Raffaele SANTORO

$\mathbb{R}$

I numeri reali e la potenza del continuo

Vieste, Liceo Scientifico Statale Lorenzo Fazzini, Anno scolastico 1977-78
(Riscrittura su computer di vecchi appunti manoscritti dati, dal 1977, a diverse generazioni di allievi)

1 Introduzione [1]

Nelle pagine che seguono affronteremo la costruzione rigorosa dei numeri reali effettuata verso la fine del secolo scorso (1872) da Georg Cantor.
La costruzione di Cantor fu la prima costruzione rigorosa dell'insieme dei numeri reali e fu contemporanea ad un'altra costruzione, altrettanto rigorosa, effettuata da R. Dedekind. La coincidenza temporale delle due costruzioni non é casuale: nacque infatti da una precisa esigenza di sistemazione rigorosa di tutta la matematica, cominciata già verso la seconda metà del secolo scorso.

Con la nascita del calcolo infinitesimale e differenziale ad opera di Newton e Leibnitz, che facevano ricorso all'evidenza geometrica nell'introdurre i concetti di limite e di continuità, e con la successiva algebrizzazione della geometria iniziatasi con Cartesio, la geometria venne detronizzata e quindi messa in secondo piano rispetto all'Algebra ed all'Analisi Matematica.

Però mentre della geometria e dei suoi metodi si conosceva una costruzione rigorosa e assiomatica, non succedeva altrettanto per l'algebra e l'aritmetica; i numeri (naturali, interi, razionali, reali) furono introdotti senza troppi scrupoli rigoristici, solo in funzione strumentale del loro uso. Infatti i numeri irrazionali erano già stati introdotti nell'antichità greca come rapporto fra grandezze incommensurabili (ad esempio lato e diagonale di un quadrato) per via, quindi, puramente geometrica; per via algebrica, invece, furono introdotti dalla necessità di risolvere equazioni del tipo $x^2 - 2 = 0$, né si aggiunse altro.

Oggi sappiamo che tutti gli insiemi numerici si possono ricondurre agli insiemi dei numeri naturali con successive estensioni. Diceva Kroneker: "I numeri naturali li ha fatti il buon Dio, tutto il resto é opera dell'uomo", dove l'espressione "il buon Dio" sta a significare semplicemente che l'uomo ha rinunciato a dare una spiegazione dei numeri naturali, essendo questi legati alla semplice e "naturale" operazione del contare.

Prima di introdurre i numeri reali secondo Cantor (a partire dai razionali), vedremo brevemente [2] come si possono introdurre i numeri interi ed i numeri razionali a partite dai numeri naturali; seguirà ancora un paragrafo sulle proprietà dell'insieme $\mathbb{Q}$ dei razionali strutturato con le operazioni '+' , '.' e con la relazione d'ordine $\leq$.

2 Numeri naturali: insieme $\mathbb{N}$.

$$\mathbb{N} = \{0,1,2\ldots\}$$

3 Numeri interi: insieme $\mathbb{Z}$.

I numeri interi si possono definire a partire dai numeri naturali nel modo seguente:

- Si considerano tutte le coppie ordinate si numeri naturali $\{(m,n)/\, m \in \mathbb{N}, n \in \mathbb{N}\}$ (intuitivamente la coppia rappresenterà il numero relativo m - n)
- Tra queste coppie si definiscono le operazioni
  '+': $(m,n)+(p,q)=(m+p,n+q)$
  '.': $(m,n)\cdot(p,q)=(mp+nq,mq+np)$
  (le definizioni riflettono quello che si fa, in pratica, per sommare e moltiplicare i due numeri m - n e p - q)
- Due coppie rappresentano lo stesso numero se $m + q = n + p$.

In termini più precisi, la relazione (definita in $\mathbb{N}\times\mathbb{N}$)

$$(m, n)\Re(p, q) \Leftrightarrow m + q = n + p$$

é una relazione di equivalenza ed i numeri relativi si ottengono identificando tutte le coppie di naturali tra loro equivalenti: i numeri interi positivi sono rappresentati da coppie del tipo (m, 0) e quelli negativi da coppie del tipo (0, m). Ad esempio:

la classe di equivalenza $[(0,0)]=\{(0,0),(1,1),(2,2),\ldots\}$ rappresenta $0\in\mathbb{Z}$,
la classe di equivalenza $[(1,0)]=\{(1,0),(2,1),(3,2),\ldots\}$ rappresenta $1\in\mathbb{Z}$,
la classe di equivalenza $[(0,1)]=\{(0,1),(1,2),(2,3),\ldots\}$ rappresenta $-1\in\mathbb{Z}$,
…
L'insieme quoziente, o insieme di tutte le classi di equivalenza, definisce l'insieme $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots,[(0,2)],[(0,1)],[(0,0)],[(1,0)],[(2,0)],\ldots\} \equiv \{\ldots,-2,-1,0,1,2,\ldots\}.$$

4 Numeri razionali: insieme $\mathbb{Q}$

$\frac{1}{2} = 0{,}5$; $\frac{4}{3} = 1{,}333 \ldots = 1{,}\overline{3}$; …
I numeri razionali o frazioni si possono definire a partire dai numeri interi.

- Si considerano tutte le coppie ordinate (x, y) di numeri interi $\{(x,y)/\, x \in \mathbb{Z}, y \in \mathbb{Z}_0\}$, con y≠0 (il simbolo (x, y) sarà poi sostituito da quello più usuale $\frac{x}{y}$).
- Tra queste coppie si definiscono le operazioni
  '+': $(x,y)+(u,v)=(xv+yu,yv)$
  '.': $(x,y)\cdot(u,v)=(xu.yv)$
  (le definizioni riflettono quello che si fa, in pratica, per sommare e moltiplicare i due frazioni $\frac{x}{y}$ e $\frac{u}{v}$).
- Due coppie (x, y) e (u, v) rappresentano lo stesso numero se $xv = yu$. In termini piú precisi:
  $$(x,y)\,\Re\,(u,v) \Leftrightarrow xv = yu\ .$$
- La relazione appena definita é una relazione di equivalenza ed *i numeri razionali si ottengono identificando tutte le coppie ordinate fra loro equivalenti. Ogni sottoinsieme di* $\mathbb{Z}\times\mathbb{Z}_0$, *costituito da tutte le coppie fra loro equivalenti in* $\Re$, *costituisce una classe di equivalenza che verrà identificata prendendo una coppia qualunque della classe*, di solito quella che noi chiamiamo frazione ridotta ai minimi termini. L'insieme di tutte queste classi, *l'insieme quoziente*, definisce l'insieme $\mathbb{Q}$:

$$\mathbb{Q} = \frac{\mathbb{Z}\times\mathbb{Z}_0}{\Re}\ .$$

Ad esempio sono equivalenti fra di loro le coppie ordinate:

(2, 3), (4, 6), (-2, -3), (-12, -18),…

Come rappresentante di questa classe di equivalenza si prende la coppia (2, 3) che definisce quella che chiamiamo frazione ridotta ai minimi termini.

La coppia (0,1), equivalente alle coppie del tipo (0,2), (0, -3), … diventa lo zero dei razionali.
La coppia (1,1), equivalente alle coppie del tipo (-3,-3), (2, 2), (7, 7), … diventa l'unità dei razionali.
I numeri interi, contenuti nei razionali, sono tutte le coppie del tipo (x, 1).

5 Corpo ordinato dei numeri razionali

Enunciamo qui, senza dimostrarle, le proprietà dell'insieme $\mathbb{Q}$ quando venga strutturato con le operazioni interne '+' , '·' e venga munito di una relazione d'ordine.

a) ($\mathbb{Q}$,+,·) é un corpo commutativo: questo significa che

($\mathbb{Q}$,+) é una struttura di gruppo abeliano
($\mathbb{Q}$\{0},·) é una struttura di gruppo abeliano
la moltiplicazione é distributiva rispetto all'addizione

b) <u>$\mathbb{Q}$ é totalmente ordinato dalla relazione '$\le$'</u>. In simboli:

$\forall x: x \le x$ (riflessività) (1)

$\forall x, \forall y: \left.\begin{matrix} x \le y \\ y \le x \end{matrix}\right\} \Rightarrow x = y$ (antisimmetria) (2)

$\forall x, \forall y, \forall z: \left.\begin{matrix} x \le y \\ y \le z \end{matrix}\right\} \Rightarrow x \le z$ (transitività) (3)

$\forall x, \forall y: x \le y \ oppure \ y \le x$ (4)

Le (1), (2) e (3) sono le note proprietà della relazione di ordine largo (in $\mathbb{Q}$), mentre la (4) stabilisce che la relazione é di ordine totale in $\mathbb{Q}$, cioè che l'insieme $\mathbb{Q}$ é totalmente ordinato dalla relazione '$\le$'.

c) <u>La relazione d'ordine é compatibile con l'addizione</u>:

$\forall x, \forall y, \forall z: \ x \le y \ \Rightarrow \ x + z \le y + z$ (5)

d) <u>Il prodotto di di due numeri maggiori o uguali a zero é un numero maggiore o uguale a zero</u>:

$\forall x, \forall y: \left.\begin{matrix} 0 \le y \\ 0 \le y \end{matrix}\right\} \Rightarrow 0 \le xy$ (6)

Si chiama corpo totalmente ordinato ogni corpo che soddisfa agli assiomi da (1) a (6).

e) <u>Il corpo $\mathbb{Q}$ é denso</u>:

$\forall x, \forall y, x \le y, \ \exists z \ \text{tale che}: \ x \le z \ \text{e} \ \ z \le y$,

cioè, comunque sono assegnati due numeri razionale *x* e *y*, con $x \le y$, esiste almeno un numero razionale *z* (e quindi infiniti) compreso tra *x* e *y*.

f) <u>Valore assoluto di un numero razionale</u>:

$$|x| = \begin{cases} x & \text{SE } 0 \le x \\ -x & \text{SE } x < 0. \end{cases}$$

Rispetto all'addizione ed alla moltiplicazione in $\mathbb{Q}$ valgono le seguenti proprietà.

$|x + y| \le |x| + |y|$

$|xy| = |x||y|$

g) <u>Intervalli</u>

In $\mathbb{Q}$ si chiama <u>intervallo aperto</u> determinato da *a* e *b* il sottoinsieme di numeri razionali compresi in senso stretto tra *a* e *b*. In simboli:

$]a,b[= \{x | a < x < b\}$ $(a \leq b)$

Se *a* = *b*, nessun *x* soddisfa la condizione di sopra e abbiamo:

$$]a,a[= \varnothing.$$

L'intervallo chiuso di estremi *a* e *b* é dato da:

$[a,b] = \{x | a \leq x \leq b\}$ $(a \leq b)$.

Se *a* = *b*, abbiamo:

$[a,a] = \{a\}$.

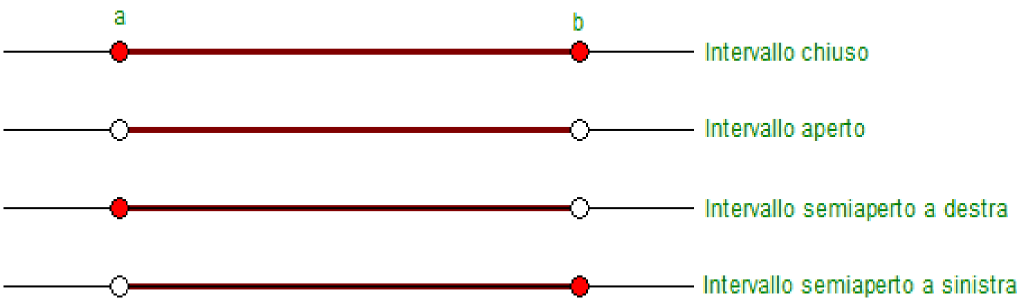
Spesso vengono utilizzati anche gli intervalli semiaperti (o semichiusi):

$[a,b[= \{x | a \leq x < b\}$

$]a,b] = \{x | a < x \leq b\}$.

Il numero $l = b - a$ é il diametro dell'intervallo determinato da *a* e *b*. Risulta sempre $l \geq 0$ perché $a \leq b$.

Gli intervalli hanno un rappresentazione intuitiva sulla retta numerica:



Un intervallo chiuso di diametro nullo ha un solo elemento. Un intervallo aperto o semiaperto di diametro nullo è vuoto.

6 Successioni di numeri razionali

Si chiama successione di numeri razionali ogni applicazione f di $\mathbb{N}$ in $\mathbb{Q}$:

$$f : \mathbb{N} \to \mathbb{Q}$$
$$f : n \to a_n \; .$$

$a_n = f(n)$ si chiama termine generale della successione. La successione sarà indicata simbolicamente con (a_n).

Esempi:

a) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ $\qquad a_n = \frac{1}{n}$

b) $\frac{1}{3}, \frac{3}{6}, \frac{5}{9}, \frac{7}{12}, \ldots$ $\qquad a_n = \frac{2n-1}{3n}$

c) 1, -1, 1, -1, … $\qquad a_n = (-1)^{n+1}$

d) $1, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{8}, \frac{1}{16}, \ldots$ $\qquad a_n = \frac{(-1)^{n+1}}{2^{n-1}}$

e) 0.3, 0.33, 0.333, … $\qquad a_n = \sum_{k=1}^{k=n} \frac{3}{10^k}$

f) 1, 1, 2, 3, 5, 8, 13, … $\qquad \begin{cases} a_1 = a_2 = 1 \\ a_{n+1} = a_n + a_{n-1} \quad (n \geq 2) \end{cases}$

g) $1, \frac{1}{2}, \frac{1}{3}, 1, \frac{1}{4}, \ldots$ $\qquad \begin{cases} a_{2n-1} = 1 \\ a_{2n} = \frac{1}{n+1} \end{cases}$

h) 2, 2, 2, 2, … $\qquad a_n = 2 \ \forall n \in \mathbb{N}$.

La successione dell'esempio h) è una particolare successione chiamata successione costante.

Si dice che una successione è crescente se si ha:

$$\forall m, \forall n, n > m \Rightarrow a_n \geq a_m .$$

Le successioni degli esempi b), e), f) sono crescenti; esse sono anche strettamente crescenti perché:

$$\forall m, \forall n, n > m \Rightarrow a_n > a_m .$$

Si dice che una successione è decrescente se si ha:

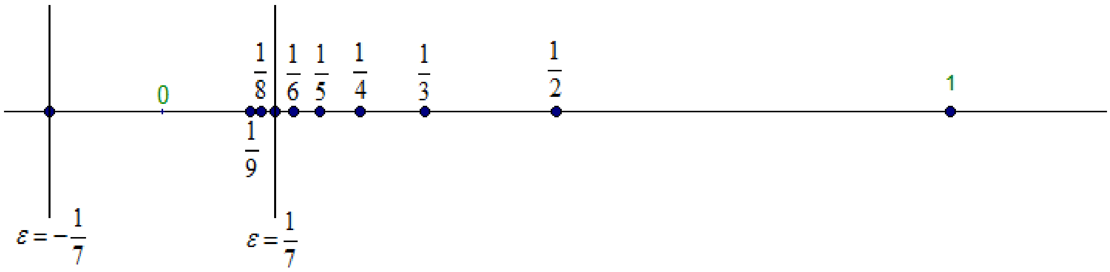
$$\forall m, \forall n, n > m \Rightarrow a_n \leq a_m .$$

La successione dell'esempio a) è decrescente, anzi è strettamente decrescente perché;

$$\forall m, \forall n, n > m \Rightarrow a_n < a_m .$$

I termini delle successioni a) e d) diventano sempre più piccoli (in valore assoluto). In termini più precisi, qualunque sia il numero ε, $\varepsilon \in \mathbb{Q}^+$, a partire da un certo termine, gli elementi della successione appartengono all'intervallo $]-\varepsilon, \varepsilon[$:

- per la successione a), scegliendo ε = 1/7, tutti i termine della successione, dal termine a_8 in poi, sono compresi nell'intervallo]-1/7,1/7[.



- per la successione d), prendendo ε = 1/5, tutti i termine della successione, dal termine a_4 in poi, sono compresi nell'intervallo]-1/5,1/5[.

Si dice allora che la successione, quando n tende all'infinito, tende a zero o anche che *la successione converge a zero*. In termini più precisi:

> Si dice che una successione (a_n) tende a zero se, per ogni ε, (ε∈ℚ+), tutti i termini della successione, a partire da un certo termine di posto n_0, appartengono all'intervallo]-ε, ε[:
> $\forall \varepsilon\ (\varepsilon \in \mathbb{Q}^+),\ \exists n_0,\ n_0 \in \mathbb{N}\ /\ n > n_0 \Longrightarrow a_n \in]-\varepsilon, \varepsilon[$.

Quando la successione (a_n) tende a zero, si scrive:

$$a_n \longrightarrow 0, \text{ oppure } \lim_{n\to\infty} a_n = 0.$$

É facile verificare che la somma di due successioni che tendono a zero è una successione che tende a zero:

$$\left.\begin{array}{l} a_n \to 0 \\ b_n \to 0 \end{array}\right\} \Rightarrow a_n + b_n \to 0.$$

Analogamente, il prodotto di due successioni che tendono a zero è una successione che tende a zero:

$$\left.\begin{array}{l} a_n \to 0 \\ b_n \to 0 \end{array}\right\} \Rightarrow a_n \cdot b_n \to 0.$$

Infine, se la successione tende a zero, lo stesso accade per la successione $\lambda(a_n)$, $\forall \lambda \in \mathbb{Q}$:

$$\forall\lambda\in\mathbb{Q},\ (a_n)\to 0\ \Rightarrow\ \lambda(a_n)\to 0.$$

Però, non sempre le successioni convergenti tendono a zero, anzi accade piuttosto che convergano verso un altro (razionale o no) $a \neq 0$. Per stabilire se una successione razionale converge verso un numero a, diamo la seguente definizione:

> Una successione convergente (a_n)tende ad a se la successione $(a - a_n)$ tende a zero: $a_n \to a$, oppure $\lim_{n\to\infty} a_n = a \Leftrightarrow \lim_{n\to\infty}(a - a_n) = 0$.

Esempi:

- La successione dell'esempio b) tende a 2/3. Infatti abbiamo (costruendoci la successione differenza b_n):
$$b_n = \frac{2}{3} - a_n = \frac{2}{3} - \frac{2n-1}{3n} = \frac{1}{3n};$$
- la successione $b_n = \frac{1}{3n}$ è il prodotto del numero razionale 1/3 per la successione di termine generale $1/n$ dell'esempio a), che abbiamo visto convergere a zero. Quindi, per quanto visto sopra, anche la successione:
$$b_n = \frac{2}{3} - a_n$$
tende a zero e a_n tende a 2/3.

- La successione:
$a_1 = 0{,}3;\ a_2 = 0{,}33;\ a_3 = 0{,}333;\ \ldots$
converge a 1/3 = 0,333… . Infatti la successione: $b_n = \frac{2}{3} - a_n$ tende a zero:
$b_1 = 0{,}0333\ldots;\ b_2 = 0{,}00333\ldots;\ b_3 = 0{,}000333\ldots;\ \ldots$

Come prima, è facile dimostrare che la somma ed il prodotto di due o più successioni convergenti è ancora una successione convergente. Ma c'è di più: si può dimostrare che

$$\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$$
$$\lim_{n\to\infty}(a_n \cdot b_n) = \lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n$$
$$\lim_{n\to\infty} \lambda(a_n) = \lambda \lim_{n\to\infty} a_n,\ \forall\lambda\in\mathbb{Q}$$

7 Criterio di convergenza di Cauchy

Fino ad ora abbiamo considerato la convergenza di successioni razionali di cui conoscevamo già il limite di convergenza. A volte, però, è solo necessario sapere se una successione razionale converge oppure no, senza conoscerne il limite verso cui converge, e questo anche perché è molto spesso difficile calcolare tale limite. Perciò stabiliremo ora un criterio (necessario) di convergenza delle successioni in $\mathbb{Q}$; questo criterio è il *criterio di Cauchy*:

Se una successione razionale converge ad a, allora, comunque si sceglie un $\varepsilon \in \mathbb{Q}+$, è possibile trovare un indice n_0 tale che:
$\forall\, n > n_0$, $\forall m > n_0$ risulta: $|a_n - a_m| < \varepsilon$.

Infatti, se la successione razionale converge ad a, allora, $\forall \varepsilon/2 \in \mathbb{Q}+$, esiste un $n_0 \in \mathbf{N}$ tale che, $\forall m > n_0$ risulta:

$$|a - a_m| < \frac{\varepsilon}{2};$$

varrà anche la relazione, per $n > m$:

$$|a_m - a| < \frac{\varepsilon}{2}.$$

Allora:

$$|a_n - a_m| = |(a_n - a) + (a - a_m)| \leq |a_n - a| + |a - a_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Dunque $|a_n - a_m| < \varepsilon$ (come volevasi dimostrare, c.v.d.).

"… questo criterio … si riferisce soltanto ai termini della successione presa in esame, e non suppone la conoscenza di alcun numero oltre ad essi. In parole povere, il criterio esige che i termini della successione si addensino gli uni agli altri, sicché la differenza fra uno di essi (scelto abbastanza in avanti) ed un qualunque termine successivo diventi piccola ad arbitrio..." [3].

Come si è già anticipato, il criterio di convergenza di Cauchy è solo necessario e non sufficiente: esistono cioè successioni razionali che, pur soddisfacendo al criterio di Cauchy, non convergono ad alcun numero razionale.

Consideriamo un numero decimale periodico: $a = 2{,}2\overline{35}$, ed a partire da questo costruiamoci la successione (a_n):
$a_1 = 2{,}2; \qquad a_2 = 2{,}23; \qquad a_3 = 2{,}235; \qquad a_4 = 2{,}2353; \quad a_5 = 2{,}23535; \ldots$
questa successione soddisfa il criterio di Cauchy e converge ad un numero razionale. Infatti abbiamo:

$$\left(10^3 a = 2235{,}\overline{35},\ 10a = 22{,}\overline{35}\right) \Rightarrow 10^3 a - 10a = 2213 \Rightarrow a = \frac{2213}{990} \in \mathbb{Q}.$$

In generale, ogni sviluppo decimale periodico converge ad un numero razionale: ammettiamo la facile dimostrazione che è simile a quella del caso particolare precedente.

Consideriamo ora un allineamento decimale limitato non periodico: $a_0, m_1 m_2 \ldots m_n \ldots$. A partire da questo allineamento costruiamoci la successione razionale:

$$b_1 = a_0, m_1; \quad b_1 = a_0, m_1 m_2; \ \ldots \qquad b_n = a_0, m_1 m_2 \ldots m_n; \ \ldots\ .$$

Tale successione verifica il criterio di Cauchy:

$$b_{n+1} - b_n = \frac{m_{n+1}}{10^{n+1}} \leq \frac{9}{10^{n+1}} < \frac{10}{10^{n+1}} = \frac{1}{10^n};$$

posto $\varepsilon = 10^{-n}$, $\exists n_0 = 10^n \in \mathbb{N}$ / $\forall n > n_0$:

$$|b_{n+1} - b_n| < \frac{1}{10^n} = \epsilon.$$

Però tale successione non converge ad alcun numero *razionale*, perché, se fosse $\lim_{n\to\infty} b^n = a \in \mathbb{Q}$, a dovrebbe essere razionale, contro l'ipotesi che è invece uno sviluppo illimitato non periodico.
Pertanto abbiamo bisogno di ampliare l'insieme numerico $\mathbb{Q}$ per far sì che ogni successione razionale di Cauchy converga ad un numero appartenente al nuovo insieme, ampliamento di $\mathbb{Q}$.
Ovviamente, questo nuovo insieme numerico che andremo a definire dovrà contenere come suo sottoinsieme proprio l'insieme $\mathbb{Q}$; non solo, ma, oltre ad avere tutte le proprietà strutturali già viste di $\mathbb{Q}$, dovrà eventualmente risultare una struttura 'più ricca', proprio perché dovrà permettere la convergenza di tutte le successioni di Cauchy.

8 Esistenza dei numeri irrazionali

Sappiamo che l'equazione $x^2 - 2 = 0$ non è risolubile in $\mathbb{Q}$. I greci conoscevano già una dimostrazione di questo fatto. La dimostrazione la troviamo negli "Elementi" di Euclide.
Supponiamo che esista un numero razionale x il cui quadrato sia uguale a 2; possiamo, allora, rappresentare x con una frazione irriducibile $\frac{m}{n}$:

$$x = \frac{m}{n} \Rightarrow x^2 = \frac{m^2}{n^2} = 2 \Rightarrow m^2 = 2n^2; \ (*)$$

Da quest'ultima espressione risulta che m^2 è un numero pari, quindi anche m sarà pari e potremo scrivere:

$$m = 2m' \text{ con } m' \in \mathbb{N}.$$

Con questa sostituzione la (*) diventa:

$$4m'^2 = 2n^2 \Rightarrow 2m'^2 = n^2;$$

da quest'ultima espressione risulta che anche n^2 è pari e quindi anche n è pari; allora, se m e n sono pari, avranno in comune il fattore 2, contro l'ipotesi che $x = \frac{m}{n}$ è una frazione irriducibile.
Siamo arrivati ad una conclusione assurda supponendo che x sia razionale; quindi è assurda quest'ultima ipotesi: $x = \sqrt{2}$ non è razionale. D'altra parte, però, $\sqrt{2}$ rappresenta la misura della diagonale di un quadrato di lato 1; quindi la sua esistenza è altrettanto legittima come qualunque altro numero razionale.
Non abbiamo, dunque, motivi di dubitare dell'esistenza di numeri come $\sqrt{2}$. Però non servirebbe a nulla creare un nuovo simbolo come $\sqrt{2}$ senza verificare che questa estensione della nozione di numero non conduce a contraddizioni.
Noi abbiamo accennato brevemente, nei paragrafi 3 e 4, alle estensioni successive di $\mathbb{N}$.
Per assicurare l'esistenza di interi relativi abbiamo considerato delle classi di equivalenza in $\mathbb{N}$x$\mathbb{N}$. Poiché tutte le operazioni conducono a coppie i cui elementi appartengono a $\mathbb{N}$, la teoria degli interi relativi non può essere contraddittoria, se è coerente l'aritmetica di $\mathbb{N}$.
Analogamente, l'esistenza dei razionali è assicurata dalla studio di classi di equivalenza in $\mathbb{Z}$x$(\mathbb{Z} - \{0\})$,

Si tratta ora di considerare l'ampliamento di $\mathbb{Q}$ ad $\mathbb{R}$. Un tale ampliamento è diverso dagli ampliamenti considerati fino ad ora. Infatti la costruzione di $\mathbb{R}$ richiede la nozione di limite. *Questa differenza indica il passaggio dall'algebra all'analisi matematica*.

9 Costruzione dei numeri reali: insieme $\mathbb{R}$

Nel seguito indicheremo con $S_{\mathbb{Q}}$ l'insieme delle successioni di $\mathbb{Q}$ e con $\mathscr{C}\,(\subset S_{\mathbb{Q}})$ l'insieme delle successioni fondamentali (cioè che soddisfano il criterio di Cauchy).
Se (a_n) e (b_n) appartengono a $\mathscr{C}$, le successioni

$$(a_n + b_n) = (a_1 + b_1, a_2 + b_2, \dots) \text{ e } (a_n b_n) = (a_1 b_1, a_2 b_2, \dots)$$

appartengono ancora a $\mathscr{C}$. Infatti:

$$(a_n), (b_n) \in \mathscr{C} \Leftrightarrow \forall \varepsilon \in \mathbb{Q}^+, \exists n_0 \in \mathbb{N} / \forall n, m > n_0 \Rightarrow$$
$$|a_n - a_m| < \varepsilon \text{ e } |b_n - b_m| < \varepsilon \Rightarrow$$
$$|(a_n + b_n) - (a_m + b_m)| \leq |a_n - a_m| + |b_n - b_m| < 2\varepsilon,$$

Per cui $(a_n + b_n)$ è una successione di Cauchy, cioè appartiene a $\mathscr{C}$.

Facilmente si dimostra anche che se $\big((a_n), (b_n)\big) \in \mathscr{C} \times \mathscr{C}, (a_n b_n) \in \mathscr{C}$.

In $\mathscr{C}$ possiamo allora definire le operazioni di addizione e di moltiplicazione, ponendo $\forall \big((a_n), (b_n)\big) \in \mathscr{C} \times \mathscr{C}$:

$$(a_n) + (b_n) = (a_n + b_n)$$
$$(a_n) \cdot (b_n) = (a_n b_n)$$

Rispetto a queste operazioni, $\mathscr{C}$ costituisce un anello: lo zero è costituito dalla successione avente tutti i suoi elementi uguali a zero: (0), l'opposto di (a_n) è la successione (ancora fondamentale) $(-a_n)$, l'unità è la successione costituita da tutti uno: (1). Non possiamo prendere questo anello $(\mathscr{C}, +, \cdot)$ come ampliamento di $\mathbb{Q}$, perché, come abbiamo già detto alla fine del paragrafo 7, il nuovo insieme che andiamo a costruire deve per lo meno risultare un corpo commutativo come $\mathbb{Q}$, e poi avere altre caratteristiche sue proprie. Quindi gli elementi di $\mathscr{C}$ non possiamo identificarli con i nuovi numeri che vogliamo definire; però possiamo considerare il passaggio al limite e identificare i nuovi numeri con il limite a cui tendono le diverse successioni di $\mathscr{C}$.
"L'insieme dei nuovi enti contiene una copia esatta dei numeri razionali, perché ogni numero razionale si può identificare con la successione costante i cui termini sono tutti uguali al numero dato. C'è una complicazione dovuta al fatto che successioni diverse possono tendere allo stesso limite; allora bisogna 'identificare' tra loro tutte le successioni la cui differenza tende a zero; questa operazione, detta passaggio al quoziente, è frequentissima in matematica, ed è già presente nella definizione dei numeri razionali" [4].
Definiamo allora in $\mathscr{C}$ la seguente relazione $\mathfrak{R}$:

$$\forall \big((a_n), (a'_n)\big) \in \mathscr{C} \times \mathscr{C}, (a_n) \mathfrak{R} (a'_n) \Leftrightarrow \lim_{n\to\infty} (a_n - a'_n) = 0.$$

Proviamo che **$\mathfrak{R}$ è una relazione di equivalenza in $\mathscr{C}$**:

<u>Proprietà riflessiva</u>:

$\forall(a_n)\in\mathscr{C}:\ (a_n)\mathfrak{R}(a_n)$ perché: $\lim_{n\to\infty}(a_n-a_n)=0$.

<u>Proprietà simmetrica</u>:

$$\forall\big((a_n),(a'_n)\big)\in\mathscr{C}\times\mathscr{C}:$$
$$(a_n)\mathfrak{R}(a'_n)\Leftrightarrow\lim_{n\to\infty}(a_n-a'_n)=0\ \Leftrightarrow$$
$$\lim_{n\to\infty}(a'_n-a_n)=0\Leftrightarrow(a'_n)\mathfrak{R}(a_n).$$

<u>Proprietà transitiva</u>:

$$\forall\big((a_n),(a'_n),(a''_n)\big)\in\mathscr{C}\times\mathscr{C}\times\mathscr{C}:$$
$$[(a_n)\mathfrak{R}(a'_n),(a'_n)\mathfrak{R}(a''_n)]\Leftrightarrow\Big[\lim_{n\to\infty}(a_n-a'_n)=0,\lim_{n\to\infty}(a'_n-a''_n)=0\Big]\Rightarrow$$
$$[\ \forall\varepsilon\in\mathbb{Q}^+,\exists n_0\in\mathbb{N}/\ \forall n>n_0:|a_n-a'_n|<\varepsilon\ ,|a'_n-a''_n|<\varepsilon\ ]\Longrightarrow$$
$$|a_n-a''_n|\le|a_n-a'_n|\ +|a'_n-a''_n|<2\varepsilon\ \Rightarrow$$
$$\lim_{n\to\infty}(a_n-a''_n)\ =0\Longrightarrow$$
$$(a_n)\mathfrak{R}(a''_n).$$

Inoltre, utilizzando le proprietà del valore assoluto viste alla fine del paragrafo 5, possiamo provare che (esercizio per il lettore):

$$(a_n)\mathfrak{R}(a'_n)\ \wedge(b_n)\mathfrak{R}(b'_n)\Longrightarrow\begin{cases}(a_n+b_n)\mathfrak{R}(a'_n+b'_n)\\ (a_nb_n)\mathfrak{R}(a'_nb'_n)\end{cases}\qquad(*)$$

La relazione di equivalenza $\mathfrak{R}$, definita in $\mathscr{C}$, determina una partizione di $\mathscr{C}$ in classi di equivalenza, ogni classe $[(a_n)]_\mathfrak{R}$ essendo costituita da tutte le successioni fondamentali (a'_n) in relazione con (a_n), cioè tali che la successione $\big(a_n-a'_n\big)$ converga a zero. Nell'insieme quoziente $\mathscr{C}/\mathfrak{R}$, cioè nell'insieme delle classi suddette, si può definire un'operazione di addizione e di moltiplicazione ponendo :

$$[(a_n)]_\mathfrak{R}+[(b_n)]_\mathfrak{R}=[(a_n+b_n)]_\mathfrak{R}$$
$$[(a_n)]_\mathfrak{R}\cdot[(b_n)]_\mathfrak{R}=[(a_n\cdot b_n)]_\mathfrak{R}.$$

Tali definizioni sono ben poste in virtù delle (*), affermanti che la somma (o il prodotto) di una qualunque successione $(a'_n)\in[(a_n)]_\mathfrak{R}$ e $(b'_n)\in[(b_n)]_\mathfrak{R}$ è una successione di $[(a_n+b_n)]_\mathfrak{R}$ (o di $[(a_n\cdot b_n)]_\mathfrak{R}$).

Poiché $\mathscr{C}$ è un anello, anche $\mathscr{C}/\mathfrak{R}$ è un anello rispetto alle operazioni ora definite ; lo zero, che denoteremo con 0, è la classe individuata dalla successione nulla (0) è quindi la classe costituita da tutte le successioni che tendono a zero; l'unità, che denoteremo con 1, è la classe individuata dalla successione (1) e quindi costituita da tutte le successioni che tendono a 1. Tale anello, $\mathscr{C}/\mathfrak{R}$, come l'anello $\mathscr{C}$, risulta essere anche commutativo. Inoltre si può dimostrare che ogni elemento di $\mathscr{C}/\mathfrak{R}$-$[(0)]_\mathfrak{R}$ ammetto inverso; quindi ($\mathscr{C}/\mathfrak{R}$, +, $\cdot$) risulta essere un corpo commutativo, cioè un campo. Ma il campo è la più povera struttura che cercavamo per il nostro nuovo insieme numerico. Allora identifichiamo l'insieme quoziente $\mathscr{C}/\mathfrak{R}$ con l'insieme dei numeri reali $\mathbb{R}$:

$$\frac{\mathscr{C}}{\Re} = \mathbb{R}.$$

Quindi gli elementi di questo nuovo insieme numerico, cioè i numeri reali, vengono identificati con le classi di equivalenza di $\mathscr{C}/\Re$. Se α, β, … denotano gli elementi di ℝ, avremo:

$$\alpha \equiv [(a_n)]_{\Re}, \beta \equiv [(b_n)]_{\Re}, \ldots$$

L'insieme ℝ, strutturato con le operazioni (interne ad ℝ) somma e prodotto, risulta essere un corpo commutativo:

(ℝ, +, ·) <u>corpo commutativo</u>

dove

$+ : \mathbb{R} x \mathbb{R} \to \mathbb{R} \ / \ (\alpha, \beta) \to \alpha + \beta$, $\quad \cdot : \mathbb{R} x \mathbb{R} \to \mathbb{R} \ / \ (\alpha, \beta) \to \alpha\beta$

Lasciando al lettore l'idea intuitiva di numero reale positivo e di numero reale negativo, si vede subito che il campo ℝ è totalmente ordinato dalla relazione ⩽ :

$$\alpha \leqslant \beta \Leftrightarrow \alpha - \beta \leqslant 0;$$

(ℝ, +, ·, ⩽) <u>campo totalmente ordinato</u>

Facciamo ora vedere che effettivamente ℝ è un ampliamento di ℚ. Infatti ad ogni numero razionale $a \in \mathbb{Q}$ rimane associato univocamente il numero reale α individuato dalla successione fondamentale

$$(a) = (a, a, \ldots, a, \ldots)$$

Rimane così determinata l'applicazione iniettiva:

$$\varphi : \mathbb{Q} \to \mathbb{R}, \qquad \varphi : a \to [(a_n)]_{\Re}, \qquad \varphi(a) = [(a_n)]_{\Re} \in \mathbb{R}$$

Siccome abbiamo manifestamente:

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

la struttura (ℚ, +, ·, ⩽) e (ℚ', +, ·, ⩽) con ℚ' = φ(ℚ), sono isomorfe e possiamo identificare il campo ℚ con il sottocampo ℚ' di ℝ, a meno dell'isomorfismo φ. Allora ℚ'⊂ℝ ⟹ ℚ⊂ℝ:

<u>ℝ può considerarsi</u>, dunque, <u>un ampliamento di ℚ.</u>

Prima di chiudere questo paragrafo vogliamo solo aggiungere che, in ℝ, le nozioni di successioni convergenti e di successioni di Cauchy sono coincidenti. In ℝ ogni successione convergente soddisfa il criterio di Cauchy, ed ogni successione che soddisfa il criterio di

Cauchy è convergente. Per questo si dice che, in ℝ, il criterio di Cauchy rappresenta una successione necessaria e sufficiente. Anzi, se costruiamo in ℝ delle successioni di Cauchy e ragioniamo in modo analogo a quanto fatto prima, si dimostra che

$$\frac{\mathscr{C}_{\mathbb{R}}}{\Re} = \mathbb{R}$$

dove $\mathscr{C}_{\mathbb{R}}$ è l'insieme delle successioni di Cauchy ad elementi in ℝ. Per questo si dice pure che <u>l'insieme ℝ è chiuso o completo</u>.

Il valore assoluto di un numero reale si definisce in modo analogo a quanto fatto in ℚ:

$$|\alpha| = \begin{cases} \alpha & \mathbf{SE}\ 0 \le \alpha \\ -\alpha & \mathbf{SE}\ \alpha < 0 \end{cases}$$

Si prova facilmente che, dato comunque un numero reale α ed un numero ε (piccolo a piacere), esistono infiniti numeri razionali a tali che $|\alpha - a| < \varepsilon$. Per questa ragione diremo che <u>il campo ℚ</u>, pensato immerso mediante φ in ℝ, <u>è denso in ℝ</u> .
L'insieme <u>ℝ-ℚ</u> lo chiameremo <u>insieme dei numeri irrazionali</u>.

10 <u>Potenza o numero cardinale di un insieme</u>

Gli insiemi numerici che abbiamo considerato: **ℕ**, ℤ, ℚ, ℝ, sono tutti insiemi infiniti, cioè insiemi tali che noi possiamo estrarre da questi quanti elementi vogliamo senza che per questo gli elementi dell'insieme considerato si esauriscano.

Possiamo numerare gli insiemi infiniti o, ancora, *possiamo stabilire se un insieme infinito ha più elementi di un altro insieme infinito*?

Sappiamo che la cosa è certamente possibile per gli insiemi finiti, per cui abbiamo due possibilità di fare ciò: o contare gli elementi di tutti e due gli insiemi, oppure cercare di stabilire una corrispondenza tra gli elementi di tutti e due gli insiemi. Se questa corrispondenza è tale che a ciascun elemento del primo insieme corrisponda uno ed un solo elemento del secondo insieme e viceversa (corrispondenza biunivoca) noi diciamo che i due insiemi hanno lo stesso numero di elementi. Per esempio, consideriamo un insieme di spettatori e l'insieme dei posti a sedere di una sala cinematografica: invece di contare gli elementi dei due insiemi, se tutti gli spettatori sono seduti e se tutti i posti a sedere sono occupati, diciamo che i due insiemi hanno lo stesso numero di elementi, e solo in questo caso.

Questo criterio della corrispondenza biunivoca per confrontare il numero di elementi di due insiemi è un criterio potente in quanto è applicabile non solo agli insiemi finiti ma anche agli insiemi infiniti.

> Due insiemi A e B si dicono equipotenti se è possibile porre tra di essi una corrispondenza biunivoca: $A \sim B \Leftrightarrow \exists\varphi\ /\ \varphi: A \leftrightarrow B$.

Questa relazione (∼) si chiama anche relazione di equipotenza ed è una relazione di equivalenza definita nella totalità degli insiemi. Infatti:

- è riflessiva A∼A
- è simmetrica A∼ B ⇒ B ∼ A
- è transitiva (A∼ B, B ∼ C) ⇒ A∼ C.

La ∼ , essendo una relazione di equivalenza, induce nell'insieme di tutti gli insiemi G una partizione in classi di equivalenza, in ciascuna delle quali ci sono tutti e soli gli insiemi equipotenti fra di loro: nella prima classe ci sarà solo l'insieme vuoto, nella seconda classe tutti gli insiemi con un solo elemento, nella terza classe tutti gli insiemi con due elementi, ecc; e questo indipendentemente dalla natura degli elementi appartenenti agli insiemi.

Chiameremo <u>potenza di un insieme A</u>, e scriveremo <u>potA</u>, <u>la classe di tutti gli insiemi equipotenti ad A</u>.

Se l'insieme A ha un numero finito di elementi, potA è il <u>numero cardinale finito</u> relativo ad A (scritto cardA). Ad esempio, se A = $\{a, b, c\}$, allora cardA = 3.

Se, invece, A è costituito da un numero non finito di elementi, potA prende il nome di <u>numero cardinale transfinito</u>.

Dati due insiemi A e B, supponiamo che si possa stabilire una corrispondenza biunivoca tra A ed una parte di B. Diremo allora che la potenza di A è minore o ugual alla potenza di B e scriveremo: potA⩽potB. Tale definizione è ben posta perché se A' è equipotente ad A (cioè se A'∈ potA) e B' è equipotente a B (cioè se B' ∈ potB), evidentemente si potrà porre una corrispondenza biunivoca tra A' ed una parte di B'.

La relazione ⩽ definita tra le potenze è una relazione d'ordine; infatti gode evidentemente della proprietà riflessiva e transitiva ed inoltre gode della proprietà antisimmetrica in base al seguente <u>teorema di Cantor-Bernstein</u>, di cui ometteremo la dimostrazione:

> Se un insieme A può essere messo in corrispondenza biunivoca con una parte propria di B e l'insieme B si può mettere in corrispondenza biunivoca con una parte propria di A, allora A e B sono equipotenti:
> (potA ⩽ potB, potB ⩽ potA) ⟹ potA = potB.

Facciamo notare che, affinché abbiano senso le premesse di questo teorema, è necessario che gli insiemi A e B siano infiniti.

Cantor, quando enunciò la prima volta questo teorema (senza dimostrarlo, in quanto la dimostrazione fu fatta da altri), non disse esplicitamente che gli insiemi A e B dovevano essere infiniti per tacitare alcune critiche sull'infinito attuale, in quanto era ancora viva la tradizione aristotelica di considerare solo gli infiniti in potenza [5].

Cantor aveva aperto la strada all'infinito attuale rompendo con una tradizione bi millenaria.

11 Insiemi numerabili

Gli elementi dell'insieme $\mathbb{N}$ possono, almeno in linea di principio, essere numerati, contandoli uno di seguito all'altro; per questo diciamo che l'<u>insieme $\mathbb{N}$ è numerabile</u>. Però, in virtù della relazione di equipotenza fra insiemi, saranno numerabili anche tutti gli insiemi che possono essere messi in corrispondenza biunivoca con l'insieme $\mathbb{N}$.
Alla potenza della classe degli insiemi numerabili Cantor ha dato un nome particolare: $\aleph_0$ (da leggere *alef zero*)

$$\boxed{\text{pot}\mathbb{N} = \aleph_0}$$

Esempi:

a) <u>L'insieme dei numeri pari è numerabile</u>. Infatti basta considerare la biiezione f: $n \leftrightarrow 2n$

$\mathbb{N}$: 1 2 3 4 …
P : 2 4 6 8…

e questo nonostante sia manifestamente $P \subset \mathbb{N}$!

b) <u>L'insieme $\mathbb{Z}$ è numerabile</u>. Infatti possiamo stabilire fra $\mathbb{N}$ e $\mathbb{Z}$ la biiezione:

$\mathbb{N}$:	1	2	3	4	5	6	7…
$\mathbb{Z}$:	0	1	-1	2	-2	3	-3…

c) <u>L'insieme $\mathbb{Q}$ è numerabile</u>.
"Non si commetta l'errore di sottovalutare l'importanza matematica e filosofica di questo risultato, di cui dimostreremo la validità. E' evidente infatti che ad ogni numero naturale 1, 2, 3 corrispondono le frazioni 1/1, 2/1, 3/1 … . Ma l'insieme $\mathbb{Q}$ ha infiniti altri elementi! Di più: presi due numeri naturali, ad esempio 5 e 8, è possibile o no determinare un numero naturale compreso tra essi. In questo caso sì, per esempio 6 o 7; ma il risultato non vale sempre. Basta prendere due naturali consecutivi, ad esempio 4 e 5, e già non esiste più alcun numero naturale maggiore di 4 e minore di 5. Questo limita notevolmente la 'capacità' dell'insieme dei naturali di contenere elementi: esso non è <u>denso</u>. Bene l'insieme dei razionali, invece, è denso. Presi due termini qualunque 7/15 e 19/5, esiste sempre almeno un elemento compreso fra essi, per esempio:

$$\frac{\frac{7}{15}+\frac{19}{2}}{2}=\frac{32}{15} \qquad (\ldots)$$

Analogamente tra 7/15 e 32/15 è compreso, per es.:

$$\frac{\frac{7}{15}+\frac{32}{15}}{2}=\frac{39}{30}\ .$$

Analogamente, tra 7/15 e 39/30 è compreso, per es.:

$$\frac{\frac{7}{15}+\frac{39}{30}}{2}=\frac{53}{60}$$

e così via all'infinito.
Eppure, contro il senso comune, contro l'intuizione, Cantor afferma, come abbiamo detto, che i naturali e i razionali possono essere messi in corrispondenza biunivoca. Vediamo come.

Se abbiamo il numero razionale t/r (con $r \neq 0$), supponiamo di averlo ridotto ai minimi termini, cioè di aver semplificato, come si dice in gergo scolastico, t con r. Dunque partiamo dal presupposto di non considerare 10/30 diverso da 1/3 o da 20/60. Sotto questa ipotesi, definiamo l'altezza di un numero razionale n/m come segue: $h = n + m$, supposto $n \neq 0$, $m \neq 0$. Dato un valore, per esempio 5, il numero delle frazioni possibili

che l’hanno come altezza è finito. Nell’esempio proposto, deve essere $n + m = 5$, quindi si hanno i seguenti casi: ¼, 2/3, 3/2, 4/1.
Consideriamo tutti i razionali che hanno altezza 2. Ce n’è uno solo: 1/1, che mettiamo in una orizzontale che per ora ha un solo elemento:
1/1.
Consideriamo tutti i razionali che hanno altezza 3: sono ½ e 2/1. Mettiamo prima ½ e poi 2/1 nell’orizzontale precedente che diventa
1/1, ½, 2/1.
Consideriamo tutti i razionali che hanno altezza 4: sono 1/3, 2/2, 3/1. Ma 2/2 è riducibile ad 1/1 che avevamo già incontrato e quindi lo scartiamo. I restanti, nell’ordine 1/3 e 3/1, li aggiungiamo alla orizzontale, ottenendo
1/1, ½, 2/1, 1/3, 3/1.
Procediamo in modo analogo. Le altezze sono espresse da numeri naturali, quindi sono numerabili. All’interno di ciascun insieme di razionali egualmente ‘alti’, c’è un numero finito di termini: quando li disponiamo nella orizzontale, li mettiamo in modo tale che il numeratore sia crescente. Cosa abbiamo ottenuto? Che, sempre almeno in via teorica, abbiamo enumerato tutti i razionali: dunque l’insieme [$\mathbb{Q}$] è numerabile. La corrispondenza biunivoca tra razionali e naturali è rappresentata come segue:

h=2	h=3		h=4		h=5				…
1/1	½	2/1	1/3	3/1	¼	2/3	3/2	4/1	…
1	2	3	4	5	6	7	8	9	…

In maniera estremamente semplice abbiamo dimostrato un risultato che solo cent’anni fa sembrava non solo innaturale ma impossibile e che ancora, probabilmente, a qualche lettore sembrerà paradossale” [6].

d) Una dimostrazione più semplice si basa sul seguente diagramma:

1/1		½	→	1/3		¼	→	1/5		1/6	→	1/7		1/8
↓	↗		↙		↗		↙		↗		↙		↗	
2/1		2/2		2/3		2/4		2/5		2/6		2/7		2/8
	↙		↗		↙		↗		↙		↗			
3/1		3/2		3/3		3/4		3/5		3/6		3/7		3/8
↓	↗		↙		↗		↙		↗					
4/1		4/2		4/3		4/4		4/5		4/6		4/7		4/8
	↙		↗		↙		↗							
5/1		5/2		5/3		5/4		5/5		5/6		5/7		5/8
↓	↗		↙		↗									
6/1		6/2		6/3		6/4		6/5		6/6		6/7		6/8
	↙		↗											
7/1		7/2		7/3		7/4		7/5		7/6		7/7		7/8
↓	↗													
8/1		8/2		8/3		8/4		8/5		8/6		8/7		8/8

Partendo da 1/1 e seguendo le frecce (eliminando i numeri in rosso già presi in considerazione), si percorre l'intero insieme dei razionali positivi. In modo analogo si procede per quelli negativi.

12 Insiemi non numerabili: potenza del continuo

Un insieme infinito che non può essere messo in corrispondenza biunivoca con $\mathbb{N}$ viene detto non numerabile.
Dimostriamo il seguente teorema:

L'insieme $\mathbb{R}$ dei numeri reali è non numerabile.

Per dimostrare il teorema basta dimostrare che non è numerabile un suo sottoinsieme proprio: l'insieme dei numeri reali compresi tra 0 e 1.
Supponiamo per assurdo che tale insieme sia numerabile; allora possiamo scrivere:

$$(*) \quad \begin{cases} \alpha_1 = 0, a_{11}a_{12} \dots a_{1n} \dots \\ \alpha_2 = 0, a_{21}a_{22} \dots a_{2n} \dots \\ \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots . \\ \alpha_n = 0, a_{n1}a_{n2} \dots a_{nn} \dots \\ \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots . \end{cases}$$

Qui a_{ik} denota la k-esima cifra decimale del numero α_i .
Costruiamo un numero decimale

$$\beta = 0, b_1 b_2 \dots b_n \dots$$

con il procedimento diagonale di Cantor, in modo che b_1 sia una cifra arbitraria diversa da a_{11}, b_2 una cifra arbitraria diversa da a_{22}, ecc.; in generale b_n deve essere una cifra arbitraria diversa da a_{nn}. Il numero β così costruito non può appartenere alla successione (*). Infatti β differisce da α_1 almeno per la prima cifra decimale, da α_2 per la seconda cifra decimale, ecc.; in generale, poiché $b_n \neq a_{nn}$ per ogni n, β è diverso da tutti i numeri α_i della successione (*). Di conseguenza l'insieme dei numeri reali compresi tra 0 e 1 non è numerabile.
In questa dimostrazione c'è un piccolo 'errore'. Infatti certi numeri possono avere diversi sviluppi decimali o avendo 0 come periodo o avendo 9 come periodo; per esempio

$$\frac{1}{2} = 0{,}5000 \dots = 0.4999 \dots$$

Dunque se i numeri sono rappresentati da sviluppi decimali distinti, non è detto che siano diversi. Allora è necessario costruire il numero β con più prudenza, evitando le cifre 0 e 9; per esempio, ponendo $b_n = 2$ per $a_{nn} = 1$ e $b_n = 1$ per $a_{nn} \neq 1$, la dimostrazione è corretta.

La potenza dei numeri reali, superiore alla potenza del numerabile, viene detta potenza del continuo e si indica con c:

$$\boxed{\mathrm{pot}\mathbb{R} = c > \aleph_0}$$

Abbiamo allora trovato un insieme con potenza superiore a quella del numerabile.
Esistono insiemi la cui potenza è compresa tra $\aleph_0$ e c?

Cantor ha supposto che tali insiemi non esistono: questa ipotesi viene chiamata in matematica

$\boxed{\textbf{ipotesi del continuo}}$

Solo recentemente [7] sono stati considerati degli insiemi che non soddisfano a tale ipotesi; la teoria degli insiemi che ne è risultata viene chiamata teoria non cantoriana degli insiemi. L'analisi matematica che è stata sviluppata su tali insiemi numerici viene chiamata analisi non standard.

Note bibliografiche

[1] Corrado Mangione : "*Logica e problemi dei fondamenti nella seconda metà dell'Ottocento*" in L: Geymonat, *Storia del pensiero filosofico e scientifico*, Garzanti, 1971, Vol. V, pp. 755-764.

[2] Gabriele Lolli : "*Nuovi modelli del sistema dei numeri reali*" in "*Le Scienze*", n. 48, Agosto 1972, p. 87 e segg..

[3] Friederich Waismann : *Introduzione al pensiero matematico*, Boringhieri, 1968, p. 203

[4] Gabriele Lolli : op. cit., p. 87

[5] B. D'Amore – M.L.M. Matteuzzi : *Dal Numero alla struttura – Breve storia della matematica moderna*, Zanichelli, 1975, p. 82

[6] *Ibidem*, pp. 85-87

[7] P.J.Cohen – R. Hersh : "*La teoria non cantoriana degli insiemi*" in "*Le Scienze*", n. 1, Settembre 1968, pp. 86 e segg.