

1. CARDINALITÀ

In queste note discuteremo il concetto di cardinalità di un insieme, che significa, parlando informalmente, la sua grandezza o il suo numero di elementi. Tale concetto è naturale per gli insiemi finiti, meno per quelli infiniti. Lo studente conosce tale nozione dai corsi dei primi anni, ma qui la vedremo in modo più approfondito. Per semplicità *considereremo solo insiemi non vuoti* in quanto sarebbe un po' fastidioso definire un'applicazione definita sull'insieme vuoto o concetti simili. Questo si potrebbe anche fare e risulterebbe, come intuitivo, che $\emptyset \prec A$ per ogni insieme A non vuoto, usando le notazioni che introdurremo tra poco. Quindi, anche se non detto in modo esplicito, ogni insieme A , B , ecc. sarà considerato non vuoto anche se non detto esplicitamente. Ovviamente quando considereremo l'insieme delle parti di un insieme A , tra i suoi elementi ci sarà anche l'insieme vuoto, ma questo è un altro discorso. Notiamo che non ci preoccupiamo se nelle dimostrazioni useremo l'assioma di scelta, perché ritenuto "normale", e in genere non evidenzieremo questo fatto. Ricordo che $f : A \rightarrow B$ è detta iniettiva se $f(x) = f(y) \Rightarrow x = y$, è detta suriettiva se per ogni $b \in B$ esiste $a \in A$ tale che $f(a) = b$, è detta biiettiva se è sia iniettiva sia suriettiva.

Dati due insiemi A e B noi porremo $A \preceq B$ oppure $B \succeq A$ se esiste un'applicazione iniettiva da A in B , $A \simeq B$ se esiste un'applicazione biiettiva da A in B , ossia se A e B sono in corrispondenza biunivoca, e infine $A \prec B$ oppure $B \succ A$ se $A \preceq B$ ma non è vero che $A \simeq B$. In altri termini $A \simeq B$ significa intuitivamente che A e B sono grandi uguali, potendosi identificare, $A \preceq B$ significa che A è al massimo grande come B , essendo grande come un suo sottoinsieme. Notiamo le seguenti proprietà.

Proposizione 1.1.

- a) $A \simeq A$,
- b) Se $A \simeq B$ allora $B \simeq A$,
- c) Se $A \simeq B$ e $B \simeq C$, allora $A \simeq C$,
- d) Se $A \subseteq B$ allora $A \preceq B$,
- e) Se $A \preceq B$ e $B \preceq C$, allora $A \preceq C$,
- f) Se $A \preceq B$, $A \simeq C$, $B \simeq D$, allora $C \preceq D$.

Dim. Le dimostrazioni sono molto semplici. Ad esempio, se $A \subseteq B$, allora l'applicazione di inclusione da A in B è chiaramente iniettiva, ed è biiettiva se $B = A$. Questo prova a) e d). Per provare b) basta osservare che, se ϕ è un'applicazione biiettiva da A in B , allora ϕ^{-1} è un'applicazione biiettiva da B in A . Per provare c) basta osservare che, se ϕ è un'applicazione biiettiva da A in B , e ψ è un'applicazione biiettiva da B in C , allora $\psi \circ \phi$ è un'applicazione biiettiva da A in C . Osservando che la composizione di applicazioni iniettive è iniettiva, un ragionamento analogo prova e), e f) segue da c) ed e). ■

Le affermazioni a), b), e c) nella precedente proposizione dicono in sostanza che la relazione $\simeq$ tra insiemi è una relazione di equivalenza. Inoltre c) ed e) dicono in sostanza che se nelle relazioni $\simeq$ e $\preceq$ sostituiamo gli insiemi dati con insiemi in corrispondenza biunivoca queste continuano a valere. Tale fatto sarà usato implicitamente nel seguito. Si potrebbe dire che la cardinalità di un insieme è da questo punto di vista la sua classe di equivalenza rispetto alla relazione $\simeq$. Bisogna dire però che è un po' delicato formalizzare tale concetto

dato che quando si parla di relazione di equivalenza e di classe di equivalenza bisognerebbe considerare sottoinsiemi di un dato insieme, quindi bisognerebbe considerare tutti gli insiemi come sottoinsiemi di un dato insieme, ma è noto che non esiste alcun insieme che contiene tutti gli insiemi, poiché tale concetto porterebbe a contraddizioni (antinomia di Russel). Si potrebbe ovviare a tale inconveniente, ma questo richiederebbe nozioni un po' tecniche di teoria degli insiemi (tipo classi) che non tutti gli studenti hanno. Si potrebbe anche parlare di cardinalità di un insieme usando la teoria degli ordinali, ma tralascieremo anche questo punto di vista per lo stesso motivo. Preferiremo affidarci al concetto vago che la cardinalità di un insieme è la "grandezza" dell'insieme nel senso del suo "numero di elementi" anche se l'insieme considerato è infinito, e usare invece come concetto rigoroso che due insiemi A e B hanno la stessa cardinalità se $A \simeq B$, e che A ha cardinalità più piccola di B se $A \prec B$. Notiamo ancora

Proposizione 1.2. *Dati due insiemi non vuoti A e B , sono equivalenti le seguenti*

- i) $A \preceq B$,
- ii) *Esiste un'applicazione suriettiva da B in A .*

Dim. Se vale i) sia ϕ un'applicazione iniettiva da A in B . Allora definiamo un'applicazione suriettiva ψ da B in A nel seguente modo: $\psi(y) = x$ tale che $\phi(x) = y$ se tale x esiste, ossia se $y \in \text{Im}(\phi)$, e notiamo che tale x è unico poiché abbiamo supposto ϕ iniettiva; $\psi(y) = x_1$, ove x_1 è un arbitrario elemento di A , se $y \notin \text{Im}(\phi)$. Segue dalla definizione che $\psi(\phi(x)) = x$ per ogni $x \in A$, quindi ψ è suriettiva, e quindi vale ii). Viceversa, se vale ii), sia $\psi : B \rightarrow A$ suriettiva. Allora definiamo $\phi : A \rightarrow B$ iniettiva nel seguente modo. Sia $\phi(x) = y$ dove y è un qualunque elemento di B tale che $\psi(y) = x$. Un tale elemento esiste sicuramente dato che ψ è supposta suriettiva. Allora si ha $\psi(\phi(x)) = x$ per ogni $x \in A$, e quindi ϕ è iniettiva (se $\phi(x_1) = \phi(x_2)$, allora $x_1 = x_2$), e quindi segue i). Notiamo che definendo ϕ usiamo l'assioma della scelta, poichè, tra gli elementi $y \in B$ tali che $\psi(y) = x$, ne scegliamo arbitrariamente uno. ■

Quando gli insiemi A e B sono finiti è intuitivamente chiaro, e si può anche provare, che $A \preceq B$ se e solo se $\#A \leq \#B$, e $A \simeq B$ se e solo se $\#A = \#B$. In realtà per provare ciò rigorosamente, bisognerebbe precisare bene i fondamenti della teoria degli insiemi, in particolare che cosa è il numero di elementi di un insieme. Una definizione ragionevole è che un insieme ha n elementi se è in corrispondenza biunivoca con l'insieme $\{1, \dots, n\}$ e diremo che un insieme è finito se ha n elementi per qualche naturale n . A questo punto usiamo un fatto ben noto agli studenti, che si può provare per induzione, ossia che un'applicazione iniettiva da un $\{1, \dots, n\}$ in sé è anche biiettiva. Se A ha n elementi e B ha M elementi con $n \leq m$, poiché $\{1, \dots, n\} \subseteq \{1, \dots, m\}$, si ha che $A \preceq B$, e ovviamente, se $m = n$, allora $A \simeq B$. Viceversa, siano A e B insiemi finiti aventi rispettivamente n e m elementi. Se $A \preceq B$, allora $\{1, \dots, n\} \preceq \{1, \dots, m\}$, e segue che $n \leq m$ poiché c'è un'applicazione iniettiva da $\{1, \dots, n\}$ in $\{1, \dots, m\}$, e, se $m < n$, allora tale applicazione va da $\{1, \dots, n\}$ in sé ed è iniettiva, ma non suriettiva, assurdo. Se $A \simeq B$, allora $m = n$, perché se fosse $m > n$, allora la corrispondenza biunivoca tra $\{1, \dots, n\}$ e $\{1, \dots, m\}$ darebbe un'applicazione iniettiva da $\{1, \dots, m\}$ in $\{1, \dots, n\}$, con $m > n$, che non può esistere per quanto appena visto (con n ed m scambiati). Se invece A è un insieme finito, per esempio con n elementi, e B è un insieme infinito, allora $A \prec B$. Infatti possiamo facilmente costruire un'applicazione

iniettiva ϕ da A in B per ricorrenza nel seguente modo: Sia $A = \{x_1, \dots, x_n\}$, e una volta definiti $\phi(x_i)$ per $i \leq k$ tutti diversi tra di loro l'insieme $\{\phi(x_i) : i = 1, \dots, k\}$ non è tutto B , poiché altrimenti, l'applicazione sarebbe suriettiva, e quindi una corrispondenza biunivoca tra i primi k elementi di A e B , e quindi B avrebbe k elementi, contro l'ipotesi che B è infinito. Quindi possiamo definire $\phi(x_{k+1})$ un qualunque elemento di B diverso da ogni $\phi(x_i)$ con $i = 1, \dots, k$. Segue dalla costruzione che ϕ è iniettiva. D'altra parte, non esiste un'applicazione biiettiva ϕ da A in B , poiché per definizione un insieme in corrispondenza biunivoca con un insieme finito è finito (e con lo stesso numero di elementi). Quindi B sarebbe finito contro ipotesi. Abbiamo provato che $A \preceq B$, ma non è vero che $A \simeq B$, e quindi $A \prec B$, come annunciato.

Osservazione 1.3. Il fatto che un insieme finito non sia mai in corrispondenza biunivoca con un suo sottoinsieme proprio (che ha ovviamente un numero minore di elementi) sembra un fatto del tutto ovvio, e chi non ha esperienza con la cardinalità potrebbe pensare che valga anche per gli insiemi infiniti. Invece nell'ambito degli insiemi infiniti succede esattamente il contrario, nel senso che, dato un qualunque insieme infinito A esiste un suo sottoinsieme proprio B di A in corrispondenza biunivoca con A , e precisamente questo vale, ad esempio, se $B = A \setminus \{x_0\}$ ove x_0 è un arbitrario elemento di A . Infatti, dato che A è infinito, possiamo costruire induttivamente per $i = 1, 2, 3, \dots$, elementi x_i di A , tutti diversi tra di loro e diversi da x_0 poiché, una volta costruiti $x_1, \dots, x_n$, ci sarà sicuramente un elemento x_{n+1} di A diverso da loro, altrimenti A sarebbe finito e con $n + 1$ elementi. Allora, definiamo ϕ da A in $B = A \setminus \{x_0\}$ ponendo $\phi(x_i) = x_{i+1}$ e $\phi(x) = x$ se $x \neq x_i$ per ogni $i = 0, 1, 2, 3, \dots$. Si vede facilmente che ϕ è una biiezione da A in B . Ovviamente si deduce ora per induzione sul numero di elementi di C che se C è un sottoinsieme finito dell'insieme infinito A allora $A \setminus C \simeq A$. ■

Noi ci aspetteremmo intuitivamente che la relazione $\preceq$ abbia le proprietà delle relazioni di ordine totale: ossia se $A \preceq B$ e $B \preceq A$, allora $A \simeq B$, e inoltre vale sempre una delle due relazioni $A \preceq B$, $B \preceq A$. Tali proprietà sono vere ma la loro dimostrazione non è ovvia, in quanto la relazione $\preceq$ non è un concetto generico "intuitivo", ma è basato su una definizione precisa. Vediamo la dimostrazione.

Teorema 1.4 (di Cantor-Bernstein). *Dati due insiemi A e B , se $A \preceq B$ e $B \preceq A$, allora $A \simeq B$.*

Dim. Per ipotesi esiste un'applicazione iniettiva ϕ da A in B , ed esiste un'applicazione iniettiva ψ da B in A . Dobbiamo provare che A e B sono in corrispondenza biunivoca. Ponendo $\gamma = \psi \circ \phi$ e $C = \psi(B) \subseteq A$, dato che ψ è iniettiva abbiamo che B è in corrispondenza biunivoca con C , quindi è sufficiente trovare una biiezione da A in C . Inoltre, ovviamente γ è iniettiva da A in C . Si ha ovviamente $\gamma(A) \subseteq C \subseteq A$. Allora, ponendo $A_n = \gamma^n(A)$, $C_n = \gamma^n(C)$, si dimostra subito per induzione che

$$A_0 \supseteq C_0 \supseteq A_1 \supseteq C_1 \supseteq A_2 \supseteq C_2 \cdots \quad (1.1)$$

ove γ^n indica per definizione γ composto con se stesso n volte, e γ^0 denota la mappa identità, quindi $A_0 = A$ e $C_0 = C$. Allora definiamo una biiezione f da A in C nel seguente modo:

$$f(x) = \begin{cases} \gamma(x) & \text{se } x \in \bigcup_{n=0}^{\infty} (A_n \setminus C_n) \\ x & \text{altrimenti} \end{cases}.$$

Proviamo che f è effettivamente una biiezione da A in C . Poniamo per comodità

$$D_n = A_n \setminus C_n, \quad D = \bigcup_{n=0}^{\infty} D_n, \quad D_{\infty} = A \setminus D.$$

Si ha

$$A = \bigcup \{D_n : n = 0, 1, 2, \dots, \infty\}, \quad D_n \text{ a due a due disgiunti}, \quad (1.2)$$

$$f \text{ è una biiezione da } D_n \text{ in } D_{n+1} \quad (1.3)$$

ove ovviamente si intende $\infty + 1 = \infty$. La (1.2) segue subito da (1.1). Proviamo ora (1.3). Se $n = \infty$ questo è evidente poiché f coincide con l'identità su D_{∞} . Sia $n < \infty$ e proviamo innanzitutto che f mappa D_n in D_{n+1} .

Se $x \in D_n = A_n \setminus C_n$, allora $x = \gamma^n(u)$ per qualche $u \in A$, e inoltre $u \notin C$, poiché se $u \in C$, allora $x = \gamma^n(u) \in C_n$, contro ipotesi. Quindi $\gamma(x) = \gamma^{n+1}(u) \in \gamma^{n+1}(A) = A_{n+1}$, ma $\gamma(x) \notin C_{n+1}$ poiché, in caso contrario, $\gamma(x) = \gamma^{n+1}(v)$ per qualche $v \in C$, ma per l'iniettività, di γ^{n+1} si dovrebbe avere $v = u \notin C$, contraddizione. In conclusione $\gamma(x) \in A_{n+1} \setminus C_{n+1} = D_{n+1}$, e f mappa D_n in D_{n+1} .

Facciamo ora vedere che f è suriettiva da D_n in D_{n+1} . Dato $y \in D_{n+1}$ dobbiamo fare vedere che esiste $x \in D_n$ tale che $(f(x) =) \gamma(x) = y$. Per quanto visto sopra con n al posto di $n+1$ e x al posto di y , si ha $y = \gamma^{n+1}(u)$ per qualche $u \in A \setminus C$. Allora $y = \gamma(x)$ con $x = \gamma^n(u)$. Per quanto visto sopra con $n+1$ al posto di n , $x \in D_n$, come volevamo.

Dato che su D_n f coincide con γ che è iniettiva, allora f è iniettiva su D_n e (1.3) è provata. Da (1.2) e (1.3) è praticamente evidente che f è una biiezione da A nell'unione di tutti gli $f(D_n) = D_{n+1}$, con $n \in \mathbb{N} \cup \{\infty\}$, ossia $D_1 \cup D_2 \cup D_3 \cup \dots \cup D_{\infty}$, ossia $A \setminus D_0 = A \setminus (A \setminus C) = C$. Dimosteremo questo nei dettagli, ma prima voglio notare che questo procedimento è del tutto analogo a quanto visto nell'osservazione 1.3, ossia abbiamo decomposto l'insieme A in un insieme (D_{∞} nel nostro caso) che rimane fisso, e in una successione di insiemi disgiunti tale che ognuno è mandato nel successivo. Qui D_n gioca il ruolo che il punto x_n giocava nell'osservazione 1.3.

È evidente da quanto detto sopra che f prende valori in C . Sia $y \in C$. Allora esiste $n = 1, \dots, \infty$ tale che $y \in D_n$. Per (1.3) esiste $x \in D_{n-1} \subseteq A$ tale che $f(x) = y$. Proviamo che f è iniettiva. Siano $x_1, x_2 \in A$ con $x_1 \neq x_2$, e proviamo che $f(x_1) \neq f(x_2)$. Se x_1 e x_2 sono elementi dello stesso D_n , $f(x_1) \neq f(x_2)$ poiché f è iniettiva su ogni D_n per (1.3), se invece $x_1 \in D_n$, $x_2 \in D_{n'}$ con $n \neq n'$, allora $f(x_1) \in D_{n+1}$, $f(x_2) \in D_{n'+1}$, e dato che $n' + 1 \neq n + 1$ e i D_n sono a due a due disgiunti, allora $f(x_1) \neq f(x_2)$. ■

Corollario 1.5. a) Se $A \preceq B$ e $B \prec C$, allora $A \prec C$.

b) Se $A \prec B$ e $B \preceq C$, allora $A \prec C$.

Dim. Dato che a) e b) si provano in modi simile ci limitiamo a provare a). Per Prop. 1.1 e), si ha $A \preceq C$. D'altra parte, se fosse $A \simeq C$, si avrebbe simultaneamente $C \preceq B$ e $B \preceq C$, e quindi per il teorema di Cantor-Bernstein, $B \simeq C$, contro ipotesi. ■

Il seguente teorema è interessante ed utile da sapere, ma comunque non lo useremo nel seguito. Lo provo solo per chi è curioso.

Teorema 1.6. *Dati gli insiemi A e B , allora o $A \preceq B$ o $B \preceq A$.*

Dim. La dimostrazione usa il ben noto Lemma di Zorn, per la cui dimostrazione è essenziale l'assioma di scelta, e in realtà è equivalente ad esso. Si può trovare la dimostrazione del lemma di Zorn su Wikipedia. Nell'insieme $\mathcal{A}$ delle terne (C, D, f) con C sottoinsieme di A , D sottoinsieme di B , e f applicazione biiettiva da C in D , mettiamo un ordine parziale $\leq$ definito in questo modo: diciamo che $(C; D; f) \leq (C'; D'; f')$ se $C \subseteq C'$, $D \subseteq D'$ e $f(x) = f'(x)$ se $x \in C$, ossia f' è un'estensione di f . È facile vedere che $\leq$ definisce effettivamente un ordine parziale su $\mathcal{A}$. Proviamo che se $\mathcal{B}$ è un sottoinsieme totalmente ordinato di $\mathcal{A}$, allora $\mathcal{B}$ ha un maggiorante. Poniamo $\bar{C}$ l'unione di tutti i C tali che $(C, D, f) \in \mathcal{B}$, e $\bar{D}$ l'unione di tutti i D tali che $(C, D, f) \in \mathcal{B}$, e definiamo $\bar{f} : \bar{C} \rightarrow \bar{D}$ in questo modo: Se $x \in \bar{C}$ allora esiste $(C, D, f) \in \mathcal{B}$ tale che $x \in C$, e poniamo $\bar{f}(x) = f(x)$. Tale definizione non dipende dal C scelto in quanto, se abbiamo un altro $(C', D', f') \in \mathcal{B}$ tale che $x \in C'$, allora $f(x) = f'(x)$, poiché, essendo $\mathcal{B}$ totalmente ordinato o $(C, D, f) \leq (C', D', f')$ o $(C', D', f') \leq (C, D, f)$. In entrambi i casi, per definizione di $\leq$, si ha $f(x) = f'(x)$. Dalla definizione segue facilmente che $(\bar{C}, \bar{D}, \bar{f}) \in \mathcal{A}$, e $(C, D, f) \leq (\bar{C}, \bar{D}, \bar{f})$ per ogni $(C, D, f) \in \mathcal{B}$, ossia $(\bar{C}, \bar{D}, \bar{f})$ è un maggiorante di $\mathcal{B}$. Possiamo dunque applicare il lemma di Zorn e concludere che $\mathcal{A}$ ha un elemento massimale (C_1, D_1, f_1) . Vedremo che si deve avere

$$(C_1 = A) \vee (D_1 = B), \quad (1.4)$$

e quindi f_1 è o una biiezione tra A e un sottoinsieme di B o tra un sottoinsieme di A e B , e questo conclude la dimostrazione. Per provare (1.4) basta notare che in caso contrario C_1 è un sottoinsieme proprio di A e D_1 è un sottoinsieme proprio di B . Siano ora $x_1 \in A \setminus C_1$, $y_1 \in B \setminus D_1$, e poniamo $C_2 = C_1 \cup \{x_1\}$, $D_2 = D_1 \cup \{y_1\}$, e definiamo $f_2 : C_2 \rightarrow D_2$ ponendo

$$f_2(x) = \begin{cases} f_1(x) & \text{se } x \in C_1, \\ y_1 & \text{se } x = x_1. \end{cases}$$

Allora si vede facilmente che f_2 è una biiezione da C_2 a D_2 , e inoltre $(C_1, D_1, f_1) \leq (C_2, D_2, f_2)$, e questo contraddice l'ipotesi che (C_1, D_1, f_1) sia massimale. ■

Vediamo ora un nuovo concetto ossia quello di insieme numerabile.

Definizione 1.7. *Un insieme A si dice numerabile se è in corrispondenza biunivoca con $\mathbb{N}$ ossia se $A \simeq \mathbb{N}$.*

Notiamo che $\mathbb{N}$ è in corrispondenza biunivoca con $\mathbb{N} \setminus \{0\}$ per osserv. 1.3 quindi A è numerabile se e solo se $A \simeq \mathbb{N} \setminus \{0\}$. Questo significa che possiamo scrivere $A = \{x_1, x_2, x_3, \dots\}$, ossia possiamo "numerare" o contare gli elementi di A .

Proposizione 1.8. *Ogni insieme infinito contiene un sottoinsieme numerabile.*

Dim. Per la costruzione in Osserv. 1.3, esiste B sottoinsieme di A della forma $B = \{x_1, x_2, x_3, \dots\}$ con gli x_i tutti diversi tra loro. Allora l'applicazione $i \mapsto x_i$ è una biiezione da $\mathbb{N} \setminus \{0\}$ in B , che è dunque numerabile. ■

Corollario 1.9. *Se A è infinito e C è numerabile, allora si ha $C \preceq A$.*

Dim. Sia B come nella dimostrazione precedente. Allora $B \simeq \mathbb{N} \simeq C$, e d'altra parte $B \preceq A$. Per concludere basta applicare Propos. 1.1. ■

Corollario 1.10. *Se A è un insieme numerabile, e B è un sottoinsieme infinito di A , allora B è numerabile.*

Dim. Si ha $B \preceq A$ per ipotesi, e d'altra parte $A \preceq B$ per Corollario 1.9. Per il teorema di Cantor-Bernstein $A \simeq B$. ■

Corollario 1.11. *Un insieme A è finito o numerabile se e solo se $A \preceq \mathbb{N}$. Perciò A è finito o numerabile se e solo se esiste un'applicazione suriettiva da $\mathbb{N}$ in A .*

Dim. Se A è finito allora $A \preceq \mathbb{N}$ per il discorso prima di Osserv. 1.3. Se A è numerabile $A \preceq \mathbb{N}$ da definizione. Viceversa se $A \preceq \mathbb{N}$, allora o A è finito, o in caso contrario, è in corrispondenza biunivoca con un sottoinsieme, ovviamente infinito, di $\mathbb{N}$, che per per Corollario 1.10, è numerabile, e quindi A stesso è numerabile. La seconda affermazione è una conseguenza immediata di Propos. 1.2. ■

Notiamo che i precedenti enunciati affermano in sostanza che il numerabile è la "più piccola cardinalità infinita". A questo punto sorge spontanea la domanda se tutti gli insiemi infiniti sono numerabili. La risposta è no, come mostrato dal seguente ben noto teorema.

Teorema 1.12. *Se A è un insieme, allora $A \prec \mathcal{P}(A)$, ove $\mathcal{P}(A)$ indica l'insieme delle parti di A .*

Dim. L'applicazione da A in $\mathcal{P}(A)$ definita da $x \mapsto \{x\}$ è chiaramente iniettiva, e quindi $A \preceq \mathcal{P}(A)$. Resta da provare che non è vero che $A \simeq \mathcal{P}(A)$, ossia che data ϕ applicazione da A in $\mathcal{P}(A)$, ϕ non è biiettiva. Sia

$$E = \{x \in A : x \notin \phi(x)\}.$$

Allora se fosse $E = \phi(\bar{x})$ si avrebbe dalla definizione di E , $\bar{x} \in E \iff \bar{x} \notin E$, il ché è chiaramente impossibile. Quindi E non appartiene all'immagine di ϕ , e ϕ non è suriettiva. ■

Segue dal Teorema 1.12 che $\mathcal{P}(\mathbb{N})$ ha cardinalità strettamente superiore al numerabile. Si dice che un insieme che è in corrispondenza biunivoca con $\mathcal{P}(\mathbb{N})$ ha la cardinalità del *continuo*. Vedremo che, come ben noto, ad esempio $\mathbb{R}$ ha la cardinalità del continuo. Ovviamente usando Teorema 1.12 si possono trovare insiemi di cardinalità sempre più grande, dato che per ogni insieme si trova un insieme di cardinalità più grande. La congettura (di Cantor) che non esiste alcuna cardinalità strettamente compresa tra il numerabile e il continuo, ossia non esiste alcun insieme A tale che $\mathbb{N} \prec A \prec \mathcal{P}(\mathbb{N})$, è nota come *Ipotesi del continuo*, ed è stata dimostrata *indecidibile*, ossia, nell'ambito degli abituali assiomi della teoria degli insiemi, non si può provare né che l'ipotesi del continuo è vera né che è falsa. Vediamo ora che combinando in modo opportuno insiemi numerabili si ottengono insiemi numerabili, e poi vedremo esempi di insiemi numerabili.

Proposizione 1.13. *L'unione di una famiglia finita o numerabile di insiemi finiti e numerabili è un insieme finito o numerabile, ed è numerabile se almeno uno degli insiemi è infinito.*

Dim. Facciamo prima il caso di unione finita, e grazie da un ovvio passaggio induttivo, possiamo limitarci a studiare il caso dell'unione di due insiemi. Siano A_1 e A_2 insiemi finiti o numerabili. Per Corollario 1.11 esistono applicazioni suriettive $\phi_1 : \mathbb{N} \setminus \{0\} \rightarrow A_1$, $\phi_2 : \mathbb{N} \setminus \{0\} \rightarrow A_2$. Definiamo un'applicazione suriettiva $\phi : \mathbb{N} \setminus \{0\} \rightarrow A_1 \cup A_2$ ponendo $\phi(1) = \phi_1(1)$, $\phi(2) = \phi_2(1)$, $\phi(3) = \phi_1(2)$, $\phi(4) = \phi_2(2)$, $\phi(5) = \phi_1(3)$, $\phi(6) = \phi_2(3)$, ecc. In questo modo ϕ ha come valori sia l'immagine di ϕ_1 sia l'immagine di ϕ_2 e quindi è suriettiva su $A_1 \cup A_2$. Quindi, sempre per Corollario 1.11, $A_1 \cup A_2$ è finito o numerabile.

Vediamo ora il caso dell'unione numerabile, ossia supponiamo che abbiamo insiemi A_i , $i \in \mathbb{N} \setminus \{0\}$, tutti finiti o numerabili, e mostriamo che $A := \bigcup_{i \in \mathbb{N} \setminus \{0\}} A_i$ è finito o numerabile.

Siano come prima $\phi_i : \mathbb{N} \setminus \{0\} \rightarrow A_i$ applicazioni suriettive, e definiamo un'applicazione suriettiva $\phi : \mathbb{N} \setminus \{0\} \rightarrow A$, usando il tipico *procedimento diagonale*. Poniamo ossia $\phi(1) = \phi_1(1)$, $\phi(2) = \phi_2(1)$, $\phi(3) = \phi_1(2)$, $\phi(4) = \phi_3(1)$, $\phi(5) = \phi_2(2)$, $\phi(6) = \phi_1(3)$, $\phi(7) = \phi_4(1)$, $\phi(8) = \phi_3(2)$, $\phi(9) = \phi_2(3)$, $\phi(10) = \phi_1(4)$ ecc., ossia prima prendiamo i $\phi_i(j)$ con $i + j = 2$, poi con $i + j = 3$, poi con $i + j = 4$ ecc. In questo modo, dato che ogni elemento di A è della forma $\phi_i(j)$, l'immagine di ϕ è tutto A . Il fatto che, se almeno uno degli insiemi è infinito l'unione è numerabile è ovvio, perché l'unione in tal caso non può essere un insieme finito. ■

Corollario 1.14. *Se A è numerabile e B è finito o numerabile, allora il prodotto cartesiano $A \times B$ è numerabile.*

Dim. Basta notare che $A \times B = \bigcup_{b \in B} A \times \{b\}$. Dato che, per ogni $b \in B$, chiaramente $A \times \{b\}$ è in corrispondenza biunivoca con A , e quindi è numerabile, la tesi segue da Proposizione 1.13, tenuto conto che ovviamente $A \times B$ è infinito. ■

Osservazione 1.15. Propos. 1.13 permette di mostrare che alcuni insiemi noti sono numerabili. Ad esempio $\mathbb{Z}$ è numerabile in quanto unione degli insiemi numerabili $\mathbb{N}$ e $-\mathbb{N}$, che è numerabile in quanto chiaramente in corrispondenza biunivoca con $\mathbb{N}$. Anche $\mathbb{Q}$ è numerabile in quanto $\mathbb{Q} = \bigcup_{n \in \mathbb{N} \setminus \{0\}} Q_n$, ove $Q_n := \{\frac{p}{n} : p \in \mathbb{Z}\}$, e ovviamente ogni Q_n è

numerabile in quanto la mappa $p \mapsto \frac{p}{n}$ è una biiezione da $\mathbb{Z}$ in Q_n . Notiamo che segue ora da Corollario 1.10 che ogni sottoinsieme infinito di $\mathbb{Q}$ è numerabile.

Proviamo infine che l'insieme dei numeri reali algebrici è numerabile. Ricordo che per definizione un numero reale x è algebrico se è soluzione di un'equazione polinomiale di grado positivo a coefficienti interi. Allora l'insieme dei numeri algebrici è l'unione al variare di $n \in \mathbb{N} \setminus \{0\}$ di S_n , ove denotiamo con S_n l'insieme delle soluzioni reali di tutte le possibili equazioni algebriche della forma $a_m x^m + a_{m-1} x^{m-1} + \dots + a_0$, con $m > 0$ e $m + \sum_{i=0}^m |a_i| = n$ e tutti gli a_i interi. Poiché l'insieme di tutte le equazioni di tale tipo è finito dato che m può al massimo variare da 1 a n , e tutti i coefficienti, che sono al massimo $n + 1$, variano nell'insieme formato da $2n + 1$ elementi, degli interi tra $-n$ ed n , e quindi possiamo avere

al massimo $(n+1)(2n+1)^{n+1}$ equazioni ognuna delle quali ha al massimo n soluzioni, i numeri appartenenti a S_n sono al massimo $n(n+1)(2n+1)^{n+1}$ e quindi un numero finito. Ovviamente le maggiorazioni precedenti possono essere molto migliorate, ma questo non ha importanza per il nostro ragionamento. ■

Proposizione 1.16. *Se A è infinito e non numerabile, e B è un sottoinsieme numerabile di A , allora $A \setminus B \simeq A$.*

Dim. Notiamo che l'enunciato è del tutto simile a quello di Osservaz. 1.3, e di fatto sarà anche simile la dimostrazione. Poniamo $B_0 = B$, e notiamo che dato che, $A = B_0 \cup (A \setminus B_0)$, per Propos. 1.13, $A \setminus B_0$ è infinito e non numerabile, altrimenti sarebbe numerabile anche A , quindi per Propos. 1.8 contiene un sottoinsieme numerabile B_1 . Ora, rimpiazzando B_0 con l'insieme numerabile $B_0 \cup B_1$, ripetiamo il procedimento: $A \setminus (B_0 \cup B_1)$ è infinito e non numerabile e quindi contiene un insieme numerabile B_2 . Proseguendo in questo modo troveremo dei sottoinsiemi B_i di A , $i \in \mathbb{N}$, disgiunti tra di loro e numerabili. Poniamo ora $C = \bigcup_{i=0}^{\infty} B_i$, $C' = \bigcup_{i=1}^{\infty} B_i$. Allora C e C' sono entrambi numerabili per Propos. 1.13, quindi c'è un'applicazione $g : C \rightarrow C'$ biettiva. Ponendo ora

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

è facile vedere che f è una biezione da A in $A \setminus B$. ■

Corollario 1.17. *Se A è infinito e non numerabile, e B è un insieme numerabile, allora $A \cup B \simeq A$.*

Dim. L'insieme $A \cup B$ contiene A , e quindi è infinito e non numerabile per Corollario 1.9. Allora $(A \cup B) \setminus B \simeq A \cup B$ per Propos. 1.16. Dato che $(A \cup B) \setminus B \subseteq A \subseteq A \cup B$, si ha $A \cup B \simeq (A \cup B) \setminus B \preceq A \preceq A \cup B$, e quindi, per il teorema di Cantor-Bernstein, $A \cup B \simeq A$. ■

Vediamo ora che alcuni ben noti insiemi, e in particolare $\mathbb{R}$, hanno la cardinalità del continuo.

Lemma 1.18. *Si ha $[0, 1[\simeq \mathcal{P}(\mathbb{N})$ ossia $[0, 1[$ ha la cardinalità del continuo.*

Dim. Proveremo in realtà che $[0, 1[\simeq \mathcal{P}(\mathbb{N} \setminus \{0\})$, ma questo è equivalente all'enunciato del lemma, dato che $\mathbb{N}$ e $\mathbb{N} \setminus \{0\}$ sono in corrispondenza biunivoca. Scriviamo $x \in [0, 1[$ in forma binaria, ossia

$$x = \sum_{n=1}^{+\infty} \frac{x_n}{2^n}, \quad x_n \in \{0, 1\}. \quad (1.5)$$

Come è noto tale scrittura non è unica, in quanto, per esempio, $\frac{1}{2} = \sum_{n=2}^{+\infty} \frac{1}{2^n}$, però diventa unica se assumiamo, come faremo, che x_n non è definitivamente 1. Sia ora $g : [0, 1[\rightarrow \mathcal{P}(\mathbb{N} \setminus \{0\})$ definita da

$$g(x) = \{n \in \mathbb{N} \setminus \{0\} : x_n = 1\}.$$

Allora, ovviamente g è iniettiva, poichè, se $g(x) = g(x')$, allora $x_n = 1 \iff n \in g(x) \iff n \in g(x') \iff x'_n = 1$, e dato che x_n e x'_n valgono 0 o 1, allora $x_n = x'_n$ per ogni n , e, grazie ad (1.5), $x = x'$. Invece g non è suriettiva, in quanto, per la nostra assunzione, si vede subito che l'immagine di g è data da

$$B := \mathcal{P}(\mathbb{N} \setminus \{0\}) \setminus A, \quad A := \bigcup_{h=1}^{\infty} A_h, \quad A_h := \left\{ C \in \mathcal{P}(\mathbb{N} \setminus \{0\}) : n \in C \quad \forall n > h \right\}.$$

Allora g è una biiezione da $[0, 1[$ in B , e quindi $[0, 1[\simeq B$. Dato che $\mathcal{P}(\mathbb{N} \setminus \{0\}) \succ \mathbb{N} \setminus \{0\}$ per Teorema 1.12, per Propos. 1.16 basta provare che A è numerabile per concludere. In base a Propos. 1.13, basterà provare che ogni A_h è finito per dedurre che A è numerabile (è ovvio che A è infinito). Ma si vede facilmente che l'applicazione da $\mathcal{P}(\{1, \dots, h\})$ a A_h definita da $E \mapsto E \cup \{h+1, h+2, h+3, \dots\}$ è una biiezione, e quindi, essendo finito $\mathcal{P}(\{1, \dots, h\})$, è finito anche A_h . ■

Teorema 1.19. *Se E è un sottoinsieme di $\mathbb{R}$ con interno non vuoto, allora E ha la cardinalità del continuo. In particolare $\mathbb{R}$ ha la cardinalità del continuo.*

Dim. Proveremo che, se E è un sottoinsieme di $\mathbb{R}$ con interno non vuoto, allora $E \simeq \mathbb{R}$, così tutti i sottoinsiemi di $\mathbb{R}$ con interno non vuoto hanno la stessa cardinalità, e quindi la stessa di $[0, 1[$, che ovviamente ha interno non vuoto, e per Lemma 1.18, hanno la cardinalità del continuo. Dato che E ha interno non vuoto, esistono numeri reali a e b con $a < b$ tali che $E \supseteq]a, b[$. Proveremo che $]a, b[\simeq \mathbb{R}$. Per trovare una biiezione da $]a, b[$ in $\mathbb{R}$ notiamo che la funzione $\tan$ è una biiezione da $] -\frac{\pi}{2}, \frac{\pi}{2}[$ in $\mathbb{R}$. Ora adatteremo tale funzione all'intervallo $]a, b[$. Precisamente la funzione $x \mapsto \tan\left(-\frac{\pi}{2} + \frac{\pi}{b-a}(x-a)\right)$ è una biiezione da $]a, b[$ in $\mathbb{R}$. quindi $]a, b[\simeq \mathbb{R}$. D'altra parte, dato che $]a, b[\subseteq E \subseteq \mathbb{R}$, abbiamo $\mathbb{R} \simeq]a, b[\preceq E \preceq \mathbb{R}$, e quindi, per il teorema di Cantor-Bernstein, $E \simeq \mathbb{R}$. ■

Ricordo che ci sono dimostrazioni dirette del fatto che $\mathbb{R}$ non è numerabile. Quella forse più nota si basa sul fatto che, se $\mathbb{R}$ fosse numerabile, i numeri reali si potrebbero mettere in ordine in modo che $\mathbb{R} = \{a_1, a_2, a_3, \dots\}$, e allora, se a è un numero reale, che nel suo sviluppo decimale ha la prima cifra (dopo la virgola) diversa dalla prima cifra di a_1 , la seconda diversa dalla seconda cifra decimale di a_2 , e in genere la n -ma cifra decimale diversa dalla n -ma cifra decimale di a_n , prendendo tutte le cifre di a diverse da 0 e 9, tale numero a è sicuramente diverso da a_n in quanto ha diversa la cifra decimale n -ma e quindi a è un numero reale diverso da tutti gli a_n , contraddizione. Ricordo che può capitare che due diversi sviluppi decimali rappresentino lo stesso numero reale, ma questo solo quando uno dei due sviluppi decimali è 9 da un certo punto in poi e l'altro è 0 da un certo punto in poi. Per questo ho preso a che non ha cifre decimali che valgono 0 o 9. Un'altra dimostrazione si basa sul fatto che, se $\mathbb{R} = \{a_1, a_2, a_3, \dots\}$, allora prendiamo un intervallo compatto non vuoto I_1 non contenente a_1 , poi induttivamente un intervallo

compatto non vuoto I_n contenuto in I_{n-1} , non contenente a_n . Allora l'intersezione I di tutti gli I_n è non vuota e quindi contiene un numero reale a , che è necessariamente diverso da tutti gli a_n , poiché $a_n \notin I_n$ e quindi $a_n \notin I$. Altri sottoinsiemi di $\mathbb{R}$ che hanno la cardinalità del continuo si possono trovare usando Propos. 1.16, per esempio $\mathbb{R} \setminus \mathbb{Q} \simeq \mathbb{R}$. Ora vediamo che anche il prodotto cartesiano $[0, 1[\times [0, 1[$ ha la cardinalità del continuo, e questo comporta il fatto paradossale che un quadrato ha "tanti punti quanti il suo lato".

Teorema 1.20. *Si ha $[0, 1[\times [0, 1[\simeq [0, 1[$.*

Dim. Si ha ovviamente

$$[0, 1[\preceq [0, 1[\times [0, 1[$$

in quanto l'applicazione $x \mapsto (x, 0)$ da $[0, 1[$ in $[0, 1[\times [0, 1[$ è iniettiva. Definiamo ora un'applicazione iniettiva ϕ da $[0, 1[\times [0, 1[$ in $[0, 1[$. Scriviamo un punto $x \in [0, 1[$ come il suo sviluppo decimale $x = 0.x_1x_2x_3\dots$, con x_i che non valgono 9 da un certo punto in poi. Allora sia $\phi(x, x') = 0.x_1x'_1x_2x'_2x_3x'_3\dots$, ossia ϕ mischia le cifre di x e di x' . Allora ϕ è a valori in $[0, 1[$, e inoltre è iniettiva in quanto se $\phi(x, x') = \phi(y, y')$ allora x ha le stesse cifre decimali di y , e x' ha le stesse cifre decimali di y' . Quindi $x = y$ e $x' = y'$, e $(x, x') = (y, y')$. Segue che $[0, 1[\times [0, 1[\preceq [0, 1[$ e per il teorema di Cantor-Bernstein $[0, 1[\times [0, 1[\simeq [0, 1[$. ■

Corollario 1.21. *$\mathbb{R}^n$ ha la cardinalità del continuo. Inoltre, se E è un sottoinsieme di $\mathbb{R}^n$ che contiene un insieme avente la cardinalità del continuo, allora E ha la cardinalità del continuo.*

Dim. Si vede subito che se $A \simeq B$ e $C \simeq D$ allora $A \times C \simeq B \times D$. Quindi, dato che $[0, 1[\simeq \mathbb{R}$, si ha $\mathbb{R}^2 \simeq [0, 1[\times [0, 1[\simeq [0, 1[\simeq \mathbb{R}$. Adesso segue per induzione su n che $\mathbb{R}^n \simeq \mathbb{R}$. Sia ora $E \subseteq \mathbb{R}^n$, $E \supseteq A$, con $A \simeq \mathbb{R}$. Allora $\mathbb{R} \simeq A \preceq E \preceq \mathbb{R}^n \simeq \mathbb{R}$, e $E \simeq \mathbb{R}$ per il teorema di Cantor-Bernstein. ■

Abbiamo visto in Corollario 1.14 che il prodotto cartesiano di insiemi numerabili è numerabile, e negli ultimi enunciati che il prodotto di due insiemi con la cardinalità del continuo ha la cardinalità del continuo. Come generalizzazione si può provare che se A e B sono infiniti e $A \preceq B$, allora $A \times B \simeq B$, e si può provare anche che $A \cup B \simeq B$. La dimostrazione generale di questi fatti comunque richiederebbe delle tecniche di teoria degli insiemi che oltrepassano gli argomenti di queste note. Concluderò con degli esercizi.

1) Provare che se $A \simeq \mathbb{R}$ e $\emptyset \neq B \preceq \mathbb{R}$, allora $A \cup B \simeq \mathbb{R}$ e $A \times B \simeq \mathbb{R}$. Si intende di provare queste affermazioni senza usare i risultati non dimostrati citati poco sopra.

2) Provare che se $A = \bigcup_{i \in I} A_i$, $B = \bigcup_{i \in I} B_i$, e A_i sono insiemi a due a due disgiunti, e B_i sono insiemi a due a due disgiunti, e $A_i \simeq B_i$ per ogni $i \in I$, allora $A \simeq B$. Qui si intende che I è un qualunque insieme non vuoto, finito o infinito. Notiamo che questo enunciato è usato in casi particolari nella dimostrazione del teorema di Cantor-Bernstein e nella dimostrazione di Propos. 1.16.

3) Trovare una biiezione da $]0, 1[$ in $[0, 1]$.