non vuoto $(0, 1)$ non possiede elemento minimo.

Esempio 6.7. Ogni ordinamento totale su un insieme finito è un buon ordinamento. In particolare, ogni ordinamento parziale su un insieme con al più un elemento è un buon ordinamento.

Proposizione 6.8. *Sia $(X, \leq)$ è un insieme bene ordinato, $y \notin X$. Allora l'ordinamento su $X' = X \cup \{y\}$ che estende quello di X ponendo $x \leq y$ per ogni $x \in X'$ è ancora un buon ordinamento.*

Dimostrazione. La verifica che si tratti di un ordinamento parziale è immediata, ed è quindi sufficiente mostrare che ogni sottoinsieme non vuoto di X' ha elemento minimo.

Se $\emptyset \neq U \subset X'$ non contiene y, allora $U \subset X$ e l'esistenza del minimo di U segue dal fatto che X è bene ordinato. Se invece U contiene y propriamente, il minimo di $U \setminus \{y\} \subset X$ è anche minimo di U. Se infine $U = \{y\}$, allora y è chiaramente il suo minimo. □

Se $(X, \leq)$ è un insieme bene ordinato e $Y \subset X$, allora anche Y è bene ordinato[13] dalla restrizione a Y di $\leq$, poiché ogni sottoinsieme non vuoto di Y è anche sottoinsieme di X e ammette quindi minimo.

In generale, il fatto che un ordinamento parziale su X induca buoni ordinamenti su alcuni (anche molti) sottoinsiemi dice però poco sul fatto che $\leq$ sia un buon ordinamento anche su X, come mostrano i seguenti esempi.

Esempio 6.9.
- L'unione di sottoinsiemi bene ordinati può non essere bene ordinata. In effetti, ogni $(X, \leq)$ è unione dei suoi sottoinsiemi di cardinalità 1, che sono tutti bene ordinati, ma un ordinamento parziale è raramente un buon ordinamento.
- L'unione crescente di sottoinsiemi bene ordinati può non essere bene ordinata. In effetti, per ogni scelta di $k \in \mathbb{Z}$ il sottoinsieme $X_k = \{z \in \mathbb{Z} \mid z \geq k\}$ è bene ordinato rispetto all'ordinamento naturale di $\mathbb{Z}$; inoltre gli insiemi $X_k, k \in \mathbb{Z}$, sono contenuti l'uno nell'altro. Tuttavia la loro unione $(\mathbb{Z}, \leq)$ non è un insieme bene ordinato.

Esiste però un modo di ovviare a questo problema.

Definizione 6.10. Sia $(X, \leq)$ un insieme parzialmente ordinato. Il sottoinsieme $U \subset X$ si dice *segmento iniziale*[14] di X quando $u \in U, x \leq u \implies x \in U$.

Esempio 6.11. Ciascun sottoinsieme $\{0, 1, \ldots, n\}$ è un segmento iniziale di $(\mathbb{N}, \leq)$. Nessuno dei sottoinsiemi X_k dell'esempio precedente è un segmento iniziale di $(\mathbb{Z}, \leq)$.

Quando $(X, \leq)$ è un insieme bene ordinato, i segmenti iniziali **propri** di X hanno una descrizione molto semplice.

Lemma 6.12. *Sia $(X, \leq)$ un insieme bene ordinato. Se $U \subsetneq X$ è un segmento iniziale di X, allora esiste $x_0 \in X$ tale che $U = X_{<x_0} := \{x \in X \mid x < x_0\}$.*

Dimostrazione. Se $U \subsetneq X$, sia $x_0 = \min(X \setminus U)$. Se $x < x_0$ allora $x \in U$ per minimalità di x_0. Viceversa, se $x \in U, x_0 \leq x$, allora $x_0 \in U$ in quanto U è un segmento iniziale; ma questo è un assurdo. □

Osservazione 6.13. Qualche osservazione al volo.
- Innanzitutto, i sottoinsiemi della forma $X_{<x_0}$ sono sempre segmenti iniziali (propri) di X per ogni scelta di x_0. In effetti, se $u \in X_{<x_0}$ e $x \leq u$, allora $x \leq u < x_0$ e quindi $x < x_0$.
- Se U è un segmento iniziale proprio di X, esiste un **unico** x_0 tale che $U = X_{<x_0}$. In effetti, se $c \neq d$, allora a meno di scambiare i due elementi possiamo supporre che $c < d$. Ma allora $c \in X_{<d}$ mentre $c \notin X_{<c}$ e pertanto i due sottoinsiemi sono diversi.
- Se $U \neq X$ sono bene ordinati e U è un segmento iniziale di X, allora $u < x$ per ogni $u \in U, x \in X \setminus U$. In effetti, abbiamo visto che $U = X_{<x_0}$ dove $x_0 = \min X \setminus U$. Se $u \in U$, allora $u < x_0$. Inoltre, se $x \in X \setminus U$, allora $x_0 \leq x$ per minimalità di x_0. In conclusione, $u < x_0 \leq x$ e quindi $u < x$.
- Supponiamo di avere due sottoinsiemi $U, V \subset X$ e sapere che uno tra U e V sia segmento iniziale dell'altro. Allora basta esibire un elemento $v \in V \setminus U$ per concludere che è U ad essere segmento iniziale di U.

Proposizione 6.14. *Sia $(X, \leq)$ un insieme parzialmente ordinato e $\{U_i\}_{i \in I}$ sottoinsiemi bene ordinati (distinti) con la proprietà che comunque presi $i, j \in I$, uno tra U_i e U_j è segmento iniziale dell'altro. Allora l'unione $U = \bigcup_{i \in I} U_i$ è ancora un sottoinsieme bene ordinato di X.*

Dimostrazione. Se $Y \subset U$ è un sottoinsieme non vuoto, esiste sicuramente $i \in I$ tale che $Y \cap U_i \neq \emptyset$. Indichiamo con y_0 il minimo di $Y \cap U_i$ che esiste in quanto U_i è bene ordinato. Sia $y \in Y$: se $y \in U_i$ allora $y \in Y \cap U_i$ e quindi $y_0 \leq y$; se invece $y \notin U_i$, scegliamo $j \in I$ in modo che $y \in U_j$. Allora $U_j \setminus U_i$ è non vuoto perché contiene y e quindi U_i è un segmento iniziale di U_j. Per l'osservazione appena fatta, $U_i \ni y_0 < y \in U_j \setminus U_i$. In conclusione, y_0 è il minimo di Y. □

L'importanza degli insiemi bene ordinati nel contesto dell'assioma della scelta risiede nella seguente affermazione.

Proposizione 6.15. *Sia $f : A \to B$ un'applicazione suriettiva. Se $\leq$ è un buon ordinamento su A, allora l'applicazione*

$$B \ni b \mapsto \min f^{-1}(b) \in A$$

è un'inversa destra di f.

7. Dimostrazione del Teorema di Zermelo

(Ri)elenchiamo adesso alcuni enunciati dei quali vogliamo mostrare l'equivalenza.

Assioma della scelta: prima forma. Se A, B sono insiemi e A è non vuoto, allora per ogni applicazione suriettiva $f : A \to B$ esiste un'applicazione $g : B \to A$ tale che $f \circ g = \mathrm{id}_B$.

Assioma della scelta: seconda forma. Sia I un insieme e $\{X_i\}_{i \in I}$ una famiglia di insiemi non vuoti. Allora esiste un'applicazione $\varphi : I \to \bigcup_{i \in I} X_i$ tale che $\varphi(i) \in X_i$.

Teorema di Zermelo. Ogni insieme possiede (almeno) un buon ordinamento.

---

[13] ed è quindi automaticamente una catena!

[14] A differenza di quanto fatto a lezione, ho deciso di promuovere anche X a segmento iniziale di se stesso.

Lemma di Zorn. Un insieme parzialmente ordinato non vuoto, ogni cui catena possiede un maggiorante[15], ha necessariamente elementi massimali.

Abbiamo appena visto che dal Teorema di Zermelo segue la prima forma dell'assioma della scelta, mentre avevamo già mostrato che dalla prima forma segue la seconda. Per arrivare all'equivalenza tra le quattro affermazioni, dimostreremo prima il Teorema di Zermelo utilizzando il Lemma di Zorn, per poi ricavare il Lemma di Zorn a partire dalla seconda forma dell'assioma della scelta.

Proposizione 7.1. *Se il Lemma di Zorn è valido, allora ogni insieme possiede un buon ordinamento.*

Dimostrazione. Sia X un insieme. Vogliamo costruire, utilizzando il Lemma di Zorn, un buon ordinamento su X. L'insieme

$$\mathcal{F} = \{(U, \leq_U) \,|\, U \subset X,\ \leq_U \text{ è un buon ordinamento su } U\}$$

è sicuramente non vuoto, poiché contiene la coppia $(\emptyset, \emptyset)$. Si vede facilmente[16] che la relazione su $\mathcal{F}$ definita da

$$(U, \leq_U) \preceq (V, \leq_V) \iff U \text{ è segmento iniziale di } V, \text{ e l'ordinamento } \leq_V \text{ estende } \leq_U$$

è un ordinamento parziale su $\mathcal{F}$.

Mostriamo che $\mathcal{F}$ è un insieme induttivo. Se $\{U_i\}_{i\in I}$ è una catena in $\mathcal{F}$, sia $U = \bigcup_{i\in I} U_i$. Se $u, u' \in U$, possiamo trovare $i \in I$ in modo che U_i li contenga entrambi. Definiamo allora $u \leq_U u'$ se $u \leq_{U_i} u'$: questa definizione non dipende da i in quanto gli ordinamenti dei sottoinsiemi $U_i, i \in I$, coincidono sugli elementi comuni. Pertanto $(U, \leq_U)$ è un insieme parzialmente ordinato e possiamo usare la Proposizione 6.14 (ponendo $X = U$) per mostrare che $\leq_U$ è un buon ordinamento su U.

Rimane da mostrare che ogni U_i è un segmento iniziale di U, cioè che se $x \in U, u \in U_i$ e $x \leq u$, allora x deve appartenere ad U_i. Effettivamente, se per assurdo $x \notin U_i$, allora $x \in U_j$ per qualche $j \in I$ e poiché $U_j \setminus U_i$ è non vuoto (in quanto contiene x), allora U_i sarebbe segmento iniziale di U_j. In tale situazione, abbiamo visto che gli elementi di U_i sono tutti inferiori a quelli di $U_j \setminus U_i$: $x \leq u$ sarebbe quindi impossibile. Questo mostra che $(U_i, \leq_{U_i}) \preceq (U, \leq_U)$ per ogni $i \in I$, e $(U, \leq_U)$ è quindi un maggiorante della catena data.

Essendo $\mathcal{F}$ un insieme parzialmente ordinato non vuoto e induttivo, deve possedere almeno un elemento massimale $(Y, \leq_Y)$. Tuttavia, se $Y \subsetneq X$, e $x \in X \setminus Y$, allora possiamo costruire $Y' = Y \cup \{x\}$ come nella Proposizione 6.8, e confutare la massimalità di $(Y, \leq_Y)$; Y sarebbe un segmento iniziale di Y' poiché $Y = Y'_{<x}$.

Abbiamo finalmente concluso: ciascun elemento massimale di $\mathcal{F}$ fornisce un buon ordinamento su X. □

Rimane da dimostrare che il Lemma di Zorn segue dalla seconda forma dell'assioma della scelta. Questo è il punto più delicato e richiederà un po' di attenzione.

8. L'assioma della scelta implica il Lemma di Zorn

In tutto ciò che segue, $\mathcal{F}$ è un insieme parzialmente ordinato non vuoto e induttivo **privo** di elementi massimali. Poiché per ogni $x \in \mathcal{F}$ possiamo trovare $x' \in \mathcal{F}$ tale che $x < x'$, ogni catena $C \subset \mathcal{F}$ non solo possiede almeno un maggiorante, ma anche un *maggiorante stretto*, un elemento m cioè tale che $c < m$ per ogni $c \in C$.

Se I è l'insieme di tutte le catene in $\mathcal{F}$, e $X_i, i \in I$, è l'insieme dei maggioranti stretti di i in $\mathcal{F}$, sia $f : I \to \bigcup_{i\in I} X_i$ una funzione di scelta: f sceglie, per ogni catena $i \in I$, un suo maggiorante stretto $f(i) \in \mathcal{F}$.

Definizione 8.1. Un sottoinsieme $A \subset \mathcal{F}$ si dice f-sottoinsieme se

- A è bene ordinato dalla relazione d'ordine di $\mathcal{F}$;
- per ogni $a \in A$ vale $f(A_{<a}) = a$.

Non è complicato esibire f-sottoinsiemi. Innanzitutto, il sottoinsieme vuoto è tecnicamente un f-sottoinsieme. Inoltre, se $a_0 = f(\emptyset)$, allora $\{a_0\}$ è un f-sottoinsieme, come si verifica facilmente. Allo stesso modo, se $a_1 = f(\{a_0\})$, allora $\{a_0, a_1\}$ è nuovamente un f-sottoinsieme. Definendo ricorsivamente $a_n = f(\{a_0, a_1, \dots, a_{n-1}\})$, si vede facilmente che $\{a_0, a_1, \dots, a_k\}$ è un f-sottoinsieme per ogni $k \in \mathbb{N}$. Gli f-sottoinsiemi non sono necessariamente finiti. Ad esempio $\{a_n \,|\, n \in \mathbb{N}\}$ è un f-sottoinsieme infinito. Una corretta intuizione è che, presi due f-sottoinsiemi, *"uno dei due comincia con l'altro"*.

Ogni f-sottoinsieme $A \subset \mathcal{F}$ è bene ordinato e quindi totalmente ordinato; di conseguenza è chiaramente una catena di $\mathcal{F}$. Allora, detto $x = f(A)$, il sottoinsieme $A' = A \cup \{x\}$ è nuovamente un f-sottoinsieme: che sia bene ordinato segue dalla Proposizione 6.8, in quanto x è più grande di ciascun elemento di A; per mostrare la validità della seconda condizione, invece, manca solo osservare che $f(A'_{<x}) = f(A) = x$. Riassumendo:

Proposizione 8.2. *Se $A \subset \mathcal{F}$ è un f-sottoinsieme, allora anche $A' = A \cup \{f(A)\}$ è un f-sottoinsieme. In particolare, nessun f-sottoinsieme è massimale rispetto all'inclusione.*

Il nostro obiettivo è ora quello di arrivare ad una contraddizione. La strategia è quella di mostrare che l'unione di tutti gli f-sottoinsiemi di $\mathcal{F}$ è ancora un f-sottoinsieme, che è necessariamente il più grande di tutti. Questo confliggerà con la proposizione appena dimostrata. Procediamo!

Lemma 8.3. *Se $A \neq B$ sono f-sottoinsiemi di $\mathcal{F}$, allora uno dei due è segmento iniziale dell'altro.*

[15] Un insieme parzialmente ordinato che soddisfa questa ulteriore condizione è detto *induttivo*.

[16] L'unica affermazione non ancora dimostrata è che un segmento iniziale di un segmento iniziale è un segmento iniziale, ma questo è immediato.

Dimostrazione. Innanzitutto, A e B sono entrambi bene ordinati. A meno di scambiare A con B, supponiamo che B non sia contenuto[17] in A e poniamo $b_0 = \min B \setminus A$. Allora $B_{<b_0} \subset A$. Se quest'inclusione è un'uguaglianza, abbiamo finito.

Supponiamo per assurdo che invece $B_{<b_0} \subsetneq A$, e poniamo $a_0 = \min A \setminus B_{<b_0}$. Come prima, $A_{<a_0} \subset B_{<b_0}$: vogliamo mostrare che questa inclusione è ora effettivamente un'uguaglianza. Sia $b \in B_{<b_0}$. Se $b \geq a_0$, allora $a_0 \leq b < b_0$ mostrerebbe che $a_0 < b_0$ il che contraddice la definizione di a_0. Poiché l'ordinamento su A è totale, deve allora valere $b < a_0$. L'elemento b è però anche contenuto in A, in quanto $b \in B_{<b_0} \subsetneq A$. Questo dimostra che $B_{<b_0} \subset A_{<a_0}$, e quindi l'uguaglianza, dal momento che l'inclusione opposta era già nota.

In conclusione, $A_{<a_0} = B_{<b_0}$. Ricordando che A, B sono entrambi f-sottoinsiemi, abbiamo allora

$$A \ni a_0 = f(A_{<a_0}) = f(B_{<b_0}) = b_0,$$

il che è una contraddizione, poiché b_0, per sua definizione, non appartiene ad A. □

Lemma 8.4. *L'unione di tutti gli f-sottoinsiemi di $\mathcal{F}$ è ancora un f-sottoinsieme.*

Dimostrazione. Poiché f-sottoinsiemi distinti sono uno segmento iniziale dell'altro, il fatto che l'unione di tutti gli f-sottoinsiemi di $\mathcal{F}$ sia bene ordinata segue dalla Proposizione 6.14.

Per quanto riguarda la seconda condizione, sia M l'unione di tutti gli f-sottoinsiemi di $\mathcal{F}$. Se $m \in M$, allora $m \in A$ per qualche f-sottoinsieme $A \subset \mathcal{F}$. Sia $x \in M$: se $x \notin A$, allora $x \in B$ per qualche altro f-sottoinsieme B. Poiché $B \setminus A$ è non vuoto, allora A è segmento iniziale di B e quindi $x > m$. Questo mostra che gli elementi di M che sono minori di m sono tutti contenuti in A e più esplicitamente che $M_{<m} = A_{<m}$. Poiché A è un f-sottoinsieme, abbiamo allora

$$f(M_{<m}) = f(A_{<m}) = m,$$

e anche M è un f-sottoinsieme di $\mathcal{F}$. □

Proposizione 8.5. *Se vale la seconda forma dell'assioma della scelta, allora ogni insieme parzialmente ordinato non vuoto e induttivo possiede elementi massimali.*

Dimostrazione. Supponiamo (per assurdo) che esista un insieme parzialmente ordinato non vuoto e induttivo $\mathcal{F}$ privo di elementi massimali. Se f è una funzione di scelta che associa ad ogni catena in $\mathcal{F}$ un suo maggiorante stretto, allora l'unione M degli f-sottoinsiemi di $\mathcal{F}$ è un f-sottoinsieme di $\mathcal{F}$ che contiene ogni altro f-sottoinsieme.

Tuttavia, come abbiamo già visto, $M \cup f(M)$ è ancora un f-sottoinsieme, il che contraddice la massimalità di M tra gli f-sottoinsiemi di $\mathcal{F}$. □

9. Scelta e cardinalità

La duttilità del Lemma di Zorn permette di dimostrare molte proprietà interessanti degli insiemi infiniti, anche quando non sono numerabili. Elencherò qui alcune delle più immediate.

9.1. **Confrontabilità delle cardinalità.**

Proposizione 9.1. *Siano X e Y insiemi. Allora $|X| \leq |Y|$ oppure $|Y| \leq |X|$.*

Dimostrazione. Sull'insieme $\mathcal{F} = \{(A, f) \mid A \subset X, f : A \to Y \text{ iniettiva}\}$ 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 $\mathcal{F}$ possiede elementi massimali, dobbiamo mostrare che ogni catena in $\mathcal{F}$ possiede un maggiorante.

Sia $C = \{(A_i, f_i)\}_{i \in I}$ una catena in $\mathcal{F}$. 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 $a, b \in A$ 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 $(A, f) \in \mathcal{F}$: 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 $\mathcal{F}$.

Sia $(A, f) \in \mathcal{F}$ 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 $\mathcal{F}$, 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. □

9.2. **Cardinalità di unioni numerabili di insiemi.**

Abbiamo già visto che ogni sottoinsieme infinito di $\mathbb{N}$ è numerabile. Pertanto l'affermazione $|X| \leq |\mathbb{N}|$ è equivalente a dire che X è finito o numerabile[18]. Di conseguenza $|X| < |\mathbb{N}|$ è equivalente a dire che X è finito.

Viceversa, che cosa vuol dire $|\mathbb{N}| \leq |X|$? Se X contiene un sottoinsieme numerabile, è sicuramente infinito. E' vero anche il contrario?

Lemma 9.2. *Ogni insieme infinito contiene un sottoinsieme numerabile.*

[17] Se ciascuno dei due è contenuto nell'altro, sono uguali!

[18] Si dice anche che X è *al più 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 finito $Y \subset X$ sceglie un elemento nel suo complementare (non vuoto!) $X \setminus Y$ — 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

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

si ottiene l'applicazione iniettiva desiderata[19]. □

Lemma 9.3. *Ogni insieme infinito possiede una partizione in sottoinsiemi tutti numerabili.*

Dimostrazione. Sia X un insieme infinito, e poniamo

$$\mathcal{F} = \{\{U_i\}_{i \in I} \mid \text{ gli } U_i \text{ sono sottoinsiemi numerabili e disgiunti di } X\}.$$

Se $X_0 \subset X$ è un sottoinsieme numerabile, allora $\{X_0\}$ appartiene a $\mathcal{F}$, e quindi $\mathcal{F}$ è non vuoto. Gli elementi di $\mathcal{F}$ appartengono a $P(P(X))$ e possiamo quindi ordinare $\mathcal{F}$ per inclusione. Sia $\{\mathcal{U}_\alpha\}_{\alpha \in A}$ una catena in $\mathcal{F}$: ciascun $\mathcal{U}_\alpha$ è una famiglia di sottoinsiemi numerabili disgiunti di X, e comunque presi $\alpha, \beta \in A$, si ha $\mathcal{U}_\alpha \subset \mathcal{U}_\beta$ o viceversa. In altre parole, tutti i sottoinsiemi numerabili di X contenuti in $\mathcal{U}_\alpha$ appartengono anche a $\mathcal{U}_\beta$ o viceversa.

Consideriamo $\mathcal{U} = \bigcup_{\alpha \in A} \mathcal{U}_\alpha$. E' ancora una collezione di sottoinsiemi numerabili di X e contiene sicuramente ciascun $\mathcal{U}_\alpha$. Per mostrare che è un maggiorante della catena, va solo mostrato che $\mathcal{U} \in \mathcal{F}$, e cioè che i sottoinsiemi della famiglia $\mathcal{U}$ sono a due a due disgiunti. Ora, se $X', X'' \in \mathcal{U}$, allora $X' \in \mathcal{U}_\alpha$, $X'' \in \mathcal{U}_\beta$ per un'opportuna scelta di $\alpha, \beta \in A$; per la condizione di catena, uno tra $\mathcal{U}_\alpha$ e $\mathcal{U}_\beta$ li contiene entrambi, e quindi $X' \cap X'' = \emptyset$.

L'insieme $\mathcal{F}$ soddisfa pertanto le ipotesi del Lemma di Zorn, e possiede quindi elementi massimali. Sia $\{U_i\}_{i \in I}$ un tale elemento massimale. Se l'unione $\bigcup_{i \in I} U_i$ ha complementare infinito in X, allora possiamo scegliervi un sottoinsieme numerabile e aggiungerlo alla famiglia, rendendola così strettamente più grande, contraddicendo la massimalità. Di conseguenza l'unione ha complementare finito, e possiamo aggiungere questa quantità finita di elementi a uno degli U_i lasciandolo numerabile e producendo così una partizione di X in sottoinsiemi numerabili disgiunti. □

Corollario 9.4. *Sia X un insieme infinito e Y un insieme finito. Allora*

$$|X| = |X \cup Y| = |X \setminus Y|.$$

Dimostrazione. Sia X il nostro insieme, e $\{U_i, i \in I\}$ una sua partizione in sottoinsiemi U_i tutti numerabili[20]. Per il Corollario 2.3, 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 2.3, 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 9.5. *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 2.4 e 2.7), e si incollano le applicazioni invertibili $f_i : U_i \to U_i \times Y$. □

Corollario 9.6. *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 9.7. *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 9.8. Gli ultimi due corollari generalizzano il Corollario 2.3 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 9.9. *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.*

[19] 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.*

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

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 9.10. E' importante sottolineare che il Corollario 2.9 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 $\emptyset$.

Lemma 9.11. *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, $|X| = |Y|$. □

9.3. **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 9.12. *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 $\mathcal{F} = \{(A, f) \,|\, A \subset X, f : A \to A \times A \text{ è un'applicazione invertibile}\}$ — che è non vuoto perché ogni sottoinsieme numerabile di X possiede una corrispondenza biunivoca con il suo quadrato cartesiano — definiamo una relazione d'ordine[21] 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 $(\mathcal{F}, \leq)$ soddisfa le ipotesi del Lemma di Zorn: in effetti se $C = \{(A_i, f_i), i \in I\}$ è una catena in $\mathcal{F}$, 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 $\mathcal{F}$. Voglio adesso mostrare che se (A, f) è un elemento massimale di $\mathcal{F}$, 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 $(B, g) \in \mathcal{F}$ 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 2.9 e all'Osservazione 9.10.

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

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

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 $(A, f) \in \mathcal{F}$ 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 9.13. *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 $\phi \times \mathrm{id}_Y : Y \times Y \to X \times Y$. Pertanto, $|X \times Y| \leq |Y \times Y| = |Y|$. Utilizzando le due disuguaglianze si ottiene $|X \times Y| = |Y|$. □

Corollario 9.14. *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. □

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

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