Alma Mater Studiorum · Università di Bologna

Facoltà di scienze matematiche, fisiche e naturali

Corso di Laurea Triennale in Matematica

CARDINALITÁ DI INSIEMI E NUMERI CARDINALI

Tesi di Laurea in Logica Matematica

Relatore:
Chiar.mo Prof.
PIERO PLAZZI

Presentata da:
LORENZO RUARO

III Sessione
Anno Accademico 2014/2015

Indice

Introduzione

Questo breve elaborato si pone l'obiettivo di esaminare (quanto meno parzialmente) la natura degli insiemi finiti e infiniti (oltre che la caratteristica di elemento assorbente degli insiemi infiniti rispetto al'operazione di unione, sottrazione insiemistica, prodotto cartesiano e parzialmente dell'"elevamento a potenza" nei confronti di insiemi di potenza inferiore) attraverso le relazioni di equipotenza e lo studio dei numeri ordinali e cardinali (con le loro applicazioni alla teoria degli insiemi). Esamineremo, quindi, il lavoro del matematico Gregor Cantor e la sua formalizzazione nella teoria degli insiemi moderna.

Nei capitoli che seguiranno saranno enunciati numerosi teoremi, ma solamente nel capitolo 2 ne forniremo le dimostrazioni, per tutti gli altri rimando a [Abian 1972].

Capitolo 1

Premesse Utili

1.1 Assiomi della teoria degli insiemi di Zermelo-Fraenkel

In questa sezione elencheremo gli assiomi (e alcune loro dirette conseguenze) della teoria degli insiemi di Zermelo-Fraenkel che ci permetteranno di affrontare gli argomenti trattati nei successivi capitoli:

Assioma 1.1 (Assioma di estensione)**.** Un insieme X è uguale a un insieme Y se e solo se X e Y hanno gli stessi elementi.

Assioma 1.2 (Assioma delle potenze)**.** Per ogni insieme X esiste l'insieme i cui elementi sono tutti e soli i sottoinsiemi di X (cioè l'insieme potenza di X).

Assioma 1.3 (Assioma della somma)**.** Per ogni insieme X esiste l'insieme di tutti e soli gli elementi di tutti gli elementi di X.

Assioma 1.4 (Schema di rimpiazzamento)**.** Sia $P(a,\ b)$ una proprietà. Se P è un funzionale (ovvero, se a ogni a corrisponde uno e un solo b tale per cui $P(a,\ b)$), allora dato un insieme X esiste un insieme Y contenente tutte e sole le immagini di elementi di X secondo P.

Lo schema di rimpiazzamento implica l'assioma della coppia:

Assioma 1.5 (Assioma della coppia)**.** Dati X e Y insiemi qualunque, esiste sempre un terzo insieme Z che li contiene come elementi.

Con tale assioma abbiamo, quindi, la possibilità di formare il singoletto di ogni insieme, proprietà che ci tornerà utile nel prossimo assioma:

Assioma 1.6 (Assioma dell'infinità)**.** Esiste un insieme W tale che:

1. $\emptyset \in W$
2. $x \in W \longrightarrow (x \cup \{x\} \in W)$

In seguito all'assioma dell'infinità, abbiamo il seguente teorema (che non dimostreremo) che ci permetterà di interpretare i numeri naturali come insiemi:

Teorema 1.1.1.
Esiste un unico insieme ω tale che:

1. $\emptyset \in \omega$*;*
2. *Se x è un elemento di ω, lo è anche il suo immediato successivo x^+ (ossia, $x \cup \{x\}$).*
3. *ω è un sottoinsieme di ogni altro insieme soddisfacente alle condizioni (1) e (2).*

tale insieme ω è equivalente all'insieme $\mathbb{N}$ di tutti i numeri naturali, infatti, possiamo definire i numeri naturali nel modo seguente:

$0 = \emptyset$

$1 = \{\emptyset\} = \{0\}$

$2 = \{\emptyset,\ \{\emptyset\}\} = 1 \cup \{1\} = \{0,\ 1\}$

$3 = \{\emptyset,\ \{\emptyset\},\ \{\emptyset,\ \{\emptyset\}\}\} = 2 \cup \{2\} = \{0,\ 1,\ 2\}$

$4 = \{\emptyset,\ \{\emptyset\},\ \{\emptyset,\ \{\emptyset\}\},\ \{\emptyset,\ \{\emptyset\},\ \{\emptyset,\ \{\emptyset\}\}\}\} = 3 \cup \{3\} = \{0,\ 1,\ 2,\ 3\}$

...

Nelle dimostrazioni e negli enunciati dei teoremi dei successivi capitoli assumeremo sempre tali assiomi.

1.2 Assioma della scelta

Indipendente dagli assiomi della teoria degli insiemi di Zermelo-Fraenkel, ma ugualmente fondamentale, vi è l'assioma della scelta:

Assioma 1.7 (Assioma della scelta)**.** Per ogni insieme X esiste una funzione f tale che, per ogni elemento non vuoto y di X, $f(y) \in y$.

Una funzione f che, dunque, *sceglie* un elemento da ogni elemento non vuoto di un insieme X, si chiama *funzione di scelta* per X.

Tale assioma può essere riformulato in maniera equivalente con i seguenti teoremi:

Lemma 1.2.1 (Lemma di Zorn)**.**
Sia P un insieme parzialmente ordinato non vuoto tale che ogni suo sottoinsieme totalmente ordinato abbia un maggiorante. Allora P ha almeno un elemento massimale

Nella sezione seguente vedremo meglio le definizioni di insiemi parzialmente o totalmente ordinati.

Un altro teorema equivalente all'assioma della scelta è il teorema di Zermelo o teorema del buon ordinamento che vedremo nella sezione seguente.

Importanti risultati ottenuti tramite l'assioma della scelta sono, per esempio:

- Il teorema di Hahn-Banach;
- Ogni spazio vettoriale non nullo ammette una base.

Come nel caso degli assiomi della sezione precedente, nelle dimostrazioni e negli enunciati dei teoremi dei successivi capitoli assumeremo sempre l'assioma della scelta.

1.3 Teoremi e definizioni utili

In questa sezione enuncieremo delle definizioni e dei teoremi particolarmente importanti per i capitoli seguenti.

Definizione 1.1 (Ordine parziale)**.** Un sottoinsieme P del prodotto cartesiano $S \times S$ si dice un ordine parziale nell'insieme S se sono verificate le seguenti condizioni:

1. $(x,\ x) \in P$, per ogni elemento x di S (relazione riflessiva) .
2. Se $(x,\ y) \in P$ e $(y,\ x) \in P$ allora $x = y$ per ogni elemento x e y di S (relazione antisimmetrica).
3. Se $(x,\ y) \in P$ e $(y,\ z) \in P$ allora $(x,\ z) \in P$ per tutti gli elementi x, y e z di S (relazione transitiva).

Per cui abbiamo la seguente definizione:

Definizione 1.2 (Insieme parzialmente ordinato)**.** Una coppia ordinata $(S, \leq$ $)$ si dice un insieme parzialmente ordinato se e solo se $\leq$ è un ordine parziale sull'insieme S.

Definizione 1.3 (Ordinamento totale)**.** Un ordinamento parziale $\leq$ su un insieme S si dice un ordinamento totale (o semplice) in S se e solo se:

$$x \leq y \quad \text{o} \quad y \leq x$$

per ogni coppia di elementi x e y di S.

Analogamente per il caso di ordinamento parziale, abbiamo che la coppia ordinata $(S, \leq)$ si dice insieme totalmente ordinato se e solo se $\leq$ è un ordine totale sull'insieme S.

Definizione 1.4 (Elemento minimo di un insieme)**.** Sia $(S, \leq)$ un insieme parzialmente ordinato. Un elemento $p \in S$ si dice *il minimo* elemento di S se e solo se

$$p \leq x \quad \text{per ogni} \quad x \in S$$

.

Definizione 1.5 (Elemento massimo di un insieme)**.** Sia $(S, \leq)$ un insieme parzialmente ordinato. Un elemento $p \in S$ si dice *il massimo* elemento di S se e solo se

$$x \leq p \quad \text{per ogni} \quad x \in S$$

.

Definizione 1.6 (Segmento iniziale)**.** Sia $(S, \leq)$ un insieme parzialmente ordinato. Per ogni elemento a di S, l'insieme

$$I(a) = \{x \ \mid \ (x \in S) \wedge (x < a) \ \}$$

si dice segmento iniziale di P determinato da a.

Definizione 1.7 (Insieme ben ordinato)**.** Un insieme parzialmente ordinato tale che ogni suo sottoinsieme non vuoto ha un elemento minimo, si dice un insieme ben ordinato.

Teorema 1.3.1 (Teorema del Buon Ordinamento)**.**
Ogni insieme possiede un buon ordinamento.

La condizione di Buon ordinamento ci permette di formulare il seguente teorema che ci sarò di vitale importanza per definire le operazioni tra ordinali e cardinali:

Teorema 1.3.2 (Teorema di induzione transfinita)**.**
Sia W un insieme ben ordinato e sia V un sottoinsieme di W tale che per ogni elemento $x \in W$ valga la seguente condizione:

$$I(x) \subset V \quad \textit{implica} \quad x \in V$$

Allora V=W.

Abbiamo, conseguentemente, un teorema particolarmente importante per le dimostrazioni del capitolo 2:

Teorema 1.3.3 (Teorema di ricorrenza finita)**.**
Sia g una funzione da un insieme E in E e sia e un elemento di E. Allora esiste un'unica funzione f dall'insieme di tutti i numeri naturali $\mathbb{N}$ in E tale che

$$f(0) = e \qquad e \qquad f(m^+) = g(f(m)) \quad \textit{per ogni } m \tag{1.1}$$

dove, con m^+ si indica il successivo immediato di m.

Come ultimo teorema da tenere a mente nelle premesse utili abbiamo il seguente:

Teorema 1.3.4 (Teorema di ricorrenza transfinita)**.**
Sia g una funzione dall'insieme potenza $\mathcal{P}(E)$ di un insieme E in E e sia e un elemento di E. Sia W un insieme ben ordinato il cui primo elemento sia u. Allora esiste una funzione f da W in E tale che:

$$f(u) = e \qquad e \qquad f(w) = g(f(I(w)))$$

per ogni elemento w di W tale che $w \neq u$.

Capitolo 2

Equipotenza di insiemi

2.1 Insiemi finiti e infiniti

Partiamo subito dalla definizione di equipotenza:

Definizione 2.1 (Equipotenza)**.** Due insiemi X e Y si dicono equipotenti (o si dice che vi è un'equipotenza tra X e Y) se e solo se esiste un'applicazione biunivoca da X a Y.

Per esprimere che due insiemi X e Y sono equipotenti scriviamo:

$$X \cong Y$$

Considerando tale definizione, abbiamo che la relazione di equipotenza tra insiemi è una relazione (non in senso insiemistico) di equivalenza, infatti, sapendo che f è un'equipotenza tra due insiemi X e Y, si ha che anche la sua inversa f^{-1} è un'equipotenza (questa volta tra gli insiemi Y e X), inoltre, se f e g sono due equipotenze, rispettivamente, tra X e Y e tra Y e Z, abbiamo che la composizione $g \circ f$ è un'equipotenza tra X e Z.
Formalizzando, abbiamo:

1. $X \cong X$ (riflessività)
2. $X \cong Y \to Y \cong X$ (simmetria)
3. $X \cong Y$ e $Y \cong Z$ implica $X \cong Z$ (transitività)

Definizione 2.2 (Insieme Infinito)**.** Un insieme si dice *infinito* se e solo se ha (almeno) un sottoinsieme proprio che è equipotente all'insieme stesso.

Definizione 2.3 (Insieme Finito)**.** Un insieme si dice *finito* se e solo se non è infinito.

Da queste due definizioni otteniamo immediatamente che l'insieme vuoto $\emptyset$ è perciò finito (e, conseguentemente, ogni insieme infinito è non vuoto).

Definizione 2.4 (Insieme Numerabile)**.** Un insieme si dice *numerabile* se e solo se è equipotente all'insieme di tutti i numeri naturali $\mathbb{N}$.

Da tale definizione otteniamo che l'insieme dei numeri naturali positivi $\mathbb{N}^+$ e l'insieme dei numeri naturali pari sono numerabili (e quindi sono equipotenti all'insieme dei numeri naturali $\mathbb{N}$). Tale affermazione si verifica trovando un'applicazione biunivoca dall'insieme $\mathbb{N}$ a uno dei due insiemi precedenti utilizzando, rispettivamente, la funzione $f(x) = x + 1$ per l'insieme $\mathbb{N}^+$ (tale funzione è banalmente biunivoca da $\mathbb{N}$ a $\mathbb{N}^+$, mentre è iniettiva da $\mathbb{N}$ a $\mathbb{N}$) e la funzione $f(x) = 2x$ per l'insieme dei numeri naturali pari (anche questa è una funzione biunivoca da $\mathbb{N}$ ai naturali pari e iniettiva da $\mathbb{N}$ a $\mathbb{N}$). Analogamente, si può verificare che anche l'insieme dei numeri naturali dispari e l'insieme di tutti i numeri naturali maggiori di un numero naturale n sono numerabili.
Inoltre, abbiamo un teorema molto importante:

Teorema 2.1.1.
Un insieme è infinito se e solo se contiene un sottoinsieme numerabile.

Dimostrazione. Chiamiamo S il nostro insieme infinito. Consideriamo il sottoinsieme proprio (infinito) P di S. Essendo S un insieme infinito, abbiamo che esiste, per definizione, una equipotenza g (ovvero una funzione biunivoca) tra S e P.
Essendo P un sottoinsieme proprio di S, si vede che $S \setminus P \neq \emptyset$ e che quindi esiste (almeno) un elemento $e_0 \in (S \setminus P)$. Sia $e_1 = g(e_0)$. Dato che $e_1 \in P$, si ha che $e_0 \neq e_1$. Tuttavia, $e_1 \in S$ e, dunque tramite l'applicazione g ha un'immagine $g(e_1)$ appartenente a P. Sia $e_2 = g(e_1)$. Essendo g biunivoca (e in particolare iniettiva) $e_1 \neq e_2$ (in quanto, abbiamo che $e_0 \neq e_1$ implica, se g è iniettiva, che $g(e_0) \neq g(e_1)$, ma $g(e_0) = e_1$ e $g(e_1) = e_2$, da cui il risultato) ed essendo $e_0 \notin P$, si vede che e_0, e_1 ed e_2 sono tre elementi distinti di S.
Per ricorrenza si riesce, dunque a ottenere una successione infinita di e_0, e_1, e_2, ... di elementi distinti di S.
Più rigorosamente, tramite il teorema della ricorrenza finita abbiamo che esiste un'unica applicazione f da $\mathbb{N}$ in S, tale che:

$$f(0) = e_0 \quad \text{e} \quad f(m^+) = g(f(m)) \quad \text{per ogni} \quad m \tag{2.1}$$

dove m^+ è, come al solito, il numero immediatamente successivo al numero naturale m, g è l'equipotenza definita precedentemente ed e_0 è l'elemento definito precedentemente di $S \setminus P$.

Per dimostrare l'implicazione da sinistra a destra, basta dimostrare che f è un'applicazione biunivoca tra $\mathbb{N}$ e un sottoinsieme di S.
Dimostriamo, per prima cosa, l'iniettività di tale funzione, ricordando che ogni elemento non nullo m di $\mathbb{N}$ ha un unico antecedente immediato m^- (rispetto all'ordinamento naturale di $\mathbb{N}$).
Si supponga per assurdo che f non sia iniettiva e sia n il più piccolo numero naturale (che esiste grazie al buon ordinamento di $\mathbb{N}$) tale che:

$$f(n) = f(k) \quad \text{con} \quad n \neq k \tag{2.2}$$

Chiaramente $k > n$. Inoltre, $n > 0$ dato che $f(0) \in (S \setminus P)$ e $f(m) \in P$ per ogni $m > 0$. Dunque $k > n > 0$. Ma allora, grazie a (2.1) e (2.2), si ha:

$$f(n) = g(f(n^-)) = g(f(k^-)) = f(k)$$

Dato che, però, g è una funzione biunivoca e, in particolare, iniettiva, le uguaglianze precedenti implicano

$$f(n^-) = f(k^-) \quad \text{con} \quad n^- \neq k^-$$

Così, abbiamo, però, trovato un numero che soddisfa la (2.2) e che è più piccolo di n, per cui abbiamo un assurdo e, quindi, f è necessariamente iniettiva.
Dimostriamo, ora, la suriettività della funzione f. Poiché f ristretta a P (quindi escludendo l'elemento e_0) è definita per ricorrenza come composizione di funzioni, possiamo osservare che, dato che g, per ipotesi, è suriettiva allora $g \circ f$ è anch'essa suriettiva e, conseguentemente , per come è stata costruita, anche la f.
Abbiamo, dunque, che l'applicazione f è una corrispondenza biunivoca tra $\mathbb{N}$ e un sottoinsieme di S (in questo nostro caso P). Quindi, se S è un insieme infinito, questo contiene un sottoinsieme numerabile.

Dimostriamo, infine, l'implicazione da destra a sinistra: ovvero che se S ha un sottoinsieme numerabile E, allora S è un insieme infinito.
Dalla definizione di insieme numerabile possiamo supporre che

$$E = \{e_0,\ e_1,\ e_2,\ ...\}$$

Consideriamo il sottoinsieme proprio $S \setminus \{e_0\}$. Si vede chiaramente che esiste una funzione f da S a $S \setminus \{e_0\}$ tale che:

$$\begin{cases} f(x) = x, & \text{per ogni } x \in (S \setminus E) \\ f(e_m) = e_{m+1}, & \text{per } m = 0,\ 1,\ 2,\ ... \end{cases}$$

f è una funzione biunivoca tra S e il suo sottoinsieme proprio $S \smallsetminus \{e_0\}$, quindi abbiamo, per definizione che S è un insieme infinito. □

Tale teorema ci permette di dire, dunque, che l'insieme di tutti i numeri naturali $\mathbb{N}$, l'insieme di tutti i numeri interi $\mathbb{Z}$, l'insieme di tutti i numeri razionali $\mathbb{Q}$ e l'insieme di tutti i numeri reali $\mathbb{R}$, sono tutti infiniti.

Ora abbiamo, invece, un teorema di caratterizzazione degli insiemi finiti:

Lemma 2.1.1.
Per ogni insieme infinito S e ogni elemento a, $S \smallsetminus \{a\}$ è un insieme infinito.

Dimostrazione. Questo risultato è una conseguenza diretta del teorema 2.1.1 considerando il fatto che S, essendo infinito, deve contenere una successione infinita

$$e_0,\ e_1,\ e_2,\ \ldots$$

□

Teorema 2.1.2.
Un insieme è finito se e solo se è equipotente a un numero naturale (inteso come insieme).

Dimostrazione. Per prima cosa dimostriamo l'implicazione da sinistra a destra. Sia, dunque S un insieme finito. Supponiamo che S non sia vuoto (perché nel caso lo fosse, allora sarebbe uguale al numero naturale 0, inteso naturalmente come insieme, e quindi equipotente a esso). Allora l'insieme S si può ben ordinare. Possiamo, quindi denotare con x^+ il successivo immediato di x in S secondo il suo buon ordinamento, se x non è l'ultimo elemento di S. Consideriamo, dunque, l'applicazione g da S in S data da:

$$g(x) = \begin{cases} x^+, & \text{se } x \text{ non è l'ultimo elemento di } S \\ x, & \text{se } x \text{ è l'ultimo elemento di } S \end{cases}$$

Supponiamo per assurdo che S non sia equipotente ad alcun numero naturale (e che quindi non esista nessuna funzione biunivoca tra S e alcun numero naturale). Per il teorema della ricorrenza finita esiste un'unica applicazione f da da $\mathbb{N}$ in S, tale che:

$$f(0) = e \quad \text{ e } \quad f(m^+) = g(f(m))$$

dove e è il primo elemento di S e m^+ è il successivo immediato del numero naturale m.

Per quanto stiamo supponendo S non è equipotente ad alcun numero naturale, quindi, dati due numeri naturali m ed n, si vede che $m \neq n$ implica $f(m) \neq f(n)$. Abbiamo, dunque, che f è un'applicazione iniettiva da $\mathbb{N}$ in S, quindi S deve avere un sottoinsieme numerabile e, per il teorema 2.1.1 S è perciò infinito, ma questo è in contraddizione con l'ipotesi che S sia finito per cui, se S è finito, allora deve essere equipotente a un numero naturale (sempre inteso come insieme).

Ora vediamo l'implicazione da destra a sinistra, ovvero, dimostriamo che se S è equipotente a un numero naturale, allora è necessariamente finito. Per dimostrare ciò, poiché il teorema 2.1.1 ci implica che un insieme equipotente a un insieme finito è esso stesso finito, basta dimostrare che ogni numero naturale è un insieme finito.
Tale dimosrazione la si fa per induzione.
Il numero naturale 0, essendo uguale all'insieme vuoto $\emptyset$, è finito.
Supponiamo, ora, che il numero naturale n sia finito, dobbiamo dimostrare che $n^+ = n \cup \{n\}$ è finito. Per assurdo, sia $n \cup \{n\}$ infinito, allora, per il lemma 2.1.1, $(n \cup \{n\}) \smallsetminus \{n\} = n$ è infinito, risultato che contraddice l'ipotesi che n sia finito. Per cui abbiamo un assurdo e, conseguentemente, $n \cup \{n\}$ deve essere finito.
Abbiamo quindi che ogni numero naturale è finito e perciò se un insieme è equipotente a un numero naturale allora tale insieme è finito. $\square$

Tale teorema giustifica la seguente definizione che ci tornerà utile in seguito:

Definizione 2.5. Per ogni numero naturale n, si dice che un insieme ha n elementi se e solo se è equipotente al numero naturale n.

Ora vediamo la generalizzazione del lemma 2.1.1 (di cui non daremo la dimostrazione), contenente anche un'osservazione sull'equipotenza:

Lemma 2.1.2.
Se S è un insieme infinito e A è un insieme finito, allora $S \smallsetminus A$ è un insieme infinito. Inoltre,

$$(S \smallsetminus A) \cong S \quad e \quad (S \cup A) \cong S$$

Adesso abbiamo un teorema di caratterizzazione degli insiemi di numeri naturali:

Teorema 2.1.3.
Un insieme di numeri naturali è infinito se e solo se non ha massimo (tale insieme si dice che è illimitato).

Dimostrazione. Dimostriamo per prima cosa l'implicazione da sinistra a destra e supponiamo per assurdo che S sia un insieme limitato, ovvero supponiamo che esista un numero naturale n tale che sia maggiore di ogni elemento di S. Conseguentemente, considerando n come un insieme, abbiamo che ogni elemento di S è un elemento di n e, quindi, $S \subset n$. Sappiamo, però, per il teorema 2.1.2, che n è un insieme finito, ma ogni sottoinsieme di un insieme finito è esso stesso finito (come diretta conseguenza del teorema 2.1.1) per cui abbiamo un assurdo. S è perciò illimitato.
Dimostriamo ora l'implicazione da destra a sinistra. Consideriamo la funzione g da S in S tale che:

$$f(n) = f(k) \quad \text{con} \quad n \neq k \tag{2.3}$$

Con m che è il più piccolo numero naturale appartenente a S e tale che $n < m$. Poiché S è illimitato allora la (2.3) esiste. Per il teorema di ricorrenza finita, esiste una funzione f da $\mathbb{N}$ in S, tale che:

$$f(0) = e \qquad \text{con } e \text{ primo elemento di } S \qquad f(m^+) = g(f(m))$$

Si vede chiaramente che f è iniettiva, dato che, secondo la (2.3), $f(n) < f(n^+)$. Per cui, corestringendo la f alla sua immagine abbiamo che tale applicazione stabilisce un'equipotenza tra $\mathbb{N}$ e un sottoinsieme di S. S contiene quindi un sottoinsieme numerabile e quindi è infinito. □

Da questo teorema segue l'ultimo della sezione del quale non diamo la dimostrazione.

Teorema 2.1.4.
Un insieme è infinito se e solo se per ogni numero naturale n contiene un sottoinsieme equipotente a n.

2.2 Teoremi sulla equipotenza di insiemi

In questa sezione analizzeremo solo alcuni dei teoremi più importanti sulla equipotenza di insiemi.

Lemma 2.2.1.
Sia $A \cong P$ e sia $B \cong S$. Se $A \cap B = \emptyset$ e $P \cap S = \emptyset$, allora:

$$(A \cup B) \cong (P \cup S)$$

Dimostrazione. Sia f un'equipotenza tra A e P e sia g un'equipotenza tra B e S. Allora, chiaramente, $f \cup g$ è un'equipotenza tra $A \cup B$ e $P \cup S$ (l'ipotesi che $A \cap B = \emptyset$ e $P \cap S = \emptyset$ mantiene l'iniettività di $f \cup g$). □

Lemma 2.2.2.
Sia $A \cong P$ e sia $B \cong S$, allora:

$$(A \times B) \cong (P \times S)$$

Dimostrazione. Sia, come al solito, f un'applicazione biunivoca tra A e P e sia g un'applicazione biunivoca tra B ed S. Allora esiste un'applicazione data da $h((a,\ b)) = (f(a),\ g(b))$, con $a \in A$ e $b \in B$.
Si vede chiaramente che tale applicazione è una biezione tra $(A \times B)$ e $(P \times S)$. $\square$

Teorema 2.2.1.
Se $A \cong P$ e $B \cong S$, allora $A^B \cong P^S$.

Dimostrazione. Consideriamo, come nei teoremi precedenti, che f sia un'applicazione biunivoca tra A e P e g sia un'applicazione biunivoca tra B ed S. Un elemento di A^B è una funzione da B in A. Si può quindi pensare come un insieme di coppie ordinate (b, a) con $b \in B$ e $a \in A$. Supponiamo che $\{(b, a) \mid ...\}$ rappresenti un elemento di A^B. Un'applicazione h da A^B a P^S data da:

$$h(\{(b,\ a) \mid ...\}) = \{(g(b),\ f(a)) \mid ...\}$$

è chiaramente un'applicazione biunivoca in quanto anche g ed f sono a loro volta applicazioni biunivoche.

Teorema 2.2.2.
Siano A, B e C insiemi qualunque. Allora

$$\left(A^B\right)^C \cong A^{B \times C}$$

Dimostrazione. Per prima cosa vediamo che un elemento di $\left(A^B\right)^C$ è un insieme di coppie ordinate del tipo $\{(c,\ \{(b,\ a) \mid ...\}) \mid ...\}$ con $a \in A$, $b \in B$ e $c \in C$. D'altra parte, però, un elemento di $A^{B \times C}$ è un insieme di coppie ordinate del tipo $\{((b,\ c),\ a) \mid ...\}$ sempre con $a \in A$, $b \in B$ e $c \in C$.
Esiste un'appicazione h da $\left(A^B\right)^C$ a $A^{B \times C}$ tale che:

$$h(\{(c,\ \{(b,\ a) \mid ...\}) \mid ...\}) = \{((b,\ c),\ a) \mid ...\}$$

Tale applicazione è biunivoca, per cui abbiamo che $\left(A^B\right)^C \cong A^{B \times C}$ $\square$

Ora abbiamo un teorema molto importante che avrà numerose applicazioni in seguito:

Teorema 2.2.3.
Sia A un insieme formato da due elementi distinti. Allora A^S è equipotente all'insieme di tutti i sottoinsiemi (ossia all'insieme delle parti o all'insieme potenza) di S, $\mathcal{P}(S)$.

Dimostrazione. Per il teorema 2.2.1, A^S è equipotente a $\{0,\ 1\}^S$, in quanto, per ipotesi $A \cong \{0,\ 1\}$. Sappiamo, però, che $\{0,\ 1\}^S$ è l'insieme di tutte le funzioni da S in $\{0,\ 1\}$. Per dimostrare il teorema, quindi, ci basta costruire una funzione biunivoca tra l'insieme delle parti $\mathcal{P}(S)$ di S e l'insieme di tutte le funzioni da S in $\{0,\ 1\}$.
Sia E un sottoinsieme di S. Associamo a E la seguente funzione da S in $\{0,\ 1\}$:

$$f(x) = \begin{cases} 1, & \text{per ogni } x \in E \\ 0, & \text{per ogni } x \in S \smallsetminus E \end{cases}$$

Per ogni sottoinsieme di S, abbiamo, quindi una funzione associata da S in $\{0,\ 1\}$. L'applicazione che ci associa, quindi, a ogni sottoinsieme di S (e dunque a ogni elemento di $\mathcal{P}(S)$) una funzione da S in $\{0,\ 1\}$ (e, pertanto un elemento di $\{0,\ 1\}^S$) è chiaramente un'applicazione biunivoca, perciò $A^S \cong \mathcal{P}(S)$.
Come sappiamo, considerando i numeri naturali come insiemi, $\{0,\ 1\} = 2$ allora:

$$2^S \cong \mathcal{P}(S) \tag{2.4}$$

□

Da tale teorema si deriva direttamente il successivo:

Teorema 2.2.4.
Siano A e B insiemi qualunque. Se $A \cong B$, allora $\mathcal{P}(A) \cong \mathcal{P}(B)$.

2.3 Esempi di equipotenze di insiemi numerabili

In questa sezione mostreremo alcuni esempi concreti di equipotenze di insiemi numerabili: tratteremo, quindi, insiemi particolarmente familiari quali i numeri naturali, i numeri interi e i numeri razionali.

Teorema 2.3.1.
Sia S un sottoinsieme di $\mathbb{N}$. Allora S è finito o numerabile.

Dimostrazione. Consideriamo solamente il caso in cui S non sia finito e dimostriamo che è necessariamente numerabile. Denotiamo con $\sigma(x)$ il successivo immediato di x in S e sia s il primo elemento di S. Per il teorema di ricorrenza finita, esiste una funzione f da $\mathbb{N}$ in S tale che:

$$f(0) = s \quad \text{e} \quad f(x^+) = \sigma(f(x))$$

Chiaramente tale funzione è un'equipotenza di $\mathbb{N}$ su S. Per cui abbiamo necessariamente che S è numerabile. □

Abbiamo, ora, un teorema particolarmente importante per la caratterizzazione dell'unione numerabile di insiemi numerabile:

Teorema 2.3.2.
L'insieme di tutti i numeri naturali è un'unione di un'infinità numerabile di insiemi numerabili a due a due disgiunti.

Dimostrazione. Consideriamo, per ogni numero naturale n, l'insieme $P_n = \{x \mid x = 2^n(2k+1) - 1,\ \text{per qualche } k \in \mathbb{N}\}$.
Tali insiemi sono del tipo :

$$P_0 = \{0,\ 2,\ 4,\ 6,\ 8,\ ...\}$$

$$P_1 = \{1,\ 5,\ 9,\ 13,\ 17,\ ...\}$$

$$P_2 = \{3,\ 11,\ 19,\ 27,\ 35,\ ...\}$$

$$...$$

Possiamo, dunque, vedere che $\mathbb{N} = P_0 \cup P_1 \cup P_2 \cup ...$, con $P_i \cap P_j = \emptyset$ se $i \neq j$. □

Corollario 2.3.1.
Ogni insieme numerabile è un'unione di una infinità numerabile di insiemi numerabili a due a due disgiunti.

Il teorema seguente sarebbe un'immediata conseguenza del teorema 2.3.2, ma lo dimostriamo mostrando esplicitamente un'equipotenza.

Teorema 2.3.3.
Sia $\mathbb{N}$ l'insieme di tutti i numeri naturali, allora vale:

$$\mathbb{N} \times \mathbb{N} \cong \mathbb{N} \tag{2.5}$$

Dimostrazione. Costruiamo immediatamente l'applicazione f che stabilisce un'equipotenza tra $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$:

$$f(m,\ n) = \frac{1}{2}(m+n+1)(m+n)+n$$

La dimostrazione sarebbe conclusa con la costruzione di tale funzione, ma vogliamo mostrare una caratteristica di tale applicazione.
Si dice che f *conta* $\mathbb{N} \times \mathbb{N}$ *per diagonali* e ciò è giustificato dal diagramma seguente:
$(0,\ 0) \to 0,\quad (1,\ 0) \to 1,\quad (2,\ 0) \to 3,\quad (3,\ 0) \to 6,\ ...$
$(0,\ 1) \to 2,\quad (1,\ 1) \to 4,\quad (2,\ 1) \to 7,\quad ...$
$(0,\ 2) \to 5,\quad (1,\ 2) \to 8,\quad ...$
$(0,\ 3) \to 9,\quad ...$
...
Si vede, contando appunto per diagonali, che l'immagine di f è, quindi, tutto $\mathbb{N}$. □

Si hanno, quindi, questi corollari:

Corollario 2.3.2.
L'unione di un numero finito o numerabile di insiemi finiti o numerabili è un insieme finito o numerabile

Corollario 2.3.3.
Per ogni numero naturale positivo n, si ha:

$$(\mathbb{N})^n \cong \mathbb{N}$$

Con il corollario 2.3.3 che è una generalizzazione del teorema 2.3.3. Inoltre, tramite questi due corollari e grazie al teorema 2.2.1 si ha:

$$\mathbb{N} \cong \mathbb{N} \cup (\mathbb{N})^2 \cup (\mathbb{N})^3 \cup (\mathbb{N})^4 \cup \quad ...$$

Che giustifica (insieme ai due corollari immediatamente precedenti e al teorema 2.3.3) il seguente corollario:

Corollario 2.3.4.
L'insieme di tutte le successioni finite di un insieme numerabile è un insieme numerabile.

Dimostrazione. Un elemento di tutte le successioni finite di $\mathbb{N}$ su $\mathbb{N}$ è, per esempio:

$$(n_1,\ n_2,\ n_3,\ ...,\ n_k)$$

La funzione che associa a tale successione il numero naturale

$$2^{n_1} + 2^{n_1+n_2+1} + \ ... \ + 2^{n_1+n_2+ \ ... \ n_k+k-1}$$

è una funzione iniettiva su $\mathbb{N}$, ovvero è una funzione biunivoca tra l'insieme di tutte le successioni finite di un insieme numerabile e un sottoinsieme infinito i $\mathbb{N}$. Tale sottoinsieme essendo non finito, per il teorema 2.3.1 è, dunque, numerabile. □

Corollario 2.3.5.
L'insieme di tutti i sottoinsiemi finiti di un insieme numerabile è un insieme numerabile.

Iniziamo, ora, a vedere dei teoremi applicabili agli insiemi citati all'inizio della sezione.

Teorema 2.3.4.
L'insieme di tutti i numeri interi, $\mathbb{Z}$ è numerabile.

Dimostrazione. L'applicazione f così definita:

$$f(x) = \begin{cases} 2x, & \text{se } x \text{ è un intero non negativo} \\ -2x-1, & \text{se } x \text{ è un intero negativo} \end{cases}$$

è una funzione biunivoca da $\mathbb{Z}$ a $\mathbb{N}$ (considerando 0 come numero intero non negativo), per cui si ha $\mathbb{Z} \cong \mathbb{N}$. □

Teorema 2.3.5.
L'insieme di tutti i numeri razionali, $\mathbb{Q}$ è numerabile.

Dimostrazione. Possiamo supporre che ogni numero razionale si possa rappresentare come frazione irriducibile p/q, con p numero intero e q naturale positivo. Dimostreremo tale teorema mostrando che gli elementi di $\mathbb{Q}$ si possono disporre in una successione infinita come segue.

Disponiamo, in ordine di grandezza gli elementi di $\mathbb{Q}$ per i quali $|p| + q = 1$.

Facciamo seguire a ciò la disposizione in ordine di grandezza degli elementi di $\mathbb{Q}$ per i quali $|p| + q = 2$.

Disponiamo, poi, sempre in ordine di grandezza, gli elementi di $\mathbb{Q}$ per i quali $|p| + q = 3$ e così via...

In tal modo otteniamo la successione:

$$\frac{0}{1}; \quad -\frac{1}{1}, \frac{1}{1}; \quad -\frac{2}{1}, -\frac{1}{2}, \frac{1}{2}, \frac{2}{1}; \quad -\frac{3}{1}, -\frac{1}{3}, \frac{1}{3}, \frac{3}{1}; \quad -\frac{4}{1}, -\frac{3}{2}, -\frac{2}{3}, -\frac{1}{4}, \ldots$$

Se consideriamo tutti gli elementi di tale successione come degli insiemi a sé stanti (e perciò sono insiemi finiti), ci riconduciamo alle ipotesi del corollario 2.3.2 in quanto la quantità di tali insiemi è numerabile per la costruzione degli insiemi stessi. □

Teorema 2.3.6.
L'insieme di tutti i numeri algebrici è numerabile.

Dimostrazione. Un numero si dice algebrico se è radice di un polinomio

$$a_n x^n + a_{n-1}x^{n-1} + \ \ldots \ + a_1 x + a_0 \qquad \text{con} \ \ n > 0 \quad \text{e} \ \ a_n \neq 0$$

dove a_i è un intero per $i = 0,\ 1,\ \ldots,\ n$.
A tale polinomio possiamo associare la successione $(a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0)$, dal corollario 2.3.4 e poiché ogni sottoinsieme di un insieme numerabile è finito o numerabile (come conseguenza del teorema 2.3.1) abbiamo che l'insieme di tali polinomi è numerabile e, perciò li possiamo disporre nella successione seguente:

$$P_1(x),\ P_2(x),\ P_3(x),\ \ldots$$

Un polinomio come quello precedente non può avere più di n radici distinte. Quindi, disponiamo, per prima cosa tutte le radici del polinomio $P_1(x)$ in ordine di grandezza crescente delle loro parti reali e, nel caso di uguaglianza delle loro parti reali, in ordine di grandezza delle loro parti immaginarie. Successivamente disponiamo in ordine simile tutte le radici del polinomio $P_2(x)$ e così via. Così facendo, l'insieme dei numeri algebrici si può disporre in una successione infinita e, con una giustificazione simile a quella della conclusione della dimostrazione del teorema 2.3.6, si arriva a provare la tesi. □

Teorema 2.3.7.
Ogni insieme infinito di intervalli che a due a due non si sovrappongono e che hanno più di un elemento è numerabile.

Dimostrazione. Ricordiamo che, dati due numeri reali a e b, gli insiemi

$$[a,\ b] = \{x \in \mathbb{R} \mid a \leq x \leq b\ \}$$

$$[a,\ b[= \{x \in \mathbb{R} \mid a \leq x < b\ \}$$

$$]a,\ b] = \{x \in \mathbb{R} \mid a < x \leq b\ \}$$
$$]a,\ b[= \{x \in \mathbb{R} \mid a < x < b\ \}$$

si dicono *intervalli*.
Si dice che due intervalli non si sovrappongono se non hanno nessun elemento in comune, eccetto, al più i loro estremi (quando esistono). Se un intervallo di numeri reali che contiene al più un numero reale, necessariamente contiene un numero razionale. Essendo che tali intervalli non si sovrappongono, allora, a ognuno di essi viene associato un unico numero razionale ed essendo che i numeri razionali sono un insieme numerabile, abbiamo anche che tale insieme di intervalli è numerabile. □

Concludiamo la sezione con questi due teoremi dei quali non diamo le dimostrazioni:

Teorema 2.3.8.
Sia S un insieme infinito e sia D un insieme numerabile. Allora:

$$S \cup D \cong S$$

Teorema 2.3.9.
Per ogni insieme numerabile D e ogni sottoinsieme finito e non vuoto E si ha:

$$(D \cup E) \cong (D \smallsetminus E) \cong (D \times E) \cong (E \times D) \cong D^E \cong D$$

dove, come al solito, D^E è l'insieme di tutte le funzioni da E in D.

2.4 Esempi di equipotenze di insiemi non numerabili

In questa sezione, al contrario di quella precedente, forniremo degli esempi di equipotenze di insiemi non numerabili oltre che a dare la definizione di *non numerabile* e di *potenza del continuo.*

Definizione 2.6 (Insieme non numerabile)**.** Un insieme si dice *non numerabile* se e solo se è infinito e non numerabile.

Poiché tale definizione è riservata solamente a un insieme infinito, dato un qualsiasi insieme S, si può presentare solamente una delle seguenti alternative:

S è finito,

S è numerabile,

S è non numerabile.

Un primo esempio di insieme non numerabile è l'insieme di tutti i numeri reali $\mathbb{R}$.

Lemma 2.4.1.
Data una qualunque successione infinita di numeri reali, esiste un numero reale diverso da ogni elemento di quella successione.

Dimostrazione. Ogni numero reale si può rappresentare in modo unico nella forma

$$e, a_1 a_2 a_3 \ ...$$

dove e è un intero e $a_1,\ a_2,\ a_3,\ ...$ è una successione infinita di cifre nella quale non c'è mai una successione infinita di nove (nel caso di un numero decimale finito si avrà una successione infinita di zeri).
Sia ora

$$\begin{gathered} e_1, a_1 a_2 a_3 \ ... \\ e_2, b_1 b_2 b_3 \ ... \\ ... \\ e_n, h_1 h_2 h_3 \ ... \\ ... \end{gathered} \tag{2.6}$$

una successione infinita di nueri reali. Si consideri il numero reale

$$0, k_1 k_2 k_3 \ ... \ k_n \ ... \tag{2.7}$$

con:

$$k_1 = 0, \text{ se } a_1 \neq 0 \ \text{ e } \ k_1 = 1, \text{ se } a_1 = 0$$

$$k_2 = 0, \text{ se } b_2 \neq 0 \ \text{ e } \ k_2 = 1, \text{ se } b_2 = 0$$

$$...$$

$$k_n = 0, \text{ se } h_n \neq 0 \ \text{ e } \ k_n = 1, \text{ se } h_n = 0$$

Chiaramente (2.7) è un numero reale diverso da ogni elemento della successione (2.6). Infatti, confrontandolo con $e_1, a_1 a_2 a_3$ ... differisce nel primo posto decimale; confrontandolo con $e_2, b_1 b_2 b_3$ ... differisce nel secondo posto decimale e così via. □

Teorema 2.4.1.
L'insieme di tutti i numeri reali $\mathbb{R}$ è non numerabile.

Dimostrazione. Supponiamo per assurdo che $\mathbb{R}$ sia numerabile. Se fosse numerabile, allora tutti i suoi elementi si potrebbero disporre in una successione infinita come la (2.6). In base al lemma 2.4.1, nessuna successione infinita di numeri reali può contenere ogni numero reale, conseguentemente la nostra supposizione è falsa e quindi non è vero che $\mathbb{R}$ sia numerabile. Chiaramente, però, $\mathbb{R}$ è infinito, pertanto è non numerabile. □

Tale teorema giustifica la seguente definizione:

Definizione 2.7 (Potenza del continuo)**.** Si dice che un insieme ha la *potenza del continuo* se e solo se è equipotente all'insieme di tutti i numeri reali.

Abbiamo, quindi, un primo teorema sulla non numerabilità:

Teorema 2.4.2.
Un insieme non numerabile resta equipotente a se stesso se si aggiunge a esso o se si toglie da esso un insieme finito o numerabile.

Dimostrazione. In base al lemma 2.1.2 e al teorema 2.3.8, per dimostrare questo teorema ci basta far vedere che se H è un insieme non numerabile e D è un sottoinsieme numerabile di H, allora

$$H \setminus D \cong H$$

Poiché $S \cup D \cong S$ per ogni insieme infinito S e per ogni insieme numerabile D, abbiamo che:

$$H \cong (H \setminus D) \cup D$$

Ma, dato che $H \setminus D$ è infinito per il lemma 2.1.2 (perché se non lo fosse si avrebbe che H è necessariamente numerabile) otteniamo:

$$H \cong (H \setminus D) \cup D \cong H \setminus D$$

□

In base ai teoremi 2.4.1, 2.4.2, 2.3.5 e 2.3.6 abbiamo i seguenti lemmi:

Lemma 2.4.2.
Un insieme della potenza del continuo rimane equipotente a se stesso se gli si aggiunge o gli si toglie un insieme finito o numerabile.

Lemma 2.4.3.
L'insieme di tutti i numeri irrazionali $\mathbb{R} \setminus \mathbb{Q}$ ha la potenza del continuo.

Lemma 2.4.4.
L'insieme di tutti i numeri trascendenti (ovvero di tutti i numeri reali non algebrici) ha la potenza del continuo.

Lemma 2.4.5.
L'insieme di tutti i numeri reali positivi è equipotente all'insieme di tutti i numeri reali dell'intervallo aperto unitario $]0,\ 1[$.

Dimostrazione. Si vede immediatamente che la funzione

$$f(x) = \frac{x}{1+x}$$

stabilisce una corrispondenza biunivoca tra $\mathbb{R}^+$ e l'insieme di tutti i numeri reali x tali che $0 < x < 1$. □

Come immediata conseguenza del lemma 2.4.5 abbiamo il seguente lemma:

Lemma 2.4.6.
L'insieme di tutti i numeri reali dell'intervallo aperto $]-1,\ 1[$ *ha la potenza del continuo.*

Dimostrazione. Basta mettere in corrispondenza biunivoca l'intervallo aperto $]-1,\ 1[$ con l'insieme di tutti i numeri reali tramite la seguente applicazione:

$$f(x) = \begin{cases} \frac{x}{1+x}, & \text{se } x \text{ è un reale non negativo} \\ -\frac{|x|}{1+|x|}, & \text{se } x \text{ è un reale negativo} \end{cases}$$

Si vede banalmenteche tale funzione è biunivoca, da cui il risultato. □

Da questi due lemmi abbiamo il teorema seguente:

Teorema 2.4.3.
Siano a e b due numeri reali tali che $a < b$. Allora, l'insieme di tutti i numeri reali x tali che $a < x < b$ o $a \leq x < b$ o $a < x \leq b$ o $a \leq x \leq b$ ha la potenza del continuo.

Dimostrazione. L'applicazione

$$g(x) = \frac{b-a}{2}x + \frac{b+a}{2}$$

stabilisce una corrispondenza biunivoca tra l'intervallo aperto di numeri reali $]-1, 1[$ e l'intervallo aperto di numeri reali $]a, b[$.
Il lemma 2.4.6 ci garantisce, così, che l'insieme dei numeri reali $\mathbb{R}$ è equipotente (tramite la transitività dell'equipotenza) all'intervallo di numeri reali $]a, b[$. Gli altri casi si ottengono tramite l'applicazione del lemma 2.4.2, da cui il risultato. □

Con i seguenti lemmi dimostreremo, ora, che l'insieme potenza dei numeri naturali ha la potenza del continuo. Denotiamo, come al solito con $2^{\mathbb{N}}$ l'insieme di tutte le successioni (infinite) costituite solamente dai termini 0 e 1.

Lemma 2.4.7.
Sia E l'insieme di tutti gli elementi di $2^{\mathbb{N}}$ tali che abbiano un numero finito di elementi uguali a 1. Allora E è numerabile.

Dimostrazione. Ci basta dimostrare che E è equipotente all'insieme P di tutti i sottoinsiemi finiti di numeri naturali ($P \subset \mathcal{P}(\mathbb{N})$). La numerabilità ci è assicurata dal corollario 2.3.5 e come diretta conseguenza del teorema 2.3.1.
L'equipotenza cercata la si può facilmente ottenere associando alla successione infinita, per esempio:

$$1,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ ...$$

L'insieme finito di numeri naturali

$$\{0,\ 2,\ 5,\ 6,\ 8\}$$

i cui elementi indicano le posizioni occupate da 1 nella successione infinita.
$\square$

Lemma 2.4.8.
Sia C l'insieme di tutti gli elementi di $2^{\mathbb{N}}$ tali che abbiano un numero infinito di elementi uguali a 1. Allora C è equipotente a $2^{\mathbb{N}}$.

Dimostrazione. Abbiamo ovviamente che $C = 2^{\mathbb{N}} \setminus E$ con E insieme definito nel lemma 2.4.7. $2^{\mathbb{N}} \setminus E$ è chiaramente infinito in quanto, per esempio, contiene tutte le successioni di 0 e 1 ciascuna delle quali ha esattamente un termine uguale a 0.
Grazie al teorema 2.3.8, abbiamo che:

$$(2^{\mathbb{N}} \setminus E) \cong (2^{\mathbb{N}} \setminus E) \cup E \cong 2^{\mathbb{N}}$$

$\square$

Lemma 2.4.9.
L'insieme di tutti i numeri reali dell'intervallo $]0,\ 1]$ *è equipotente a* $2^{\mathbb{N}}$.

Dimostrazione. Ogni numero reale $x \in]0,\ 1]$ ha un'unica rappresentazione diadica decimale (in base 2) nella quale non può esistere una successione infinita di 0. Per esempio,

$$0,0110010101... \tag{2.8}$$

è una rappresentazione diadica di tal tipo. Associamo, quindi, alla (2.8) la successione (infinita):

$$0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1,\ ...$$

Questa è, chiaramente, un'equipotenza tra $]0,\ 1]$ e l'insieme C del lemma 2.4.8, per cui, per la transitività dell'equipotenza abbiamo il risultato cercato. □

Lemma 2.4.10.
Sia $\mathbb{R}$ l'insieme di tutti i numeri reali e sia $\mathbb{N}$ l'insieme di tutti i numeri naturali. Allora:

$$\mathbb{R} \cong 2^{\mathbb{N}}$$

Dimostrazione. Per il teorema 2.4.3 abbiamo che l'intervallo di numeri reali $]0,\ 1]$ è equipotente a $\mathbb{R}$, da cui il risultato. □

Con questi lemmi abbiamo direttamente la dimostrazione del seguente teorema:

Teorema 2.4.4.
L'insieme di tutti i numeri reali è equipotente all'insieme delle parti dell'insieme dei numeri naturali.

Per concludere la sezione abbiamo un teorema del quale non diamo la dimostrazione:

Teorema 2.4.5.
Per ogni insieme C che ha la potenza del continuo, per ogni insieme numerabile D e per ogni insieme finito E con più di un elemento, si ha:

$$(C \times E) \cong (C \times D) \cong C^E \cong 2^D \cong E^D \cong D^D \cong C^D \cong C$$

2.5 Altri teoremi di Cantor

In questa sezione tratteremo i teoremi di equipotenza di Cantor più importanti a partire dal *teorema di Cantor-Bernstein-Schroeder*.
Per dimostrare tale teorema partiamo da due lemmi (il secondo deriva direttamente dal primo) che mostriamo senza dimostrazione:

Lemma 2.5.1.
Sia f un'applicazione da un insieme A in un insieme B e sia g un'applicazione da B in A. Allora esiste un sottoinsieme C di A tale che

$$A \setminus g(B \setminus f(C)) = C$$

Lemma 2.5.2.
Sia f un'applicazione da un insieme A in un insieme B e sia g un'applicazione da B in A. Allora esiste un sottoinsieme C di A e un sottoinsieme M di B tali che:

$$f(C) = M$$
$$(A \setminus C) = g(B \setminus M)$$

Teorema 2.5.1 (Teorema di Cantor-Bernstein-Schroeder)**.**
Due insiemi ciascuno dei quali è equipotente a un sottoinsieme dell'altro sono equipotenti.

Dimostrazione. Tale teorema si può anche riformulare come "*Dati due insiemi A e B, se esistono due funzioni iniettive $f : A \longrightarrow B$ e $g : B \longrightarrow A$, allora $A \cong B$*". In base al lemma 2.5.2, esistono un sottoinsieme C di A e un sottoinsieme M di B tali che:

$$f(C) = M$$

$$(A \setminus C) = g(B \setminus M)$$

Dato che g è un'applicazione iniettiva (e suriettiva) da $(B \setminus M)$ su $(A \setminus C)$, allora, anche la sua inversa g^{-1} è un'applicazone biunivoca da $(A \setminus C)$ su $(B \setminus M)$. Perciò possiamo definire l'applicazione h da A in B data da:

$$\begin{aligned} h &= f \quad \text{su } C \\ h &= g^{-1} \text{ su } A \setminus C \end{aligned} \tag{2.9}$$

Tale applicazione è una biezione da A su B, per cui $A \cong B$ come si voleva. □

Come teoremi che sono conseguenze del teorema di Cantor-Bernstein-Schroeder (e come conseguenza del teorema 2.4.5), abbiamo:

Teorema 2.5.2.
L'insieme di tutte le funzione continue dall'insieme di tutti i numeri reali nell'insieme di tutti i numeri reali ha la potenza del continuo.

Teorema 2.5.3.
L'insieme di tutte le funzioni differenziabili dall'insieme di tutti i numeri reali nell'insieme di tutti i numeri reali ha la potenza del continuo.

Abbiamo, ora i teoremi, rispettivamente della diagonale e di Cantor.

Teorema 2.5.4 (Teorema diagonale).
Sia f un'applicazione da un insieme S a $\mathcal{P}(S)$. Allora il sottoinsieme P di S dato da:

$$P = \{x \mid (x \in S) \wedge (x \notin f(x))\}$$

non appartiene al rango di f.

Dimostrazione. In pratica dobbiamo far vedere che per nessun elemento $y \in S$ si ha $f(y) = P$. Supponiamo, per assurdo che $y \in S$ sia tale che $f(y) = P$. Necessariamente o $y \in P$ o $y \notin P$.
Se $y \in P$, per la nostra definizione di P, si ha $y \notin P$ e, poiché $f(y) = P$, si ha $y \notin P$, che è una contraddizione.
Supponiamo, ora, che $y \notin P$, allora, sempre in base alla nostra definizione di P, si ha $y \in f(y)$ e, essendo $f(y) = P$, si vede che $y \in P$, che è una contraddizione.
Abbiamo, quindi che la nostra supposizione è falsa, pertanto, per nessun $y \in S$ avviene che $f(y) = P$ (P non appartiene al rango di f). □

Teorema 2.5.5 (Teorema di Cantor).
Nessun insieme è equipotente al suo insieme delle parti.

Dimostrazione. Supponiamo per assurdo che f sia una biezione tra un insieme S e l'insieme delle parti $\mathcal{P}(S)$. Il sottoinsieme

$$\{x \mid (x \in S) \wedge (x \notin f(x))\}$$

di S è ovviamente un elemento di $\mathcal{P}(S)$ il quale, per il teorema diagonale, non può essere il corrispondente di alcun elemento di S. Questo contraddice il fatto che f è una corrispondenza biunivoca tra S e $\mathcal{P}(S)$. Da cui la validità del teorema. □

In particolare tramite questo ultimo teorema della sezione possiamo affermare l'esistenza di molti insiemi non numerabili quali, per esempio $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$, ... Inoltre, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ è un primo esempio di insieme infinito che non è né numerabile né ha la potenza del continuo.

2.6 Confrontabilità delle potenze di insiemi

Per prima cosa introduciamo la seguente definizione:

Definizione 2.8. Si dice che un insieme X ha potenza minore o uguale a quella di un insieme Y:

$$X \preceq Y$$

se e solo se X è equipotente a un sottoinsieme di Y. Inoltre, si dice che X ha potenza minore di Y:

$$X \prec Y$$

se e solo se X è equipotente a un sottoinsieme di Y e X non è equipotente a Y.

Per il teorema di Cantor-Bernstein-Schroeder abbiamo anche che, per tutti gli insiemi X e Y, se $X \preceq Y$ e $Y \preceq X$, allora $X \cong Y$.

Abbiamo, quindi, il teorema seguente del quale non daremo la dimostrazione:

Teorema 2.6.1.
Dati comunque due insiemi, uno è equipotente a un sottoinsieme dell'altro.

Dal teorema 2.6.1 e dal teorema di Cantor-Bernstein-Schroeder si ottiene:

Teorema 2.6.2 (Teorema del Confronto)**.**
Due insiemi sono equipotenti oppure uno e uno solo di essi è equipotente a un sottoinsieme dell'altro.

Dimostrazione. Supponiamo che A e B siano due insiemi non equipotenti, allora, per il teorema 2.6.1, almeno uno degli insiemi A e B è equipotente a un sottoinsieme dell'altro, ma, in base a quanto abbiamo supposto, uno solo degli insiemi A e B può essere equipotente a un sottoinsieme dell'altro, perché, altrimenti, in virtù del teorema di Cantor-Bernstein-Schroeder, sarebbero equipotenti. □

Abbiamo, perciò:

Corollario 2.6.1 (Legge di tricotomia)**.**
Per tutti gli insiemi X e Y uno e uno solo dei tre casi seguenti si può verificare:

$$X \prec Y \quad o \quad Y \prec X \quad o \quad X \cong Y$$

Ora abbiamo tre teoremi conclusivi del capitolo dei quali daremo solamente gli enunciati, ma non le dimostrazioni:

Teorema 2.6.3.
Se A e B sono insiemi infiniti equipotenti e disgiunti, allora

$$(A \cup B) \cong A$$

Teorema 2.6.4.
Se A è un insieme infinito, allora

$$A \times A \cong A$$

Teorema 2.6.5.
Per ogni insieme infinito E e ogni insieme B

$$B^E \cong 2^E \quad se \quad e \quad solo \quad se \quad 2 \preceq B \preceq 2^E.$$

2.7 Dimostrazioni alternative a quelle presentate nel capitolo

Vediamo di seguito tre dimostrazioni alternative che hanno il pregio di mostrare direttamente una equipotenza tra gli insiemi (utilizzando come ausilio per le dimostrazioni solamente il teorema di Cantor-Bernstein-Schroeder) a due teoremi del capitolo appena concluso.

Per prima cosa vediamo una dimostrazione alternativa al teorema 2.4.4:

Teorema 2.7.1.
L'insieme di tutti i numeri reali $\mathbb{R}$ è equipotente all'insieme delle parti dell'insieme dei numeri naturali, $\mathcal{P}(\mathbb{N})$.

Dimostrazione. Per provare l'equipotenza tra $\mathbb{R}$ e $\mathcal{P}(\mathbb{N})$, sfruttiamo il teorema di Cantor-Bernstein-Schroeder e costruiamo una applicazione iniettiva da $\mathbb{R}$ a $\mathcal{P}(\mathbb{N})$ e ne costruiamo un'altra da $\mathcal{P}(\mathbb{N})$ a $\mathbb{R}$.

Partiamo dalla costruzione della funzione iniettiva da $\mathbb{R}$ a $\mathcal{P}(\mathbb{N})$, ovvero mostriamo che qualsiasi numero reale può essere identificato da uno e un solo elemento di $\mathcal{P}(\mathbb{N})$ (ovvero da un sottoinsieme di $\mathbb{N}$).

- Numeri naturali ($0 \in \mathbb{N}$):
  basta associare il sottoinsieme di $\mathbb{N}$ contenente solamente l'elemento considerato.
  $$n \mapsto \{n\}$$

- Numeri interi negativi:
  basta prendere il sottoinsieme di $\mathbb{N}$ contenente il valore assoluto del numero intero e il numero successivo (per indicare il segno negativo).
  $$n \mapsto \{|n|\,,\ |n| + 1\}$$

- Numeri decimali finiti (positivi):
  Possiamo considerare i numeri decimali finiti positivi con la seguente rappresentazione in cifre in base 10:

$$x_1x_2...x_l, y_1y_2...y_m$$

  - con parte decimale più lunga della parte intera o lunga quanto la parte intera ($m \geq l$):
    basta prendere il sottoinsieme di $\mathbb{N}$ contenente la parte intera del numero considerato e, come secondo elemento del sottoinsieme, la parte decimale preceduta da un 1 (per indicare la virgola) e seguita da 001.

$$x_1x_2...x_l, y_1y_2...y_m \mapsto \{x_1x_2...x_l,\ 1y_1y_2...y_m001\}$$

  - con parte decimale più corta della parte intera ($m < l$):
    basta prendere il sottoinsieme di $\mathbb{N}$ contenente la parte intera del numero considerato e, come secondo elemento del sottoinsieme, la parte decimale preceduta da un 1 (per indicare la virgola) e seguita da $\underbrace{00...0}_{l-m \text{ zeri}}001$.

$$x_1x_2...x_l, y_1y_2...y_m \mapsto \left\{x_1x_2...x_l,\ 1y_1y_2...y_m\underbrace{00...0}_{l-m \text{ zeri}}001\right\}$$

- Numeri decimali finiti (negativi):
  Prendiamo come sottoinsieme di $\mathbb{N}$ quello del caso dei numeri decimali finiti positivi (dove per la parte intera ne prendiamo il valore assoluto) al quale aggiungiamo il numero successivo alla parte intera in valore assoluto (per indicare il segno -).

- Numeri decimali infiniti (positivi):
  Il procedimento per prendere il sottoinsieme di $\mathbb{N}$ è leggermente diverso da quelli esposti precedentemente, in quanto il sottoinsieme che andremo a scegliere sarà sicuramente infinito. Costruiamo, dunque, il sottoinsieme di $\mathbb{N}$ associato al nostro numero decimale infinito positivo:
  Come primo elemento, come di consueto, prendiamo la parte intera (che supponiamo essere composta da l cifre).
  Come secondo elemento prendiamo il numero composto dalle prime $l+1$ cifre della parte decimale (con l numero delle cifre della parte intera)

e preceduto da un 1 per identificare la virgola. Nel caso in cui le k cifre decimali direttamente successive alle prime $l+1$ cifre della parte decimale siano tutte uguali a 0 (con l'elemento della parte decimale di posizione $l+k+1$ non nullo), prendiamo, come secondo elemento del sottoinsieme di $\mathbb{N}$, il numero composto dalle prime $l+k$ preceduto da un 1 (sempre per identificare la virgola).
Come terzo elemento del sottoinsieme prendiamo il numero composto dalle $m+1$ cifre della parte decimale direttamente successive all'ultima cifra del secondo elemento del sottoinsieme, con m numero delle cifre di quest'ultimo (contando anche l'1 iniziale). Anche in questo caso, se le j cifre successive all'ultima sono tutte nulle (sempre con l'elemento della parte decimale di posizione $2m+j$ non nullo), invece del numero composto dalle $m+1$ cifre, consideriamo, come terzo elemento del sottoinsieme, il numero composto dalle $m+j$ cifre decimali direttamente successive a quelle considerate nel passo precedente.
Costruiamo gli elementi successivi del sottoinsieme di $\mathbb{N}$ in modo analogo, sempre tenendo conto dell'eventuale presenza di cifre decimali nulle.

Per esempio, prendiamo $1,0003200000034550567 12....$ A questo numero viene associato il sottoinsieme di $\mathbb{N}$ seguente:

$$\{1,\ 1000,\ 32000000,\ 345505671,\ 2...,\ ...\}$$

- Numeri decimali infiniti (negativi):
  Si ragiona come nel caso dei numeri decimali infiniti positivi, solo che, per identificare il segno negativo, aggiungiamo, al sottoinsieme di $\mathbb{N}$ il numero naturale successivo a quello in valore assoluto della parte intera (che viene presa in valore assoluto anch'essa nel sottoinsieme di $\mathbb{N}$).

  Per esempio, prendiamo $-1,00032000000345505671 2....$ A questo numero viene associato il sottoinsieme di $\mathbb{N}$ seguente:

$$\{1,\ 2,\ 1000,\ 32000000,\ 345505671,\ 2...,\ ...\}$$

Ora costruiamo una funzione iniettiva da $\mathcal{P}(\mathbb{N})$ a $\mathbb{R}$. Preso un qualsiasi elemento di $\mathcal{P}(\mathbb{N})$ lo associamo univocamente a un numero reale nel modo seguente:

1. Prendiamo il numero più piccolo del sottoinsieme di $\mathbb{N}$ considerato e questo formerà la parte intera del numero reale associato;

2. Come primo gruppo di cifre della parte decimale prendiamo il secondo numero più piccolo del sottoinsieme considerato, preceduto e seguito da un numero di zeri pari a quello delle sue cifre (basterebbe solo la condizione di "preceduto", ma preferiamo identificare tale numero chiaramente);

3. Poi prendiamo, come secondo gruppo di cifre della parte decimale, il numero immediatamente successivo in ordine crescente del sottoinsieme considerato, preceduto e seguito da un numero di zeri pari a quello delle sue cifre;

4. Ripetiamo il procedimento fino all'ultimo elemento (se c'è, altrimenti il numero così identificato sarà decimale illimitato);

5. Finiti gli elementi del sottoinsieme (nel caso sia finito) poniamo come ultima cifra decimale un 1.

6. Al sottoinsieme $\emptyset$ associamo π.

Per esempio, al sottoinsieme $\{1,\ 2,\ 1000,\ 32000000,\ 345505671\}$ associamo il numero reale:

$$1,0200000100000000000000000320000000000000000000000003455056710000000001$$

Abbiamo quindi, due funzioni iniettive, una da $\mathbb{R}$ a $\mathcal{P}(\mathbb{N})$ e l'altra da $\mathcal{P}(\mathbb{N})$ a $\mathbb{R}$, quindi, per il teorema di Cantor-Bernstein-Schroeder, abbiamo che $\mathbb{R} \cong \mathcal{P}(\mathbb{N})$. $\square$

Ora vediamo due dimostrazioni alternative al lemma 2.4.5 (generalizzato a tutti i numeri reali):

Lemma 2.7.1.
L'insieme di tutti i numeri reali $\mathbb{R}$ *è equipotente all'insieme di tutti i numeri reali dell'intervallo chiuso* $[0,1]$.

Dimostrazione. Come nella dimostrazione del teorema precedente, sfruttiamo il teorema di Cantor-Bernstein-Schroeder e costruiamo una applicazione iniettiva da $\mathbb{R}$ a $[0,1]$ e ne costruiamo un'altra da $[0,1]$ a $\mathbb{R}$.

Partiamo dalla costruzione della funzione iniettiva da $\mathbb{R}$ a $[0,1]$.
Dato un qualsiasi numero reale, costruiamo l'elemento associato di $[0,1]$ nel modo seguente:

1. Come parte intera prendiamo lo 0;

2. Come prima cifra decimale prendiamo 1 se il numero reale è positivo e 2 se il numero reale è negativo;

3. Come seconda cifra decimale prendiamo 1 se il numero reale ha parte intera nulla e 2 altrimenti;

4. Il gruppo successivo di cifre decimali è dato dalle cifre della parte intera (in valore assoluto) del numero reale considerato, preceduto e seguito da un numero di zeri pari al numero di cifre della parte intera;

5. Come ultimo gruppo di cifre decimali, si prende semplicemente la parte decimale del numero reale considerato.

Per esempio, prendiamo $-1,23323455056712...$. A questo numero viene associato il numero:

$$0,2201023323455056712...$$

Mentre nel caso di $0,000345$ abbiamo associato il numero:

$$0,11000000345$$

.
Ora come funzione iniettiva da $[0,\ 1]$ a $\mathbb{R}$ prendiamo, semplicemente, l'inclusione.
Per il teorema di Cantor-Bernstein-Schroeder, abbiamo, quindi, che $\mathbb{R} \cong [0,1]$. □

Adesso vediamo la seconda dimostrazione alternativa allo stesso lemma:

Lemma 2.7.2.
L'insieme di tutti i numeri reali positivi è equipotente all'insieme di tutti i numeri reali dell'intervallo aperto $]0,1[$.

Dimostrazione. Possiamo subito far vedere l'equipotenza tra i due insiemi tramite l'applicazione seguente:

$$f(x) = \frac{1}{2}(\frac{2}{\pi}\arctan(x) + 1)$$

che è ovviamente una funzione da $\mathbb{R}$ a $]0,1[$ (biunivoca). □

Capitolo 3

Numeri Ordinali

Tratteremo il capitolo sui numeri ordinali come una sintetica introduzione a questi ultimi in quanto ci servono per poi definire i numeri cardinali e con essi il concetto di cardinalità. Detto ciò, i numeri ordinali sono la "naturale" generalizzazione dei numeri naturali ai fini di descrivere la posizione di un elemento all'interno di una sequenza. Vedi sempre [Abian 1972].

3.1 Introduzione ai numeri ordinali

Partiamo subito con la definizione di numero ordinale:

Definizione 3.1. Un insieme S si dice un (numero) ordinale se e solo se S si può ben ordinare in modo che per ogni elemento v di S, il segmento iniziale $I(v)$ di S sia uguale a v.

Per esempio l'insieme di tutti i numeri naturali (intesi come insiemi) w è un numero ordinale e così lo sono ciascuno degli insiemi seguenti:

$$w \cup \{w\} \quad \text{e} \quad w \cup \{w\} \cup \{w \cup \{w\}\}$$

Inoltre, un ordinale che sia un insieme finito si dice *ordinale finito*, mentre un ordinale che sia un insieme infinito si dice *ordinale infinito* o *ordinale transfinito.*

Introduciamo, ora la definizione di insieme transitivo (proprietà molto utile per i numeri ordinali):

Definizione 3.2 (Insieme transitivo)**.** Un insieme S si dice transitivo se ogni suo elemento x è anche un suo sottoinsieme.

Abbiamo, quindi, un primo teorema di caratterizzazione dei numeri ordinali:

Teorema 3.1.1.
Un insieme w è un numero ordinale se e solo se:

1. *Ogni elemento di w è un sottoinsieme di w (w è transitivo);*
2. *w è ben ordinato da $\subset$;*
3. *Nessun elemento di w è elemento di se stesso.*

Alternativamente, un insieme w è un numero ordinale se e solo se:

1. *Ogni elemento di un elemento di w è un elemento di w;*
2. *w è ben ordinato da ($\in$ o $\subset$);*
3. *Nessun elemento di w è elemento di se stesso.*

Come conseguenza immediata abbiamo che ogni numero ordinale è segmento iniziale di un qualche numero ordinale.
Introduciamo ora la nozione di insiemi simili, che ci servirà per apprezzare le caratteristiche degli ordinali e successivamente dei cardinali:

Definizione 3.3. (Insiemi Simili) Due insiemi bene ordinati X e Y si dicono simili ($X \simeq Y$) se esiste una applicazione biunivoca f da X a Y tale che conservi l'ordine (per ogni $a, b \in X$ con $a \leq b$, allora $f(a) \leq f(b)$).

Per cui abbiamo che:

Teorema 3.1.2.
Due numeri ordinali sono uguali se e solo se sono simili.

Come immediata conseguenza di tale teorema abbiamo la legge di tricotomia per i numeri ordinali:

Teorema 3.1.3.
Per tutti i numeri ordinali v e w, si presenta solamente uno dei seguenti casi:

1. *$v = w$;*
2. *$v \in w$;*
3. *$w \in v$.*

Come anticipato nell'introduzione al capitolo i numeri ordinali sono la generalizzazione dei numeri naturali, per cui abbiamo che i numeri naturali sono ordinali e, in particolare, per vedere quando avviene il viceversa abbiamo il seguente teorema:

Teorema 3.1.4.
Un numero ordinale è finito se e solo se è un numero naturale.

Definiamo, ora, l'ordinale successivo (immediato):

Definizione 3.4 (Successivo immediato)**.** Per ogni numero ordinale v si definisce il suo successivo immediato come il suo successivo insiemistico (che è ancora un ordinale):

$$S(v) := v \cup \{v\} = v^+$$

Per cui abbiamo, come conseguenza di tale definizione, la definizione di *antecedente immediato*: un ordinale u è antecedente immediato di un ordinale v se e solo se v è il successivo immediato di u. Conseguentemente, tutti i numeri ordinali hanno un successivo immediato, mentre non necessariamente tutti hanno un antecedente immediato, per esempio l'ordinale w (inteso come insieme di tutti i numeri naturali) ha successivo immediato, che è $w \cup \{w\}$, ma non ha antecedente immediato.

Questa caratteristica giustifica la seguente definizione:

Definizione 3.5 (Ordinale Limite)**.** Un numero ordinale non nullo si dice un ordinale limite se e solo se non ha alcun antecedente immediato.

Da cui abbiamo il teorema:

Teorema 3.1.5.
Per ogni numero ordinale w si ha:

1. $\cup w = w^-$ *se e solo se w non è un ordinale limite e* $w \neq 0$ *e*

2. $\cup w = \cup_{v<w} v = w$ *se e solo se w è un ordinale limite oppure w=0*

Quindi, dato un qualsiasi numero ordinale v si presenta uno e uno solo dei tre casi seguenti:

1. $v = \emptyset$;

2. v è il successivo di un qualche numero ordinale;

3. v è un ordinale limite.

Una interessante osservazione è quella che non esiste un insieme che contenga tutti gli ordinali, infatti, se per assurdo tale insieme esistesse, allora il suo successivo immediato sarebbe anch'esso un numero ordinale e quindi sarebbe contenuto nell'insieme di tutti gli ordinali, portando a una contraddizione.

Come ultimo teorema della sezione abbiamo:

Teorema 3.1.6.
Per Ogni insieme ben ordinato W esiste un unico numero ordinale simile a W.

Per il teorema del buon ordinamento si può generalizzare tale risultato a *per ogni insime S esiste un numero ordinale equipotente a S.*

3.2 Aritmetica Ordinale

In questa sezione vedremo, brevemente le operazioni elementari (e alcune loro proprietà) tra numeri ordinali, cominciando con l'addizione, poi passando alla moltiplicazione e per finire con l'elevamento a potenza.

3.2.1 Addizione di numeri ordinali

Introduciamo il concetto di addizione tra numeri ordinali tenendo bene in mente la connessione che vi è tra tali numeri e gli insiemi bene ordinati. Per cui, dati comunque due ordinali u e w costruiamo gli insiemi $u \times \{1\}$ e $v \times \{2\}$. Su tali insiemi definiamo, rispettivamente, i seguenti ordini:

1. Per tutti gli elementi a e b di u, $(a,\ 1) \leq (b,\ 1)$ se $a \leq b$ in u;

2. Per tutti gli elementi m e n di v, $(m,\ 2) \leq (n,\ 2)$ se $m \leq n$ in v;

3. Per tutti gli elementi a di u e per tutti gli elementi m di v vale che $(a,\ 1) \leq (m,\ 2)$.

Per cui abbiamo (con tali ordini) che $u \times \{1\}$ e $v \times \{2\}$ sono disgiunti e ben ordinati. E quindi l'unione di tali insiemi sarà simile a un ordinale somma degli ordinali u e v. Equivalentemente, usiamo la seguente definizione di addizione per ricorsione:

Definizione 3.6. Siano u e v due ordinali, allora:

$$u + v = \begin{cases} u & \text{se } v = 0 \\ S(u+p) & \text{se } v \text{ è un ordinale successore, } v = S(p) \\ \cup_{p<v}(u+p) & \text{se } v \text{ è un ordinale limite, } v = \cup_{p<v} p \end{cases}$$

Tale definizione è corretta per il teorema di ricorrenza transfinita.

Alcune proprietà dell'addizione tra numeri ordinali sono le seguenti (considerando u, v e p ordinali):

1. $u + 0 = 0 + u = u$;

2. $u + 1 = S(u)$;

3. $u + (v + p) = (u + v) + p$ (Proprietà associativa).

Nel caso di numeri ordinali finiti (e quindi nel caso di numeri naturali) vale anche la proprietà commutativa dell'addizione, ma nel caso generale questa non vale. Infatti, ogni numero ordinale v ha un successore diverso da v, mentre sommare a sinistra un numero ordinale infinito (per esempio $\mathbb{N}$) con un numero naturale (per esempio 1) ci ridà ovviamente il numero ordinale infinito ω.

3.2.2 Moltiplicazione di numeri ordinali

Come nel caso dell'addizione, presi comunque due ordinali u e v consideriamo l'insieme ottenuto dal prodotto cartesiano tra u e v, $u \times v$ e vi definiamo *l'ordine antilessicografico* nel modo seguente: Se $(a,\ b), (m,\ n) \in u \times v$ allora $(a,\ b) < (m,\ n)$ se e solo se $b < n$ oppure $b = n,\ a < m$. L'insieme $u \times v$ è, perciò ben ordinato e l'unico ordinale simile a esso è, dunque, il prodotto dei numeri ordinali u e v. Per cui abbiamo, per ricorrenza:

Definizione 3.7. Siano u e v due ordinali, allora:

$$u \cdot v = \begin{cases} 0 & \text{se } v = 0 \\ (u \cdot p) + u & \text{se } v \text{ è un ordinale successore, } v = S(p) \\ \cup_{p<v}(u \cdot p) & \text{se } v \text{ è un ordinale limite, } v = \cup_{p<v} p \end{cases}$$

Alcune proprietà della moltiplicazione di numeri ordinali sono le seguenti (considerando u, v e p ordinali):

1. $u \cdot 0 = 0 \cdot u = 0$;

2. $u \cdot 1 = 1 \cdot u = u$;

3. $u \cdot (v \cdot p) = (u \cdot v) \cdot p$ (Proprietà associativa);

4. $u \cdot (v + p) = (u \cdot v) + (u \cdot p)$ (Proprietà distributiva a sinistra).

Nel caso di numeri ordinali finiti (e quindi nel caso di numeri naturali) vale anche la proprietà commutativa della moltiplicazione, ma nel caso generale questa non vale. Infatti, per esempio:

$$\omega \cdot n \neq \omega$$

$$n \cdot \omega = \omega$$

sono chiaramente due risultati diversi, con n numero naturale e quindi ordinale, mentre ω è l'ordinale insieme di tutti i numeri naturali.

3.2.3 Elevamento a potenza di numeri ordinali

Come nell'aritmetica ordinaria, l'elevamento a potenza si definisce come una moltiplicazione ripetuta, per cui possiamo subito darne la definizione per ricorrenza:

Definizione 3.8. Siano u e v due ordinali, allora:

$$u^v = \begin{cases} 1 & \text{se } v = 0 \\ (u^p) \cdot u & \text{se } v \text{ è un ordinale successore, } v = S(p) \\ \cup_{p<v}(u^p) & \text{se } v \text{ è un ordinale limite, } v = \cup_{p<v} p \end{cases}$$

Alcune proprietà dell'elevamento a potenza di numeri ordinali sono le seguenti (considerando u, v e p ordinali):

1. $0^0 = 1,\ 0^u = 0 (1 \leq u)$;
2. $u^1 = u$;
3. $u^{v+p} = u^v \cdot u^p$;
4. $u^{v \cdot p} = (u^v)^p$.

Nel caso di ordinali finiti l'elevamento a potenza conserva tutte le sue proprietà nell'aritmetica ordinaria, come per le operazioni precedenti, però, questo non vale nel caso di ordinali infiniti. Per esempio:

$$n^\omega \cdot n^\omega = \omega \cdot \omega = \omega^2$$

$$(n \cdot n)^\omega = (n^2)^\omega = \omega$$

sono palesemente due risultati diversi, con n numero naturale e quindi ordinale, mentre ω è l'ordinale insieme di tutti i numeri naturali.

Capitolo 4

Numeri Cardinali

Avendo definito e dato alcune proprietà dei numeri ordinali nel precedente capitolo, ci apprestiamo a definire i numeri cardinali, che svolgono un ruolo di vitale importanza per poter confrontare la "grandezza" (o la quantità di elementi) di insiemi qualunque.

4.1 Introduzione ai numeri cardinali

Prima di introdurre la nozione di numero cardinale riprendiamo la definizione di Equipotenza del capitolo 2 e definiamo il concetto di cardinalità:

Definizione 4.1 (Cardinalità di un insieme)**.** Dato un qualsiasi insieme S si dice cardinalità di tale insieme (e si scrive $|S|$) il più piccolo ordinale s tale che $S \cong s$.

Questa nozione ci permette di meglio apprezzare i vari teoremi del capitolo 2 in quanto a ogni insieme viene associato il numero dei suoi elementi e quindi la ricerca di equipotenze tra i vari insiemi si riduce a verificare delle uguaglianze (o disuguaglianze) in aritmetica ordinale transfinita.
Quindi abbiamo il concetto di numero cardinale:

Definizione 4.2 (Numero Cardinale)**.** Sia u un numero ordinale, si dice che questo è un numero cardinale se e solo se $u = |u|$.

Per cui abbiamo, come nel caso degli ordinali, che tutti e soli i cardinali finiti sono i numeri naturali. Se un cardinale è un insieme finito, questo si dice *cardinale finito*, mentre se un cardinale è un insieme infinito si dice *cardinale infinito* o *cardinale transfinito*. Come conseguenza del teorema 2.1.1 il più piccolo cardinale infinito è ω, l'insieme di tutti i numeri naturali. Inoltre tale numero cardinale è l'unico numerabile e si indica anche con $\aleph_0$.

Come conseguenza diretta di tale definizione abbiamo i seguenti teoremi:

Teorema 4.1.1.
Due numeri cardinali sono uguali se e solo se sono equipotenti.

Teorema 4.1.2.
Ogni numero ordinale è equipotente a un unico numero cardinale.

Teorema 4.1.3.
Ogni insieme è equipotente a un unico numero cardinale.

Questo ultimo teorema ci garantisce che un qualsiasi insieme è dunque dotato di una cardinalità. Da ciò abbiamo che si indica solitamente con $\aleph$ l'unico cardinale equipotente all'insieme di tutti i numeri reali $\mathbb{R}$. Essendo perciò $\mathbb{R}$ non numerabile, chiaramente anche $\aleph$ è non numerabile e per la Definizione 2.7, $\aleph$ ha potenza del continuo.
Pertanto abbiamo (con abuso di notazione) che $2^{\aleph_0} = \aleph$ e, per il teorema di Cantor, abbiamo che $\aleph_0 \neq \aleph$.

Conseguentemente, abbiamo:

Teorema 4.1.4.
Nessun numero cardinale è equipotente a qualche suo segmento iniziale.

Questo ci implica che nessun numero cardinale è equipotente a qualcuno dei suoi elementi.
Definiamo ora l'ordinamento naturale tra cardinali:

Definizione 4.3. Per tutti i numeri cardinali a e b, diremo che a è minore o uguale a b (indicandolo come usuale con $a \leq b$) se e solo se a è uguale a un segmento iniziale di b oppure a è uguale a b.

Questo ordinamento definisce un buon ordinamento su ogni insieme di numeri cardinali. Come nel caso dei numeri ordinali abbiamo anche per i cardinali la legge di tricotomia:

Teorema 4.1.5.
Per tutti i numeri cardinali a e b, si presenta solamente uno e uno solo dei seguenti casi:

1. $a=b$;
2. $a \in b$;
3. $b \in a$.

Da cui, nessun numero cardinale è elemento di se stesso.

Definizione 4.4 (Cardinale successore)**.** Sia a un numero cardinale, allora il minimo cardinale strettamente maggiore di esso è il suo successore cardinale (indicato con a^+). Si dice che b è un numero cardinale successore se $b = a^+$ per qualche a (il successore di a esiste sempre per il teorema di Cantor sulla potenza).

Essendo i numeri cardinali dei numeri ordinali possiamo notare che, dato un numero cardinale a, il suo successore ordinale $S(a)$ non coincide necessariamente con il suo successore cardinale a^+. Tale concetto coincide per i numeri cardinali finiti (ovvero per i numeri naturali), mentre per i numeri cardinali transifiniti ciò non è più valido.

Definizione 4.5 (Cardinale limite)**.** Si dice che a è un cardinale limite se $a > \omega$ e a non è un numero cardinale successore.

Anche in questo caso, il concetto di cardinale limite non coincide con quello di ordinale limite infatti, per esempio, w è un ordinale limite mentre non è un cardinale limite.
Abbiamo, dunque, la seguente definizione:

Definizione 4.6. La successione dei numeri cardinali transfiniti è definita per ricorrenza transfinita utilizzando i numeri ordinali:

1. $\aleph_0 = \omega$
2. $\aleph_{a+1} = \aleph_a^+$ (con a numero ordinale)
3. $\aleph_a = \cup_{b<a}\aleph_b$ (se a è un ordinale limite)

Conseguentemente a tale definizione abbiamo i seguenti teoremi:

Teorema 4.1.6.
Siano u e v due numeri ordinali, allora $u < v$ implica $\aleph_u < \aleph_v$.

Teorema 4.1.7.
Per ogni insieme non vuoto A di ordinali, $\cup_{a\in A}(\aleph_a) = \aleph_b$, con $b = \cup_{a\in A}a$.

Teorema 4.1.8.
Per ogni numero cardinale infinito c, esiste un unico numero ordinale v tale che:

$$c = \aleph_v$$

Teorema 4.1.9.
$\aleph_a$ è un numero cardinale successore se e solo se a è un ordinale successore.
$\aleph_a$ è un numero cardinale limite se e solo se a è un ordinale limite.

4.2 Aritmetica Cardinale

Come nel capitolo sui numeri ordinali possiamo definire anche sui numeri cardinali le operazioni di addizione, moltiplicazione e di elevamento a potenza, queste però sono sostanzialmente diverse da quelle ordinali.

4.2.1 Addizione di numeri cardinali

Iniziamo subito con il definire l'addizione tra numeri cardinali:

Definizione 4.7. Siano a e b due numeri cardinali, allora:

$$a \oplus b = \begin{cases} |(a \times \{0\}) \cup (b \times \{1\})| & \text{se } a \text{ e } b \text{ sono numeri cardinali finiti} \\ max\,\{a,\ b\} & \text{se almeno uno tra } a \text{ e } b \text{ è un cardinale infinito} \end{cases}$$

La definizione dell'operazione di addizione deriva direttamente dal concetto di cardinalità, infatti dati due insiemi A e B tali che siano equipotenti, rispettivamente, ai numeri cardinali a e b (e che quindi abbiano una cardinalità di a e b) si definisce l'addizione dei cardinali a e b a partire dalla cardinalità dell'unione di due insiemi disgiunti equipotenti a A e B. Nel caso di cardinali transfiniti, l'addizione in tal caso ha senso come conseguenza dei teoremi sull'infinità del capitolo 2.

Alcune delle proprietà di cui gode l'addizione tra numeri cardinali sono le seguenti (considerando a, b e c numeri cardinali):

1. $a \oplus b = b \oplus a$ (Proprietà commutativa);
2. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ (Proprietò associativa).

Da queste due si vede come l'addizione nel caso dei numeri cardinali è diversa nel caso degli ordinali (in quanto per gli ordinali non vale la proprietà commutativa). Come nel caso degli ordinali, però, l'addizione di numeri cardinali coincide con l'addizione dei numeri naturali quando si lavora con cardinali finiti.

4.2.2 Moltiplicazione di numeri cardinali

Come nel caso dell'addizione, iniziamo subito con il definire la moltiplicazione tra numeri cardinali:

Definizione 4.8. Siano a e b due numeri cardinali, allora:

$$a \otimes b = \begin{cases} |a \times b| & \text{se } a \text{ e } b \text{ sono numeri cardinali finiti} \\ max\,\{a,\ b\} & \text{se almeno uno tra } a \text{ e } b \text{ è un cardinale infinito e } a, b \neq 0 \end{cases}$$

Come nel caso dell'addizione, la definizione dell'operazione di moltiplicazione deriva direttamente dal concetto di cardinalità, infatti dati due insiemi A e B tali che siano equipotenti, rispettivamente, ai numeri cardinali a e b (e che quindi abbiano una cardinalità di a e b) si definisce la moltiplicazione dei cardinali a e b a partire dalla cardinalità del prodotto cartesiano degli insiemi A e B, $A \times B$. Nel caso di cardinali transfiniti, la moltiplicazione in tal caso ha quel risultato come conseguenza del teorema 2.6.4.

Alcune delle proprietà di cui gode la moltiplicazione tra numeri cardinali sono le seguenti (considerando a, b e c numeri cardinali):

1. $a \otimes b = b \otimes a$ (Proprietà commutativa);
2. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ (Proprietà associativa);
3. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ (Proprietà distributiva rispetto all'addizione).

Come nel caso dell'addizione, anche la moltiplicazione, se effettuata tra numeri cardinali finiti, coincide con la moltiplicazione definita tra numeri naturali.

4.2.3 Elevamento a potenza di numeri cardinali

Definiamo l'elevamento a potenza dei numeri cardinali con l'ausilio di insiemi di funzioni:

Definizione 4.9. Siano a e b due numeri cardinali e siano due insiemi A e B di cardinalità, rispettivamente, a e b. Allora abbiamo:

$$a^b = |A|^{|B|}$$

Di seguito abbiamo alcune delle proprietà di cui gode l'elevamento a potenza di numeri cardinali (considerando a, b e c numeri cardinali):

1. $0^a = 0$ (se $a \neq 0$);
2. $1^a = 1$;
3. $a^0 = 1$;
4. $a^1 = a$;
5. $a^{b \oplus c} = a^b \otimes a^c$;
6. $(a \otimes b)^c = a^c \otimes b^c$;

7. $a^{b \otimes c} = (a^b)^c$.

Anche in questo caso, l'operazine di elevamento a potenza di numeri cardinali finiti coincide con l'elevamento a potenza ordinario. Nel caso di cardinali infiniti, invece, tale operazione è significativamente differente dall'elevamento a potenza di numeri ordinali, infatti, per esempio (considerando ω l'insieme di tutti i numeri naturali):

$$2^\omega = \cup_{a \in \omega} 2^a = \aleph_0 \qquad \text{nel caso ordinale (in quanto } \omega \text{ è ordinale limite)}$$

$$2^\omega = |2|^{|\omega|} = 2^{\aleph_0} = \aleph = |\mathbb{R}| \quad \text{nel caso cardinale.}$$

4.3 Ipotesi del Continuo

In questa ultima sezione introdurremo due ipotesi che tentano di dare una classificazione dei cardinali transfiniti e, conseguentemente, della natura degli insiemi di cardinalità infinita.

Le osservazioni sui teoremi 2.5.5 e 4.1.3 e la definizione 4.6 hanno portato Cantor, nel 1878, a porsi la seguente domanda: Poiché abbiamo necessariamente una successione di cardinali transfiniti data da $\aleph_0$, $\aleph_1$, $\aleph_2$, ... , essendo che $\aleph_0 = |\mathbb{N}|$ e avendo posto $\aleph = |\mathbb{R}| = |2|^{|\mathbb{N}|} = 2^{|\mathbb{N}|} = 2^{\aleph_0}$ è lecito dedurre che $\aleph_1 = 2^{\aleph_0}$? Cantor per rispondere a tale domanda propose la sua ipotesi del continuo:

Ipotesi del continuo: $\aleph_1 = 2^{\aleph_0} = \aleph$

Ovvero che nessun insieme contenuto in $\mathbb{R}$ può avere una cardinalità infinita intermedia tra $\aleph_0$ e $\aleph$ (che è uguale ad $\aleph_1$ secondo l'ipotesi del continuo).

Naturalmente, questa domanda poteva essere estesa al caso delle cardinalità degli insiemi di potenza maggiore a quella del continuo e ai cardinali $\aleph$ con indice superiore a 1. Da cui abbiamo (sempre avanzata da Cantor) l'ipotesi generalizzata del continuo:

Ipotesi generalizzata del continuo: $\aleph_{a+1} = 2^{\aleph_a}$ per ogni a ordinale

Questa ipotesi ci dice che tutti gli insiemi con cardinalità infinita maggiore di $\aleph_0$ sono equipotenti a un qualche insieme potenza.

La vera domanda adesso è: questa ipotesi è effettivamente provabile? Nel

tentare di rispondere a questa domanda Kurt Gödel nel 1940, dimostrò l'impossibilità di dimostrare falsa l'ipotesi del continuo usando il sistema di assiomi di Zermelo-Fraenkel e l'assioma della scelta. Nel 1963, Paul Cohen dimostrò, a partire da tali assiomi che l'ipotesi del continuo non può nemmeno essere dimostrata vera.
L'ipotesi del continuo è, dunque, una di quelle *proposizioni indecidibili* la cui esistenza è garantita dai teoremi di incompletezza dello stesso Gödel. Essendo quindi l'ipotesi del continuo una proposizione indecidibile, nulla, teoricamente, ci vieta di provare a costruire un modello che tenti di negare tale ipotesi. A tutt'oggi non è ancora stato presentato un modello esauriente che neghi l'ipotesi del continuo (in quanto quest'ultima è ancora oggetto di discussione e problema non totalmente risolto). Questo ci fa capire quanto ancora poco sappiamo della natura degli insiemi con cardinalità non numerabile e quanto ancora ci sia da scoprire nel ramo della teoria degli insiemi.

Bibliografia

[1] [Abian 1972] Abian, Alexander, *La teoria degli insiemi e l'aritmetica transfinita*, Milano, Feltrinelli, 1972.

[2] [Plazzi 2011] Plazzi, Piero, *Teorie degli insiemi - Numeri ordinali e cardinali*, elaborato dattiloscritto, 2011.

[3] [Nagel Newman 1992] Nagel, Ernest e Newman, James R., *La prova di Gödel*, Torino, Bollati Boringhieri, 1992.

[4] [Kunen 1980] Kunen, Kenneth, *Set theory: an introduction to independence proofs*, Amsterdam-New York-Oxford, North-Holland, 1980.