Note sugli insiemi

Alberto Zanardo

Febbraio 2003

1 Insiemi finiti e insiemi infiniti

Definizione 1.1 (1) *L'insieme X è* infinito *se esiste una funzione iniettiva da $\mathbb{N}$ in X.* (2) *L'insieme X è* D-infinito *(Dedekind-infinito) se esiste una funzione biiettiva da X su un suo sottoinsieme proprio.*

Teorema 1.2 *Ogni insieme X è infinito se e solo se è D-infinito.*

Dimostrazione. Sia f una iniezione da $\mathbb{N}$ in X e sia φ una qualsiasi funzione iniettiva da $\mathbb{N}$ in un suo sottoinsieme proprio, per esempio $\varphi(n) = 2n$. Allora la funzione g, da X in X, definita da

$$\begin{cases} g(x) = x & \text{se } x \notin f[\mathbb{N}] \\ g(x) = f(\varphi(f^{-1}(x))) & \text{se } x \in f[\mathbb{N}] \end{cases}$$

è una biiezione tra X e un suo sottoinsieme proprio $Y = (X - f[\mathbb{N}]) \cup f[\varphi[\mathbb{N}]]$. Sia f una biiezione da X in un suo sottoinsieme proprio. Scelto un $x_0 \in X - f[X]$, definiamo la successione $x_0, x_1, \ldots, x_n, \ldots$ tramite: $x_{n+1} = f(x_n)$. Questa successione è una funzione iniettiva da $\mathbb{N}$ in X: se per qualche $n < m$, $x_n = x_m$, allora, poiché f è iniettiva, $x_{n-1} = x_{m-1},\ x_{n-2} = x_{m-2}, \ldots, x_0 = x_{m-n}$, ma per ipotesi x_0 non appartiene all'immagine di f, mentre x_{m-n} vi appartiene. ∎

In una versione formalizzata della teoria degli insiemi, il numero 0 viene identificato con l'insieme vuoto ed il successore del naturale n viene definito come $n \cup \{n\}$. I primi naturali sono quindi gli insiemi

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

Risulta in particolare che ogni naturale è l'insieme dei suoi predecessori: $n = \{0, \ldots, n-1\}$.

In questo contesto, possiamo considerare un'ulteriore nozione di finitezza e dire che X è N-finito se esiste una biiezione da X su un naturale. Un insieme è N-infinito se non è N-finito. Con l'Assioma della Scelta (v. §7) si dimostra che le nozioni di D-infinito e N-infinito coincidono. Senza l'Assioma della Scelta si può dimostrare solo che ogni insieme D-infinito è anche N-infinito.

2 Confronto tra insiemi

Definizione 2.1 *L'insieme X ha* cardinalità *minore o uguale dell'insieme Y (in simboli, $|X| \leq |Y|$) se esiste una funzione iniettiva da X in Y. Gli insiemi X e Y hanno cardinalità uguale ($|X| = |Y|$) se esiste una funzione biiettiva da X su Y. X ha* cardinalità *minore dell'insieme Y ($|X| < |Y|$) se $|X| \leq |Y|$ e $|X| \neq |Y|$. Se $|X| = |Y|$, si dice che X e Y sono* equipotenti.

La relazione $\leq$ appena definita è transitiva: se $f : X \to Y$ e $g : Y \to Z$ sono funzioni iniettive allora la funzione composta $h = g \circ f$ definita da $h(x) = g(f(x))$ è una funzione iniettiva da X in Z. Meno semplice è dimostrare che è antisimmetrica nel senso che da $|X| \leq |Y|$ e $|Y| \leq |X|$ segue $|X| = |Y|$. Il seguente lemma ed il successivo teorema dimostrano appunto questo.

Lemma 2.2 *Se $X_1 \subseteq Y_0 \subseteq X_0$ e $|X_1| = |X_0|$, allora $|Y_0| = |X_0|$.*

Dimostrazione. Sia φ una funzione biiettiva da X_0 su X_1. Dobbiamo definire una funzione biiettiva ψ da X_0 su Y_0. Cominciamo facendo coincidere ψ con φ sugli elementi di $X_0 - Y_0$ e ponendo $\psi(x) = x$ per $x \in Y_0 - X_1$. A questo punto bisogna definire ψ su X_1. Posto $X_2 = \varphi[X_1]$ e $Y_1 = \varphi[Y_0]$, osserviamo che $X_1 \supseteq Y_1 \supseteq X_2$ e che φ è una biiezione da X_1 su X_2, e quindi possiamo procedere come sopra. La definizione completa di ψ si ottiene iterando il procedimento. Formalmente, costruiamo due successioni di insiemi

$$\begin{array}{cccccc} X_0 & X_1 = \varphi[X_0] & X_2 = \varphi[X_1] & X_3 = \varphi[X_2] & \dots \\ Y_0 & Y_1 = \varphi[Y_0] & Y_2 = \varphi[Y_1] & Y_3 = \varphi[Y_2] & \dots \end{array}$$

Osserviamo che $X_0 \supseteq Y_0 \supseteq X_1 \supseteq Y_1 \supseteq \dots$. Definiamo la funzione ψ tramite

$$\psi(x) = \begin{cases} \varphi(x) & \text{se, per qualche } n,\ x \in X_n - Y_n \\ x & \text{altrimenti} \end{cases}$$

La funzione ψ è una biiezione da X_0 su Y_0.

(a) $\psi[X_0] \subseteq Y_0$. Infatti, $\varphi[X_0] \subseteq X_1 \subseteq Y_0$ e, se $x \notin X_n - Y_n$ per ogni $n \in \mathbb{N}$, allora in particolare $x \in Y_0$.

(b) ψ è iniettiva. Dati $x \neq x' \in X_0$, se $\psi(x)$ e $\psi(x')$ sono entrambi determinati in base alla prima clausola della definizione di ψ, o entrmbi determinati in base alla seconda clausola, allora $\psi(x) \neq \psi(x')$. Supponiamo $x \in X_k - Y_k$ e $x' \notin X_n - Y_n$ per ogni $n \in \mathbb{N}$. Dalla definizione delle successioni X_n e Y_n (e dal fatto che φ è iniettiva) abbiamo $\psi(x) \in X_{k+1} - Y_{k+1}$ e quindi $\psi(x) \neq x' = \psi(x')$.

(c) ψ è suriettiva. Dato $y \in Y_0$, se $y \notin X_n - Y_n$ per ogni $n \in \mathbb{N}$, allora $y = \psi(y)$. Se $y \in X_k - Y_k$, allora $k > 0$ e $\varphi^{-1}(y) \in X_{k-1} - Y_{k-1}$; quindi $y = \psi(\varphi^{-1}(y))$. ∎

Teorema 2.3 *(Schröder-Bernstein). Se* $|X| \leq |Y|$ *e* $|Y| \leq |X|$, *allora* $|X| = |Y|$.

Dimostrazione. Siano f e g rispettivamente una funzione iniettiva da X in Y e una funzione iniettiva da Y in X. La funzione composta $\varphi = g \circ f$ è una biiezione da X su un suo sottoinsieme X_1 $(= g[f[X]])$. Posto $Y_0 = g[Y]$, abbiamo $X_1 \subseteq Y_0 \subseteq X$ perché $f[X] \subseteq Y$. Poiché $|Y| = |Y_0|$, basta ora dimostrare che esiste una biiezione da X su Y_0 e per questo possiamo usare il lemma precedente. ∎

Osservazione. Per quanto è stato visto finora, non ha senso scrivere $|X|$, se non in espressioni come $|X| \leq |Y|$ o analoghe. Si potrebbe dare un senso a questa scrittura intendendo con $|X|$ la classe di tutti gli insiemi che possono essere posti in corrispondenza biunivoca con X, ma maneggiare classi è spesso complicato. Si preferisce quindi indicare con $|X|$ un particolare rappresentante di tale classe, che sarà un insieme cardinale. Sarà possibile fare questo dopo aver introdotto gli insiemi ordinali e cardinali, e dopo aver mostrato, con l'Assioma della Scelta, che ogni insieme può essere posto in corrispondenza biunivoca con un cardinale. Da ciò seguirà tra l'altro che, dati comunque due insiemi X e Y, si ha $|X| \leq |Y|$ oppure $|Y| \leq |X|$.

3 Insiemi numerabili

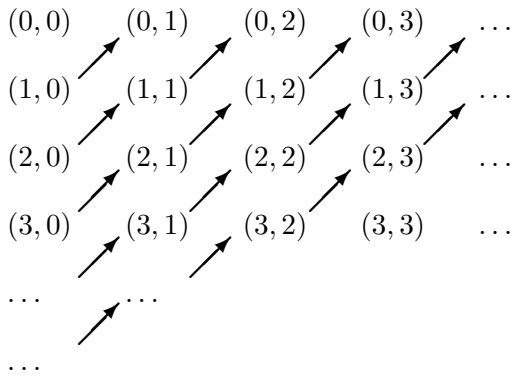
Definizione 3.1 *L'insieme* X *è numerabile se* $|X| = |\mathbb{N}|$.

I seguenti risultati mostrano che facendo unioni e prodotti cartesiani finiti di insiemi numerabili otteniamo ancora insiemi numerabili.

Proposizione 3.2 *Se l'insieme X è numerabile, allora, per ogni naturale $k > 0$, il prodotto cartesiano X^k è numerabile.*

Dimostrazione. Possiamo dimostrare solo che $\mathbb{N}^k$ è numerabile perché se f è una biiezione da $\mathbb{N}$ su X, allora $f_k : \langle n_1, \ldots, n_k\rangle \to \langle f(n_1), \ldots, f(n_k)\rangle$ è una biiezione da $\mathbb{N}^k$ su X^k. Inoltre, poiché $\mathbb{N}^k = \mathbb{N}^{k-1} \times \mathbb{N}$, basta mostrare che $\mathbb{N}^2$ è numerabile. Una funzione biiettiva da $\mathbb{N}^2$ su $\mathbb{N}$ è, per esempio, quella rappresentata nella seguente figura, dove coppie successive sono quelle collegate da una freccia e la coppia che segue $(0, n)$ è $(n + 1, 0)$.

Figura 1



La coppia $(m, 0)$ è preceduta da $1+2+\cdots+m$ coppie in questa enumerazione e quindi corrisponderà al naturale $\frac{m(m+1)}{2}$. In generale abbiamo che la coppia (m, n) corrisponde al naturale $\frac{(m+n)(n+m+1)}{2} + n$. ∎

L'insieme $\mathbb{Z}$ dei numeri interi può essere immerso in $\mathbb{N}^2$: all'intero i possiamo associare la coppia $(i, 0)$ se $i \geq 0$, o $(0, -i)$ se $i < 0$. Tale corrispondenza è iniettiva e quindi $|\mathbb{Z}| \leq |\mathbb{N}^2| = |\mathbb{N}|$. Abbiamo inoltre banalmente $|\mathbb{N}| \leq |\mathbb{Z}|$ e quindi, per il Teorema 2.3, anche l'insieme $\mathbb{Z}$ è numerabile. Per l'insieme $\mathbb{Q}$ si può fare un discorso analogo, osservando che ad ogni razionale possiamo associare una coppia di interi, e quindi anche $\mathbb{Q}$ è numerabile.

In generale, se Y è un sottoinsieme infinito dell'insieme numerabile X, allora anche Y è numerabile. Infatti, dalla caratterizzazione degli insiemi infiniti vista al §1 abbiamo $|\mathbb{N}| \leq |Y|$ e, poiché la funzione identica da Y in X è iniettiva, abbiamo anche $|Y| \leq |X| = |\mathbb{N}|$.

Non andiamo oltre il numerabile anche se consideriamo tutte le possibili successioni finite con elementi in un insieme numerabile.

Proposizione 3.3 *Se l'insieme X è numerabile, allora $\bigcup_{k\in\mathbb{N}} X^k$ è numerabile.*

Dimostrazione. Poiché ogni X^k è numerabile, ne possiamo considerare una enumerazione $x_{k,0}, x_{k,1}, \ldots, x_{k,n}, \ldots$ e quindi l'insieme $\bigcup_{k\in\mathbb{N}} X^k$ può essere indicizzato su $\mathbb{N}^2$. ∎

Da questa proposizione segue in generale che

Proposizione 3.4 *Se $\{X_i : i \in I\}$ è una famiglia di insiemi finiti o numerabili indicizzati sull'insieme finito o numerabile I, allora $\bigcup_{i\in I} X_i$ è finito o numerabile.*

Corollario 3.5 *L'insieme delle equazioni a coefficienti in $\mathbb{Z}$ e l'insieme dei reali algebrici è numerabile*[1]*.*

Dimostrazione. L'insieme delle equazioni di grado k a coefficienti in $\mathbb{Z}$ è numerabile essendo in corrispondenza biunivoca con un sottoinsieme infinito di $\mathbb{Z}^{k+1}$: l'insieme delle $(k+1)$-uple $\langle a_k, a_{k-1}, \ldots, a_0\rangle$ con $a_k \neq 0$. Da ciò segue che l'insieme di tutte le equazioni a coefficienti in $\mathbb{Z}$ è numerabile. Ogni equazione a coefficienti in $\mathbb{Z}$ ha un numero finito di soluzioni reali e quindi l'insiemi dei reali algebrici è unione numerabile di insiemi finiti. Ovviamente, l'insieme dei reali algebrici non è finito e quindi è numerabile. ∎

Un modo per enumerare effettivamente i reali algebrici è il seguente. All'equazione algebrica $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ (con $a_n \neq 0$), facciamo corrispondere la sua 'altezza' $h = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0| + n$. Per ogni valore di h, l'insieme delle equazioni algebriche di altezza h è finito ed ognuna di queste ha un numero finito di soluzioni reali. Possiamo quindi enumerare i reali algebrici, enumerando prima le soluzioni reali di tutte le equazioni di altezza 2, poi quelle delle equazioni di altezza 3 e così via. In questo modo, nella enumerazione ogni reale algebrico compare infinite volte; per evitare questo, possiamo convenire di non considerare, ad ogni passo, i numeri reali che sono stati considerati precedentemente.

[1] Un numero reale è *algebrico* se è soluzione di un'equazione a coefficienti in $\mathbb{Z}$. I reali non algebrici sono i reali *trascendenti*.

4 Insiemi più che numerabili. I numeri reali

Un insieme X è *più che numerabile* se $|X| > |\mathbb{N}|$. Per il seguente teorema, un primo esempio di insieme più che numerabile è $\mathcal{P}\mathbb{N}$, l'insieme dei sottoinsiemi di $\mathbb{N}$.

Teorema 4.1 *(Cantor) Per ogni insieme X, $|X| < |\mathcal{P}X|$.*

Dimostrazione. Ovviamente la funzione $f : x \to \{x\}$ è un'iniezione da X in $\mathcal{P}X$. Supponiamo per assurdo che esista una biiezione g da X su $\mathcal{P}X$. Indichiamo con C il sottoinsieme di X costituito da tutti e soli gli elementi x tali che $x \notin g(x)$; cioè: $C = \{x \in X : x \notin g(x)\}$. Sia $x_0 = g^{-1}(C)$; possiamo considerare questo elemento di X perché abbiamo supposto che g sia biiettiva. Dalla definizione di C abbiamo che $x_0 \in C \Leftrightarrow x_0 \notin g(x_0)$, ma $g(x_0) = C$. ∎

Questa dimostrazione è un primo esempio, forse il più famoso, del *metodo diagonale* di Cantor. L'idea di base è molto vicina a quella del *Paradosso di Russell* e infatti la clausola $x \notin g(x)$ nella definizione dell'insieme C ricorda la clausola $x \notin x$ in quel paradosso. In questo caso però non arriviamo all'assurdo, ma semplicemente alla negazione dell'esistenza di una funzione biiettiva da X su $\mathcal{P}X$. In generale, parliamo di metodo diagonale quando: 1) gli elementi di due insiemi X e Y possono essere messi in relazione tra loro (nel teorema di Cantor la relazione è l'appartenenza che vale oppure non vale tra elementi di X e di $\mathcal{P}X$), 2) l'insieme Y può essere indicizzato sull'insieme X: $Y = \{y_x : x \in X\}$ (nel teorema di Cantor, abbiamo supposto $\mathcal{P}X = \{g(x) : x \in X\}$), e 3) costruiamo situazioni critiche studiando l'insieme delle coppie del tipo (x, y_x) (nel teorema di Cantor, l'insieme critico C viene definito come $\{x : x \notin g(x)\}$).

In base al teorema di Cantor, è chiaro che possiamo considerare una gerarchia di insiemi più che numerabili: $\mathcal{P}\mathbb{N}$, $\mathcal{P}(\mathcal{P}\mathbb{N}), \ldots$.

I seguenti risultati mostrano che, se aggiungiamo o togliamo un insieme numerabile ad un insieme equipotente a $\mathcal{P}\mathbb{N}$, otteniamo ancora insiemi equipotenti a $\mathcal{P}\mathbb{N}$. Lo stesso succede se facciamo il prodotto cartesiano. In altri termini, il senso di questi risultati è che gli insiemi numerabili sono trascurabili rispetto ad insiemi equipotenti a $\mathcal{P}\mathbb{N}$. Per le dimostrazioni, usiamo il fatto che, poiché esiste una biiezione tra $\mathbb{N}$ e $\mathbb{Z}$, abbiamo anche $|\mathcal{P}\mathbb{N}| = |\mathcal{P}\mathbb{Z}|$.

Proposizione 4.2 *Siano X e Y insiemi tali che $|X| = |\mathcal{P}\mathbb{N}|$ e $|Y| = |\mathbb{N}|$. Allora:* (1) $|X \cup Y| = |\mathcal{P}\mathbb{N}|$, (2) $|X - Y| = |\mathcal{P}\mathbb{N}|$, (3) $|X \times Y| = |\mathcal{P}\mathbb{N}|$.

Dimostrazione. (1) $|\mathcal{P}\mathbb{N}| \leq |\mathcal{P}\mathbb{N} \cup \mathbb{N}| = |\mathcal{P}\mathbb{N} \cup \{\,\{-1\}, \{-2\}, \dots\}| \leq |\mathcal{P}\mathbb{Z}| = |\mathcal{P}\mathbb{N}|$.

(2) $|\mathcal{P}\mathbb{N}| = |\mathcal{P}\mathbb{Z}| \geq |\mathcal{P}\mathbb{Z} - \{\,\{-1\}, \{-2\}, \dots\}| \geq |\mathcal{P}\mathbb{N}|$.

(3) Osserviamo che f, da $\mathbb{N} \times \mathcal{P}\mathbb{N}$ in $\mathcal{P}\mathbb{Z}$, definita da $f(n, M) = \{-n\} \cup M$ è iniettiva. Quindi $|\mathcal{P}\mathbb{N}| \leq |\mathbb{N} \times \mathcal{P}\mathbb{N}| \leq |\mathcal{P}\mathbb{Z}| = |\mathcal{P}\mathbb{N}|$. ∎

Le successioni infinite i cui unici elementi sono 0 o 1 sono funzioni da $\mathbb{N}$ in $\{0, 1\}$ e il loro insieme, $S_{\{0,1\}}$, è equipotente a $\mathcal{P}\mathbb{N}$. Infatti, ad ogni successione $f : \mathbb{N} \to \{0, 1\}$ facciamo corrispondere l'insieme $M_f = \{n \in \mathbb{N} : f(n) = 1\}$; si verifica subito che la corrispondenza $f \to M_f$ è una biiezione.

Ad ogni successione $a_1, a_2, \dots$ ad elementi in $\{0, 1\}$ possiamo anche far corrispondere il numero reale r, appartenente all'intervallo $[0, 1]$, che in notazione binaria viene identificato da quella successione:

$$r \;=\; 0.a_1a_2\dots \;=\; \sum_{k=1}^{\infty} a_k \left(\frac{1}{2}\right)^k$$

Questa corrispondenza non è iniettiva perchè, per esempio, il numero $\frac{1}{2}$ corrispone sia alla successione $1, 0, 0, 0, 0, \dots$, sia alla successione $0, 1, 1, 1, 1 \dots$, e analogamente per ogni numero razionale interno a $[0, 1]$ che in notazione binaria non è periodico. Possiamo ovviare a questa situazione considerando, anziché $S_{\{0,1\}}$, l'insieme $S^* = S_{\{0,1\}} - S_c$, dove S_c è l'insieme di tutte le successioni che valgono costantemente 1 da un certo punto in poi. La corrispondenza vista sopra è una biiezione tra S^* e l'intervallo $[0, 1)$ sui reali. Abbiamo inoltre $|S^*| = |\mathcal{P}\mathbb{N}|$ perché l'insieme S_c è numerabile, e quindi $|\,[0, 1)| = |\mathcal{P}\mathbb{N}|$. L'insieme $\mathbb{R}$ dei reali è in corrispondenza biunivoca con $\mathbb{Z} \times [0, 1)$ (basta decomporre ogni reale in parte intera e parte decimale); possiamo dunque concludere $|\mathbb{R}| = |\mathcal{P}\mathbb{N}|$.

Un altro modo per vedere che l'insieme $\mathbb{R}$ non è numerabile è quello di supporre per assurdo che esista una enumerazione dell'intervallo reale $[0, 1]$:

$$\begin{aligned} r_0 &= 0.a_{00}\, a_{01}\, a_{02}\, a_{03}\, \dots \\ r_1 &= 0.a_{10}\, a_{11}\, a_{12}\, a_{13}\, \dots \\ r_2 &= 0.a_{20}\, a_{21}\, a_{22}\, a_{23}\, \dots \\ &\dots \end{aligned}$$

dove a destra abbiamo le notazioni binarie dei numeri r_i. Definiamo il numero reale r_D come $0.a'_{00}\, a'_{11}\, a'_{22}\, a'_{33}\, \dots$ con $a'_{ii} = 1$ se $a_{ii} = 0$ e $a'_{ii} = 0$ se $a_{ii} = 1$. Ovviamente r_D è diverso da ogni r_i almeno all'i-esima cifra e quindi non compare nella enumerazione, contro l'ipotesi che l'intervallo

$[0,1]$ sia numerabile. Ovviamente, in questo caso possiamo solo concludere che l'intervallo $[0,1]$ non è numerabile, ma non abbiamo dimostrato che $|\,[0,1]| = |\mathcal{P}\mathbb{N}|$

Vale la pena di osservare che la precendente dimostrazione, basata sulla definizione del numero reale $0.a'_{00}\,a'_{11}\,a'_{22}\,a'_{33}\,\ldots$ non è altro che un'ulteriore applicazione del metodo diagonale. Possiamo anzi osservare che questa costruzione non è altro che la ridimostrazione del teorema di Cantor per $X = \mathbb{N}$. Se infatti identifichiamo il reale r_i con il sottoinsieme di $\mathbb{N}$ costituito da tutti i naturali n tali che $a_{in} = 1$, abbiamo che il numero reale r_C corrisponde all'insieme C visto nella dimostrazione del teorema di Cantor.

Teorema 4.3 *Esistono numeri reali trascendenti, ed il loro insieme è equipotente $\mathcal{P}\mathbb{N}$.*

Dimostrazione. Per il Corollario 3.5, l'insieme A dei reali algebrici è numerabile. Detto T l'insieme dei reali trascendenti, abbiamo quindi $|T| = |\mathbb{R} - A| = |\mathcal{P}\mathbb{N}|$. ∎

Osservazione. Una dimostrazione dell'esistenza di numeri trascendenti precedente a quella di Cantor era stata data da Liouville che aveva mostrato che il numero reale $\sum_{k=1}^{\infty} 10^{-k!}$ e infiniti altri numeri con simili caratteristiche non potevano essere algebrici. Tra le due dimostrazioni ci sono profonde differenze. Pregi indiscutibili di quella di Cantor sono la semplicità e l'aver mostrato che l'insieme dei reali trascendenti è 'più grande' di quello dei reali algebrici. La dimostrazione di Cantor però non esibisce nessun numero trascendente, come invece fa Liouville. Oltre a questo, la dimostrazione di Liouville mette in luce importanti proprietà dei reali algebrici.

5 L'Ipotesi del Continuo

In base ad alcuni risultati visti sopra, e a tanti altri, sembra che l'unico modo per costruire insiemi più che numerabili sia quello di passare più o meno esplicitamente attraverso $\mathcal{P}\mathbb{N}$. Considerazioni di questo tipo portano a formulare l'*Ipotesi del Continuo*:

IC *Non esiste nessun insieme X tale che $|\mathbb{N}| < |X| < |\mathcal{P}\mathbb{N}|$.*

Oltre all'Ipotesi del Continuo, viene anche considerata l'*Ipotesi Generalizzata del Continuo*:

IGC *Per ogni insieme Y, non esiste nessun insieme X tale che $|Y| < |X| < |\mathcal{P}Y|$.*

In base ad IC, tenendo presente che $|\mathbb{R}| = |\mathcal{P}\mathbb{N}|$, abbiamo che, dato un qualsiasi sottoinsieme X di $\mathbb{R}$, vale una delle seguenti tre possibilità: X è finito, oppure è equipotente a $\mathbb{N}$, oppure è equipotente a $\mathbb{R}$.

Bisogna osservare che IC diventa equivalente a: *per ogni insieme* X, $|X| \leq |\mathbb{N}|$ *oppure* $|\mathcal{P}\mathbb{N}| \leq |X|$ solo dopo aver dimostrato che ogni insieme è confrontabile, nel senso della cardinalità, con $\mathbb{N}$ e con $\mathcal{P}\mathbb{N}$. Ma per dimostrare questo è necessario l'Assioma della Scelta.

6 Ordinali e cardinali

Un insieme X è *transitivo* se, per ogni insieme Y, $Y \in X \Rightarrow Y \subseteq X$. Per esempio:

- $\emptyset$ è transitivo.
- Gli insiemi $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$ sono transitivi.
- Se X è transitivo, allora $X \cup \{X\}$ è transitivo.
- Se, per ogni i nell'insieme I, X_i è transitivo, allora $\bigcup_{i \in I} X_i$ è transitivo.

Una relazione $<$ su un insieme X è un *buon ordinamento* se: (1) $<$ è transitiva e irriflessiva (per ogni $x \in X$, $x \not< x$) e (2) ogni sottoinsieme non vuoto di X ha minimo per $<$. Per esempio, la relazione $<$ tra naturali è un buon ordinamento.

Un *ordinale* è un insieme transitivo e bene ordinato dalla relazione $\in$ di appartenenza. La relazione di appartenenza tra ordinali, che risulta essere una relazione di ordine stretto, viene spesso indicata con $<$ e la classe di tutti gli ordinali viene indicata con **On**.

Gli esempi di insiemi transitivi visti sopra valgono anche come esempi di ordinali. La verifica per i primi tre è immediata, mentre per il quarto è più laboriosa.

La combinazione della della transitività e del buon ordinamento è una proprietà molto forte che dà una struttura molto rigida agli ordinali. Mostriamo per esempio che $\emptyset$ ogni ordinale $\alpha \neq \emptyset$. Se α non è vuoto, infatti, per la proprietà del buon ordinamento possiamo considerare un elemento x_0 minimo in α per la relazione $<$ (cioè per $\in$); ma x_0 deve essere l'insieme vuoto perché altrimenti, se $y \in x_0$ allora, per la transitività di α, $y \in \alpha$, contro l'ipotesi che x_0 sia minimo in α. Analogamente, se $\alpha - \{\emptyset\}$ non è vuoto, allora deve avere un minimo che risulta essere $\{\emptyset\}$. Continuando in questo modo risulta che gli insiemi $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}, \ldots$ visti sopra sono

gli unici ordinali finiti e sono contenuti in ogni ordinale infinito. Valgono inoltre le seguenti ulteriori proprietà degli ordinali, la cui dimostrazione non è immediata.

- Se α e β sono ordinali distinti, allora $\alpha \in \beta$ oppure $\beta \in \alpha$, e quindi $\alpha \subseteq \beta$ oppure $\beta \subseteq \alpha$. In particolare $|\alpha| \leq |\beta|$ oppure $|\beta| \leq |\alpha|$.
- Se α e β sono ordinali, allora α è un segmento iniziale di β o vicerversa.
- Se l'insieme X appartiene ad un ordinale allora X è un ordinale e quindi ogni ordinale è l'insieme degli ordinali che lo precedono: $\alpha = \{\beta \in \mathbf{On} : \beta < \alpha\}$.

Il *successore* di un ordinale α è l'ordinale $\alpha \cup \{\alpha\}$ e viene indicato con $\alpha + 1$. Gli ordinali $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$ sono ordinali successori, rispettivamente: $\emptyset + 1$, $(\emptyset + 1) + 1$, $((\emptyset + 1) + 1) + 1$, ... Gli ordinali che non sono successori sono chiamati *ordinali limite*. Se α è un ordinale limite, allora $\alpha = \bigcup_{\beta<\alpha} \beta$. Il più piccolo ordinale limite, che è l'insieme di tutti gli ordinali finiti, viene indicato con ω (o ω_0) ed è la chiusura dell'insieme vuoto per l'operazione di successore.

L'ordinale ω viene a coincidere con l'insieme $\mathbb{N}$ dei naturali identificando gli ordinali finiti con i numeri naturali in base alla definizione

$$n \stackrel{\text{def}}{=} (\ldots(\emptyset + \overbrace{1) + \ldots) + 1}^{n \text{ addendi}}$$

I primi naturali vengono ad essere quindi

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

Si possono definire le operazioni di somma, prodotto e potenza tra ordinali. Su ω, ma non sugli altri ordinali infiniti, tali operazioni coincidono con le solite operazioni tra naturali. Si possono considerare ordinali diversi dai numeri naturali e da ω, applicando l'operazione di successore o altre operazioni tra ordinali partendo da ω stesso. In questo modo possiamo considerare $\omega + 1$, $\omega + 1 + 1$ $(= \omega + 2)$, $\omega + 1 + 1 + \ldots$ $(= \omega + \omega = \omega \cdot 2)$ e così via. È importante osservare che questi insiemi sono numerabili.

Un ordinale α è un *cardinale* se, per nessun ordinale $\beta < \alpha$, si ha $|\alpha| = |\beta|$. L'ordinale ω è un cardinale e come tale viene indicato con $\aleph_0$. Poiché anche la classe **On** risulta bene ordinata dalla relazione $<$, ad ogni ordinale α possiamo associare un cardinale α^*: si tratta del minimo dell'insieme $\{\beta \in \mathbf{On} : |\alpha| = |\beta|\}$. Ovviamente $\alpha^* \leq \alpha$.

7 L'Assioma della Scelta

L'Assioma della Scelta asserisce che:

AS *Dato un insieme $\{X_i : i \in I\}$ di insiemi non vuoti indicizzati sull'insieme I, esiste una funzione (di scelta) C da I in $\bigcup_{i\in I} X_i$ tale che, per ogni $i \in I$, $C(i) \in X_i$.*

L'uso, spesso inconsapevole, dell'Assioma di Scelta è molto frequente in matematica; basti pensare che AS può anche essere formulato dicendo che *il prodotto cartesiano di insiemi non vuoti è non vuoto*; gli elementi del prodotto cartesiano $\prod_{i\in I} X_i$ sono infatti le funzioni f definite su I tali che, per ogni i, $f(i) \in X_i$.

I più famosi principi equivalenti ad AS sono:

- Lemma di Zorn: *Se $\langle P, \prec\rangle$ è un insieme parzialmente ordinato tale che ogni catena ha maggiorante, allora $\langle P, \prec\rangle$ ha un elemento massimale.*
- Principio del Buon Ordinamento (PBO): *Per ogni insieme X esiste un ordinale α tale che $|X| = |\alpha|$.*

In base al principio del buon ordinamento abbiamo che, dati due insiemi X e Y, $|X| \leq |Y|$ oppure $|Y| \leq |X|$; ciò è vero infatti se X e Y sono ordinali, ma, per PBO, ogni insieme può essere posto in corrispondenza biunivoca con un ordinale.

Dato l'insieme X, possiamo considerare l'insieme degli ordinali α tali che $|X| = |\alpha|$; per l'Assioma della Scelta questo insieme non è vuoto e quindi ha minimo α^* che è un cardinale. Diciamo che α^* è la *cardinalità* di X e scriviamo $|X| = \alpha^*$. Abbiamo quindi che ora l'espressione $|X|$ ha senso per ogni insieme X anche al di fuori di espressioni del tipo $|X| \leq |Y|$. Il confronto tra cardinalità, visto finora in termini di esistenza di funzioni iniettive, può ora essere visto come confronto di cardinali. Per l'Assioma della Scelta, le due nozioni coincidono.

Abbiamo visto che $\aleph_0$ è il cardinale degli insiemi numerabili. Il cardinale di $\mathcal{P}\mathbb{N}$ viene indicato con $2^{\aleph_0}$. $2^{\aleph_0}$ è la cardinalità dell'insieme delle funzioni da $\aleph_0$ in 2 ($= \{0, 1\}$) e tali funzioni possono essere viste come sottoinsiemi di $\aleph_0$. Poiché $|\mathcal{P}\mathbb{N}| = |\mathbb{R}|$, il cardinale $2^{\aleph_0}$ viene anche detto la *cardinalità del continuo* e viene indicato con $\mathbf{c}$.

Indichiamo con $\aleph_1$ il più piccolo cardinale maggiore di $\aleph_0$. Per il teorema di Cantor (Teorema 4.1), abbiamo $\aleph_1 \leq 2^{\aleph_0}$. L'Ipotesi del Continuo può ora essere riformulata come:

IC $\aleph_1 = 2^{\aleph_0}$

Il teorma di Cantor ci permette di considerare cardinali sempre più grandi: se α è un cardinale, il cardinale di $\mathcal{P}\alpha$ sarà maggiore di α. L'esistenza di $\aleph_1$ segue da questo fatto e analogamente possiamo considerare il più piccolo cardinale, $\aleph_2$, più grande di $\aleph_1$; poi possiamo considerare $\aleph_3$ e così via. Si dimostra che $\bigcup_{n\in\omega} \aleph_n$ è un cardinale, che indichiamo con $\aleph_\omega$. A questo punto si può andare avanti in modo analogo e considerare $\aleph_{\omega+1}, \aleph_{\omega+2}, \ldots$ In generale, abbiamo che, dato un ordinale α, possiamo condiderare "l'α-esimo" cardinale che indichiamo con $\aleph_\alpha$.

Il cardinale $\aleph_{\alpha+1}$ è il più piccolo cardinale maggiore di $\aleph_\alpha$ e, sempre per il teorma di Cantor, abbiamo $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$. Anche l'Ipotesi Generalizzata del Continuo può dunque essere riformulata in termini di ordinali e cardinali:

IGC Per ogni ordinale α, $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$

8 Non-contraddittorietà e indipendenza

Data una teoria degli insiemi, per esempio la teoria ZF di Zermelo-Fränkel, le prime questioni poste dall'introduzione di nuovi principi, come l'Assioma della Scelta o l'Ipotesi del Continuo, sono questioni di *non-contraddittorietà* e di *indipendenza*. Da un lato cioè vogliamo essere sicuri che aggiungendo i nuovi assiomi non otteniamo una teoria contraddittoria (che equivale a dire che le negazioni dei nuovi assiomi non sono deducibili dalla teoria di partenza) e, dall'altro lato, è importante sapere se i nuovi assiomi siano indipendenti, cioè se non siano già deducibili nella teoria di partenza (che equivale a dire che questa teoria non diventa contraddittoria aggiungendo la negazione dei nuovi assiomi). La soluzione al problema della non-contraddittorietà è stata data da Kurt Gödel negli anni '30 con il seguente risultato

> *Se la teoria* ZF *è non-contraddittoria, allora le teorie* ZF+AS *e* ZF + AS + IGC *sono non-contraddittorie*

Il problema dell'indipendenza è stato risolto da Paul Cohen negli anni '60, che con il metodo del *forcing*, da lui inventato, ha dimostrato i seguenti risultati:

> *Se la teoria* ZF *è non-contraddittoria, allora* AS *non è dimostrabile in* ZF

> *Se la teoria* ZF *è non-contraddittoria, allora* IC *non è dimostrabile in* ZF+AS

Osservazione. Gli enunciati dei teoremi di Gödel e di Cohen hanno la forma "*Se la teoria* ZF *è non-contraddittoria, allora ... ...* "; la validità dei risultati di non-contraddittorietà e di indipendenza è cioè subordinata al fatto che la teoria degli insiemi di partenza sia non-contraddittoria. Questo è un punto molto delicato e difficile. Non solo non è stata data nessuna dimostrazione della non-contraddittorietà della teoria degli insiemi, ma, per il *Teorema di Incompletezza di Gödel*, tale dimostrazione non è possibile se usiamo, come fa gran parte della matematica moderna, solo i mezzi forniti dalla teoria degli insiemi. La non-contraddittorietà della teoria degli insiemi viene di fatto accettata.

Osservazione. L'indipendenza di IC da ZF+AS equivale a dire che la teoria ottenuta da ZF+AS aggiungendo come assioma la negazione dell'Ipotesi del Continuo, cioè $2^{\aleph_0} \neq \aleph_1$, è non contraddittoria. Ci sono tanti modi tuttavia per negare l'Ipotesi del Continuo: $2^{\aleph_0} = \aleph_2$, $2^{\aleph_0} = \aleph_3$, ..., e ci si può chiedere se ognuna di queste uguaglianze sia non-contraddittoria con ZF+AS. La dimostrazione del teorma di Cohen risponde anche a questa domanda e risulta che c'è una vastissima possibilità di scelta per quanto riguarda il valore di $2^{\aleph_0}$. Per quanto riguarda i primi cardinali, abbiamo che, per ogni naturale $n > 1$, la teoria ZF+AS+ $2^{\aleph_0} = \aleph_n$ è non-contraddittoria, mentre ZF+AS+ $2^{\aleph_0} = \aleph_\omega$ è contraddittoria.

Osservazione. Ricordiamo che $2^{\aleph_0}$ è la cardinalità di $\mathbb{R}$. Dai teoremi di Gödel e dall'osservazione precedente segue che ci sono infiniti modi di attribuire una cardinalità all'insieme dei reali senza ottenere una teoria contraddittoria e che l'unico modo per assegnare una cardinalità a $\mathbb{R}$ è quello di fissarla esplicitamente con un opportuno assioma. In altri termini, possiamo dire che non è possibile determinare *quanti* siano i numeri reali.