ELEMENTI DI TEORIA DEGLI INSIEMI
Dispensa 2

Mauro Di Nasso

Ultimo aggiornamento: March 18, 2024

CHAPTER 2

Cardinalità numerabile e cardinalità del continuo

Adesso che tutta la terminologia di base è stata introdotta, possiamo finalmente cominciare ad entrare nel vivo della teoria degli insiemi.

Come anticipato nell'*Introduzione*, in questa prima fase procederemo in modo semi-formale, così come si farebbe in una qualunque altra disciplina matematica, rimandando a più avanti le questioni legate ai fondamenti logici della teoria. Più precisamente, ci baseremo sui tre principi insiemistici formulati nel primo capitolo, ma assumeremo anche come conosciute le nozioni fondamentali che si usano nella pratica, e i relativi risultati di base. In particolare, assumeremo come note le nozioni di numero *naturale, intero, razionale, reale.*

Ricordiamo la seguente fondamentale definizione.

Definizione 0.1. Un insieme A si dice *finito* se è equipotente ad un segmento iniziale $\{1, \ldots, n\}$ dei numeri naturali. A si dice *infinito* in caso contrario.

Nel seguito useremo direttamente le proprietà fondamentali dei numeri naturali, interi, razionali, reali, e degli insiemi finiti ed infiniti, tra cui le seguenti:

- Un sottoinsieme di un insieme finito è finito, e il soprainsieme di un insieme infinito è infinito.
- L'unione di un numero finito di insiemi finiti è un insieme finito.
- Il principio del *buon ordinamento* dei numeri naturali, cioè la proprietà che ogni insieme non vuoto $A \subseteq \mathbb{N}$ ha minimo;
- Il principio di *induzione* sui numeri naturali[1];
- Il procedimento di *ricorsione* (o di "induzione", come si dice usualmente con termine improprio) per definire successioni;
- La proprietà di *completezza* dei numeri reali;
- La proprietà di *densità* dei numeri razionali nei numeri reali: "Se $r < s$ sono due numeri reali, allora esiste $q \in \mathbb{Q}$ tale che $r < q < s$".

È bene chiarire che tutte queste nozioni, proprietà e principi saranno reintrodotti e dimostrati in modo formale più avanti. Inoltre, tutte le dimostrazioni date in questo capitolo, saranno formalizzabili all'interno della teoria assiomatica che presenteremo, e quindi saranno da considerarsi del tutto rigorose.

[1] Vedremo in seguito che il principio di induzione e la proprietà del buon ordinamento sono in realtà proprietà equivalenti.

1. Equipotenza

La cruciale nozione di equipotenza è stata introdotta da Cantor nella seconda metà del XIX per catturare l'idea di "grandezza" o "cardinalità" di un insieme infinito. Per un insieme finito A, la cardinalità è data da quell'unico numero naturale n per cui si ha una bigezione $f : \{1, \dots, n\} \to A$; tale numero n rappresenta la "quantità" degli elementi di A. Partendo dalla considerazione che due insiemi finiti hanno lo stesso numero di elementi se e solo se esiste una bigezione tra di loro, Cantor propose la seguente definizione generale:

Definizione 1.1. Due insiemi A e B sono *equipotenti* o hanno la stessa *cardinalità* se esiste una funzione biunivoca $f : A \to B$. In questo caso scriviamo $|A| = |B|$.

Un primo esempio importante è il seguente:

Proposizione 1.2. *L'insieme delle funzioni caratteristiche su un insieme X è equipotente all'insieme delle parti, cioè* $|2^X| = |\mathcal{P}(X)|$.

Dim. Sia $\Psi : \mathcal{P}(X) \to 2^X$ la funzione che associa ad ogni sottoinsieme $A \subseteq X$ la corrispondente funzione caratteristica χ_A. Come abbiamo già osservato nel capitolo precedente, ogni funzione $\chi : X \to \{0, 1\}$ è la funzione caratteristica di uno ed un solo sottoinsieme $A_\chi \subseteq X$, precisamente $A_\chi = \{x \in X \mid \chi(x) = 1\}$, e quindi Ψ è biunivoca. □

Le seguenti proprietà dell'equipotenza sono la controparte insiemistica delle uguaglianze algebriche $a^b \cdot a^c = a^{b+c}$ e $(a^b)^c = a^{bc}$, dove l'unione disgiunta corrisponde alla somma, il prodotto cartesiano corrisponde al prodotto, e l'esponenziale corrisponde all'insieme delle funzioni.

La nostra notazione $|A| = |B|$ è giustificata dal fatto che l'equipotenza gode delle tre proprietà di relazione di equivalenza.

Proposizione 1.3.
1. *Proprietà riflessiva*: $|A| = |A|$;
2. *Proprietà simmetrica*: Se $|A| = |B|$ allora $|B| = |A|$;
3. *Proprietà transitiva*: Se $|A| = |B|$ e $|B| = |C|$ allora $|A| = |C|$.

Dim. (1) La funzione identità $\mathrm{id}_A : A \to A$ è banalmente una bigezione. (2) Se $f : A \to B$ è una bigezione, allora anche la sua inversa $f^{-1} : B \to A$ è una bigezione. (3) Se $f : A \to B$ e $g : B \to C$ sono bigezioni, allora anche la composizione $g \circ f : A \to C$ è una bigezione. □

Attenzione! Non possiamo propriamente parlare dell'equipotenza come di una relazione di equivalenza perché si tratterebbe di una relazione avente come dominio la collezione di tutti gli insiemi. Come vedremo fra poco (vedi Corollario 1.8), assumere che esista l'insieme di tutti gli insiemi porta a contraddizioni.

Attenzione! Abbiamo scritto $|A| = |B|$ per intendere che A e B sono equipotenti, ma la scrittura $|A|$ da sola *non* ha (per il momento) alcun significato.[2]

[2] L'intuizione ci suggerirebbe di attribuirgliene uno come classe di equivalenza, definendo $|A| = \{B \mid |A| = |B|\}$. Anche in questo caso però, assumere che una tale collezione sia un insieme condurrebbe a contraddizioni perché la sua unione sarebbe l'insieme di tutti gli insiemi.

È bene anticipare che, quando avremo sviluppato una teoria assiomatica degli insiemi, i problemi evidenziati sopra saranno superati. Avremo infatti un modo rigoroso per definire degli speciali oggetti, detti *cardinali*, che saranno i rappresentanti canonici delle “classi” di equipotenza. Precisamente, per ogni insieme A esisterà ed unico un cardinale κ tale che $|A| = |\kappa|$. A quel punto scriveremo direttamente $|A| = \kappa$, e diremo che κ è la *cardinalità* dell'insieme A.[3]

La relazione di equipotenza è coerente con le operazioni insiemistiche di unione disgiunta, prodotto cartesiano, insieme delle funzioni, e insieme potenza.

Esercizio 1.4. Supponiamo che $|A| = |A'|$ e $|B| = |B'|$. Allora
(1) $|A \cup B| = |A' \cup B'|$ se $A \cap B = A' \cap B' = \emptyset$;
(2) $|A \times B| = |A' \times B'|$;
(3) $|\mathrm{Fun}(A, B)| = |\mathrm{Fun}(A', B')|$;
(4) $|\mathcal{P}(A)| = |\mathcal{P}(A')|$.

Esercizio 1.5.
(1) $|A^B \times A^C| = |A^{B \cup C}|$ quando $A \cap B = \emptyset$.
(2) $|(A^B)^C| = |A^{(B \times C)}|$.

Ciò che rende significativa la teoria delle cardinalità è il fatto che non tutti gli insiemi infiniti sono tra loro equipotenti. Cantor dimostrò infatti che per ogni insieme assegnato, ne esiste uno di cardinalità diversa.

Come primo esempio, consideriamo i numeri naturali $\mathbb{N}$, e l'insieme $2^{\mathbb{N}}$ delle funzioni caratteristiche su $\mathbb{N}$.

Teorema 1.6. *Non esistono funzioni suriettive* $\Psi : \mathbb{N} \to 2^{\mathbb{N}}$, *dunque* $|\mathbb{N}| \neq |2^{\mathbb{N}}|$.

Dim. Supponiamo data una funzione $\Psi : \mathbb{N} \to 2^{\mathbb{N}}$ qualunque. Vogliamo dimostrare che Ψ *non* è suriettiva. Per ogni $n \in \mathbb{N}$, denotiamo con $(a_{n,k} \mid k \in \mathbb{N})$ la successione $\Psi(n)$.

$$\begin{array}{cccccccc}
\mathbf{a_{11}} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} & \dots \\
a_{21} & \mathbf{a_{22}} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} & \dots \\
a_{31} & a_{32} & \mathbf{a_{33}} & a_{34} & a_{35} & a_{36} & a_{37} & \dots \\
a_{41} & a_{42} & a_{43} & \mathbf{a_{44}} & a_{45} & a_{46} & a_{47} & \dots \\
a_{51} & a_{52} & a_{53} & a_{54} & \mathbf{a_{55}} & a_{56} & a_{57} & \dots \\
a_{61} & a_{62} & a_{63} & a_{64} & a_{65} & \mathbf{a_{66}} & a_{67} & \dots \\
a_{71} & a_{72} & a_{73} & a_{74} & a_{75} & a_{76} & \mathbf{a_{77}} & \dots \\
 & & & & & & & \\
a_{n1} & a_{n2} & a_{n3} & a_{n4} & a_{n5} & a_{n6} & a_{n7} & \dots
\end{array}$$

Per ogni n, sia $b_n = 0$ se $a_{n,n} = 1$; e sia $b_n = 1$ se invece $a_{n,n} = 0$. Allora la successione $(b_k \mid k \in \mathbb{N})$ non appartiene all'immagine di Ψ. Infatti, per ogni n, $\Psi(n) = (a_{n,k} \mid k \in \mathbb{N}) \neq (b_k \mid k \in \mathbb{N})$, visto che per la definizione data, l'n-esimo elemento $a_{n,n} \neq b_n$. $\square$

[3] Anche a questo riguardo è interessante il ruolo fondamentale rivestito dall'*assioma di scelta*. Infatti si può dimostrare che senza assioma di scelta, non esiste alcun modo “definibile” per individuare un unico rappresentante in ogni classe di equipotenza (Teorema di Pincus del 1974).

Il metodo usato nella dimostrazione di sopra è noto come "argomento diagonale". La successione $(b_k \mid k \in \mathbb{N})$ è stata infatti definita a partire dagli elementi $a_{n,n}$ i cui indici stanno sulla diagonale di $\mathbb{N} \times \mathbb{N}$. Usando lo stesso procedimento diagonale, più in generale si dimostra che nessun insieme è equipotente al corrispondente insieme delle parti.[4]

Teorema 1.7 (Cantor). *Per ogni insieme A, non esistono funzioni suriettive $f : A \to \mathcal{P}(A)$. Dunque $|A| \neq |\mathcal{P}(A)|$.*

Dim. Data una funzione $f : A \to \mathcal{P}(A)$, dimostriamo che il seguente insieme *non* appartiene all'immagine di f:

$$B = \{a \in A \mid a \notin f(a)\}.$$

Supponiamo per assurdo che esista un elemento $\alpha \in A$ con $f(\alpha) = B$. Si hanno due possibilità. Se $\alpha \in B$ allora, per definizione di X, avremmo che $\alpha \notin f(\alpha) = B$, contro l'ipotesi. Se invece $\alpha \notin B$, di nuovo per la definizione di B, avremmo che $\alpha \in f(\alpha) = B$, contro l'ipotesi. Entrambi i casi ci portano ad una conseguenza assurda, e concludiamo che f non può essere suriettiva. $\square$

Osserviamo che la dimostrazione dei Teoremi 1.6 e 1.7 sono essenzialmente le stesse. Infatti, identifichiamo ogni sottoinsieme $A \subseteq \mathbb{N}$ con la corrispondente funzione caratteristica $\chi_A \in 2^{\mathbb{N}}$. Prendendo $\Psi(n) = \chi_{f(n)}$, l'insieme B definito nella dimostrazione del teorema di sopra, ha come funzione caratteristica χ_B precisamente la successione $b = (b_k \mid k \in \mathbb{N})$, come definita con l'argomento diagonale nella dimostrazione del Teorema 1.6.

Corollario 1.8. Non può esistere l'insieme universale $V = \{x \mid x = x\}$ che contiene tutti gli insiemi.

Dim. Se V fosse un insieme, allora avremmo che $V = \mathcal{P}(V)$. Infatti, $\mathcal{P}(V) \subseteq V$, perché banalmente ogni elemento di $\mathcal{P}(V)$ è un insieme. Per vedere l'altra inclusione ricordiamo che – in conseguenza del principio di estensionalità – non esistono atomi, e quindi per noi gli elementi di un insieme sono essi stessi insiemi (ogni insieme è un insieme di insiemi). Allora $A \in V \Rightarrow A \subseteq V$, e quindi $V \subseteq \mathcal{P}(V)$, come volevamo. Finalmente otteniamo un assurdo perché se $V = \mathcal{P}(V)$, allora banalmente la funzione identità $\imath : V \to \mathcal{P}(V)$ sarebbe suriettiva, contro il teorema di Cantor. $\square$

Notiamo che, ripercorrendo la dimostrazione del Teorema di Cantor nel caso della funzione identità $\imath : V \to \mathcal{P}(V)$, la collezione $\{x \in V \mid x \notin \imath(x)\} = \{x \mid x \notin x\}$ è la collezione paradossale di Russell.

Abbiamo così trovato, dopo la proprietà di Russell "$x \notin x$", un secondo esempio di proprietà *non* ammissibile, cioè "$x = x$", cui non possiamo applicare il principio di comprensione.

[4] Ricordiamo che per ogni X, l'insieme delle parti $\mathcal{P}(X)$ è equipotente all'insieme delle funzioni caratteristiche 2^X (vedi Proposizione 1.2).

2. Ordine tra cardinalità

Oltre alla nozione di uguaglianza tra grandezze data dall'equipotenza, c'è anche una naturale nozione di confrontabilità.

DEFINIZIONE 2.1. Diciamo che l'insieme A ha *cardinalità minore o uguale* a quella di B, e scriviamo $|A| \leq |B|$, se vale una delle due seguenti proprietà equivalenti:

(1) Esiste una funzione iniettiva $f : A \to B$;
(2) Esiste un sottoinsieme $A' \subseteq B$ tale che $|A| = |A'|$.

Useremo la disuguaglianza stretta $|A| < |B|$ se $|A| \leq |B|$ ma $|A| \neq |B|$.

Che le due condizioni di sopra siano equivalenti, segue dalla ovvia osservazione che una funzione $f : A \to B$ è iniettiva se e solo se $f : A \to \mathrm{imm}(f)$ è biunivoca. Notiamo inoltre che la definizione data è coerente con l'equipotenza; vale infatti la seguente proprietà:

PROPOSIZIONE 2.2. *Se* $|A| = |A'|$ *e* $|B| = |B'|$*, allora* $|A| \leq |B| \Leftrightarrow |A'| \leq |B'|$.

DIM. Siano $f : A \to A'$ e $g : B \to B'$ bigezioni. Se $|A| \leq |B|$, prendiamo $h : A \to B$ iniettiva. Allora anche $g \circ h \circ f^{-1} : A' \to B'$ è iniettiva, perché composizione di funzioni iniettive. Analogamente per l'altra implicazione.

$$\begin{tikzcd}
A \arrow[r, "h"] & B \\
A' \arrow[u, "f^{-1}"] \arrow[r, "g \circ h \circ f^{-1}"] & B' \arrow[u, "g"]
\end{tikzcd}$$

□

Il prossimo teorema è di importanza centrale nella teoria delle cardinalità, ed è utilissimo nella pratica per dimostrare l'equipotenza fra insiemi. La sua dimostrazione non è facile, ed è rimandata a quando tratteremo la teoria assiomatica degli insiemi.

TEOREMA 2.3 (Cantor-Bernstein).
Se esistono funzioni iniettive $f : A \to B$ *e* $g : B \to A$*, allora esiste una funzione biunivoca* $h : A \to B$*. In formula:* $|A| \leq |B|$ *e* $|B| \leq |A| \;\Rightarrow\; |A| = |B|$.

Il minore o uguale tra cardinalità gode delle tre proprietà di ordine parziale, e questo giustifica la scrittura $|A| \leq |B|$.

PROPOSIZIONE 2.4.

(1) *Proprietà riflessiva*: $|A| \leq |A|$;
(2) *Proprietà anti-simmetrica*: Se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$;
(3) *Proprietà transitiva*: Se $|A| \leq |B|$ e $|B| \leq |C|$, allora $|A| \leq |C|$.

PROOF. (1) è banale. (2) è il teorema di Cantor-Bernstein. (3). Basta notare che se $f : A \to B$ e $g : B \to C$ sono iniettive, allora anche la composizione $g \circ f : A \to C$ è iniettiva. □

In modo del tutto simile all'equipotenza, anche la relazione di minore o uguale tra cardinalità è coerente con le operazioni insiemistiche di unione disgiunta, prodotto cartesiano, insieme delle funzioni, e insieme potenza.

Esercizio 2.5. Supponiamo che $|A| \leq |A'|$ e $|B| \leq |B'|$. Allora

(1) $|A \cup B| \leq |A' \cup B'|$ se $A \cap B = A' \cap B' = \emptyset$;
(2) $|A \times B| \leq |A' \times B'|$;
(3) $|\mathrm{Fun}(A, B)| \leq |\mathrm{Fun}(A', B')|$;
(4) $|\mathcal{P}(A)| \leq |\mathcal{P}(A')|$.

Dati due insiemi A e B, nella pratica è spesso più facile trovare una funzione suriettiva $g : B \to A$ piuttosto che una funzione iniettiva $f : A \to B$. Le due proprietà sono equivalenti, ma per dimostrare una delle due implicazioni è necessario l'uso dell'assioma di scelta.

Proposizione 2.6.

(1) *Se $|A| \leq |B|$, allora esiste una funzione suriettiva $g : B \to A$.*
(2) (AC). *Se esiste $g : B \to A$ suriettiva, allora $|A| \leq |B|$.*

Dim. (1). Prendiamo $f : A \to B$ iniettiva. Per ogni $b \in \mathrm{imm}(f)$, sia $g(b) \in A$ quell'unico elemento tale che $f(g(b)) = b$ (l'unicità segue dall'ipotesi di f iniettiva). Fissiamo poi un qualunque elemento $a_0 \in A$ e poniamo $g(b) = a_0$ se $b \notin \mathrm{imm} f$. Resta così definita una funzione suriettiva $g : B \to A$.

(2). Data una funzione $g : B \to A$ suriettiva, usando l'assioma di scelta possiamo prendere una sua inversa destra f, cioè una funzione $f : A \to B$ tale che $g \circ f = \mathrm{id}_A$ (cf. Proposizione **??**). Una tale f è necessariamente iniettiva, e quindi $|A| \leq |B|$. □

Esercizio 2.7. Dimostrare che sono proprietà equivalenti:

(1) Assioma di scelta.
(2) Per ogni relazione binaria, $|\mathrm{dom}(R)| \leq |R|$.
(3) Per ogni relazione binaria, $|\mathrm{imm}(R)| \leq |R|$.

Come curiosità, e come indicazione dell'importanza dell'assioma di scelta nella teoria delle cardinalità, anticipiamo qui due importanti risultati che dimostreremo più avanti. Si tratta di due formulazioni equivalenti dell'assioma di scelta che andranno ad aggiungersi a quelle già viste nella Proposizione **??**.

Teorema. *Ognuna delle due seguenti proprietà è equivalente all'assioma di scelta:*

(1) *(Confrontabilità) Per ogni A e B, si ha che $|A| \leq |B|$ o $|B| \leq |A|$.*
(2) *Per ogni A infinito, $|A \times A| = |A|$.*

3. Cardinalità numerabile

Iniziamo finalmente lo studio delle cardinalità, iniziando con il caso numerabile. Seguendo l'uso comune in matematica, *non* includeremo il numero 0 tra i numeri naturali, cioè

$$\mathbb{N} = \{1, 2, 3, \ \ldots \ , n, n+1, \ldots\}.$$

Useremo la notazione $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ per denotare l'insieme degli interi non negativi.

Definizione 3.1. Un insieme A ha *cardinalità numerabile* se $|A| = |\mathbb{N}|$. In questo caso scriviamo $|A| = \aleph_0$, che si legge: "A ha cardinalità aleph-zero".

Un'*enumerazione* di A è una funzione biunivoca $(a_n \mid n \in \mathbb{N})$ da $\mathbb{N}$ in A.[5]

Scriveremo $\aleph_0 \leq |A|$ e $|A| \leq \aleph_0$ per intendere rispettivamente $|\mathbb{N}| \leq |A|$ e $|A| \leq |\mathbb{N}|$.[6]

Per gli insiemi numerabili, la proprietà (2) della Proposizione **??** si può dimostrare senza fare uso dell'assioma di scelta.

Esercizio 3.2. Senza assumere l'assioma di scelta, dimostrare che se B è numerabile, allora $|A| \leq |B|$ se e solo se esiste una funzione suriettiva $g : B \to A$.

Proposizione 3.3. Se $A \subseteq \mathbb{N}$ è un sottoinsieme infinito, allora $|A| = \aleph_0$.

Dim. Procedendo per ricorsione, definiamo la successione:

$$a_1 = \min A\,; \quad a_{n+1} = \min\left(A \setminus \{a_1, \ldots, a_n\}\right).$$

Visto che A è infinito, per ogni n abbiamo che $A \neq \{a_1, \ldots, a_n\}$, quindi la differenza insiemistica $A \setminus \{a_1, \ldots, a_n\}$ non è vuota, e la definizione è ben posta. Chiaramente, la successione $(a_n \mid n \in \mathbb{N})$ è crescente, e quindi iniettiva e illimitata. Inoltre la sua immagine $\{a_n \mid n \in \mathbb{N}\} = A$. Infatti, è immediato verificare per induzione che per ogni k, si ha $\{a_1, \ldots, a_k\} = A \cap [1, a_k]$, e quindi

$$\{a_n \mid n \in \mathbb{N}\} = \bigcup_{k \in \mathbb{N}} \{a_1, \ldots, a_k\} = \bigcup_{k \in \mathbb{N}} \left(A \cap [1, a_k]\right) = A.$$

Resta così dimostrato che la sequenza $(a_n \mid n \in \mathbb{N})$ è la bigezione cercata. $\square$

Corollario 3.4. Se A è un insieme infinito e $|A| \leq \aleph_0$ allora $|A| = \aleph_0$.

Dim. Per ipotesi esiste una funzione iniettiva $f : A \to \mathbb{N}$. Dunque $|A| = |\mathrm{imm}(f)|$ dove $\mathrm{imm}(f)$ è un sottoinsieme infinito di $\mathbb{N}$. Allora, applicando la proposizione precedente, si ottiene che $|A| = |\mathrm{imm}(f)| = \aleph_0$. $\square$

In conseguenza dei risultati di sopra, otteniamo una dimostrazione del Teorema di Cantor-Bernstein nel caso particolare in cui uno dei due insiemi è numerabile.

Corollario 3.5. *Sia B un insieme numerabile. Se $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$.*

Dim. Visto che $|A| \leq |B| = \aleph_0$, la tesi segue dal corollario precedente una vostra mostrato che A è infinito. Supponiamo per assurdo che A sia finito; allora esisterebbe $n \in \mathbb{N}$ ed una bigezione $f : A \to \{1, \ldots, n\}$. Dall'ipotesi $|\mathbb{N}| = |B| \leq |A|$ sappiamo che esiste una funzione iniettiva $g : \mathbb{N} \to A$. Ma allora la composizione $f \circ g : \mathbb{N} \to \{1, \ldots, n\}$ sarebbe iniettiva.[7] $\square$

---

[5] Per alcuni autori, una enumerazione di A è una funzione *suriettiva* da $\mathbb{N}$ su A. Noi invece chiediamo anche l'iniettività, in modo da non avere ripetizioni.

[6] Per il momento, per noi $\aleph_0$ è solo un simbolo. Quando svilupperemo la teoria in modo assiomatico, $\aleph_0$ sarà uno speciale insieme che viene preso come rappresentante canonico di tutti gli insiemi numerabili.

[7] Qui diamo per nota la seguente proprietà, intuitivamente evidente: "Per ogni $n \in \mathbb{N}$ non esistono funzioni iniettive $\varphi : \mathbb{N} \to \{1, \ldots, n\}$". Tale proprietà sarà dimostrata formalmente più avanti, a partire dagli assiomi della teoria di Zermelo-Fraenkel (vedi Proposizione ??).

Come è suggerito dal sottoindice "zero", $\aleph_0$ rappresenta la più piccola delle cardinalità infinite. Vale infatti il

TEOREMA 3.6. (AC) *Se A è un insieme infinito allora esiste un sottoinsieme numerabile $A' \subseteq A$, e quindi $\aleph_0 \leq |A|$.*

DIM. Per l'assioma di scelta, possiamo prendere una funzione f tale che $f(B) \in B$ per ogni sottoinsieme non vuoto $B \subseteq A$. Adesso procediamo in modo del tutto simile a sopra, e definiamo per ricorsione la successione:

$$a_1 = f(A)\,; \quad a_{n+1} = f\left(A \setminus \{a_1, \ldots, a_n\}\right).$$

Visto che A è infinito, $A \setminus \{a_1, \ldots, a_n\} \neq \emptyset$ per ogni n, e dunque il passo induttivo a_{n+1} è ben definito. È immediato verificare che gli elementi a_n sono tutti distinti, e la successione $(a_n \mid n \in \mathbb{N})$ è la funzione iniettiva cercata. $\square$

C'è una differenza importante tra la dimostrazione della Proposizione 3.3 e di quest'ultimo teorema. Mentre nella Proposizione 3.3 ogni elemento a_n è definito in modo univoco come il minimo di un certo insieme di numeri naturali, nella dimostrazione del Teorema 3.6 i termini a_n sono stati "scelti" dentro certi insiemi non vuoti. Per definire la successione $(a_n \mid n \in \mathbb{N})$ è stato quindi necessario usare una funzione di scelta su A, per la cui esistenza occorre l'assioma di scelta.

Nel caso numerabile, le proprietà (2) e (3) dell'Esercizio 2.7 non richiedono l'assioma di scelta.

ESERCIZIO 3.7. Senza usare l'assioma di scelta, dimostrare che se R è una relazione binaria numerabile, allora $|\mathrm{dom}(R)| \leq |R|$ e $|\mathrm{imm}(R)| \leq |R|$.

Mostriamo ora che togliere o aggiungere un numero finito di elementi da un insieme infinito, non ne cambia la cardinalità.

PROPOSIZIONE 3.8. *Sia A un insieme numerabile e sia B un insieme finito. Allora $|A \setminus B| = |A \cup B| = |A|$.*

DIM. Consideriamo l'insieme $B' = B \setminus A$. Chiaramente $B' = \{b'_1, \ldots, b'_k\} \subseteq B$ è finito, B' è disgiunto da A, e $A \cup B' = A \cup B$. Fissata una bigezione $f : \mathbb{N} \to A$, definiamo la funzione $g : \mathbb{N} \to A \cup B$ ponendo:

$$g(n) = \begin{cases} b'_n & \text{se } n \leq k \\ f(n-k) & \text{se } n > k. \end{cases}$$

(Se $B' = \emptyset$, poniamo $g = f$.) Si può verificare direttamente che g è una bigezione, e quindi $|A \cup B| = |A|$.

L'altra equipotenza $|A \setminus B| = |A|$ si dimostra in modo analogo. Notiamo che $A \setminus B$ è infinito, altrimenti $A = (A \setminus B) \cup B$ sarebbe l'unione di due insiemi finiti, e quindi sarebbe finito, contro l'ipotesi. Inoltre $|A \setminus B| \leq |A| = \aleph_0$ e quindi, per il Corollario 3.4, esiste una bigezione $\varphi : \mathbb{N} \to A \setminus B$. Consideriamo l'insieme finito $B'' = B \cap A = \{b''_1, \ldots, b''_m\}$. Chiaramente B'' è disgiunto da $A \setminus B$ e $A = (A \setminus B) \cup B$. La seguente funzione $\psi : A \setminus B \to A$ è una bigezione:

$$\psi(n) = \begin{cases} b''_n & \text{se } n \leq m \\ \varphi(n-m) & \text{se } n > m. \end{cases}$$

(Se $B'' = \emptyset$ poniamo $\psi = \varphi$.) $\square$

Con l'assioma di scelta, la proprietà di sopra si estende a tutti gli insiemi infiniti.

Proposizione 3.9. (AC) Sia A un insieme infinito e B un insieme finito. Allora $|A \setminus B| = |A \cup B| = |A|$.

Dim. Sia $B' = A \cap B$. Chiaramente B' è finito in quanto sottoinsieme di B; inoltre $A \setminus B'$ è infinito, altrimenti $A = (A \setminus B') \cup B'$ sarebbe finito perché unione di due insiemi finiti. Per il Teorema 3.6, possiamo prendere un insieme numerabile $A' \subseteq A \setminus B'$. Per la Proposizione precedente, $|A'| = |A' \cup B'| = |A' \cup B|$. Sia ora $C = (A \setminus A') \setminus B' = A \setminus (A' \cup B')$. Visto che $A \setminus B = A \setminus B' = A' \cup C$, $A = (A' \cup B') \cup C$, e $A \cup B = (A' \cup B) \cup C$, e che si tratta di unioni disgiunte, possiamo concludere che $|A \setminus B| = |A| = |A \cup B|$, come volevamo.

$\square$

Esercizio 3.10. (AC) Sia X un insieme infinito. Se la differenza simmetrica $X \triangle Y$ è finita, allora $|X| = |Y| = |X \cap Y| = |X \cup Y|$.[8] (Se l'insieme X è numerabile, la proprietà si dimostra senza usare l'assioma di scelta).

4. Esempi fondamentali di insiemi numerabili

Immaginiamoci un albergo con infinite camere, numerate con i numeri naturali.[9] Supponiamo che tutte le stanze dell'albergo siano occupate, e che arrivi un nuovo cliente. Per quanto a prima vista possa sembrare impossibile, c'è un modo per risistemare gli ospiti in modo da alloggiare anche il nuovo arrivato; infatti, tutto quello che ci occorre è una bigezione $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$. Ad esempio, se chiediamo ad ogni ospite di spostarsi nella camera successiva, cioè se consideriamo la bigezione $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ dove $f : n \mapsto n + 1$, allora si libera la camera 1 dove possiamo sistemare il nuovo cliente. Un simile procedimento si può adottare anche nel caso in cui arrivi un numero finito di nuovi ospiti, perchè esistono bigezioni $f : \mathbb{N} \to \mathbb{N} \setminus \{1, \ldots, k\}$ per ogni k (ad esempio, $f : n \mapsto n + k$).

Consideriamo ora la situazione in cui si presentino infiniti nuovi clienti, uno per ogni numero naturale. Ci chiediamo se sia possibile anche in questo caso risistemare i vecchi clienti nelle camere in modo da liberare posti per tutti i nuovi arrivati. La risposta è positiva; ad esempio basta far spostare ogni ospite nella camera il cui numero è il doppio di quella che ha; in questo modo rimangono libere tutte e sole le camere con numero dispari. A questo punto, il nuovo cliente corrispondente al numero n sarà alloggiato nella camera con l'n-esimo numero dispari, cioè nella camera $2n - 1$.

Notiamo che la strategia adottata sopra si basa sull'esistenza di una bigezione tra l'unione di due copie dei numeri naturali, corrispondenti ai vecchi ospiti e ai nuovi clienti, e l'insieme dei numeri naturali, cioè le stanze dell'albergo. Più in generale, vale il seguente risultato.

Proposizione 4.1. Se A e B sono numerabili, anche $A \cup B$ è numerabile.

[8] Ricordiamo la *differenza simmetrica*: $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$.

[9] Questo tipo di albergo immaginario è spesso chiamato "albergo di Hilbert", perchè fu proprio Hilbert ad introdurlo per illustrare i paradossi dell'equipotenza tra insiemi infiniti.

Dim. Per ipotesi esistono due bigezioni $f : A \to \mathbb{N}$ e $g : B \to \mathbb{N}$. Allora si ottiene una funzione iniettiva $h : A \cup B \to \mathbb{N}$ ponendo:[10]

$$h(x) = \begin{cases} 2 \cdot f(x) & \text{se } x \in A \\ 2 \cdot g(x) - 1 & \text{se } x \in B \setminus A \end{cases}$$

Visto che f e g sono funzioni iniettive, dalla definizione segue subito che anche h è una funzione iniettiva. Notiamo inoltre che l'immagine di h è infinita perché include tutti i numeri pari. Se A e B sono disgiunti, l'immagine di h ricopre anche tutti i numeri dispari, e quindi la funzione h è biunivoca. Nel caso generale, abbiamo che $A \cup B$ è equipotente all'immagine di h, che è un sottoinsieme infinito di $\mathbb{N}$. Applicando la Proposizione 3.6, concludiamo che $|A \cup B| = \aleph_0$. □

Come immediata conseguenza, otteniamo che anche l'insieme degli interi è numerabile.

Corollario 4.2. $|\mathbb{Z}| = \aleph_0$.

Dim. Basta osservare che $\mathbb{Z} = \mathbb{Z}_{\leq 0} \cup \mathbb{N}$, dove $\mathbb{Z}_{\leq 0} = \{-n \mid n \in \mathbb{N}\} \cup \{0\}$ è chiaramente numerabile. □

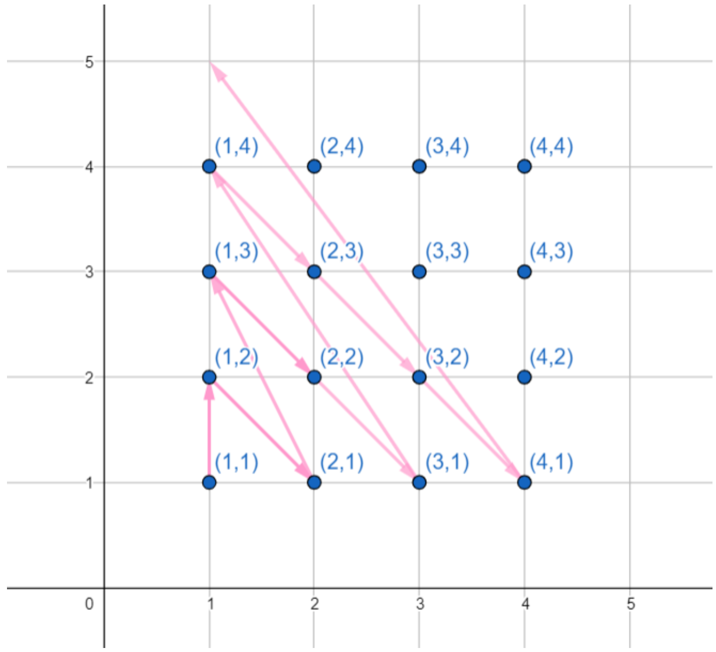
Sviluppando la storiella dell'albergo, supponiamo ora di avere infiniti piani, uno per ogni numero naturale, in ciascuno dei quali ci siano infinite camere, una per ogni numero naturale. Se abbiamo due piani occupati, possiamo risistemare tutti gli ospiti dei due piani nelle camere di un solo piano; basta infatti ragionare come nell'esempio precedente, dove i vecchi ospiti siano quelli di un piano, e i nuovi arrivati quelli dell'altro. Supponiamo ora che tutte le camere di tutti i piani siano occupate. Ci chiediamo se sia possibile sistemare tutti i clienti in un unico piano. Anche in questo caso, per quanto appaia paradossale, la cosa è possibile, perchè esistono bigezioni tra il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ ed $\mathbb{N}$ (possiamo pensare alla coppia ordinata (n, m) come alla camera n posta al piano m).

Proposizione 4.3. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Vista la particolare importanza di questo risultato, ne diamo due dimostrazioni diverse.

Dim. 1. L'idea intuitiva di questa dimostrazione è data dalla possibilità di "enumerare" tutte le coppie ordinate $(n, m) \in \mathbb{N} \times \mathbb{N}$ procedendo nel modo diagonale rappresentato in figura:

[10] Notiamo che h è anche suriettiva se e solo se A e B sono disgiunti.



Prendiamo un generica coppia (n, m), e cerchiamo di stabilire quale posizione occupa nella enumerazione indicata in figura. Si comincia contando la coppia $(1, 1)$; poi si contano le 2 coppie $(1, 2)$ e $(2, 1)$ la cui somma delle coordinate è 3; poi si contano le 3 coppie $(1, 3)$, $(2, 2)$ e $(3, 1)$ la cui somma delle coordinate è 4; poi si contano le 4 coppie $(1, 4)$, $(2, 3)$, $(3, 2)$ e $(4, 1)$ la cui somma delle coordinate è 5; e così via, fino ad arrivare a contare le $m+n-2$ coppie la cui somma delle componenti è $m+n-1$. Restano infine da contare n coppie dove la somma delle componenti è $n+m$, e cioè $(1, m+n)$, $(2, m+n-1)$, $\ldots$, (n, m). Dunque, per arrivare fino alle coppia (n, m), in tutto abbiamo contato $1+2+3+\ldots+(n+m-2)+n$ coppie. Il numero della posizione che la coppia (n, m) occupa nella nostra enumerazione è allora il seguente:[11]

$$f(n, m) \;=\; 1+2+3+\ldots+(n+m-2)+n \;=\; \frac{(n+m-2)(n+m-1)}{2}+n.$$

Che la funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ così definita sia biunivoca, è evidente dalla sua definizione. $\square$

Una dimostrazione alternativa si ottiene sfruttando una fondamentale proprietà algebrica dei numeri naturali, e cioè l'esistenza ed unicità della fattorizzazione in numeri primi.

Dim. 2. Ricordiamo che ogni naturale $k \in \mathbb{N}$ si scrive in modo unico nella forma $k = 2^\alpha(2\beta+1)$ per opportuni interi $\alpha, \beta \geq 0$. Si ha quindi una bigezione

[11] Ricordiamo che la somma dei primi k interi positivi è data da:

$$1+2+\ldots+k = \frac{k(k+1)}{2}.$$

$f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}$ dove $f(n,m) = 2^n(2m+1)$.[12] Verifichiamo questo fatto in dettaglio. Per ogni $a \in \mathbb{N}$, sia $g(a) = \alpha$ dove α è il più grande esponente $\alpha \in \mathbb{N} \cup \{0\}$ tale che 2^α divide a (dunque $\alpha = 0$ se e solo se a è dispari). Sia inoltre $h(a) = \frac{1}{2} \cdot \left(\frac{a}{2^{g(a)}} + 1\right)$. Si può verificare direttamente che la funzione $\Psi : \mathbb{N} \to \mathbb{N}_0 \times \mathbb{N}_0$ dove $\Psi(a) = (g(a), h(a))$ è la funzione inversa di f, che è dunque una bigezione. Infine, visto che $|\mathbb{N}_0| = |\mathbb{N}|$, possiamo concludere che $|\mathbb{N}| = |\mathbb{N}_0 \times \mathbb{N}_0| = |\mathbb{N} \times \mathbb{N}|$. $\square$

Come immediato corollario, ricaviamo anche che tutti i prodotti cartesiani finiti $A_1 \times \ldots \times A_k$ di insiemi A_i numerabili, sono numerabili.

Nonostante l'intuizione possa suggerire che ampliando l'insieme ordinato *discreto* dei naturali all'insieme ordinato *denso* dei razionali si ottenga un insieme più "grande", la cardinalità rimane numerabile.

PROPOSIZIONE 4.4. *L'insieme dei numeri razionali $\mathbb{Q}$ è numerabile.*

DIM. Ogni numero razionale $q \in \mathbb{Q}$ si può scrivere in modo unico nella *forma canonica* "ridotta ai minimi termini" $q = \frac{n}{m}$ dove $n \in \mathbb{Z}$ è un intero, $m \in \mathbb{N}$ è un naturale, e il massimo comune divisore $\mathrm{MCD}(n,m) = 1$. La forma canonica determina così una funzione iniettiva $\Psi : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$, e perciò $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$. Visto che $\mathbb{Q}$ è un insieme infinito e $|\mathbb{Q}| \leq \aleph_0$, segue necessariamente che $|\mathbb{Q}| = \aleph_0$ (cf. Corollario 3.4). $\square$

Più esplicitamente, un possibile modo di enumerare i numeri razionali è il seguente. Iniziamo con il numero 0; poi, per ogni $k \in \mathbb{N}$, elenchiamo tutte le frazioni $\pm\frac{n}{m}$ dove $n, m \in \mathbb{N}$ sono tali che $n + m = k + 1$ (sono esattamente $2k$ frazioni), cancellando poi quelle che non sono ridotte ai minimi termini, in modo da evitare ripetizioni. Dunque $q_1 = 0$; poi per $k = 1$ abbiamo $q_2 = -\frac{1}{1}$, $q_3 = \frac{1}{1}$; per $k = 2$ abbiamo $q_4 = -\frac{2}{1}$, $q_5 = -\frac{1}{2}$, $q_6 = \frac{2}{1}$, $q_7 = \frac{1}{2}$; per $k = 3$ abbiamo $q_8 = -\frac{3}{1}$, $q_9 = -\frac{1}{3}$, $q_{10} = \frac{3}{1}$, $q_{11} = \frac{1}{3}$ (dove abbiamo omesso le frazioni $-\frac{2}{2}$ e $\frac{2}{2}$ perché non ridotte ai minimi termini); e così via.

ESERCIZIO 4.5. Dimostrare che ogni famiglia di intervalli di numeri reali a due a due disgiunti ha cardinalità al più numerabile.

La numerabilità di $\mathbb{Q}$ permette di dimostrarne la seguente caratterizzazione come insieme ordinato denso.

TEOREMA 4.6 (Cantor). *Sia $(X, <)$ un insieme totalmente ordinato denso senza massimo né minimo. Se $|X| = \aleph_0$ allora $(X, <)$ è isomorfo a $(\mathbb{Q}, <)$.*

DIM. Fissiamo un'enumerazione $(x_n \mid n \in \mathbb{N})$ degli elementi di X, ed un'enumerazione $(q_n \mid n \in \mathbb{N})$ degli elementi di $\mathbb{Q}$. Notiamo che tali enumerazioni non necessariamente rispettano l'ordine, cioè non possiamo aspettarci che $x_n < x_m$ (o $q_n < q_m$) quando $n < m$.

Per definire un isomorfismo di ordini $\psi : X \to \mathbb{Q}$, poniamo intanto $\psi(x_1) = q_1$. Se $x_2 < x_1$, definiamo $\psi(x_2) = q_k$ dove k è il più piccolo indice tale che $q_k < q_1$; e se $x_2 > x_1$, definiamo $\psi(x_2) = q_k$ dove k è il più piccolo indice tale che $q_k > q_1$. Prendiamo ora q_2. Se $q_2 = \psi(x_2)$, non facciamo niente. Altrimenti, se $q_2 < q_1, q_k$ poniamo $\psi(x_h) = q_2$ dove h è il più piccolo indice tale che $x_h < x_1, x_2$, e se $q_2 > q_1, q_k$, definiamo $\psi(x_h) = q_2$ dove h è il più piccolo indice tale che $x_h > x_1$.

[12] Ricordiamo che $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ denota l'insieme degli interi non negativi.

Infine se q_2 è compreso tra q_1 e q_k (cioè se $q_1 < q_2 < q_k$ oppure $q_k < q_2 < q_1$), allora poniamo $\psi(x_h) = q_2$, dove h è il più piccolo indice tale che x_h è compreso tra x_1 e x_2. L'idea è proseguire in questo modo.

Per formalizzare e rendere rigorosa la costruzione accennata sopra, procediamo per ricorsione su $n \in \mathbb{N}$, definendo isomorfismi d'ordine parziali $\psi_n : X_n \to Q_n$ tra sottoinsiemi finiti $X_n \subset X$ e $Q_n \subset \mathbb{Q}$ in modo che:

- ψ_{n+1} è un'estensione di ψ_n;
- $x_1, \ldots, x_n \in X_n$ e $q_1, \ldots, q_n \in Q_n$.

Per la base $n = 1$, poniamo $X_1 = \{x_1\}$, $Q_1 = \{q_1\}$, e $\psi_1 : x_1 \mapsto q_1$. Definiamo ora ψ_{n+1} a partire da ψ_n. Lo faremo in due passi, con un procedimento che viene spesso chiamato *back and forth* ("avanti e indietro"). Precisamente, definiremo prima un'estensione intermedia $\vartheta_n : X'_n \to Q'_n$ di ψ_n dove $x_{n+1} \in X'_n$; e poi l'estensione $\psi_{n+1} : X_{n+1} \to Q_{n+1}$ di ϑ_n dove $q_{n+1} \in Q_{n+1}$. In questo modo avremo che $x_1, \ldots, x_n, x_{n+1} \in X_{n+1}$ e $q_1, \ldots, q_n, q_{n+1} \in Q_{n+1}$, come voluto.

Poniamo intanto $\vartheta_n(x) = \psi_n(x)$ per ogni $x \in X_n$, in modo che ϑ_n risulti un'estensione di ψ_n. Se $x_{n+1} \in X_n$ non facciamo niente, perché abbiamo già definito $\vartheta_n(x_{n+1}) = \psi_n(x_{n+1})$. Se $x_{n+1} < \min X_n$, definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid q_n < \min Q_n\}$; e analogamente, se $x_{n+1} > \max X_n$, definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid q_n > \max Q_n\}$. Infine, se $y < x_{n+1} < y'$ dove $y < y'$ sono due elementi consecutivi di X_n, definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid \psi_n(y) < q_n < \psi_n(y')\}$. In questo modo, abbiamo esteso ψ_n ad un isomorfismo d'ordine parziale $\vartheta_n : X'_n \to Q'_n$ dove $X'_n = X_n \cup \{x_{n+1}\}$ e $Q'_n = Q_n \cup \{\vartheta_n(x_{n+1})\}$.

Per definire l'estensione ψ_{n+1} di ϑ_n procediamo in modo simile a sopra. Poniamo intanto $\psi_{n+1}(x) = \vartheta_n(x)$ per ogni $x \in X'_n$, in modo che ψ_{n+1} risulti un'estensione di ϑ_n, e quindi di ψ_n. Se $q_{n+1} \in Q'_n$ non facciamo niente, perché esiste già un elemento $x \in X'_n$ tale che $\psi_{n+1}(x) = \vartheta_n(x) = q_{n+1}$. Se $q_{n+1} < \min Q'_n$, allora poniamo $\psi_{n+1}(x_k) = q_{n+1}$ dove $k = \min\{n \mid x_n < \min X'_n\}$; e analogamente se $q_{n+1} > \max Q'_n$, poniamo $\psi_{n+1}(x_k) = q_{n+1}$ dove $k = \min\{n \mid x_n > \max X'_n\}$. Se invece $r < q_{n+1} < r'$ dove $r < r'$ sono due elementi consecutivi di Q'_{n+1}, prendiamo gli elementi consecutivi $y < y'$ in X'_n tali che $r = \vartheta_n(y)$ e $r' = \vartheta_n(x')$; poi prendiamo $k = \min\{n \mid y < x_n < y'\}$, e definiamo $\psi_{n+1}(x_k) = q_{n+1}$. In questo modo, abbiamo esteso ϑ_n, e quindi ψ_n, ad un isomorfismo d'ordine $\psi_{n+1} : X_{n+1} \to Q_{n+1}$ dove $X_{n+1} = X_n \cup \{x_{n+1}, \psi_{n+1}^{-1}(q_{n+1})\}$ e $Q_{n+1} = Q_n \cup \{\vartheta_n(x_{n+1}), q_{n+1}\}$. È immediato verificare dalle definizioni che l'unione $\psi = \bigcup_n \psi_n$ è un isomorfismo d'ordine tra $X = \bigcup_n X_n$ e $\mathbb{Q} = \bigcup_n Q_n$.

Come osservazione finale, notiamo come l'ipotesi che i due insiemi ordinati $\mathbb{Q}$ ed X siano densi senza massimo né minimo sia necessaria affinché tutte le definizioni date risultino ben poste. $\square$

Col prossimo risultato mostriamo che un'unione al più numerabile di insiemi al più numerabili è al più numerabile.

Teorema 4.7. (AC)
Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \aleph_0$ e $|A_i| \leq \aleph_0$ per ogni $i \in I$. Allora anche l'unione $|\bigcup_{i\in I} A_i| \leq \aleph_0$.

Dim. Per ogni $i \in I$, l'insieme $\mathcal{F}_i = \{\psi \mid \psi : \mathbb{N} \to A_i \text{ suriettiva}\}$ è non vuoto e quindi, grazie all'assioma di scelta, esiste una I-sequenza $(\psi_i \mid i \in I) \in \prod_{i\in I} \mathcal{F}_i$.

Fissiamo inoltre una funzione suriettiva $\varphi : \mathbb{N} \to I$. Definiamo infine la funzione $F : \mathbb{N} \times \mathbb{N} \to \bigcup_{i\in I} A_i$ ponendo $F(n,m) = \psi_{\varphi(n)}(m)$. Se $a \in \bigcup_{i\in I} A_i$, allora $a \in A_j$ per un opportuno j, e possiamo prendere $n \in \mathbb{N}$ tale che $\varphi(n) = j$, e $m \in \mathbb{N}$ tale che $\psi_j(m) = a$. Si verifica facilmente che $F(n,m) = a$. Questo dimostra la suriettività di F, e dunque $|\bigcup_{i\in I} A_i| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0$. □

Attenzione. Nel caso in cui possa essere definita esplicitamente una sequenza $(\psi_i \mid i \in I)$ di funzioni suriettive $\psi_i : \mathbb{N} \to A_i$, allora il risultato precedente si dimostra senza usare l'assioma di scelta.

Esercizio 4.8. (AC) Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \aleph_0$ e $|A_i| \leq \aleph_0$ per ogni $i \in I$.

(1) Se esiste un insieme A_j infinito allora l'unione $|\bigcup_{i\in I} A_i| = \aleph_0$.
(2) Se gli insiemi $A_i \neq \emptyset$ sono a due a due disgiunti e I è infinito allora l'unione $|\bigcup_{i\in I} A_i| = \aleph_0$.

Notazione 4.9. Dato un insieme non vuoto X, denotiamo con:

- $\mathrm{Fin}(X) = \{A \subseteq X \mid A \text{ finito}\}$ l'insieme dei *sottoinsiemi finiti* di X.
- $\mathrm{FSeq}(X) = \bigcup_{n\in\mathbb{N}} \mathrm{Fun}(\{1,\dots,n\}, X) = \{\sigma \mid \exists n \in \mathbb{N}\ \ \sigma : \{1,\dots,n\} \to X\}$ l'insieme delle *sequenze finite* di elementi di X.

Si usa spesso la scrittura $(a_i \mid i = 1,\dots,n)$, o anche direttamente $(a_1, a_2, \dots, a_n)$, per denotare la sequenza finita σ dove $\sigma(i) = a_i$ per $i = 1, 2, \dots, n$.[13]

Per convenzione, si impone che anche la *sequenza vuota* $(\cdot)$, cioè l'insieme vuoto, appartenga a $\mathrm{FSeq}(X)$.

Esercizio 4.10. Supponiamo che $|X| = |Y|$. Allora $|\mathrm{Fin}(X)| = |\mathrm{Fin}(X)|$ e $|\mathrm{FSeq}(X)| = |\mathrm{FSeq}(Y)|$. Lo stesso risultato vale se rimpiazziamo la relazione di equipotenza con la relazione di minore o uguale tra cardinalità.

Denotiamo con $\mathrm{FSeq}^{\uparrow}(\mathbb{N}) = \{\sigma \in \mathrm{FSeq}(\mathbb{N}) \mid i < j \Rightarrow \sigma(i) < \sigma(j)\}$ l'insieme delle *sequenze finite crescenti* di numeri naturali.

Proposizione 4.11. $|\mathrm{FSeq}^{\uparrow}(\mathbb{N})| = |\mathrm{FSeq}(\mathbb{N})| = |\mathrm{Fin}(\mathbb{N})| = \aleph_0$.

Dim. La funzione iniettiva $f : \mathbb{N} \to \mathrm{Fin}(\mathbb{N})$ dove $f(n) = \{n\}$ è chiaramente iniettiva, dunque $\aleph_0 \leq |\mathrm{Fin}(\mathbb{N})|$. Dato $A \in \mathrm{Fin}(A)$, disponiamo i suoi elementi in ordine crescente $A = \{a_1 < a_2 < \ldots < a_n\}$, e definiamo $g(A) = (a_1, a_2, \dots, a_n) \in \mathrm{FSeq}(\mathbb{N})^{\uparrow}$. La funzione g è iniettiva, e quindi $|\mathrm{Fin}(\mathbb{N})| \leq |\mathrm{FSeq}^{\uparrow}(\mathbb{N})|$. Dall'inclusione $\mathrm{FSeq}^{\uparrow}(\mathbb{N}) \subseteq \mathrm{FSeq}(\mathbb{N})$ segue poi banalmente che $|\mathrm{FSeq}^{\uparrow}(\mathbb{N})| \leq |\mathrm{FSeq}(\mathbb{N})|$. Per concludere, resta allora da dimostrare che $|\mathrm{FSeq}(\mathbb{N})| \leq \aleph_0$.

A questo scopo, consideriamo $(p_n \mid n \in \mathbb{N})$, la successione crescente dei numeri primi: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, *etc.* Per ogni sequenza finita $(a_1, a_2, \dots, a_n)$ di numeri naturali, poniamo:

$$\vartheta(a_1, a_2, \dots, a_n) = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}.$$

[13] Attenzione, questa notazione può essere ambigua. Ad esempio (a_1, a_2) può denotare la sequenza σ con dominio $\{1, 2\}$ e dove $\sigma(1) = a_1$ e $\sigma(2) = a_2$, ma può anche denotare la coppia ordinata di Kuratowski $\{\{a_1\}, \{a_1, a_2\}\}$. Quale dei due possibili significati intenderemo sarà sempre chiaro dal contesto.

Nel caso della sequenza vuota, poniamo $\vartheta(\,\cdot\,) = 1$. L'unicità della scomposizione in fattori primi garantisce l'iniettività di ϑ, e dunque $|\mathrm{FSeq}(\mathbb{N})| \leq |\mathbb{N}|$, come volevamo.

Una dimostrazione alternativa della disuguaglianza $|\mathrm{FSeq}(\mathbb{N})| \leq \aleph_0$ è la seguente. Se ad ogni sequenza finita (non vuota) $\langle a_1, \ldots, a_k\rangle$ facciamo corrispondere la k-upla ordinata $(a_1, \ldots, a_k) \in \mathbb{N}^k$, si ottiene una bigezione tra $\mathrm{FSeq}(\mathbb{N})$ (senza la sequenza vuota) e $\bigcup_{k\in\mathbb{N}} \mathbb{N}^k$. Basta allora notare che quest'ultimo insieme è numerabile perché unione numerabile di insiemi numerabili. $\square$

Vedremo più avanti che, usando l'assioma di scelta, si può dimostrare che $|\mathrm{FSeq}(X)| = |\mathrm{Fin}(X)| = |X|$ per ogni insieme infinito X.

ESERCIZIO 4.12. Sia X un insieme tale che $\aleph_0 \leq |X| = |X \times X|$. Senza mai utilizzare l'*assioma di scelta*, dimostrare che $|\mathrm{FSeq}(X)| = |X|$.

PROPOSIZIONE 4.13. L'insieme $\mathbb{Z}[X]$ dei polinomi a coefficienti interi è numerabile.

DIM. Ad ogni polinomio $P(X) = a_0 + a_1X + \ldots + a_nX^n$ a coefficienti interi, si può associare la sequenza finita $(a_0, a_1, \ldots, a_n)$. Questa corrispondenza determina una funzione iniettiva $f : \mathbb{Z}[X] \to \mathrm{FSeq}(\mathbb{Z})$, dunque $|\mathbb{Z}[X]| \leq |\mathrm{FSeq}(\mathbb{Z})| = |\mathrm{FSeq}(\mathbb{N})| = \aleph_0$. Banalmente $\mathbb{Z}[X]$ è infinito, e quindi $|\mathbb{Z}[X]| = \aleph_0$. $\square$

Il prossimo risultato è un famoso teorema dimostrato da Cantor. Fu una delle prime importanti applicazioni della sua teoria delle cardinalità.

TEOREMA 4.14. *L'insieme dei numeri reali algebrici è numerabile.*[14]

DIM. È un risultato noto dell'algebra che ogni polinomio non nullo $P(X) \in \mathbb{Z}[X]$ di grado n ha al più n radici reali; dunque $\mathrm{Root}(P(X)) = \{r \in \mathbb{R} \mid P(r) = 0\}$ è finito. Notiamo che l'insieme $\mathcal{A}$ dei numeri reali algebrici si ottiene come la seguente unione

$$\mathcal{A} \;=\; \bigcup_{P(X)\in\mathbb{Z}[X]\setminus\{0\}} \mathrm{Root}(P(X)).$$

Visto che $|\mathbb{Z}[X] \setminus \{0\}| = |\mathbb{Z}[X]| = \aleph_0$, l'insieme $\mathcal{A}$ è al più numerabile perché è unione numerabile di insiemi finiti. Inoltre $\mathcal{A}$ è infinito perché banalmente $\mathbb{Z} \subseteq \mathcal{A}$, e dunque otteniamo la tesi.

Infine osserviamo che l'assioma di scelta non è necessario in questo caso, perchè è possibile definire in modo canonico una funzione suriettiva $f_{P(X)} : \mathbb{N} \to \mathrm{Root}(P(X))$ per ogni $P(X) \in \mathbb{Z}[X]$ che ammette radici reali.[15]

$\square$

Come vedremo nel prossimo paragrafo, i numeri reali *non* sono numerabili, e dunque, come conseguenza diretta del teorema di sopra, si ottiene l'esistenza di una infinità più che numerabile di numeri trascendenti.

[14] Ricordiamo che un numero $r \in \mathbb{R}$ si dice *algebrico* se esiste un polinomio non nullo a coefficienti interi $P(X) \in \mathbb{Z}[X]$ tale che $P(r) = 0$, e si dice *trascendente* se non è algebrico.

[15] Basta ordinare esplicitamente gli elementi di $\mathrm{Root}(P(X)) = \{r_1 < \ldots < r_n\}$ e poi porre $f_{P(X)}(k) = r_k$ per $k \leq n$ e $f_{P(X)}(k) = r_1$ per $k > n$.

5. Cardinalità del continuo

Il fatto che i numeri reali non sono numerabili può essere dimostrato direttamente a partire da proprietà di ordine.

TEOREMA 5.1. $|\mathbb{R}| \neq \aleph_0$.

DIM. Supponiamo per assurdo che i numeri reali siano numerabili. Visto che l'insieme ordinato $(\mathbb{R}, <)$ è denso senza massimo né minimo, allora per il teorema di Cantor si avrebbe che $(\mathbb{R}, <) \cong (\mathbb{Q}, <)$. Questo assurdo perché il primo è un ordine *completo*, mentre i razionali non lo sono.[16] $\square$

Un modo alternativo, più preciso, di dimostrare che i numeri reali non sono numerabili, è mostrare che sono equipotenti alle parti dei numeri naturali.

TEOREMA 5.2. $|\mathbb{R}| = |2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.

DIM. Per ogni successione $(a_n \mid n \in \mathbb{N}) \in 2^{\mathbb{N}}$ a valori in $\{0, 1\}$, poniamo

$$\varphi((a_n \mid n \in \mathbb{N})) \;=\; \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

Visto che la successione $S_N = \sum_{n=1}^{N} a_n/10^n$ è crescente e limitata, per la *completezza* di $\mathbb{R}$ esiste il limite $\lim_{N\to\infty} S_N = \sum_{n=1}^{\infty} a_n/10^n$, e dunque la nostra definizione è ben posta.[17]

Dimostriamo ora che la funzione $\varphi : 2^{\mathbb{N}} \to \mathbb{R}$ così definita è iniettiva, e dunque $|2^{\mathbb{N}}| \leq |\mathbb{R}|$. Se $(a_n \mid n \in \mathbb{N}) \neq (b_n \mid n \in \mathbb{N})$, prendiamo $k = \min\{n \mid a_n \neq b_n\}$, e denotiamo con $r = \sum_{n<k} a_n/10^n = \sum_{n<k} b_n/10^n$; se $k = 1$, conveniamo che $r = 0$. Supponiamo che $a_k = 1$ e $b_k = 0$ (se invece $a_k = 0$ e $b_k = 1$ la dimostrazione è del tutto analoga). Valgono le disuguaglianze

$$\begin{aligned}\varphi((a_n \mid n \in \mathbb{N})) - r \;&=\; \sum_{n=k}^{\infty} \frac{a_n}{10^n} \;\geq\; \frac{1}{10^k} \;> \\ &> \sum_{n=k+1}^{\infty} \frac{1}{10^n} \;\geq\; \sum_{n=k+1}^{\infty} \frac{b_n}{10^n} \;=\; \varphi((b_n \mid n \in \mathbb{N})) - r.\end{aligned}$$

Sia ora $\psi : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ la funzione definita ponendo $\psi(r) = \{q \in \mathbb{Q} \mid q < r\}$. Dalla *densità* di $\mathbb{Q}$ in $\mathbb{R}$ segue che ψ è iniettiva. Infatti se $r < r'$, prendendo un numero razionale q con $r < q < r'$, si ha che $q \in \psi(r')$ ma $q \notin \psi(r)$, e quindi $\psi(r) \neq \psi(r')$. Concludiamo che $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| \leq |\mathbb{R}|$, e la tesi si ottiene applicando il Teorema di Cantor-Bernstein. $\square$

Notiamo che $|\mathbb{N}| < |2^{\mathbb{N}}|$, visto che il teorema di Cantor garantisce $|\mathbb{N}| \neq |2^{\mathbb{N}}|$. Dunque, nel senso preciso dato dalla nozione di cardinalità, possiamo affermare che i numeri reali sono "più numerosi" dei numeri naturali.

DEFINIZIONE 5.3. Un insieme A ha la *cardinalità del continuo* se $|A| = |\mathbb{R}|$. In questo caso si usa la notazione $|A| = \mathfrak{c}$.

---

[16] Ad esempio, l'insieme $A = \{q \in \mathbb{Q} \mid q^2 < 2\}$ è limitato superiormente ma non ha estremo superiore.

[17] Si osservi che $\varphi(\sigma)$ è il numero reale la cui scrittura decimale è $0, \sigma(1)\sigma(2)\sigma(3)\sigma(4)\ldots$.

Visto il teorema precedente, si scrive che $\mathfrak{c} = 2^{\aleph_0}$.

Esercizio 5.4. Per ogni coppia di numeri reali $a < b$, definire esplicitamente due bigezioni $\varphi_{a,b} : [a,b] \to \mathbb{R}$ e $\psi_{a,b} : [a,b] \to (a,b)$, senza usare il Teorema di Cantor-Bernstein.

Esercizio 5.5. Dimostrare che per ogni coppia di numeri reali $a < b$, i seguenti intervalli hanno tutti la cardinalità $\mathfrak{c}$ del continuo:

$$(-\infty, b),\ (-\infty, b],\ (a,b),\ [a,b),\ (a,b],\ [a,b],\ (b,+\infty),\ [b,+\infty).$$

È naturale chiedersi se esistano cardinalità intermedie comprese tra $\aleph_0$ e $\mathfrak{c}$. L'ipotesi che questo non accada è nota come

- **Ipotesi del continuo**. *Se $A \subseteq \mathbb{R}$ è un sottoinsieme infinito di reali, allora $|A| = |\mathbb{N}|$ oppure $|A| = |\mathbb{R}|$.*

L'ipotesi del continuo è probabilmente l'esempio più famoso di proprietà *indecidibile*, cioè di una proprietà che non può essere nè dimostrata nè confutata a partire dai principi matematici comunemente accettati.[18]

Analogamente a quanto già visto per l'insieme $\mathbb{N}$ dei numeri naturali, il prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ è equipotente ad $\mathbb{R}$.

Proposizione 5.6. $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Diamo due diverse dimostrazioni di questo risultato, entrambe molto brevi.

Dim. 1. Siano D l'insieme dei numeri naturali dispari e P l'insieme dei numeri naturali pari. Visto che $|D| = |P| = |\mathbb{N}|$, dal Teorema 5.2 segue che $|\mathbb{R}| = |2^{\mathbb{N}}| = |2^D| = |2^P|$, da cui $|\mathbb{R} \times \mathbb{R}| = |2^D \times 2^P| = |2^{D \cup N}| = |2^{\mathbb{N}}| = |\mathbb{R}|$. □

Dim. 2. La funzione $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ dove $f : r \mapsto (r, 0)$ è iniettiva, e quindi $|\mathbb{R}| \le |\mathbb{R} \times \mathbb{R}|$. Osserviamo inoltre che la funzione $g : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N} \times \mathbb{N})$ dove $g : (A,B) \mapsto A \times B$ è iniettiva, e quindi si ottiene l'altra disuguaglianza $|\mathbb{R} \times \mathbb{R}| = |\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| \le |\mathcal{P}(\mathbb{N} \times \mathbb{N})| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. La tesi segue applicando il Teorema di Cantor-Bernstein. □

Esercizio 5.7. (AC)
Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \le \mathfrak{c}$ e $|A_i| \le \mathfrak{c}$ per ogni $i \in I$. Allora anche l'unione $|\bigcup_{i \in I} A_i| \le \mathfrak{c}$.

Esercizio 5.8. (AC) Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \le \mathfrak{c}$ e $|A_i| \le \mathfrak{c}$ per ogni $i \in I$.

(1) Se esiste $j \in I$ con $|A_j| = \mathfrak{c}$ allora l'unione $|\bigcup_{i \in I} A_i| = \mathfrak{c}$.
(2) Se gli insiemi $A_i \neq \emptyset$ sono a due a due disgiunti e $|I| = \mathfrak{c}$ allora l'unione $|\bigcup_{i \in I} A_i| = \mathfrak{c}$.

[18] A breve, cominceremo a dare un senso preciso alle espressioni usate qua sopra. Ad esempio, per "principi matematici comunemente accettati", intenderemo le proprietà formalizzate dagli assiomi della teoria degli insiemi ZFC di Zermelo-Fraenkel con scelta. Anche i concetti di "dimostrabilità" e "confutabilità" possono essere resi precisi. E tali concetti sono in effetti quelli fondamentali di cui si occupa la logica matematica.

Elenchiamo nei prossimi esercizi alcuni tra i più importanti insiemi aventi la cardinalità del continuo.

ESERCIZIO 5.9. Dimostrare che i seguenti insiemi hanno tutti la cardinalità del continuo:

(1) Le parti finite dei reali $\mathrm{Fin}(\mathbb{R})$.
(2) Le sequenze finite di reali $\mathrm{FSeq}(\mathbb{R})$.
(3) Le sequenze finite crescenti di reali $\mathrm{FSeq}^{\uparrow}(\mathbb{R})$.
(4) Le successioni di numeri naturali $\mathbb{N}^{\mathbb{N}} = \mathrm{Fun}(\mathbb{N}, \mathbb{N})$.
(5) Le successioni crescenti di numeri naturali.
(6) L'insieme $[\mathbb{N}]^{\aleph_0} = \{A \subseteq \mathbb{N} \mid |A| = \aleph_0\}$ dei sottoinsiemi infiniti di $\mathbb{N}$.
(7) Le bigezioni dei numeri naturali $\mathfrak{S}(\mathbb{N}) = \{f \in \mathbb{N}^{\mathbb{N}} \mid f \text{ bigezione}\}$.
(8) Le successioni di numeri reali $\mathbb{R}^{\mathbb{N}} = \mathrm{Fun}(\mathbb{N}, \mathbb{R})$.
(9) Le successioni crescenti di numeri reali.
(10) (AC) Le parti numerabili dei reali $[\mathbb{R}]^{\aleph_0} = \{A \subseteq \mathbb{R} \mid |A| = \aleph_0\}$.
(11) (AC) Le parti al più numerabili dei reali $[\mathbb{R}]^{\leq \aleph_0} = \{A \subseteq \mathbb{R} \mid |A| \leq \aleph_0\}$.

ESERCIZIO 5.10. Sia $\mathcal{C}^0(\mathbb{R})$ l'insieme di tutte le funzioni continue $f : \mathbb{R} \to \mathbb{R}$. Allora $|\mathcal{C}^0(\mathbb{R})| = \mathfrak{c}$.

ESERCIZIO 5.11. Sia $\mathcal{O}(\mathbb{R}^k)$ l'insieme di tutti i sottoinsiemi aperti di $\mathbb{R}^k$.[19] Allora $|\mathcal{O}(\mathbb{R}^k)| = \mathfrak{c}$.

SOLUZIONE. Per semplicità, consideriamo solo il caso $k = 2$ del piano euclideo $\mathbb{R} \times \mathbb{R}$ (il caso generale è del tutto simile). Una base di aperti della topologia è costituito dalle palle

$$B((q_1, q_2), r) = \{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} \mid d((x_1, x_2), (q_1, q_2)) < r\}$$

dove il centro (q_1, q_2) ha coordinate razionali, e il raggio $r > 0$ è razionale. Consideriamo ora la funzione $\Psi : \mathcal{O}(\mathbb{R} \times \mathbb{R}) \to \mathcal{P}(\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+)$ dove per ogni aperto A di $\mathbb{R} \times \mathbb{R}$,

$$\Psi(A) = \{(q_1, q_2, r) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+ \mid B((q_1, q_2), r) \subseteq A\}.$$

Per dimostrare che Ψ è iniettiva, fissiamo due aperti distinti $A \neq A'$. Prendiamo un punto (x_1, x_2) che ne testimonia la differenza, ad esempio $(x_1, x_2) \in A$ ma $(x_1, x_2) \notin A'$. Per la proprietà di insieme aperto, esiste una palla $B((q_1, q_2), r)$ con centro (q_1, q_2) di coordinate razionali e raggio $r > 0$ razionale, tale che $(x_1, x_2) \in B((q_1, q_2), r) \subseteq A$. In particolare $B((q_1, q_2), r) \nsubseteq A'$, dunque $(q_1, q_2, r) \in \Psi(A)$ ma $(q_1, q_2, r) \notin \Psi(A')$, e perciò $\Psi(A) \neq \Psi(A')$. Concludiamo che

$$|\mathcal{O}(\mathbb{R} \times \mathbb{R})| \leq |\mathcal{P}(\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+)| = |\mathcal{P}(\mathbb{N} \times \mathbb{N} \times \mathbb{N})| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}.$$

L'altra disuguaglianza $\mathfrak{c} \leq |\mathcal{O}(\mathbb{R} \times \mathbb{R})|$ è immediata. □

Togliendo un sottoinsieme numerabile da un insieme che ha la cardinalità del continuo, ciò che rimane ha ancora la cardinalità del continuo. Assumendo l'assioma di scelta, lo stesso risultato vale anche se togliamo un qualunque insieme purché di cardinalità minore del continuo.

PROPOSIZIONE 5.12.

[19] La $\mathcal{O}$ sta per "open".

(1) Sia $A \subset B$ dove $|A| \leq \aleph_0$ e $|B| = \mathfrak{c}$. Allora $|B \setminus A| = \mathfrak{c}$.
(2) (AC) Sia $A \subset B$ dove $|A| < \mathfrak{c}$ e $|B| = \mathfrak{c}$. Allora $|B \setminus A| = \mathfrak{c}$.

Osserviamo che, assumendo l'*ipotesi del continuo*, il contenuto delle due proprietà di sopra è identico; altrimenti, assumendo che l'*ipotesi del continuo* non valga, la proprietà (2) è chiaramente più generale (ma la sua dimostrazione richiede l'assioma di scelta).

DIM. Per comodità, supponiamo prima che $B = \mathbb{R} \times \mathbb{R}$. In questo caso $A \subset B$ è una relazione binaria (un insieme di coppie ordinate); consideriamo allora il dominio $A' = \mathrm{dom}(A) = \{x \in \mathbb{R} \mid \exists y \in \mathbb{R}\ (x, y) \in A\}$. Abbiamo già visto, senza uso dell'assioma di scelta, che se $|A| \leq \aleph_0$, allora anche $|A'| \leq \aleph_0$ (vedi Esercizio 3.7). Se invece $|A| < \mathfrak{c}$, questa volta usando l'assioma di scelta, possiamo concludere che $|A'| \leq |A| < \mathfrak{c}$. In entrambi i casi, segue necessariamente che $A' \neq \mathbb{R}$, e quindi possiamo prendere un elemento $a \in \mathbb{R} \setminus A'$. Notiamo che $\{a\} \times \mathbb{R} \subseteq (\mathbb{R} \times \mathbb{R}) \setminus A$, dunque $|(\mathbb{R} \times \mathbb{R}) \setminus A| \geq \mathfrak{c}$.

Supponiamo ora che B sia un qualunque insieme avente la cardinalità del continuo. Fissiamo una bigezione $\Psi : B \to \mathbb{R} \times \mathbb{R}$. Visto che $|\Psi(A)| = |A|$, possiamo applicare quanto già dimostrato sopra al sottoinsieme $\Psi(A) \subset \mathbb{R} \times \mathbb{R}$ al posto di A. Otteniamo così $\mathfrak{c} = |(\mathbb{R} \times \mathbb{R}) \setminus \Psi(A)| = |\Psi(B \setminus A)| = |B \setminus A|$. □

Come immediato corollario, si ottengono i seguenti risultati, che non richiedeno l'assioma di scelta.

PROPOSIZIONE 5.13.
(1) L'insieme dei numeri irrazionali ha la cardinalità del continuo.
(2) L'insieme dei numeri trascendenti ha la cardinalità del continuo.

DIM. Basta notare che gli irrazionali sono la differenza $\mathbb{R} \setminus \mathbb{Q}$, che i numeri trascendenti sono la differenza $\mathbb{R} \setminus \mathcal{A}$ dove $\mathcal{A}$ è l'insieme dei numeri algebrici, e ricordare che $|\mathbb{Q}| = |\mathcal{A}| = \aleph_0$. □

ESERCIZIO 5.14. (AC) Sia $A \subset B$ dove $|A| < |B|$. Se $|B \times B| = |B|$, allora $|B \setminus A| = |B|$.[20]

Facciamo ora un ulteriore passo in avanti con le cardinalità, e denotiamo

- $2^{\mathfrak{c}} = |2^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|$.

Chiaramente $2^{\mathfrak{c}} > \mathfrak{c}$ per il Teorema di Cantor.

A partire dall'equipotenza $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, si può dimostrare che $|\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N})|$, e quindi che $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$; in modo analogo, a partire dall'equipotenza $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$, si può dimostrare che $|\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})| = |\mathcal{P}(\mathbb{R})|$.

ESERCIZIO 5.15. Senza usare l'assioma di scelta, dimostrare che $|\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})| = 2^{\mathfrak{c}}$.

ESERCIZIO 5.16. Senza usare l'assioma di scelta, dimostrare che $|\mathbb{N}^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})^{\mathbb{R}}| = 2^{\mathfrak{c}}$.

[20] Vedremo più avanti che l'ipotesi $|B \times B| = |B|$ non è necessaria. Infatti dimostreremo che $|B \times B| = |B|$ per ogni insieme infinito (di più, dimostreremo che tale proprietà è equivalente all'*assioma di scelta*).

Esercizio 5.17. Senza usare l'assioma di scelta, dimostrare che se $A \subseteq B$ dove $|A| \leq \mathfrak{c}$ e $|B| = 2^{\mathfrak{c}}$, allora $|B \setminus A| = 2^{\mathfrak{c}}$.

Chiudiamo menzionando un'altra proprietà *indecidibile*. Provare a dimostrarla può essere istruttivo, basta non illudersi di riuscirci!

- Se $|\mathcal{P}(A)| = |\mathcal{P}(B)|$ allora $|A| = |B|$.