

# I numeri reali secondo Cantor

Stefania Gabelli

Dipartimento di Matematica, Università degli Studi Roma Tre  
Largo San L. Murialdo, 1 - 00146 Roma, Italy

e-mail: [gabelli@mat.uniroma3.it](mailto:gabelli@mat.uniroma3.it)

29 novembre 2011

## Indice

<b>1</b>	<b>Campi ordinati</b>	<b>4</b>
1.1	Campi ordinati completi . . . . .	5
1.2	Successioni convergenti . . . . .	7
1.3	Successioni di Cauchy . . . . .	9
<b>2</b>	<b>La costruzione del campo reale secondo Cantor</b>	<b>11</b>
2.1	Completamento di un campo ordinato . . . . .	11
2.2	Unicità del campo reale . . . . .	17
<b>3</b>	<b>Numeri decimali</b>	<b>18</b>
3.1	Rappresentazione di un numero reale in base $b$ . . . . .	19
3.2	Numeri periodici . . . . .	21
3.3	Unicità della rappresentazione in base $b$ . . . . .	23
<b>4</b>	<b>Numeri irrazionali</b>	<b>25</b>
4.1	Numeri trascendenti . . . . .	26
<b>5</b>	<b>La cardinalità del continuo</b>	<b>29</b>
5.1	La cardinalità di un insieme . . . . .	29
5.2	La cardinalità del numerabile . . . . .	31
5.3	La cardinalità del continuo . . . . .	34

## Introduzione

Fino alla metà dell'Ottocento il concetto di numero reale coincideva con il concetto di *misura di grandezze* ed era fondato sull'intuizione geometrica della continuità della retta.

Si fa risalire alla Scuola Pitagorica la scoperta che esistono segmenti, come ad esempio il lato e la diagonale di un quadrato, che sono *incommensurabili*, cioè che non possono essere contemporaneamente multipli interi di alcun segmento che venga assunto come unità di misura. Anche se gli antichi non consideravano le misure di segmenti come numeri, ai fini pratici operavano con esse come se lo fossero: dal punto di vista sintetico secondo le regole della *Teoria delle Proporzioni Geometriche* dovuta ad Eudosso di Cnido e codificata nel V Libro degli *Elementi* di Euclide e dal punto di vista analitico con metodi di approssimazione risalenti ai Babilonesi.

Non ci furono progressi significativi nella conoscenza dei numeri reali fino alla metà del Cinquecento, quando, con l'introduzione del formalismo algebrico, soprattutto ad opera di R. Bombelli (*Algebra*, 1572), fu possibile definire i rapporti di grandezze e le operazioni algebriche mediante simboli. Questo favorì una rilettura più moderna della *Teoria delle Proporzioni* ed una più rigorosa definizione geometrica del campo dei numeri reali. Tale punto di vista portò successivamente alla nascita della Geometria Analitica, attraverso l'opera di R. Descartes, ed alla nascita del Calcolo Infinitesimale, attraverso l'opera di I. Newton e G. W. Leibniz.

Fino a tutto il Settecento questi rami della matematica rimasero strettamente connessi, proprio in virtù del fatto che le grandezze, cioè gli oggetti dell'indagine geometrica, venivano identificate con le loro misure, cioè con gli oggetti del calcolo infinitesimale. La costruzione rigorosa del sistema dei numeri reali fu uno dei progressi più importanti del pensiero matematico del XIX secolo e segnò l'indipendenza dell'Analisi dalla Geometria.

L'obiettivo di definire in modo preciso i numeri reali fu contemporaneamente e indipendentemente raggiunto da diversi matematici con la pubblicazione tra il 1872 e il 1886 di una serie di lavori in cui venivano espone essenzialmente tre diverse costruzioni: la costruzione di Dedekind-Tannery, che riprendeva e formalizzava la Teoria delle Proporzioni di Eudosso, la costruzione di Meray-Weierstrass, in cui i numeri reali sono definiti attraverso successioni monotone di intervalli, e la costruzione di Heine-Cantor, in cui i numeri reali sono classi di equivalenza di successioni di Cauchy di numeri razionali.

In queste note illustreremo la costruzione di Cantor ed alcune proprietà algebriche dei numeri reali.

# 1 Campi ordinati

Ricordiamo per cominciare alcune nozioni sui campi ordinati. Faremo liberamente uso delle proprietà elementari delle relazioni di ordine.

Un *campo ordinato* è un campo  $K$  in cui è definita una relazione di ordinamento totale, denotata con  $\geq$ , compatibile con le operazioni, nel senso che:

- (a) Due elementi  $\alpha, \beta \in K$  sono sempre confrontabili, cioè  $\alpha \geq \beta$ , oppure  $\beta \geq \alpha$ ;
- (b) Dati  $\alpha, \beta, \gamma, \delta \in K$ , se  $\alpha \geq \beta$  e  $\gamma \geq \delta$ , allora

$$\alpha + \gamma \geq \beta + \delta; \quad \alpha\gamma \geq \beta\delta.$$

Se  $\alpha \geq \beta$  e  $\alpha \neq \beta$ , scriveremo  $\alpha > \beta$ .

Un elemento  $\alpha$  di un campo ordinato  $K$  si dice *positivo* se  $\alpha > 0$  e si dice *negativo* se  $\alpha < 0$ . Notiamo che  $\alpha$  è positivo se e soltanto se  $-\alpha$  è negativo. Infatti

$$0 > \alpha \quad \Leftrightarrow \quad 0 - \alpha = -\alpha > \alpha - \alpha = 0.$$

Denotiamo con  $P$  l'insieme degli elementi positivi di  $K$  e con  $-P$  l'insieme degli elementi negativi. Osserviamo che  $P$  è non vuoto e che somma e prodotto di elementi positivi sono ancora elementi positivi. Inoltre, poiché la relazione di ordine è totale, si ha che

$$P \cap -P = \emptyset; \quad K = P \cup \{0\} \cup -P.$$

Viceversa se  $K$  ha un sottoinsieme non vuoto  $P$  stabile rispetto all'addizione e alla moltiplicazione e tale che, per ogni  $\alpha \neq 0$ ,  $\alpha \in P$  se e soltanto se  $-\alpha \notin P$ , allora possiamo definire in  $K$  un ordinamento totale ponendo

$$\alpha \geq \beta \quad \Leftrightarrow \quad \alpha = \beta \quad \text{oppure} \quad \alpha - \beta \in P.$$

Quindi, se  $K$  è un campo ordinato, il suo ordinamento è univocamente determinato dall'insieme degli elementi positivi.

Si verifica facilmente che in un campo ordinato  $K$  vale la *regola del segno*, cioè il prodotto di due elementi positivi o di due elementi negativi è positivo, mentre il prodotto di un elemento positivo e uno negativo è negativo. Questo ci assicura che  $\alpha^2 > 0$  per ogni  $\alpha \neq 0$  e in particolare  $1 = 1^2 > 0$ . Inoltre, se  $\alpha \neq 0$ , allora  $\alpha$  e  $\alpha^{-1}$  sono entrambi positivi o negativi e, se  $\alpha \geq \beta > 0$ , allora  $\beta^{-1} \geq \alpha^{-1}$ .

Un ordinamento di  $K$  si dice *archimedeo* se, dati comunque due elementi  $\alpha, \beta > 0$ , esiste un numero intero positivo  $n$  tale che  $n\beta > \alpha$  e  $K$  si dice *archimedeo* se il suo ordinamento è archimedeo. Se  $K$  è archimedeo, ogni

suo elemento positivo  $\alpha$  è strettamente minore di qualche numero naturale  $n > 0$  (basta porre  $\beta = 1$ ); perciò, scegliendo  $n := m + 1$  come il minimo intero strettamente maggiore di  $\alpha$ , risulta  $m \leq \alpha < m + 1$ . Inoltre, per ogni elemento  $\alpha \in K$  e per ogni  $n > 0$ , esiste  $m \in \mathbb{Z}$  tale che  $\frac{m}{n} \leq \alpha < \frac{m+1}{n}$ . Infatti  $m \leq |n\alpha| < m + 1$  per qualche  $m > 0$ .

**Esempio 1.1** Il campo  $\mathbb{Q}$  dei numeri razionali è un campo ordinato secondo l'ordinamento naturale indotto da quello dei numeri interi. Precisamente, per  $a, b, c, d \in \mathbb{Z}$ , si ha

$$\frac{a}{b} \geq \frac{c}{d} \Leftrightarrow ad - bc \geq 0.$$

Inoltre questo ordinamento è l'unico possibile. Infatti, in ogni ordinamento di  $\mathbb{Q}$  deve essere  $1 > 0$  e allora, per induzione, si ottiene che l'insieme dei numeri interi positivi in questo ordinamento coincide con l'insieme dei numeri naturali.

Inoltre  $\mathbb{Q}$  è archimedeo. Per verificare questa proprietà, basta osservare che possiamo sempre ridurre due frazioni a comune denominatore; così che basta dimostrare che, dati  $a, b > 0$  in  $\mathbb{Z}$ , si ha  $nb > a$  per qualche  $n \geq 1$ . Fissato  $a$ , questo si può facilmente dimostrare per induzione su  $b$ .

Un campo ordinato  $K$  ha necessariamente caratteristica zero. Infatti la somma di due numeri positivi è un numero positivo e quindi non può essere uguale a zero. Quindi  $\mathbb{Q}$  è contenuto isomorficamente in  $K$ . Inoltre l'ordinamento di  $K$  ristretto a  $\mathbb{Q}$  coincide con l'ordinamento naturale.

Un sottoinsieme  $S$  di un campo ordinato  $K$  si dice *denso* in  $K$  se, comunque scelti due elementi  $\alpha > \beta$  di  $K$ , esiste  $\gamma \in S$  tale che  $\alpha > \gamma > \beta$ .

**Proposizione 1.2** *Un campo ordinato  $K$  è archimedeo se e soltanto se  $\mathbb{Q}$  è denso in  $K$ .*

**Dimostrazione:** Supponiamo che  $\mathbb{Q}$  sia denso in  $K$  e siano  $\alpha, \beta \in K$  due elementi positivi. Allora esistono due numeri razionali  $x, y$  tali che  $\alpha > x > 0$  e  $y > \beta$ . Poiché  $\mathbb{Q}$  è archimedeo, esiste  $n \geq 0$  tale che  $nx > y$ . Dunque  $n\alpha > nx > y > \beta$ .

Viceversa, sia  $K$  un campo ordinato archimedeo e siano  $\alpha > \beta$  due elementi di  $K$ . Allora per qualche  $n \geq 0$ ,  $n > (\alpha - \beta)^{-1}$  e quindi  $\alpha > \beta + \frac{1}{n}$ . D'altra parte, esiste  $m \in \mathbb{Z}$  tale che  $\frac{m+1}{n} > \beta \geq \frac{m}{n}$ . In conclusione,  $\alpha > \beta + \frac{1}{n} \geq \frac{m+1}{n} > \beta$ .

## 1.1 Campi ordinati completi

Dato un campo ordinato  $K$ , un suo sottoinsieme non vuoto  $S$  si dice *limitato superiormente*, se esiste un maggiorante comune di ogni elemento di  $S$ , cioè se esiste un elemento  $\mu$  tale che  $\alpha \leq \mu$  per ogni  $\alpha \in S$ . In questo caso,

può accadere che esista un più piccolo maggiorante comune (necessariamente unico), che si chiama l'*estremo superiore* di  $S$ . Se l'estremo superiore si  $S$  appartiene ad  $S$ , esso si chiama anche il *massimo* di  $S$ . Analogamente,  $S$  si dice *limitato inferiormente* se esiste un minorante comune di ogni suo elemento. Se esiste un più grande minorante comune (necessariamente unico), esso si chiama l'*estremo inferiore* di  $S$  e, se appartiene ad  $S$ , si chiama anche il *minimo* di  $S$ . Se  $S$  è limitato sia superiormente che inferiormente, diremo semplicemente che esso è *limitato*.

Se  $K$  è un campo ordinato, il *valore assoluto* di  $\alpha \in K$  è l'elemento  $|\alpha| \geq 0$  definito da  $|\alpha| = \alpha$  se  $\alpha \geq 0$  e  $|\alpha| = -\alpha$  se  $\alpha < 0$ . Usando il fatto che  $|\alpha|$  è l'unico elemento non negativo di  $K$  il cui quadrato è uguale ad  $\alpha^2$ , si verifica facilmente che:

$$|\alpha\beta| = |\alpha||\beta|, \quad |\alpha + \beta| \leq |\alpha| + |\beta| \quad (\text{Disuguaglianza Triangolare}).$$

È anche facile verificare che  $|\alpha| \leq \beta$  se e soltanto se  $-\beta \leq \alpha \leq \beta$ . Analogamente,  $|\alpha - \beta| \leq \gamma$  se e soltanto se  $\beta - \gamma \leq \alpha \leq \beta + \gamma$ . Usando ciò, possiamo notare che un sottoinsieme  $S$  di  $K$  è limitato se e soltanto se esiste un elemento  $\gamma$  tale che  $|\alpha| \leq \gamma$  per ogni  $\alpha \in S$ .

Un campo ordinato  $K$  si dice *completo* se ogni suo sottoinsieme non vuoto limitato superiormente ha un estremo superiore. Ciò equivale a dire che ogni suo sottoinsieme non vuoto limitato inferiormente ha un estremo inferiore. Infatti notiamo che l'insieme  $S$  è limitato superiormente se e soltanto se l'insieme  $-S := \{-\alpha; \alpha \in S\}$  è limitato inferiormente. Inoltre, se  $\mu$  è l'estremo superiore di  $S$ , allora  $-\mu$  è l'estremo inferiore di  $-S$ .

**Esempio 1.3** Il campo  $\mathbb{Q}$  dei numeri razionali non è completo.

Consideriamo ad esempio l'insieme  $S := \{\alpha \in \mathbb{Q}; \alpha \geq 0 \text{ e } \alpha^2 \leq 2\}$ . Allora  $S$  è non vuoto ( $0 \in S$ ) ed limitato superiormente (ad esempio da 2), ma non ha un estremo superiore. Per vedere questo, osserviamo intanto che il polinomio  $X^2 - 2$  è irriducibile su  $\mathbb{Q}$  per il criterio di Eisenstein e quindi non esistono numeri razionali il cui quadrato è uguale a 2.

Sia  $\mu \in \mathbb{Q}$ ,  $\mu > 0$ . Se  $\mu^2 < 2$ , allora  $2 - \mu^2 > 0$ . Sia  $n$  un intero positivo tale che  $n > (2\mu + 1)/(2 - \mu^2)$  ( $n$  esiste per la proprietà archimedea). Allora

$$\left(\mu + \frac{1}{n}\right)^2 = \mu^2 + \frac{2\mu}{n} + \frac{1}{n^2} \leq \mu^2 + \frac{2\mu}{n} + \frac{1}{n}.$$

Per la scelta di  $n$ ,  $\frac{2\mu+1}{n} < 2 - \mu^2$ ; quindi  $(\mu + \frac{1}{n})^2 < 2$ . Ne segue che  $\mu < \mu + \frac{1}{n} \in S$  e perciò  $\mu$  non è un maggiorante di  $S$ .

Se  $\mu^2 > 2$ ,  $\mu$  è un maggiorante di  $S$ . Sia  $n$  tale che  $\frac{1}{n} < \frac{\mu^2 - 2}{2\mu}$ , così che anche  $\mu - \frac{1}{n} > 0$  ( $n$  esiste per la proprietà archimedea). Allora

$$\left(\mu - \frac{1}{n}\right)^2 = \mu^2 - \frac{2\mu}{n} + \frac{1}{n^2} > \mu^2 - \frac{2\mu}{n}.$$

Per la scelta di  $n$ ,  $\frac{2\mu}{n} < \mu^2 - 2$ ; quindi  $(\mu - \frac{1}{n})^2 > 2$ . Questo implica che  $\mu - \frac{1}{n}$  è ancora un maggiorante per  $S$  e quindi  $\mu$  non è un estremo superiore di  $S$ .

## 1.2 Successioni convergenti

Se  $A$  è un insieme, una *successione* di elementi di  $A$ , o a valori in  $A$ , è una funzione di insiemi  $\mathbb{N} \rightarrow A$  e si indica usualmente con le notazioni

$$(a_0, a_1, \dots, a_n, \dots), \quad (a_i)_{i \geq 0}, \quad (a_i).$$

Una successione  $\alpha := (\alpha_i)$  a valori in un campo ordinato  $K$  si dice *crescente* (rispettivamente *decrescente*) se  $\alpha_i \leq \alpha_{i+1}$  (rispettivamente  $\alpha_i \geq \alpha_{i+1}$ ), per ogni  $i \geq 0$ . Per indicare che  $\alpha$  è crescente oppure decrescente, diremo che  $\alpha$  è una *successione monotona*. La successione  $\alpha := (\alpha_i)$  è contemporaneamente crescente e decrescente se e soltanto se è *costante*, cioè se  $\alpha_i = \alpha$  per qualche  $\alpha \in K$  e ogni  $i \geq 0$ . Nel seguito, denoteremo la successione costante in cui  $\alpha_i = \alpha$ , per ogni  $i \geq 0$ , con il simbolo  $(\alpha)$ .

Una *sottosuccessione* di  $\alpha := (\alpha_i)$  è una successione  $(\alpha_{i_0}, \alpha_{i_1}, \dots, \alpha_{i_n}, \dots)$  con  $i_0 < i_1 < \dots < i_n < \dots$ .

**Proposizione 1.4** *Sia  $K$  un campo ordinato. Allora ogni successione di elementi di  $K$  ha una sottosuccessione monotona.*

**Dimostrazione:** Sia  $\alpha := (\alpha_i)$  una successione di elementi di  $K$ . Se esistono infiniti indici  $k$  tali che  $\alpha_n \geq \alpha_k$  per ogni  $n \geq k$ , allora gli  $\alpha_k$  formano una sottosuccessione crescente di  $\alpha$ . Altrimenti, esiste un massimo indice  $k$  tale che  $\alpha_n \geq \alpha_k$  per ogni  $n \geq k$ . Poniamo  $\alpha_{i_0} = \alpha_{k+1}$ . Allora esiste  $i_1 > i_0$  tale che  $\alpha_{i_0} > \alpha_{i_1}$ . Di nuovo, essendo  $i_1 > k$ , esiste  $i_2 > i_1$  tale che  $\alpha_{i_1} > \alpha_{i_2}$ . Così proseguendo, per ricorsione otteniamo una sottosuccessione decrescente  $(\alpha_{i_j})$  di  $\alpha$ .

Per semplicità di notazione, diremo talvolta che una proprietà  $P$  relativa ai numeri naturali vale per  $n$  *abbastanza grande* (e scriveremo per  $n \gg 0$ ) se esiste un numero naturale  $N$  tale che  $P(n)$  sia vera per ogni  $n \geq N$ . Questo equivale a dire che  $P(n)$  non è vera al più per un numero finito di valori di  $n$ , infatti al più per  $0 \leq n < N$ .

Notiamo che, se  $P_1, \dots, P_n$  sono un numero finito di proprietà che valgono ciascuna per  $n$  abbastanza grande, supponiamo per  $n \geq N_i$  rispettivamente, allora esse valgono simultaneamente per  $n$  abbastanza grande. Infatti valgono tutte per  $n \geq N$ , dove  $N$  è il massimo degli  $N_i$ .

Si dice che la successione  $\alpha := (\alpha_i)$  è *convergente* in  $K$  e *converge a*  $\lambda$  se esiste un elemento  $\lambda \in K$  tale che, dato comunque un elemento positivo  $\epsilon \in K$ , si ha

$$|\lambda - \alpha_n| \leq \epsilon$$

per  $n \gg 0$ . Se tale elemento esiste, esso è unico e si chiama il *limite* della successione. Infatti se anche  $\nu \in K$  è tale che  $|\nu - \alpha_n| \leq \epsilon$  per  $n \gg 0$ , allora

$$|\lambda - \nu| = |\lambda - \alpha_n + \alpha_n - \nu| \leq |\lambda - \alpha_n| + |\alpha_n - \nu| \leq 2\epsilon$$

per ogni  $\epsilon \in K$  positivo. Dunque  $\lambda - \nu = 0$ , cioè  $\lambda = \nu$ . Se  $\lambda$  è il limite della successione  $\alpha := (\alpha_i)$ , scriveremo

$$\lim_{n \rightarrow \infty} \alpha_n = \lambda.$$

È ovvio che ogni successione costante  $(\alpha)$  è convergente ed ha limite  $\alpha$ .

**Proposizione 1.5** *Sia  $K$  un campo ordinato e  $\alpha := (\alpha_i)$  una successione crescente (rispettivamente decrescente) di elementi di  $K$ . Allora  $\alpha$  è convergente in  $K$  se e soltanto se l'insieme  $\{\alpha_i\}$  ha un estremo superiore (rispettivamente inferiore)  $\mu \in K$ . In questo caso,  $\mu$  è il limite di  $\alpha$ .*

**Dimostrazione:** Sia  $\alpha := (\alpha_i)$  una successione crescente di elementi di  $K$  e sia  $\mu$  l'estremo superiore dell'insieme  $\{\alpha_i\}$ . Allora, dato  $\epsilon > 0$ ,  $\mu - \frac{1}{2}\epsilon$  non è un estremo superiore. Perciò esiste  $N \in \mathbb{N}$  tale che  $\mu - \frac{1}{2}\epsilon \leq \alpha_N \leq \mu$  e, per  $n \geq N$ ,  $\mu - \frac{1}{2}\epsilon \leq \alpha_N \leq \alpha_n \leq \mu$ . Ne segue che, per  $n \geq N$ ,  $0 \leq \mu - \alpha_n \leq \frac{1}{2}\epsilon < \epsilon$ . In conclusione  $\mu$  è il limite della successione  $\alpha := (\alpha_i)$ .

Viceversa, sia  $\lambda$  il limite di  $\alpha := (\alpha_i)$ . Allora, poiché la successione è crescente,  $\lambda$  è un maggiorante per l'insieme  $\{\alpha_i\}$ . Se esiste  $\mu \in K$  tale che  $\alpha_i \leq \mu \leq \lambda$  per ogni  $i \geq 0$ , dato  $\epsilon > 0$ , si ha  $|\mu - \alpha_n| \leq |\lambda - \alpha_n| \leq \epsilon$  per  $n \gg 0$ . Allora  $\mu = \lambda$  e  $\lambda$  è l'estremo superiore dell'insieme  $\{\alpha_i\}$ .

Analogamente, si ottiene che se  $\alpha$  è una successione decrescente, limite ed estremo inferiore, se esistono, coincidono.

**Proposizione 1.6** *Sia  $K$  un campo ordinato. Se ogni successione crescente a valori in  $K$  limitata superiormente è convergente, allora  $K$  è archimedeo.*

**Dimostrazione:** Se  $K$  non è archimedeo, esistono  $\alpha, \beta \in K$ ,  $\alpha, \beta > 0$ , tali che,  $n\alpha \leq \beta$ , per ogni  $n \geq 0$ . Allora l'insieme  $\{n\alpha\}$  è limitato superiormente. D'altra parte  $(n\alpha)_{n \geq 0}$  è una successione crescente e quindi converge a qualche  $\lambda$ . Allora  $\lambda - \alpha < n\alpha < \lambda$  per  $n \gg 0$ . Questo non è possibile, perché tale disuglianza può essere soddisfatta soltanto per un unico numero intero  $n$ .

**Proposizione 1.7** *Ogni campo ordinato completo è archimedeo. Quindi  $\mathbb{Q}$  è denso in ogni campo ordinato completo.*

**Dimostrazione:** Per la Proposizione 1.5, in un campo ordinato completo  $K$  ogni successione crescente limitata superiormente è convergente. Quindi  $K$  è archimedeo per la Proposizione 1.6 e  $\mathbb{Q}$  è denso in  $K$  per la Proposizione 1.2.

### 1.3 Successioni di Cauchy

Vogliamo ora mostrare che la proprietà di completezza di un campo ordinato si può esprimere in modo equivalente attraverso il concetto di *successione di Cauchy* (o *successione fondamentale*).

Una successione  $\alpha := (\alpha_i)$  a valori in un campo ordinato  $K$  si chiama una *successione di Cauchy* o una *successione fondamentale* se, per ogni elemento positivo  $\epsilon \in K$ , esiste un numero intero positivo  $N := N(\epsilon)$  tale che

$$|\alpha_n - \alpha_m| < \epsilon \quad \text{per ogni } n, m \geq N.$$

Ricordiamo che se  $K$  è archimedeo, in particolare è completo, ogni suo elemento è minorato da un numero razionale. In questo caso quindi, per verificare che una successione è convergente o è di Cauchy basta assumere che  $\epsilon$  sia razionale.

I prossimi due risultati mostrano che le successioni di Cauchy si collocano tra le successioni convergenti e le successioni limitate.

**Proposizione 1.8** *Sia  $K$  un campo ordinato. Ogni successione convergente di elementi di  $K$  è una successione di Cauchy.*

**Dimostrazione:** Sia  $\alpha := (\alpha_i)$  una successione convergente e sia  $\lambda$  il suo limite. Allora dato un elemento positivo  $\epsilon$ , per  $n, m$  abbastanza grandi risulta  $|\alpha_n - \lambda| < \frac{1}{2}\epsilon$  e  $|\alpha_m - \lambda| < \frac{\epsilon}{2}$ . Da cui

$$|\alpha_n - \alpha_m| = |\alpha_n - \lambda + \lambda - \alpha_m| \leq |\alpha_n - \lambda| + |\alpha_m - \lambda| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Quindi  $\alpha$  è una successione di Cauchy.

**Proposizione 1.9** *Sia  $K$  un campo ordinato e sia  $\alpha := (\alpha_i)$  un successione di Cauchy a valori in  $K$ . Allora esiste un elemento positivo  $C \in K$  tale che  $|\alpha_n| \leq C$  per ogni  $n \geq 0$ .*

**Dimostrazione:** Sia  $N$  un numero intero positivo tale che  $|\alpha_n - \alpha_N| \leq 1$ , per tutti gli  $n \geq N$ ; così che  $|\alpha_n| \leq |\alpha_N| + 1$ , per tutti gli  $n \geq N$ . Allora basta scegliere  $C$  come il massimo tra  $|\alpha_1|, |\alpha_2|, \dots, |\alpha_{N-1}|, |\alpha_N| + 1$ .

Possiamo ora finalmente caratterizzare i campi ordinati completi come i campi ordinati archimedei in cui ogni successione di Cauchy è convergente.

**Teorema 1.10** *Sia  $K$  un campo ordinato. Le seguenti condizioni sono equivalenti:*

- (i)  $K$  è completo, cioè ogni suo sottoinsieme non vuoto limitato superiormente (inferiormente) ha un estremo superiore (inferiore);

- (ii) Ogni successione crescente (decrecente) di elementi di  $K$  limitata superiormente (inferiormente) è convergente;
- (iii)  $K$  è archimedeo ed ogni successione di Cauchy a valori in  $K$  è convergente.
- (iv)  $K$  è archimedeo ed ogni successione di Cauchy a valori in  $\mathbb{Q}$  ha un limite in  $K$ .

**Dimostrazione:** (i)  $\Rightarrow$  (ii) segue dalla Proposizione 1.5.

(ii)  $\Rightarrow$  (iii)  $K$  è archimedeo per la Proposizione 1.6. Sia  $\alpha := (\alpha_i)$  una successione di Cauchy a valori in  $K$ . Per la Proposizione 1.4, possiamo considerare una sottosuccessione monotona  $(\alpha_{i_j})$  di  $\alpha$ . Poiché  $\alpha$  è limitata (Proposizione 1.9), anche tale sottosuccessione lo è; quindi essa per ipotesi converge ad un limite  $\lambda$ . Mostriamo anche  $\alpha$  converge a  $\lambda$ . Poiché  $\alpha$  è una successione di Cauchy, dato in  $K$  un elemento  $\epsilon > 0$ , si ha  $|\alpha_m - \alpha_n| < \frac{1}{2}\epsilon$  per  $n \gg 0$ . D'altra parte, per  $t \gg 0$  si ha anche  $|\alpha_t - \lambda| < \frac{1}{2}\epsilon$ . Quindi, per  $n \gg 0$ ,

$$|\alpha_n - \lambda| \leq |\alpha_n - \alpha_t| + |\alpha_t - \lambda| < \epsilon.$$

(iii)  $\Rightarrow$  (iv) è evidente.

(iv)  $\Rightarrow$  (i) Sia  $S \subseteq K$  un sottoinsieme non vuoto limitato superiormente e sia  $M$  un suo maggiorante. Poiché  $K$  è archimedeo, dato  $s \in S$ , esiste un intero  $m$  tale che  $m > -s$ , così che  $-m < s < M$ . Per ogni fissato  $n \geq 0$ , sia  $\{\frac{k}{2^n}\}$  l'insieme finito delle frazioni tali che  $-m \leq \frac{k}{2^n} \leq M$  e sia  $x_n := \frac{k_n}{2^n}$  la più piccola di queste frazioni che è un maggiorante per  $S$ . Allora  $x_n - \frac{1}{2^n}$  non è un maggiorante per  $S$  e quindi per ogni  $p > n$  risulta

$$x_n - \frac{1}{2^n} < x_p,$$

infatti  $x_p$  è un maggiorante di  $S$ . D'altra parte,  $x_p \leq x_n$ , altrimenti,  $x_p := \frac{k_p}{2^p} > x_n := \frac{k_n}{2^n} = \frac{2^{p-n}k_p}{2^p}$ , contro la minimalità di  $x_p$  nell'insieme  $\{\frac{k}{2^p}\}$ . Allora  $|x_p - x_n| < \frac{1}{2^n}$  e, per  $p, q > t$ ,

$$|x_p - x_q| < \frac{1}{2^t}.$$

Questo mostra che la successione decrescente di numeri razionali  $(x_i)$  è una successione di Cauchy. Infatti, dato  $\epsilon > 0$  in  $K$ , per la proprietà archimedeo, possiamo sempre trovare un intero  $h$  tale che  $h > \epsilon^{-1}$  ed inoltre  $h < 2^t$  per qualche intero  $t$ . Dunque, per  $p, q > t \gg 0$ , si ha  $|x_p - x_q| < \frac{1}{2^t} < \epsilon$ . Allora, per ipotesi, la successione  $(x_i)$  converge ad un certo limite  $\lambda \in K$ . Notiamo che, essendo la successione decrescente,  $x_n - \frac{1}{2^n} \leq \lambda \leq x_n$  per  $n \gg 0$  (Proposizione 1.5).

Resta da mostrare che  $\lambda$  è l'estremo superiore di  $S$ . Intanto osserviamo che  $\lambda$  è un maggiorante di  $S$ . Infatti, se  $s > \lambda$  per qualche  $s \in S$ , allora, per

$n \gg 0$ ,  $2^n > (s-\lambda)^{-1}$  da cui  $\frac{1}{2^n} < s-\lambda$  e, poiché  $x_n - \frac{1}{2^n} \leq \lambda$ , addizionando, otteniamo  $x_n < s$ , il che non è possibile perché  $x_n$  è un maggiorante di  $S$ . Poi, se  $\mu$  è un maggiorante e  $\mu < \lambda$ , come prima di nuovo  $\frac{1}{2^n} < s - \lambda$  per qualche  $n \geq 0$ . Poiché  $x_n - \frac{1}{2^n}$  non è un maggiorante, esiste  $s \in S$  tale che  $x_n - \frac{1}{2^n} < s$ , da cui  $x_n - \frac{1}{2^n} < \mu$  ed infine  $x_n < \lambda$ ; il che non può essere.

**Corollario 1.11** *Ogni elemento di un campo ordinato completo è limite di una successione monotona (di Cauchy) di numeri razionali.*

**Dimostrazione:** Sia  $K$  un campo ordinato completo e sia  $x \in K$ . Allora evidentemente  $x$  è l'estremo superiore dell'insieme degli elementi  $s \in K$  tali che  $s \leq x$ . Procedendo come nella dimostrazione del Teorema 1.10 (iv)  $\Rightarrow$  (i), è allora possibile trovare una successione decrescente di numeri razionali il cui limite è  $x$ . Tale successione è necessariamente di Cauchy (Proposizione 1.8).

## 2 La costruzione del campo reale secondo Cantor

In questo paragrafo costruiremo un campo ordinato completo e mostreremo che due campi ordinati completi sono isomorfi secondo un unico isomorfismo di ordine.

Il metodo che useremo è dovuto a G. Cantor e consiste nel costruire un campo ordinato archimedeo in cui tutte le successioni di Cauchy di numeri razionali sono convergenti (Teorema 1.10).

### 2.1 Completamento di un campo ordinato

Se  $K$  è un campo, l'insieme  $\mathcal{S}$  di tutte le successioni a valori in  $K$  è un anello commutativo unitario rispetto alle usuali operazioni di addizione e moltiplicazione tra funzioni a valori in anello, definite nel seguente modo: se  $\alpha := (\alpha_i)$  e  $\beta := (\beta_i)$ , allora

$$\alpha + \beta := (\alpha_i + \beta_i); \quad \alpha\beta := (\alpha_i\beta_i).$$

Lo zero di  $\mathcal{S}$  è la successione costante (0), in cui  $\alpha_i = 0$ , per ogni  $i \geq 0$ , e la successione opposta alla successione  $\alpha = (\alpha_i)$  è la successione  $-\alpha := (-\alpha_i)$ . Inoltre l'unità moltiplicativa di  $\mathcal{S}$  è la successione costante (1), in cui  $\alpha_i = 1$ , per ogni  $i \geq 0$ .

**Lemma 2.1** *Sia  $K$  un campo ordinato. Se  $\alpha := (\alpha_i)$  e  $\beta := (\beta_i)$  sono successioni convergenti a valori in  $K$  con limite  $\lambda$  e  $\mu$  rispettivamente, allora  $-\alpha$ ,  $\alpha + \beta$  e  $\alpha\beta$  sono successioni convergenti con limite  $\lambda$ ,  $\lambda + \mu$  e  $\lambda\mu$  rispettivamente.*

**Dimostrazione:** Che  $-\alpha$  converge a  $\lambda$  segue immediatamente dalla definizione.

Per la somma, dato  $\epsilon \geq 0$ , per  $n \gg 0$ , si ha  $|\lambda - \alpha_n|, |\mu - \beta_n| < \frac{1}{2}\epsilon$ . Allora

$$|(\lambda + \mu) - (\alpha_n + \beta_n)| \leq |\lambda - \alpha_n| + |\mu - \beta_n| < \epsilon.$$

Quanto al prodotto, si ha

$$\begin{aligned} |\lambda\mu - \alpha_n\beta_n| &= |\lambda\mu - \alpha_n\mu + \alpha_n\mu - \alpha_n\beta_n| \\ &\leq |\mu||\lambda - \alpha_n| + |\alpha_n||\mu - \beta_n|. \end{aligned}$$

Ma essendo le successioni convergenti limitate (Proposizioni 1.8 e 1.9), allora  $|\alpha_n| \leq C$  per qualche  $C \geq 0$ . Inoltre, dato  $\epsilon > 0$ , per  $n \gg 0$  risulta  $|\lambda - \alpha_n| < \frac{\epsilon}{2|\mu|}$  e  $|\mu - \beta_n| < \frac{\epsilon}{2C}$ . In conclusione, per  $n \gg 0$ ,

$$\begin{aligned} |\lambda\mu - \alpha_n\beta_n| &\leq |\mu||\lambda - \alpha_n| + |\alpha_n||\mu - \beta_n| \\ &< |\mu|\frac{\epsilon}{2|\mu|} + C\frac{\epsilon}{2C} = \epsilon. \end{aligned}$$

Denotiamo con  $\mathcal{C}$  il sottoinsieme di  $\mathcal{S}$  formato da tutte le successioni di Cauchy. È evidente che  $\mathcal{C}$  contiene tutte le successioni costanti.

**Proposizione 2.2** *Sia  $K$  un campo ordinato. L'insieme  $\mathcal{C}$  di tutte le successioni di Cauchy a valori in  $K$  è un anello, contenente isomorficamente  $K$ .*

**Dimostrazione:** Siano  $\alpha := (\alpha_i)$  e  $\beta := (\beta_i)$  successioni di Cauchy. Segue subito dalla definizione che  $-\alpha := (-\alpha_i)$  è una successione di Cauchy. Mostriamo che anche  $\alpha + \beta$  e  $\alpha\beta$  lo sono, così che  $\mathcal{C}$  è un sottoanello di  $\mathcal{S}$ .

Dato  $\epsilon \geq 0$ , si ha  $|\alpha_m - \alpha_n|, |\beta_m - \beta_n| < \frac{1}{2}\epsilon$  per  $m, n \gg 0$ . Allora, per  $n \gg 0$ ,

$$|(\alpha_m + \beta_m) - (\alpha_n + \beta_n)| \leq |\alpha_m - \alpha_n| + |\beta_m - \beta_n| < \epsilon.$$

Per il prodotto, poiché le successioni di Cauchy sono limitate (Proposizione 1.9), esiste  $C \geq 0$  tale che  $|\alpha_n|, |\beta_n| \leq C$  per ogni  $n \geq 0$ . D'altra parte,  $|\alpha_m - \alpha_n|, |\beta_m - \beta_n| < \frac{1}{2C}\epsilon$  per  $m, n \gg 0$ . Allora

$$\begin{aligned} |\alpha_m\beta_m - \alpha_n\beta_n| &= |\alpha_m(\beta_m - \beta_n) + \beta_m(\alpha_m - \alpha_n)| \\ &\leq |\alpha_m||\beta_m - \beta_n| + |\beta_m||\alpha_m - \alpha_n| < C\frac{\epsilon}{2C} + C\frac{\epsilon}{2C} = \epsilon. \end{aligned}$$

L'applicazione che ad ogni  $\alpha \in K$  associa la successione costante  $(\alpha)$ , in cui  $\alpha_i = \alpha$  per ogni  $i \geq 0$ , è un omomorfismo di anelli non nullo. Dunque  $K$  è contenuto isomorficamente in  $\mathcal{C}$ .

Una successione  $\alpha := (\alpha_i)$  di elementi di  $K$  si dice una *successione nulla* se  $\alpha$  converge a 0. Cioè se, per ogni elemento positivo  $\epsilon \in K$

$$|\alpha_n| < \epsilon$$

per  $n$  abbastanza grande. Notiamo che, per definizione, la successione  $\alpha := (\alpha_i)$  converge al limite  $\lambda \in K$  se e soltanto se la successione  $\alpha - \lambda = (\alpha_i - \lambda)$  è una successione nulla. Inoltre, due successioni convergenti  $\alpha := (\alpha_i)$  e  $\beta := (\beta_i)$  hanno lo stesso limite se e soltanto se la loro differenza  $\alpha - \beta = (\alpha_i - \beta_i)$  è una successione nulla, se e soltanto se, per ogni  $\epsilon > 0$ , risulta  $|\alpha_n - \beta_m| < \epsilon$  per  $n, m \gg 0$ .

Indicheremo con  $\mathcal{N}$  l'insieme delle successioni nulle di elementi di  $K$ .

**Proposizione 2.3** *Sia  $K$  un campo ordinato. L'insieme  $\mathcal{N}$  delle successioni nulle è un ideale dell'anello  $\mathcal{C}$  delle successioni di Cauchy a valori in  $K$ .*

**Dimostrazione:** Le successioni nulle sono successioni di Cauchy (Proposizione 1.8). Inoltre esse formano un sottogruppo additivo di  $\mathcal{C}$  per il Lemma 2.1. Mostriamo che se  $\alpha := (\alpha_i)$ ,  $\beta := (\beta_i) \in \mathcal{N}$  e  $\gamma := (\gamma_i) \in \mathcal{C}$ , allora  $\alpha\gamma \in \mathcal{N}$ .

Poiché le successioni di Cauchy sono limitate (Proposizione 1.9), esiste  $C \geq 0$  tale che  $|\alpha_n| \leq C$  per ogni  $n \geq 0$ . D'altra parte,  $|\beta_n| < \frac{\epsilon}{C}$  per  $n \gg 0$ . Allora  $|\alpha_n\beta_n| = |\alpha_n||\beta_n| < C\frac{\epsilon}{C} = \epsilon$  per  $n \gg 0$ .

Per la proposizione precedente, possiamo considerare l'anello quoziente  $\hat{K} := \mathcal{C}/\mathcal{N}$ , i cui elementi sono le classi modulo  $\mathcal{N}$  delle successioni di Cauchy a valori in  $K$ . Ovvero  $\hat{K} := \{\bar{\alpha} := \alpha + \mathcal{N}; \alpha \in \mathcal{C}\}$ . Per definizione  $\bar{\alpha} = \bar{\beta}$  se e soltanto se  $\alpha - \beta$  è una successione nulla.

Il campo  $K$  è contenuto isomorficamente in  $\hat{K}$  attraverso l'omomorfismo composto  $K \rightarrow \mathcal{C} \rightarrow \hat{K} := \mathcal{C}/\mathcal{N}$  che ad ogni  $\alpha \in K$  associa la successione costante  $(\alpha) \in \mathcal{C}$ , i cui elementi sono tutti uguali ad  $\alpha$ , ed a questa la sua classe modulo  $\mathcal{N}$ . Quindi in ogni classe c'è al più una successione costante. Per semplicità di notazione, denoteremo con  $\bar{\alpha}$  la classe della successione costante  $(\alpha)$ .

Il nostro prossimo passo è mostrare che  $\hat{K}$  è un campo ordinato e che l'immersione  $K \rightarrow \hat{K}$  conserva l'ordinamento.

**Lemma 2.4** *Sia  $K$  un campo ordinato. Se  $\alpha := (\alpha_i)$  è una successione di Cauchy non nulla di elementi di  $K$ , esiste un elemento positivo  $c \in K$  tale che  $|\alpha_n| \geq c$  per  $n$  abbastanza grande.*

**Dimostrazione:** Sia  $\alpha := (\alpha_i)$  una successione di Cauchy e supponiamo che, per ogni  $c > 0$ , esista una sottosuccessione  $(\alpha_{i_j})$  tale che  $|\alpha_{i_j}| < \frac{1}{3}c$ . Per  $m, n \gg 0$  si ha  $|\alpha_m - \alpha_n| \leq \frac{1}{3}c$ , allora per  $m, n_j \gg 0$ ,  $|\alpha_m| \leq |\alpha_m - \alpha_{n_j}| + |\alpha_{n_j}| \leq \frac{2}{3}c$  e dunque  $|\alpha_n| \leq |\alpha_m| + \frac{1}{3}c \leq c$ . Ne segue che  $\alpha := (\alpha_i)$  è una successione nulla.

**Teorema 2.5** *Sia  $K$  un campo ordinato. L'anello quoziente  $\hat{K} := \mathcal{C}/\mathcal{N}$ , i cui elementi sono le classi modulo  $\mathcal{N}$  delle successioni di Cauchy a valori in  $K$ , è un campo.*

**Dimostrazione:** Basta dimostrare che, se  $\alpha := (\alpha_i)$  è una successione di Cauchy non nulla di elementi di  $K$ , esiste una successione di Cauchy  $\beta := (\beta_i)$  tale che  $\alpha\beta - 1 \in \mathcal{N}$ .

Per il Lemma 2.4, esistono un numero intero  $N$  ed un elemento  $c > 0$  tale che  $|\alpha_n| \geq c$  per  $n \geq N$ . Sia  $\beta := (\beta_i)$  la successione definita da  $\beta_i := 1$  per  $i < N$  e  $\beta_i := \alpha_i^{-1}$  per  $i \geq N$ . Allora  $\alpha_n\beta_n = 1$  per  $n \geq N$ , così che  $\alpha\beta - 1 \in \mathcal{N}$ .

Resta da mostrare che  $\beta$  è una successione di Cauchy. Poiché  $|\alpha_n| \geq c$  per  $n \gg 0$ , allora  $|\frac{1}{\alpha_n}| \leq \frac{1}{c}$  per  $n \gg 0$ . D'altra parte, dato  $\epsilon > 0$ , si ha  $|\alpha_n - \alpha_m| \leq \epsilon c^2$  per  $n, m \gg 0$ . Allora

$$|\beta_n - \beta_m| = \left| \frac{1}{\alpha_n} - \frac{1}{\alpha_m} \right| = \left| \frac{\alpha_n - \alpha_m}{\alpha_n \alpha_m} \right| \leq \frac{\epsilon c^2}{c^2} = \epsilon.$$

Per definire un ordinamento totale sul campo  $\hat{K}$ , ricordiamo che un tale ordinamento è univocamente determinato dall'insieme dei suoi elementi positivi.

Diremo che una successione di Cauchy  $\alpha := (\alpha_i)$  a valori in  $K$  è *positiva* se esiste in  $K$  un elemento  $\epsilon > 0$  tale che  $\alpha_n \geq \epsilon$  per  $n$  abbastanza grande e indicheremo con  $P$  l'insieme delle successioni di Cauchy positive. Chiaramente l'insieme  $P$  è non vuoto ed è stabile rispetto all'addizione e alla moltiplicazione, cioè  $P + P \subseteq P$  e  $P \cdot P \subseteq P$ .

Osserviamo che, per ogni successione di Cauchy non nulla  $\alpha := (\alpha_i)$ , si ha  $\alpha \in P$  se e soltanto se  $-\alpha \notin P$ . Infatti, per il Lemma 2.4, esiste un  $\epsilon > 0$  tale che  $|\alpha_n| \geq \epsilon$  per  $n \gg 0$ . Dunque  $\alpha_n \geq \epsilon$  se  $\alpha_n$  è positivo e  $-\alpha_n \geq \epsilon$  se  $\alpha_n$  è negativo. Ma se, per qualche  $m, n$  abbastanza grandi,  $\alpha_n$  è positivo e  $\alpha_m$  è negativo, allora  $\alpha_n - \alpha_m \geq 2\epsilon > 0$ , contro l'ipotesi che  $\alpha$  sia una successione di Cauchy. Quindi  $\alpha \in P$  oppure  $-\alpha \in P$ .

Questo fatto ci dice anche che una successione di Cauchy non nulla  $\alpha$  è positiva se e soltanto se  $\alpha_n > 0$  per  $n \gg 0$ . Infatti, se  $\alpha$  è positiva, per definizione  $\alpha_n$  è positivo per  $n \gg 0$ . Viceversa, se  $\alpha$  non è positiva, allora  $-\alpha$  è positiva, e dunque esiste  $\epsilon > 0$  tale che  $-\alpha_n \geq \epsilon > 0$  per  $n \gg 0$ . Perciò  $\alpha_n < 0$  per  $n \gg 0$ .

**Teorema 2.6** *Se  $K$  è un campo ordinato (rispettivamente, un campo ordinato archimedeo), il campo  $\hat{K}$  è un campo ordinato (rispettivamente, un campo ordinato archimedeo), rispetto all'ordinamento definito da*

$$\bar{\alpha} \geq \bar{\beta} \iff \bar{\alpha} = \bar{\beta} \text{ oppure } \alpha - \beta \in P.$$

*Inoltre l'isomorfismo di  $K$  in  $\hat{K}$  conserva l'ordinamento; cioè, se  $\alpha \geq \beta$  in  $K$ , allora  $\bar{\alpha} \geq \bar{\beta}$  in  $\hat{K}$ .*

**Dimostrazione:** Sia  $\overline{P}$  l'insieme degli elementi di  $\hat{K}$  rappresentati da successioni positive, cioè  $\overline{P} := \{\overline{\alpha}; \alpha \in P\}$ . La definizione è ben posta perché  $P + \mathcal{N} \subseteq P$ . Infatti, se  $\alpha := (\alpha_i) \in P$ , esiste  $\epsilon > 0$  tale che  $\alpha_n \geq \epsilon$  per  $n \gg 0$ . Allora, dato  $\beta := (\beta_i) \in \mathcal{N}$ , si ha  $|\beta_n| \leq \frac{1}{2}\epsilon$  per  $n \gg 0$  e dunque  $\alpha_n + \beta_n \geq |\alpha_n| - |\beta_n| \geq \frac{1}{2}\epsilon$ . Inoltre, per quanto visto sopra, per  $\overline{\alpha} \neq 0$ ,  $\overline{\alpha} \in \overline{P}$  se e soltanto se  $-\overline{\alpha} \notin \overline{P}$ .

Possiamo allora definire un ordinamento totale su  $\mathcal{C}/\mathcal{N}$  ponendo

$$\overline{\alpha} \geq \overline{\beta} \Leftrightarrow \overline{\alpha} = \overline{\beta} \quad \text{oppure} \quad \overline{\alpha} - \overline{\beta} = \overline{\alpha - \beta} \in \overline{P}.$$

Quindi, per definizione,

$$\overline{\alpha} > \overline{\beta} \Leftrightarrow \alpha - \beta \in P \Leftrightarrow \alpha_n - \beta_m > 0 \text{ per } n, m \gg 0.$$

Per ogni  $\alpha \in K$ , se  $\alpha > 0$  allora  $\overline{\alpha} > 0$ . Perciò l'immersione  $\alpha \mapsto \overline{\alpha}$  di  $K$  in  $\hat{K}$  conserva l'ordinamento.

Mostriamo che, se  $K$  è archimedeo, tale ordinamento è archimedeo. Siano  $\overline{\alpha}, \overline{\beta} > 0$  due elementi positivi di  $\hat{K}$ , con  $\alpha := (\alpha_i), \beta := (\beta_i)$ . Per la positività, esiste un elemento positivo  $a \in K$  tale che  $\alpha_n \geq a$  per  $n \gg 0$ , ovvero tale che  $\overline{\alpha} \geq \overline{a} > 0$ . Inoltre, poiché le successioni di Cauchy sono limitate, esiste un elemento positivo  $b \in K$  tale che  $\beta_n \leq b$  per  $n \gg 0$ , cioè tale che  $\overline{\beta} \leq \overline{b}$ . Poiché  $K$  è archimedeo, esiste  $n > 0$  tale che  $na > b$ . Allora  $n\overline{\alpha} \geq n\overline{a} > \overline{b} \geq \overline{\beta}$ .

Notiamo che, essendo  $\hat{K}$  un campo ordinato, ha senso considerare in esso i concetti di valore assoluto, limite, successione di Cauchy, successione nulla ecc.

Identificando gli elementi  $a \in K$  con la loro immagine  $\overline{a} \in \hat{K}$ , il prossimo teorema ci dice che tutte le successioni di Cauchy a valori in  $K$  convergono in  $\hat{K}$ .

**Lemma 2.7** *Sia  $K$  un campo ordinato e sia  $\alpha := (\alpha_i)$  una successione di Cauchy a valori in  $K$ . Se  $C \in K$  è tale che  $|\alpha_n| \leq C$  per  $n \gg 0$ , allora  $|\overline{\alpha}| \leq \overline{C}$ .*

**Dimostrazione:** Se  $\alpha \geq 0$ , allora  $|\alpha| = \alpha$  e bisogna dimostrare che  $\overline{C} - \overline{\alpha} \geq 0$ . Per ipotesi,  $C - \alpha_n \geq 0$ , per  $n \gg 0$ . Ma allora  $\overline{C} - \overline{\alpha} = \overline{(C - \alpha_i)} \geq 0$ , come si voleva. Se  $\overline{\alpha} < 0$ , si considera  $-\overline{\alpha}$ .

**Teorema 2.8** *Sia  $K$  un campo ordinato e sia  $\alpha := (\alpha_i)$  una successione di Cauchy a valori in  $K$ . Allora la successione  $(\overline{\alpha_i})$  converge nel campo  $\hat{K} := \mathcal{C}/\mathcal{N}$  ed il suo limite è  $\overline{\alpha} := \alpha + \mathcal{N}$ .*

**Dimostrazione:** Per ogni intero fissato  $m \geq 0$ , si ha  $\alpha - (\alpha_m) = (\alpha_i - \alpha_m)_{i \geq 0}$  e quindi, passando alle classi,

$$\overline{\alpha} - \overline{\alpha_m} = \overline{\alpha - (\alpha_m)} = \overline{(\alpha_i - \alpha_m)}.$$

Ma, poiché  $\alpha$  è una successione di Cauchy di  $K$ , per ogni elemento positivo  $\epsilon \in K$ , si ha  $|\alpha_n - \alpha_m| < \epsilon$  per  $n, m \gg 0$ . Allora per il Lemma 2.7,

$$|\bar{\alpha} - \bar{\alpha}_m| < \bar{\epsilon}$$

per  $m \gg 0$ . Questo basta per concludere che  $\bar{\alpha} - (\bar{\alpha}_i)$  è la successione nulla, perché ogni elemento positivo di  $\hat{K}$  è minorato per definizione dalla classe di una successione costante ( $\epsilon$ ), per qualche  $\epsilon > 0$  in  $K$ .

**Corollario 2.9** *Se  $K$  è un campo ordinato archimedeo, il campo  $\hat{K}$  è un campo ordinato completo. In particolare,*

- (a) (Teorema dell'estremo superiore) *Ogni sottoinsieme non vuoto di  $\hat{K}$  limitato superiormente (inferiormente) ha un estremo superiore (inferiore);*
- (b) (Teorema di convergenza di Cauchy) *Ogni successione di Cauchy a valori in  $\hat{K}$  è convergente;*
- (c) (Densità di  $\mathbb{Q}$  in  $\hat{K}$ )  *$\mathbb{Q}$  è denso in  $\hat{K}$ ;*
- (d) *Ogni elemento di  $\hat{K}$  è il limite di una successione monotona (di Cauchy) di numeri razionali.*

**Dimostrazione:** Se  $K$  è archimedeo, anche  $\hat{K}$  lo è per il Teorema 2.6. Inoltre ogni successione di Cauchy di numeri razionali è convergente in  $K$  per il Teorema 2.8. Allora  $\hat{K}$  è completo per il Teorema 1.10. (a) e (b) seguono dallo stesso Teorema 1.10 e (d) segue dal Corollario 1.11. (c) segue dal fatto che  $\hat{K}$  è archimedeo e dalla Proposizione 1.2.

Se  $K$  è un campo ordinato archimedeo, il campo ordinato completo  $\hat{K}$  ottenuto con la costruzione precedente, si chiama il *completamento di  $K$  rispetto al valore assoluto*.

Il completamento di  $\mathbb{Q}$  rispetto al valore assoluto si chiama il *campo dei numeri reali* e si indica con  $\mathbb{R}$ . Dunque, secondo questa definizione, i numeri reali sono le classi di successioni di Cauchy a valori razionali modulo l'ideale  $\mathcal{N}$  delle successioni razionali nulle.

**Osservazione 2.10** La costruzione di Cantor si può generalizzare nel seguente modo. Se  $K$  è un campo ordinato, un *valore assoluto su  $K$*  è un'applicazione  $v : K \rightarrow K$  tale che, per ogni  $x, y \in K$ :

- (1)  $v(x) \geq 0$  e  $v(x) = 0 \Leftrightarrow x = 0$ ;
- (2)  $v(xy) = v(x)v(y)$ ;
- (3)  $v(x + y) \leq v(x) + v(y)$ .

Queste proprietà ci permettono di definire le nozioni di *successione di Cauchy* e *successione nulla rispetto a  $v$*  e di costruire il *completamento di*

$K$  rispetto a  $v$  come un anello quoziente, analogamente a quanto abbiamo fatto per il valore assoluto  $v(x) = |x|$ .

Ad esempio, se  $p$  è un numero primo, il *valore assoluto  $p$ -adico* è definito su  $\mathbb{Q}$  nel seguente modo: se  $x \in \mathbb{Q}$  è non nullo e tale che  $x = p^r \frac{a}{b}$ , con  $r \geq 0$  e  $a, b$  numeri interi che non sono divisi da  $p$ , allora  $v_p(x) = \frac{1}{p^r}$ . Inoltre  $v_p(0) = 0$ .

Il completamento di  $\mathbb{Q}$  rispetto al valore assoluto  $p$ -adico si chiama il *campo dei numeri  $p$ -adici* (cf. [3, Chapter 6]).

## 2.2 Unicità del campo reale

Mostriamo ora che un qualsiasi campo ordinato completo è isomorfo a  $\mathbb{R}$ . Questo fatto rende possibile *definire assiomaticamente* il campo dei numeri reali come un campo ordinato completo.

**Lemma 2.11** *Sia  $x$  un numero reale positivo. Allora, per ogni numero intero  $n \geq 2$ , esiste un unico numero reale positivo  $z$  tale che  $z^n = x$ .*

**Dimostrazione:** Si consideri l'insieme  $S = \{y \in \mathbb{R}; y \geq 0, y^n < x\}$ . Allora  $S$  è non vuoto (perché  $0 \in S$ ) ed è limitato superiormente. Infatti, se  $x < 1$ , allora  $S$  è maggiorato da 1, se invece  $x \geq 1$ , allora  $S$  è maggiorato da  $x$  (perché se  $y \geq x$ , allora  $y^n > x$ ). Allora  $S$  ha un (unico) estremo superiore  $z$ , perché  $\mathbb{R}$  è completo, e per la proprietà archimedeica risulta  $z^n = x$ . Infatti, procedendo come nell'Esempio 1.3, si può verificare che, se  $z^n < x$ , esiste un numero intero  $m > 0$  tale che  $(z + \frac{1}{m})^n < x$ , basta ad esempio prendere  $m > ((1+z)^n - z^n)/(x - z^n)$ . Quindi  $z + \frac{1}{m} \in S$ , in contraddizione con il fatto che  $z$  è un maggiorante di  $S$ . Analogamente, se  $z^n > x$ , esiste un numero intero  $m > 0$  tale che  $(z - \frac{1}{m})^n > x$ . Quindi  $z - \frac{1}{m}$  è un maggiorante di  $S$ , in contraddizione con il fatto che  $z$  è l'estremo superiore di  $S$ .

Se  $x$  è un numero reale positivo e  $n \geq 2$ , l'unico numero reale positivo  $z$  tale che  $z^n = x$  si chiama la *radice  $n$ -sima* di  $x$  e si denota con  $\sqrt[n]{x}$ . Se  $n = 2$ , si scrive semplicemente  $z := \sqrt{x}$ .

**Proposizione 2.12** *L'unico automorfismo di  $\mathbb{R}$  è l'identità.*

**Dimostrazione:** Ogni automorfismo  $\varphi$  di  $\mathbb{R}$  è l'identità su  $\mathbb{Q}$ . Infatti, poiché  $\varphi(1) = 1$ , per induzione si ottiene che  $\varphi(n) = n$  per ogni  $n \geq 0$ . Ma ogni numero razionale si può scrivere nella forma  $t = (a - b)/c$ , con  $a, b, c \geq 0$ ; quindi  $\varphi(t) = t$ . Inoltre ogni automorfismo  $\varphi$  mantiene l'ordinamento. Infatti, ogni numero reale non negativo è un quadrato (Lemma 2.11). Dunque, dati  $x, y \in \mathbb{R}$ , se  $x - y \geq 0$ , si ha  $x - y = z^2$  e

$$\varphi(x) - \varphi(y) = \varphi(x - y) = \varphi(z^2) = \varphi(z)^2 \geq 0.$$

Inoltre  $\varphi$  è continuo, cioè, per ogni successione di numeri reali  $(\alpha_i)$ ,

$$\varphi\left(\lim_{n \rightarrow \infty} \alpha_n\right) = \lim_{n \rightarrow \infty} \varphi(\alpha_n).$$

Infatti, per definizione si ha  $\lim_{n \rightarrow \infty} \alpha_n = \lambda$  se e soltanto se, dato un numero razionale  $\epsilon > 0$ ,  $|\lambda - \alpha_n| < \epsilon$  per  $n \gg 0$ . Poiché  $\varphi(|x - y|) = |\varphi(x) - \varphi(y)|$ , allora  $\varphi(|\lambda - \alpha_n|) = |\varphi(\lambda) - \varphi(\alpha_n)| < \varphi(\epsilon) = \epsilon$ , per  $n \gg 0$ , e dunque  $\varphi(\lambda) = \lim_{n \rightarrow \infty} \varphi(\alpha_n)$ . In conclusione, dal momento che ogni numero reale  $x$  è limite di una successione di Cauchy a valori razionali (Corollario 1.11), se  $x = \lim_{n \rightarrow \infty} a_n$  con  $a_n \in \mathbb{Q}$ , si ha

$$\varphi(x) = \lim_{n \rightarrow \infty} \varphi(a_n) = \lim_{n \rightarrow \infty} a_n = x.$$

**Teorema 2.13 (Unicità del campo reale)** *Se  $K$  è un campo ordinato completo, esiste uno e un solo isomorfismo d'ordine  $\mathbb{R} \rightarrow K$ .*

*In particolare, un campo ordinato completo non ha automorfismi non banali.*

**Dimostrazione:** Poiché  $K$  completo, ogni successione di Cauchy a valori in  $\mathbb{Q}$  ha un limite in  $K$  (Teorema 1.10) e ogni elemento  $x \in K$  è limite di una successione di Cauchy  $(a_i)$  a valori razionali (Corollario 1.11). Inoltre, per definizione, due successioni convergenti la cui differenza è una successione nulla hanno lo stesso limite. Allora l'applicazione

$$\varphi : \mathbb{R} \rightarrow K; \quad (a_i) + \mathcal{N} \mapsto \lim_{n \rightarrow \infty} a_n$$

che alla classe di una successione di Cauchy a valori razionali associa il suo limite in  $K$  è ben definita ed è suriettiva. Infine, poiché il limite è compatibile con l'addizione e la moltiplicazione (Lemma 2.1), l'applicazione  $\varphi$  è un omomorfismo non nullo di campi. Quindi  $\varphi$  è un isomorfismo.

Siano poi  $x := \lim_{n \rightarrow \infty} a_n$  e  $y := \lim_{n \rightarrow \infty} b_n$ . Per come è definito l'ordinamento in  $\mathbb{R}$ ,  $(a_i) + \mathcal{N} > (b_i) + \mathcal{N} \Leftrightarrow a_n - b_m > 0$  per  $n, m \gg 0$  (Teorema 2.6). Allora,  $x - y = \lim_{n \rightarrow \infty} (a_n - b_n) > 0$  e  $x > y$ . Perciò  $\varphi$  è un isomorfismo di ordine.

Infine  $\varphi$  è unico perchè l'unico automorfismo di  $\mathbb{R}$  è l'identità (Proposizione 2.12).

### 3 Numeri decimali

Abbiamo visto nei paragrafi precedenti che ogni numero reale  $r \in \mathbb{R}$  è limite di una successione monotona di Cauchy di numeri razionali. Prendendo come modello di  $\mathbb{R}$  il campo  $\hat{\mathbb{Q}}$ , possiamo allora dire che una tale successione rappresenta  $r$  (Teorema 2.8). Vogliamo mostrare ora che, per ogni numero intero  $b \geq 2$ , è sempre possibile rappresentare il numero  $r$  con una successione di frazioni con denominatore uguale a potenze crescenti di  $b$ . Per fare questo, ci possiamo limitare a considerare il caso in cui  $r$  sia positivo.

### 3.1 Rappresentazione di un numero reale in base $b$

Poiché l'ordinamento del campo dei numeri reali è archimedeo, per ogni numero reale  $r$  esiste un più grande intero  $[r]$  minore o uguale a  $r$ . Con questa notazione, possiamo scrivere  $r = [r] + x$ , con  $0 \leq |x| < 1$ . Se  $r \geq 0$ ,  $[r]$  si dice la *parte intera* di  $r$ .

**Proposizione 3.1 (Numerazione in base  $b$ )** *Sia  $b \geq 2$  un intero fissato. Per ogni numero intero  $a \geq 0$ , esistono e sono univocamente determinati dei numeri interi  $a_1, \dots, a_n$  tali che  $0 \leq a_i \leq b - 1$  per  $i = 1, \dots, n$  e*

$$a = a_n b^n + a_{n-1} b^{n-1} + \dots + a_0.$$

**Dimostrazione:** Siano  $q_0$  e  $a_0$  il quoziente e il resto della divisione euclidea di  $a$  per  $b$  e, per  $i \geq 1$ , siano  $q_i$  e  $a_i$  il quoziente e il resto della divisione di  $q_{i-1}$  per  $b$ :

$$\begin{aligned} a &= b q_0 + a_0; & 0 \leq a_0 < b \\ q_{i-1} &= b q_i + a_i; & 0 \leq a_i < b, \quad i \geq 1 \end{aligned}$$

Allora i numeri interi  $a_i$  sono univocamente determinati e  $0 \leq a_i \leq b - 1$ . Notiamo ora che, per ogni  $i \geq 1$ , risulta  $q_i < q_{i-1}$ ; quindi si ha una catena decrescente di numeri interi positivi

$$q_0 > q_1 > \dots > q_i > \dots$$

e perciò esiste un minimo intero  $n \geq 0$  tale che  $q_n = 0$ . Allora, per tale  $n$ ,  $q_{n-1} = a_n$  e, con sostituzioni successive,

$$a = a_n b^n + a_{n-1} b^{n-1} + \dots + a_0.$$

L'espressione  $a = a_n b^n + a_{n-1} b^{n-1} + \dots + a_0$  con  $0 \leq a_i \leq b - 1$  si dice la *rappresentazione di  $a$  in base  $b$*  e si usa scrivere

$$a = (a_n a_{n-1} \dots a_0)_b.$$

Per  $b = 10$ , si ottiene l'usuale rappresentazione decimale di  $a$  e si scrive

$$a = a_n a_{n-1} \dots a_0.$$

**Proposizione 3.2** *Sia  $b \geq 2$  un intero fissato e sia  $r \in \mathbb{R}$  tale che  $0 < r \leq 1$ . Allora esistono dei numeri interi  $d_i$  tali che  $0 \leq d_i < b$  per ogni  $i \geq 1$ , e*

$$r = \frac{d_1}{b} + \frac{d_2}{b^2} + \dots + \frac{d_n}{b^n} + r_n$$

dove  $r_n < \frac{1}{b^n}$ , per ogni  $n \geq 1$ . In particolare, posto

$$S_n := \sum_{i \geq 1}^n \frac{d_i}{b^i} = \frac{a_n}{b^n},$$

la successione  $(S_n)_{n \geq 1}$  è una successione crescente di Cauchy e

$$r = \lim_{n \rightarrow \infty} S_n.$$

**Dimostrazione:** Poniamo  $x_0 := r$  e  $bx_{i-1} := d_i + x_i$ , con  $d_i := \lfloor bx_{i-1} \rfloor$  e  $0 \leq x_i < 1$  per  $i \geq 1$ . Allora  $d_i < b$  (in quanto  $0 < x_i < 1$ ) e  $x_i = \frac{1}{b}(d_{i+1} + x_{i+1})$ , per  $i \geq 0$ . Con sostituzioni successive, otteniamo allora

$$x = \frac{d_1}{b} + x_1 \frac{1}{b} = \frac{d_1}{b} + \frac{d_2}{b^2} + x_2 \frac{1}{b^2} = \dots = S_n + x_n \frac{1}{b^n},$$

per ogni  $n \geq 1$ , dove  $x - S_n = x_n \frac{1}{b^n} < \frac{1}{b^n}$  per ogni  $n \geq 1$ . Quindi  $x = \lim_{n \rightarrow \infty} S_n$ .

Se  $r \in \mathbb{R}$ ,  $0 < r \leq 1$ , è tale che

$$r = \lim_{n \rightarrow \infty} S_n := \lim_{n \rightarrow \infty} \sum_{k \geq 1}^n \frac{d_k}{b^k},$$

scriveremo

$$r = \sum_{k \geq 1} \frac{d_k}{b^k} = \frac{d_1}{b} + \frac{d_2}{b^2} + \frac{d_3}{b^3} + \dots$$

**Teorema 3.3 (Rappresentazione di un numero reale in base  $b$ )** Sia  $b \geq 2$  un intero fissato e sia  $r$  un numero reale positivo. Allora esistono dei numeri interi  $a$  e  $d_i$  tali che  $0 \leq d_i < b$  per ogni  $i \geq 1$ , e

$$r = a + \frac{d_1}{b} + \frac{d_2}{b^2} + \frac{d_3}{b^3} + \dots$$

**Dimostrazione:** Basta scegliere  $a = \lfloor r \rfloor$ , così che  $r = a + x$  con  $0 \leq x < 1$ , e applicare la proposizione precedente a  $x$ .

Dato un numero reale positivo  $r$ , se  $\lfloor r \rfloor = (a_n a_{n-1} \dots a_0)_b$  è la rappresentazione dell'intero  $\lfloor r \rfloor$  in base  $b$  (Proposizione 3.1) e  $\lfloor r \rfloor - r = \sum_{k \geq 1} \frac{d_k}{b^k}$  (Teorema 3.3), si usa scrivere

$$r = (a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_i \dots)_b.$$

Questa espressione si dice una *rappresentazione di  $r$  in base  $b$* .

Una rappresentazione di  $r$  in base 2 si chiama una *rappresentazione binaria* di  $r$ . Per  $b = 10$ , si ottiene l'usuale *rappresentazione decimale* di  $r$  e si scrive semplicemente

$$r = a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_i \dots$$

Le cifre  $d_k$ , per  $k \geq 1$ , si dicono le *cifre decimali* di  $r$  e  $r$ , così rappresentato, si dice un *numero decimale*.

Se esiste un minimo intero  $N \geq 0$  tale che  $d_i = 0$  per  $i \geq N$ , si dice che  $r$  ha una *rappresentazione finita*. In questo caso, in base 10, il numero  $r$  si dice anche un *numero decimale finito*.

Se  $r$  ha una rappresentazione finita, allora

$$r = [r] + \frac{d_1}{b} + \frac{d_2}{b^2} + \cdots + \frac{d_N}{b^N}$$

è razionale. Chiaramente se  $d_k = 0$  per  $k \geq 1$ , ovvero le cifre decimali di  $r$  sono tutte nulle, allora  $r$  è un numero intero.

### 3.2 Numeri periodici

Diremo che la rappresentazione  $r = (a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_i \dots)_b$  di un numero reale  $r$  in base  $b$  è *periodica* se esistono un minimo intero  $N \geq 0$  e un intero  $t \geq 1$  tali che  $d_{N+j} = d_{N+k}$  per  $k \equiv j \pmod{t}$ ; equivalentemente

$$d_{N+j} = d_{N+j+ht} \quad \text{per ogni } h \geq 0 \text{ e } j = 1, \dots, t.$$

In altre parole, una rappresentazione di  $r$  in base  $b$  è periodica se esiste un minimo intero  $N \geq 0$  tale che il gruppo di cifre

$$d_{N+1}, d_{N+2}, \dots, d_{N+t}$$

si ripete indefinitamente. In questo caso, il più piccolo intero  $t$  con questa proprietà si chiama il *periodo* di  $r$ . Inoltre, se  $r$  ha una rappresentazione periodica di periodo  $t$ , si scrive

$$r = (a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}})_b,$$

dove si intende che se  $N = 0$  non compaiono le cifre  $d_1, d_2, \dots, d_N$ . In base 10, si scrive più semplicemente

$$r = a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}}.$$

Le cifre  $d_{N+1}, d_{N+2}, \dots, d_{N+t}$  si dicono le *cifre del periodo*, mentre le cifre  $d_1, d_2, \dots, d_N$  si dicono le *cifre dell'antiperiodo*.

Ogni rappresentazione finita è chiaramente periodica e abbiamo già osservato che ogni numero reale che ha una rappresentazione finita è razionale. Mostriamo ora che più generalmente i numeri razionali si possono caratterizzare come i numeri reali che hanno una rappresentazione periodica (in ogni base  $b$ ).

**Teorema 3.4 (Caratterizzazione dei numeri razionali)** *Un numero reale  $r$  è razionale se e soltanto se, per ogni  $b \geq 2$ , la rappresentazione di  $r$  in base  $b$  è periodica.*

**Dimostrazione:** Supponiamo che  $r$  abbia una rappresentazione periodica di periodo  $t$ . Poiché i numeri interi sono razionali, possiamo supporre che sia

$$r = (0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}})_b.$$

Poiché  $d_{N+j} = d_{N+j+ht}$ , per  $h \geq 0$  e  $j = 1, \dots, t$ , allora, posto  $d_0 = 0$  e ricordando che  $\sum_{k \geq 0} a^k = \frac{1}{1-a}$ , si ha

$$\begin{aligned} r &= \sum_{k=0}^N \frac{d_k}{b^k} + \sum_{h \geq 0} \left( \sum_{j=1}^t \frac{d_{N+j}}{b^{N+j+ht}} \right) \\ &= \sum_{k=0}^N \frac{d_k}{b^k} + \sum_{j=1}^t \frac{d_{N+j}}{b^{N+j}} \left( \sum_{h \geq 0} \frac{1}{b^{ht}} \right) \\ &= \sum_{k=0}^N \frac{d_k}{b^k} + \sum_{j=1}^t \frac{d_{N+j}}{b^{N+j}} \left( \frac{b^t}{b^t - 1} \right). \end{aligned}$$

Perciò  $r$  è razionale.

Viceversa, sia  $r := \frac{u}{v} \in \mathbb{Q}$ , con  $0 < u < v$ . Per determinare una rappresentazione di  $r$  in base  $b$ , come nella dimostrazione del Teorema 3.3, poniamo  $x_0 := r$ ,  $d_0 := 0$  e  $bx_{i-1} := d_i + x_i$ , con  $d_i := \lfloor bx_{i-1} \rfloor$ , per  $i \geq 1$ . Moltiplicando per  $v$ , otteniamo

$$bu = vd_1 + vx_1; \quad bvx_{i-1} = vd_i + vx_i \quad \text{con } 0 \leq vx_i < v \text{ per } i \geq 1.$$

Se  $vx_h = 0$ , per un certo  $h \geq 1$ , allora per ricorsione  $d_m = 0$  per ogni  $m \geq h + 1$ . Altrimenti, poiché i numeri  $vx_i$  sono interi positivi minori di  $v$ , esistono un minimo intero  $N \geq 0$  e un minimo intero positivo  $t \leq v - 1$  tali che  $vx_N = vx_{N+t}$ . Di conseguenza  $d_{N+s} = d_{N+t+s}$ , per ogni  $s \geq 1$ . In definitiva,  $r$  è periodico di periodo  $t$  e risulta

$$r = (0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}})_b.$$

Poiché l'esistenza di una rappresentazione periodica non dipende dalla base scelta, i numeri reali che ammettono una tale rappresentazione si dicono *numeri periodici*.

Come visto nella dimostrazione del Teorema 3.4, se

$$r = 0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}}$$

è un numero decimale periodico, posto  $d_0 = 0$ , risulta

$$r = \sum_{k=0}^N \frac{d_k}{10^k} + \sum_{j=1}^t \frac{d_{N+j}}{10^{N+j}} \left( \frac{10^t}{10^t - 1} \right),$$

per qualche  $N \geq 0$  e  $t \geq 1$ . Svolgendo i calcoli, si ottiene la cosiddetta *frazione generatrice* di  $r$ :

$$\begin{aligned} r &= 0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}} = \\ &= \frac{d_1 \dots d_N d_{N+1} \dots d_{N+t} - d_1 \dots d_N}{10^N (10^t - 1)}. \end{aligned}$$

Si vede subito che la frazione generatrice di un numero decimale periodico  $r := a_n a_{n-1} \dots a_0, d_1 d_2 \dots d_N \overline{d_{N+1} d_{N+2} \dots d_{N+t}}$  è

$$\begin{aligned} a_n a_{n-1} \dots a_0 + \frac{d_1 \dots d_N d_{N+1} \dots d_{N+t} - d_1 \dots d_N}{10^N (10^t - 1)} = \\ \frac{a_n a_{n-1} \dots a_0 d_1 \dots d_N d_{N+1} \dots d_{N+t} - a_n a_{n-1} \dots a_0 d_1 \dots d_N}{10^N (10^t - 1)}. \end{aligned}$$

Usando la frazione generatrice è possibile convertire un numero decimale periodico in una frazione. Ad esempio

$$\begin{aligned} 0, \overline{53} &= \frac{53}{99}; & 0, \overline{59362} &= \frac{59362 - 59}{99900} = \frac{59303}{99900}; \\ 37, \overline{6347495} &= \frac{376347495 - 3763474}{10^5 (10^2 - 1)} = \frac{372584021}{9900000}. \end{aligned}$$

### 3.3 Unicità della rappresentazione in base $b$

Usando la frazione generatrice, otteniamo che  $0, \overline{9} = \frac{9}{9} = 1$  e dunque anche

$$0, d_1 d_2 \dots d_N \overline{9} = 0, d_1 d_2 \dots (d_N + 1).$$

Ne segue che la rappresentazione decimale di un numero razionale può non essere unica.

Il prossimo risultato mostra che più generalmente ogni numero razionale rappresentato da una frazione il cui denominatore è una potenza di  $b$  ha in base  $b$  anche una rappresentazione periodica non finita. Tuttavia questo è l'unico caso di non unicità che si può presentare, infatti faremo vedere in questo paragrafo che ogni numero reale ha una unica rappresentazione non finita in base  $b$ .

**Proposizione 3.5** *Sia  $b \geq 2$  un intero fissato. Se  $d_i < b$  per  $1 \leq i \leq N$ , si ha*

$$(0, d_1 d_2 \dots d_N \overline{(b-1)})_b = (0, d_1 d_2 \dots d_{N-1} (d_N + 1))_b.$$

**Dimostrazione:** Basta osservare che

$$\sum_{i \geq 0} \frac{b-1}{b^{(N+1)+i}} = \frac{b-1}{b^{N+1}} \sum_{i \geq 0} \frac{1}{b^i} = \frac{b-1}{b^{N+1}} \left( \frac{b}{b-1} \right) = \frac{1}{b^N}.$$

**Teorema 3.6 (Unicità della rappresentazione non finita in base  $b$ )**  
 Sia  $b \geq 2$  un intero fissato e sia  $r$  un numero reale positivo tale che

$$r = \sum_{k \geq 0} \frac{d_k}{b^k} = \sum_{k \geq 0} \frac{c_k}{b^k},$$

con  $d_0 = 0$  e  $0 \leq d_k, c_k < b$  per  $k \geq 1$ . Se non esiste alcun numero intero  $N \geq 0$  tale che  $d_i = 0$  per  $i \geq N$ , allora  $d_k = c_k$  per  $k \geq 0$ .

**Dimostrazione:** Ricordiamo che, posto

$$S_n := \sum_{k \geq 0} \frac{d_k}{b^k} \quad \text{e} \quad S'_n := \sum_{k \geq 0} \frac{c_k}{b^k},$$

risulta

$$\sum_{k \geq 0} \frac{d_k}{b^k} = \sum_{k \geq 0} \frac{c_k}{b^k} \quad \text{se e soltanto se} \quad \lim_{n \rightarrow \infty} |S_n - S'_n| = 0.$$

Supponiamo per contrapposizione che esista un minimo intero  $M$  tale che  $d_M \neq c_M$ . Allora, per  $n \geq M + 1$  risulta

$$|S_n - S'_n| \geq \frac{1}{b^M} |d_M - c_M| + \left| \sum_{k=M+1}^n \frac{d^k}{b^k} - \sum_{k=M+1}^n \frac{c^k}{b^k} \right|.$$

Poiché per ipotesi esiste  $h \geq 1$  tale che  $d_{M+h} \geq 1$ , per  $n$  abbastanza grande, si ha

$$\sum_{k=M+1}^n \frac{d^k}{b^k} \geq \frac{1}{b^{M+h}}.$$

D'altra parte risulta

$$\sum_{k=M+1}^n \frac{c^k}{b^k} < \frac{1}{b^{M-1}(b-1)}.$$

Infatti

$$\sum_{k=M+1}^n \frac{c^k}{b^k} < \sum_{k=M+1}^n \frac{b}{b^k} = \frac{1}{b^M} \sum_{i=0}^{n-M} \frac{1}{b^i},$$

da cui, ricordando che  $1 - x^m = (1 - x)(1 + x + \dots + x^{m-1})$ ,

$$\sum_{k=M+1}^n \frac{c^k}{b^k} < \frac{b^{n-M+1} - 1}{b^n(b-1)} = \frac{1}{b^{M-1}(b-1)} - \frac{1}{b^n(b-1)} < \frac{1}{b^{M-1}(b-1)}.$$

Allora, per  $n$  abbastanza grande,

$$\begin{aligned} \sum_{k=M+1}^n \frac{d^k}{b^k} - \sum_{k=M+1}^n \frac{c^k}{b^k} &> \frac{1}{b^{M+h}} - \frac{1}{b^{M-1}(b-1)} \\ &= \frac{(b-1) - b^{h+1}}{b^{M+h}(b-1)} \neq 0. \end{aligned}$$

Infine, essendo  $\frac{1}{b^M} |d_M - c_M| > \frac{1}{b^M}$ , per  $n$  abbastanza grande,

$$|S_n - S'_n| > \frac{1}{b^M} + \left| \frac{1}{b^{M+h}} - \frac{1}{b^{M-1}(b-1)} \right| > \frac{1}{b^M} > 0.$$

Ne segue che

$$\sum_{k \geq 0} \frac{d_k}{b^k} \neq \sum_{k \geq 0} \frac{c_k}{b^k}.$$

Per il teorema precedente, l'unica rappresentazione decimale non finita di 1 è  $0, \overline{9}$ .

Una successione  $a_1, a_2, \dots, a_n, \dots$  a valori numerici si dice *quasi ovunque nulla* se esiste un intero  $N \geq 0$  tale che  $a_i = 0$  per  $i \geq N$ .

**Corollario 3.7** *Per ogni  $b \geq 2$ , esiste una corrispondenza biunivoca tra i numeri reali  $r$  tali che  $0 < r \leq 1$  e le successioni a valori nell'insieme  $\mathbf{b} := \{0, 1, \dots, b-1\}$  che non sono quasi ovunque nulle.*

**Dimostrazione:** Se  $r = (0, d_1 d_2 \dots d_n \dots)_b$  è l'unica rappresentazione infinita di  $r$  in base  $b$  (Teorema 3.6),  $r$  è univocamente determinato dalla successione  $d_1, d_2, \dots, d_n, \dots$ , che non è quasi ovunque nulla.

## 4 Numeri irrazionali

I numeri reali che non sono razionali si chiamano *numeri irrazionali*. Abbiamo visto nel paragrafo precedente che i numeri irrazionali sono tutti e soli i numeri reali che hanno una rappresentazione decimale non periodica.

Si fa risalire alla scuola pitagorica la scoperta che il lato e la diagonale di un quadrato non sono commensurabili, cioè che  $\sqrt{2}$  è un numero irrazionale (vedi anche l'Esempio 1.3). Più generalmente, usando la proprietà che ogni numero intero è prodotto di numeri primi univocamente determinati, si può facilmente dimostrare che, per ogni numero intero  $d \geq 2$ , se  $\sqrt[n]{d}$  non è un numero intero, allora  $\sqrt[n]{d}$  è irrazionale, per ogni  $n \geq 2$ .

**Proposizione 4.1** *Siano  $d, n \geq 2$ . Se  $\sqrt[n]{d} \notin \mathbb{Z}$ , allora non esiste alcun numero razionale  $\alpha \in \mathbb{Q}$  tale che  $\alpha^n = d$ .*

**Dimostrazione:** Sia  $\alpha \in \mathbb{Q}$  tale che  $\alpha^n = d$ . Se  $\alpha \notin \mathbb{Z}$ , allora  $\alpha := \frac{a}{b}$  con  $\text{MCD}(a, b) = 1$ . Poiché  $a^n = db^n$ , ne segue che ogni numero primo  $p$  che divide  $d$  divide anche  $a$ . Quindi  $a^n = d^n c = db^n$ . Dividendo per  $d$ , otteniamo  $d^{n-1} c = b^n$ . Poiché  $n-1 \geq 1$ , otteniamo che ogni divisore primo  $p$  di  $d$  divide anche  $b$ . Ma allora  $\text{MCD}(a, b) \neq 1$ ; questa è una contraddizione.

Il fatto che  $\sqrt{2}$  è irrazionale implica che i numeri irrazionali costituiscono un sottoinsieme denso di  $\mathbb{R}$ .

**Teorema 4.2 (Densità dei numeri irrazionali)** *Comunque scelti  $\alpha, \beta \in \mathbb{R}$ ,  $\alpha < \beta$ , esiste un numero reale irrazionale  $\gamma$  tale che  $\alpha < \gamma < \beta$ .*

**Dimostrazione:** Possiamo ovviamente supporre che  $\alpha$  e  $\beta$  siano numeri positivi. Poiché  $\mathbb{Q}$  è denso in  $\mathbb{R}$  (Corollario 2.9), esistono  $a, b \in \mathbb{Q}$  tali che  $\alpha < a < \frac{\alpha+\beta}{2} < b < \beta$ . Quindi, poiché  $\sqrt{2}$  è irrazionale (Proposizione 4.1), anche il numero  $\gamma := a + \frac{b-a}{2}\sqrt{2}$  è irrazionale. Inoltre, essendo  $\sqrt{2} < 1 + \frac{1}{2}$ , si verifica facilmente che  $\alpha < a < \gamma < b < \beta$ .

## 4.1 Numeri trascendenti

Un numero che è radice di qualche polinomio non nullo a coefficienti razionali si chiama un *numero algebrico*. Un numero che non è algebrico si chiama un *numero trascendente*.

Ogni numero razionale  $\alpha$  è banalmente algebrico, essendo radice del polinomio  $X - \alpha \in \mathbb{Q}[X]$ ; quindi i numeri reali trascendenti sono tutti irrazionali. Se  $d$  è un numero intero positivo, il numero reale  $\sqrt[n]{d}$  è un numero algebrico, perché è radice del polinomio  $X^n - d \in \mathbb{Q}[X]$ , ma è razionale se e soltanto se è intero (Proposizione 4.1).

La teoria dei numeri algebrici coincide essenzialmente con lo studio delle proprietà dei polinomi di cui essi sono radici ed è una teoria ormai consolidata. Tutti i numeri algebrici costituiscono un sottocampo del campo complesso  $\mathbb{C}$  ed i numeri reali algebrici costituiscono un sottocampo di  $\mathbb{R}$ .

Lo studio dei numeri trascendenti è invece molto più difficile ed ha molteplici aspetti che non sembra possano ricondursi ad una teoria generale.

L'esistenza dei numeri trascendenti è stata dimostrata da J. Liouville nel 1844, come conseguenza del suo celebre *Teorema di Approssimazione* (per la dimostrazione si rimanda a [6, Paragrafo 1]).

**Teorema 4.3 (J. Liouville, 1844)** *Sia  $\alpha \in \mathbb{R}$  un numero algebrico che è radice di un polinomio irriducibile di grado  $n \geq 2$ . Allora esiste un numero positivo  $c$ , dipendente soltanto da  $\alpha$ , tale che l'ineguaglianza*

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{|q|^n}$$

*è verificata per tutte le coppie di numeri razionali  $(p, q)$ ,  $q \neq 0$ .*

Usando in negativo questo teorema, è possibile costruire molti numeri reali trascendenti, oggi chiamati *numeri di Liouville* (si veda [6, Paragrafo 4]). Un numero di Liouville è ad esempio il numero

$$\sum_{k \geq 1} \frac{1}{10^k} = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots + \frac{1}{10^n} + \cdots$$

Altri numeri trascendenti possono essere costruiti usando teoremi di approssimazione sempre più precisi. In questo contesto, il seguente teorema, chiamato per motivi storici il *Teorema di Thue-Siegel-Roth*, è considerato di fondamentale importanza ed è stato dimostrato da K. F. Roth nel 1955 [6, Paragrafo 5].

**Teorema 4.4 (K. Roth, 1955)** *Sia  $\alpha \in \mathbb{R}$  un numero algebrico e sia  $\epsilon > 0$ . Allora l'ineguaglianza*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}$$

*è verificata soltanto per un numero finito di numeri razionali  $p/q$ ,  $q > 0$ .*

Tuttavia, in generale dimostrare la trascendenza, o anche soltanto l'irrazionalità, di un particolare numero reale è molto difficile. Uno dei molti problemi importanti ancora aperti è infatti quello di stabilire se certe costanti che intervengono in Teoria dei Numeri, come ad esempio la *costante di Euler*

$$\gamma := \lim_{n \rightarrow \infty} \left( 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log n \right) = 0,577216\dots,$$

siano o no razionali.

La trascendenza del numero di Nepero

$$e := \sum_{k \geq 1} \frac{1}{k!} = 1 + \frac{1}{2} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots,$$

base del logaritmo naturale, fu congetturata da L. Euler nel 1784 e dimostrata da C. Hermite nel 1873 come conseguenza del fatto che, se  $\alpha_1, \dots, \alpha_n$  sono numeri razionali distinti,  $n \geq 1$ , i numeri  $e^{\alpha_1}, \dots, e^{\alpha_n}$  sono linearmente indipendenti su  $\mathbb{Q}$ . Questo risultato di Hermite è stato poi generalizzato da Lindemann nel seguente teorema, la cui dimostrazione si può trovare in [6, Paragrafo 10] oppure in [1, Problema 26].

**Teorema 4.5 (F. Lindemann, 1882)** *Scelti comunque  $n$  numeri algebrici distinti  $\alpha_i$  e  $n$  numeri algebrici non nulli  $A_i$ ,  $1 \leq i \leq n$ , risulta*

$$A_1 e^{\alpha_1} + A_2 e^{\alpha_2} + \dots + A_n e^{\alpha_n} \neq 0.$$

**Corollario 4.6**  *$e^\alpha$  è un numero trascendente per ogni numero algebrico  $\alpha \neq 0$ . In particolare, se  $x$  è un numero reale algebrico diverso da 0 e 1, allora  $\ln(x)$  è trascendente.*

**Dimostrazione:** Per il Teorema 4.5, se  $\alpha \neq 0$  è algebrico,  $e^\alpha$  non può essere radice di alcun polinomio a coefficienti razionali. Quindi  $e^\alpha$  è un numero

trascendente. Poiché  $x = e^{\ln(x)}$ , vediamo anche che, se  $\ln(x) \neq 0$  è algebrico, allora  $x$  è trascendente.

La trascendenza del numero  $\pi$ , che indica il rapporto tra la lunghezza della circonferenza e quella del diametro di un qualsiasi cerchio, fu congetturata da A. M. Legendre nel 1806 e dimostrata da Lindemann come conseguenza del Teorema 4.5. Essa implica l'impossibilità della *quadratura del cerchio*, ovvero l'impossibilità di costruire con riga e compasso un quadrato che abbia area uguale a quella di un cerchio assegnato.

Ricordiamo che ogni numero reale  $x$  soddisfa la formula

$$e^{ix} = \cos(x) + i \sin(x) \quad (\text{L. Euler, 1746}).$$

**Corollario 4.7**  $\pi$  è un numero trascendente.

**Dimostrazione:** Per la formula di Euler, si ha  $e^{i\pi} = -1$ . Poiché  $i$  è algebrico ed i numeri algebrici formano un campo, per il Teorema 4.5,  $\pi$  non può essere algebrico.

Nel suo discorso di apertura del secondo Congresso Internazionale della Matematica, tenutosi a Parigi nel 1900, D. Hilbert indicò quelle che riteneva le linee di sviluppo della matematica del XX secolo attraverso un elenco di problemi ancora aperti, oggi noti come i *23 problemi di Hilbert*. Il settimo di questi problemi chiedeva di stabilire se i numeri del tipo  $\alpha^\beta$ , con  $\alpha$  e  $\beta$  algebrici, come ad esempio  $2^{\sqrt{2}}$ , fossero trascendenti. Questo problema fu risolto nel 1934 da A. Gelfond e T. Schneider indipendentemente (vedi [6, Paragrafo 9]).

**Teorema 4.8 (A. Gelfond - T. Schneider, 1934)** *Se  $\alpha$  è un numero algebrico diverso da 0 e 1 e  $\beta$  è un numero irrazionale algebrico, allora  $\alpha^\beta$  è trascendente.*

**Corollario 4.9 (A. Gelfond, 1929)**  $e^\pi$  è un numero trascendente.

**Dimostrazione:** Per la formula di Euler, risulta  $e^\pi = i^{-2i}$ , dove sia  $i$  che  $-2i$  sono algebrici. Quindi possiamo applicare il Teorema 4.8.

**Corollario 4.10 (C. Siegel, 1930)**  $2^{\sqrt{2}}$  è un numero trascendente.

Per il seguente risultato più generale, A. Baker ha ricevuto la *Medaglia Fields* nel 1970. Questo premio è dedicato alla memoria del matematico J. C. Fields, che lo ha istituito nel 1936. Esso viene assegnato a matematici di età inferiore ai 40 anni, in occasione dei Congressi Internazionali di Matematica, che si svolgono ogni quattro anni.

**Teorema 4.11 (A. Baker, 1966)** *Il prodotto di un numero finito di numeri trascendenti del tipo di quelli costruiti come nei teoremi di Lindemann e Gelfond-Schneider è un numero trascendente.*

Non è ancora noto se  $\alpha^\beta$  sia trascendente quando lo sono sia  $\alpha$  che  $\beta$ . Ad esempio non è noto se  $\pi^e$  sia trascendente. Non è neanche noto se  $e + \pi$  ed  $e\pi$  siano trascendenti.

## 5 La cardinalità del continuo

Una dimostrazione indiretta dell'esistenza dei numeri trascendenti è stata data da G. F. Cantor, nel 1874. Essa si basa sul fatto che il campo  $\mathbb{R}$  dei numeri reali ha cardinalità strettamente maggiore del campo dei numeri reali algebrici. I numeri trascendenti sono allora infinitamente più numerosi dei numeri algebrici.

I risultati di Cantor sulla cardinalità sono alla base della moderna teoria degli insiemi; tuttavia i metodi usati da Cantor, essendo totalmente non costruttivi, suscitarono molti dubbi nei matematici suoi contemporanei e furono fortemente contestati. Uno dei più accaniti avversari di Cantor è stato il suo maestro L. Kronecker, il quale riteneva che gli unici processi validi in matematica fossero quelli che si concludevano dopo un numero finito di passi e per questo negava l'esistenza degli insiemi infiniti.

### 5.1 La cardinalità di un insieme

Se  $X$  è un insieme finito, il numero dei suoi elementi si indica con  $|X|$ . In questo caso evidentemente  $|X| = |Y|$  se e soltanto se  $Y$  ha tanti elementi quanti ne ha  $X$ , cioè quando  $X$  e  $Y$  possono essere messi in corrispondenza biunivoca.

Per estendere questo concetto al caso infinito, si dice che due insiemi  $X$  e  $Y$  sono *equipotenti* se esiste una corrispondenza biunivoca tra  $X$  e  $Y$ ; in questo caso scriveremo  $|X| = |Y|$ . Il fatto che, come si verifica facilmente, la relazione di equipotenza tra insiemi si comporta come una relazione di equivalenza ci permette di definire il concetto di *cardinalità di un insieme*. Precisamente, diremo che  $|X|$  è la *cardinalità* di un qualsiasi insieme equipotente a  $X$ . I numeri naturali sono le cardinalità degli insiemi finiti.

Nel caso finito, un insieme non può mai avere lo stesso numero di elementi di un suo sottoinsieme proprio. Nel caso infinito tuttavia, come già osservato da G. Galilei, può accadere che un insieme abbia la stessa cardinalità di un suo sottoinsieme proprio. Basta ad esempio notare che la corrispondenza  $\mathbb{Z} \rightarrow 2\mathbb{Z} \subsetneq \mathbb{Z}$  definita da  $x \mapsto 2x$  è biunivoca. In realtà questa proprietà *paradossale* caratterizza gli insiemi infiniti (R. Dedekind, 1888).

Se  $X$  è equipotente ad un sottoinsieme di  $Y$ , scriveremo  $|X| \leq |Y|$ . Scriveremo inoltre  $|X| < |Y|$  per indicare che  $|X| \leq |Y|$  e  $|X| \neq |Y|$ . La

scelta di usare il simbolo di ordinamento non è casuale, infatti le cardinalità possono essere totalmente ordinate.

**Teorema 5.1** *Comunque scelti  $X, Y$  e  $Z$ , valgono le seguenti proprietà:*

- (a) (Proprietà riflessiva)  $|X| \leq |X|$ ;
- (b) (Proprietà antisimmetrica) *Se  $|X| \leq |Y|$  e  $|Y| \leq |X|$ , allora  $|X| = |Y|$ ;*
- (c) (Proprietà transitiva) *Se  $|X| \leq |Y|$  e  $|Y| \leq |Z|$ , allora  $|X| \leq |Z|$ ;*
- (d) (Tricotomia) *Si verifica uno e soltanto uno dei seguenti casi:  $|X| < |Y|$ ,  $|X| = |Y|$ , oppure  $|Y| < |X|$ .*

Una dimostrazione del teorema precedente si può trovare ad esempio in [7]. Le proprietà riflessiva e transitiva sono di facile verifica. La validità della proprietà antisimmetrica è stata congetturata da G. Cantor, ma è stata dimostrata nel 1897 da E. Schröder e F. Bernstein indipendentemente. La proprietà di tricotomia, che asserisce che la relazione  $|X| \leq |Y|$  tra cardinalità è un ordinamento totale, è stata considerata vera da Cantor, ma è stata dimostrata per la prima volta da E. Zermelo, nel 1904, come conseguenza dell'*Assioma della Scelta*. Essa è in realtà una delle formulazioni equivalenti di tale assioma.

**Teorema 5.2** *Le seguenti affermazioni sono equivalenti:*

- (a) (Assioma della Scelta) *Sia  $\{S_i\}_{i \in I}$  una famiglia non vuota di insiemi non vuoti. Allora esiste una famiglia di elementi  $\{x_i\}_{i \in I}$  tale che  $x_i \in S_i$ , per ogni  $i \in I$ ;*
- (b) (Teorema di Zermelo) *Ogni insieme non vuoto  $A$  può essere bene ordinato. (Cioè è possibile definire su  $A$  un ordinamento, necessariamente totale, secondo il quale ogni sottoinsieme non vuoto di  $A$  ha un minimo);*
- (c) (Lemma di Zorn) *Se  $A$  è un insieme ordinato non vuoto in cui ogni catena (cioè ogni sottoinsieme non vuoto di  $A$  totalmente ordinato) ha un maggiorante, allora  $A$  ha (almeno) un elemento massimale;*
- (d) (Lemma di Kuratowsky) *Se  $A$  è un insieme ordinato non vuoto, ogni catena di  $A$  è contenuta in una catena massimale;*
- (e) (Tricotomia) *La relazione  $|X| \leq |Y|$  tra cardinalità è un ordinamento totale.*

Alcune linee di dimostrazione di questo teorema e le indicazioni bibliografiche relative si possono trovare in [2, Appendice A1].

L'Assioma della Scelta, sul quale sono basati molti risultati fondamentali della matematica moderna, non è sostenuto da alcun procedimento costruttivo; ad esempio non è ancora noto alcun buon ordinamento del campo reale. Benché fosse stato già largamente usato, questo assioma è stato formalmente introdotto da E. Zermelo nel 1904. Nel 1939, K. Gödel ha dimostrato che esso è consistente (cioè non è in contraddizione) con gli assiomi della teoria insiemistica adoperati correntemente (se essi sono consistenti) e, nel 1962, il suo allievo P. Cohen ha dimostrato che esso è indipendente dagli altri assiomi (se essi sono consistenti). Quindi l'Assioma della Scelta non può essere dimostrato o confutato sulla base degli altri assiomi della teoria degli insiemi e può essere accettato o meno.

## 5.2 La cardinalità del numerabile

La cardinalità dell'insieme  $\mathbb{N}$  dei numeri naturali si chiama la *cardinalità del numerabile* e si dice che  $X$  è un *insieme numerabile* se  $|X| = |\mathbb{N}|$ . Questo significa che tutti gli elementi di  $X$  possono essere ordinati in una successione, ovvero  $X = \{x_0, x_1, \dots, x_n, \dots\}$ .

I due risultati successivi mostrano che la cardinalità del numerabile è la più piccola cardinalità infinita.

**Proposizione 5.3** *Ogni sottoinsieme non vuoto di un insieme numerabile è finito o numerabile.*

**Dimostrazione:** Sia  $X = \{x_0, x_1, \dots, x_n, \dots\}$  un insieme numerabile e sia  $Y \subseteq X$  un sottoinsieme non vuoto. Per il principio del Buon Ordinamento, esiste un minimo indice  $i_0$  tale che  $x_{i_0} \in Y$ . Posto  $Y_1 := Y \setminus \{x_{i_0}\}$ , se  $Y_1 \neq \emptyset$ , esiste analogamente un minimo indice  $i_1$  tale che  $x_{i_1} \in Y_1$ . Così proseguendo, per ricorsione, si ottiene che  $Y$  è finito oppure  $Y = \{x_{i_0}, x_{i_1}, \dots, x_{i_n}, \dots\}$  è numerabile.

**Proposizione 5.4** *Ogni insieme infinito ha un sottoinsieme numerabile.*

**Dimostrazione:** Sia  $X$  un insieme infinito e  $x_0$  un suo elemento. (Qui si usa l'Assioma della Scelta). Poiché  $X$  è infinito, l'insieme  $X_1 := X \setminus \{x_0\}$  è non vuoto. Scelto  $x_1 \in X_1$ , l'insieme  $X_2 := X \setminus \{x_0, x_1\}$  è ancora non vuoto. Per ricorsione possiamo allora costruire una successione  $x_0, x_1, \dots, x_n, \dots$  di elementi di  $X$ .

L'unione di due insiemi finiti  $X$  e  $Y$  è un insieme finito per il *Principio di Inclusione-Esclusione*:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Quindi, per induzione, l'unione di  $n$  insiemi finiti è un insieme finito, per ogni  $n \geq 2$ . Un risultato analogo vale per gli insiemi numerabili.

**Teorema 5.5 (Primo procedimento diagonale di Cantor)** Sia  $\{X_i\}_{i \geq 0}$  una famiglia numerabile di insiemi numerabili e  $X$  l'unione disgiunta degli  $X_i$ . Allora  $X$  è un insieme numerabile.

**Dimostrazione:** Posto  $X_i := \{x_{i0}, x_{i1}, \dots, x_{in}, \dots\}$ , gli elementi di  $X$  possono essere disposti in una tabella infinita:

$X_0$	$x_{00}$	$x_{01}$	$x_{02}$	$x_{03}$	$x_{04}$	$\dots$	$x_{0n}$	$\dots$
$X_1$	$x_{10}$	$x_{11}$	$x_{12}$	$x_{13}$	$x_{14}$	$\dots$	$x_{1n}$	$\dots$
$X_2$	$x_{20}$	$x_{21}$	$x_{22}$	$x_{23}$	$x_{24}$	$\dots$	$x_{2n}$	$\dots$
$X_3$	$x_{30}$	$x_{31}$	$x_{32}$	$x_{33}$	$x_{34}$	$\dots$	$x_{3n}$	$\dots$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$X_i$	$x_{i0}$	$x_{i1}$	$x_{i2}$	$x_{i3}$	$x_{i4}$	$\dots$	$x_{in}$	$\dots$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

e quindi possono essere *contati in diagonale*:

$$X = \{x_{00}, x_{10}, x_{01}, x_{20}, x_{11}, x_{02}, x_{30}, x_{21}, \dots\}.$$

Precisamente, per ogni fissato  $i \geq 0$ , sia

$$D_i = \{x_{i-k,k} ; k = 0, \dots, i\} = \{x_{i0}, x_{i-1,1}, x_{i-2,2}, \dots, x_{0,i}\}$$

la  $i$ -sima diagonale. Notiamo che  $|D_i| = i + 1$ . Poiché ogni elemento  $x_{ij} \in X$  appartiene ad una e una sola diagonale, precisamente quella di indice  $k := i + j$ , allora a  $x_{ij}$  possiamo far corrispondere il numero intero

$$d_{ij} = |D_0| + |D_1| + |D_2| + \dots + |D_{i+j-1}| + (j+1) = 1 + 2 + 3 + \dots + (i+j) + (j+1).$$

In questo modo resta definita una corrispondenza biunivoca

$$X \rightarrow \mathbb{N}; \quad x_{ij} \mapsto d_{ij}.$$

**Corollario 5.6** L'unione di una famiglia numerabile di insiemi finiti o numerabili è un insieme numerabile.

**Dimostrazione:** Segue dal Teorema 5.5 e dalla Proposizione 5.4.

**Corollario 5.7** Se  $X$  è un insieme finito o numerabile e  $Y$  è infinito, allora  $|X \cup Y| = |Y|$ .

**Dimostrazione:** Poiché  $X' := X \setminus (X \cap Y)$  è un sottoinsieme di  $X$ , per la Proposizione 5.3,  $X'$  è ancora finito o numerabile e si ha  $X \cup Y = X' \cup Y$ . Sostituendo  $X$  con  $X'$ , possiamo quindi supporre che  $X \cap Y = \emptyset$ .

Sia  $Z$  un sottoinsieme numerabile di  $Y$  (Proposizione 5.4). Allora  $X \cup Z$  è numerabile (Teorema 5.5) e quindi esiste una corrispondenza biunivoca  $f : X \cup Z \rightarrow Z$ . Notando che  $X \cup Y = (X \cup Z) \cup (Y \setminus Z)$  e  $(X \cup Z) \cap (Y \setminus Z) = X \cap Y = \emptyset$ , la biiezione  $f$  si può allora estendere ad una biiezione

$$g : X \cup Y \rightarrow Y; \quad t \mapsto \begin{cases} f(t) & \text{se } t \in X \cup Z \\ t & \text{se } t \in Y \setminus Z \end{cases}.$$

**Corollario 5.8** *Sia  $Y$  un insieme infinito e  $X$  un suo sottoinsieme finito o numerabile. Se  $Y \setminus X$  è infinito, allora  $|Y| = |Y \setminus X|$ .*

**Dimostrazione:** Segue dal Corollario 5.7, osservando che  $Y = (Y \setminus X) \cup X$ .

**Corollario 5.9** *Se  $X$  è un insieme finito o numerabile e  $Y$  è numerabile, il prodotto diretto  $X \times Y$  è numerabile. In particolare, gli insiemi numerici  $\mathbb{Z}$  e  $\mathbb{Q}$  sono numerabili.*

**Dimostrazione:** Per ogni  $x \in X$ , l'insieme  $\{x\} \times Y$  è equipotente a  $Y$ , attraverso la corrispondenza biunivoca  $\{x\} \times Y \rightarrow Y$  definita da  $(x, y) \mapsto y$ . Allora  $X \times Y = \bigcup_{x \in X} \{\{x\} \times Y\}$  è una unione finita o numerabile di insiemi numerabili e pertanto è numerabile per il Teorema 5.5.

Osserviamo ora che la corrispondenza

$$\mathbb{Z} \rightarrow \{1, -1\} \times \mathbb{N}, \quad z \mapsto \begin{cases} (-1, |z|) & \text{se } z < 0 \\ (1, |z|) & \text{se } z \geq 0 \end{cases}$$

è biiettiva. Poiché per quanto appena visto l'insieme  $\{1, -1\} \times \mathbb{N}$  è numerabile e  $\mathbb{Z}$  è infinito, allora  $\mathbb{Z}$  è numerabile (Proposizione 5.3).

Infine, rappresentando un numero razionale con una frazione  $\frac{a}{b}$  con  $\text{MCD}(a, b) = 1$ , l'applicazione

$$\mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}, \quad \frac{a}{b} \mapsto (a, b)$$

è iniettiva. Quindi, procedendo come sopra, otteniamo che  $\mathbb{Q}$  è numerabile.

Per induzione, dal corollario precedente segue che il prodotto diretto di  $n$  copie di un insieme numerabile è ancora numerabile, per ogni  $n \geq 2$ .

**Corollario 5.10** *Se  $A$  è un dominio numerabile, in particolare  $A = \mathbb{Z}$ ,  $\mathbb{Q}$ , l'anello  $A[X]$  dei polinomi in una indeterminata a coefficienti in  $A$  è numerabile.*

**Dimostrazione:** Per ogni  $n \geq 0$ , indichiamo con  $P_n$  l'insieme dei polinomi su  $A$  di grado  $n$ . Per il principio di identità dei polinomi, la corrispondenza che associa ad ogni polinomio di  $P_n$  la  $(n+1)$ -pla dei suoi coefficienti è una corrispondenza biunivoca tra  $P_n$  e il prodotto diretto di  $n+1$  copie di  $A$ . Quindi, poiché  $A$  è numerabile, anche  $P_n$  è numerabile (Corollario 5.9). Per finire, notiamo che  $A[X] = (\bigcup_{n \geq 0} P_n) \cup \{0\}$ . Quindi  $A[X]$  è numerabile per il Teorema 5.5.

**Corollario 5.11 (G. Cantor, 1874)** *L'insieme  $\mathcal{A}$  di tutti i numeri algebrici è numerabile.*

**Dimostrazione:** Ogni numero algebrico è radice di un polinomio non nullo a coefficienti razionali ed ogni polinomio  $f(X)$  di grado  $n \geq 1$  ha al più  $n$  radici distinte. Indicando con  $R_f$  l'insieme delle radici di  $f(X)$ , risulta allora  $\mathcal{A} = \bigcup \{R_f ; f(X) \in \mathbb{Q}[X], f(X) \neq 0\}$ . Poiché  $\mathbb{Q}[X]$  è numerabile (Corollari 5.9 e 5.10), allora  $\mathcal{A}$  è numerabile per il Teorema 5.5.

### 5.3 La cardinalità del continuo

Mostriamo ora che il campo reale  $\mathbb{R}$  non è numerabile, cioè che  $|\mathbb{N}| < |\mathbb{R}|$ . La cardinalità di  $\mathbb{R}$  si chiama la *cardinalità del continuo*.

Cominciamo osservando che ogni intervallo reale è equipotente ad  $\mathbb{R}$ . Dati  $a, b \in \mathbb{R}$ ,  $a \leq b$ , poniamo con la notazione usuale:

$$[a, b] := \{r \in \mathbb{R}; a \leq r \leq b\} \text{ (intervallo chiuso di estremi } a \text{ e } b\text{);}$$

$$(a, b] := \{r \in \mathbb{R}; a < r \leq b\} \text{ (intervallo aperto a sinistra);}$$

$$[a, b) := \{r \in \mathbb{R}; a \leq r < b\} \text{ (intervallo aperto a destra);}$$

$$(a, b) := \{r \in \mathbb{R}; a < r < b\} \text{ (intervallo aperto).}$$

**Proposizione 5.12 (B. Bolzano, 1917)** *Ogni intervallo reale è equipotente ad  $\mathbb{R}$ . In particolare, l'intervallo  $(0, 1]$  è equipotente ad  $\mathbb{R}$ .*

**Dimostrazione:** Tutti gli intervalli reali (aperti o chiusi) di estremi fissati  $a$  e  $b$  sono equipotenti per il Corollario 5.8. Inoltre, comunque scelti  $a, b \in \mathbb{R}$ , l'applicazione  $(0, 1) \rightarrow (a, b)$  definita da  $x \mapsto a + (b - a)x$  è biunivoca. Quindi, per transitività, tutti gli intervalli sono tra loro equipotenti. Infine, l'intervallo aperto  $(-1, 1)$  è equipotente ad  $\mathbb{R}$  attraverso l'applicazione biunivoca

$$(1, -1) \rightarrow \mathbb{R}; \quad x \mapsto x/\sqrt{1 - x^2},$$

con inversa  $y \mapsto y/\sqrt{1 + y^2}$ .

Geometricamente, una corrispondenza biunivoca tra un qualsiasi segmento aperto di estremi  $A$  e  $B$  e la retta reale si può ottenere considerando la semicirconferenza di diametro uguale alla lunghezza del segmento  $AB$  e tangente alla retta nel punto medio del segmento. La proiezione ortogonale della semicirconferenza sulla retta fornisce una corrispondenza biunivoca tra la semicirconferenza ed il segmento chiuso  $AB$ , mentre la proiezione stereografica della semicirconferenza sulla retta fornisce una corrispondenza biunivoca tra la semicirconferenza privata degli estremi e la retta stessa (Figura 1).

**Teorema 5.13 (Secondo procedimento diagonale di Cantor)** *La cardinalità del continuo è strettamente maggiore della cardinalità del numerabile.*

**Dimostrazione:** Per la Proposizione 5.12, basta mostrare che l'intervallo reale  $(0, 1]$  non è numerabile. Ma questo, per il Corollario 3.7, equivale a dimostrare che non è numerabile l'insieme  $X$  delle successioni a valori nell'insieme  $S := \{0, 1, \dots, 9\}$  che non sono quasi ovunque nulle.

Supponiamo per assurdo che  $X$  sia numerabile, e quindi che

$$X = \{x_1, x_2, \dots, x_n, \dots\},$$

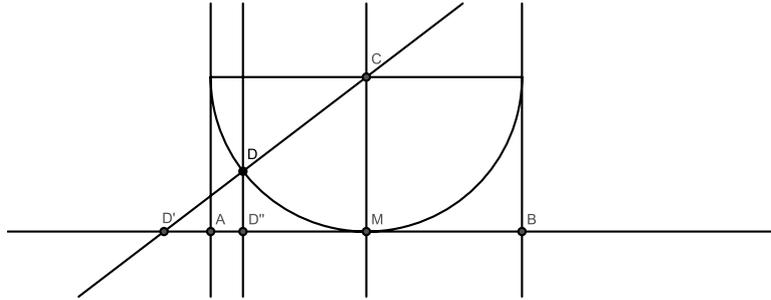


Figura 1: Proiezione stereografica: i punti  $D'$  e  $D''$  si corrispondono

dove, per ogni  $i \geq 0$ ,  $x_i = (x_{ij})_{j \geq 0}$  con  $x_{ij} \in S$ . Possiamo allora considerare la successione

$$y = (y_i) \quad \text{definita da} \quad y_i = \begin{cases} 2 & \text{se } x_{ii} = 1 \\ 1 & \text{se } x_{ii} \neq 1 \end{cases}$$

per ogni  $i \geq 0$ . La successione  $y$  non è quasi ovunque nulla, ma è differente da ogni successione  $x_i \in X$  nell'elemento di posto  $i$ . Quindi si ottiene una contraddizione e  $X$  non è numerabile.

Notiamo che, ordinando le successioni di  $X$  come

$$\begin{aligned} x_0 &= (x_{00}, x_{01}, x_{02}, x_{03}, \dots) \\ x_1 &= (x_{10}, x_{11}, x_{12}, x_{13}, \dots) \\ x_2 &= (x_{20}, x_{21}, x_{22}, x_{23}, \dots) \\ x_3 &= (x_{30}, x_{31}, x_{32}, x_{33}, \dots) \\ &\dots\dots\dots \\ x_i &= (x_{i0}, x_{i1}, x_{i2}, x_{i3}, \dots, x_{ii}, \dots) \\ &\dots\dots\dots \end{aligned}$$

la successione  $y$  si ottiene cambiando il valore degli elementi *sulla diagonale*.

**Corollario 5.14 (G. Cantor, 1874)** *L'insieme dei numeri trascendenti ha la cardinalità del continuo.*

**Dimostrazione:** Poiché l'insieme  $\mathcal{A}$  dei numeri algebrici è numerabile (Corollario 5.11), e il campo reale  $\mathbb{R}$  ha cardinalità strettamente maggiore (Teorema 5.13), l'insieme  $\mathbb{R} \setminus \mathcal{A}$  dei numeri trascendenti è infinito ed ha la stessa cardinalità di  $\mathbb{R} = (\mathbb{R} \setminus \mathcal{A}) \cup \mathcal{A}$  per il Corollario 5.7.

Ricordiamo che la corrispondenza che associa ad ogni sottoinsieme  $A$  di un insieme  $X$  la sua *funzione caratteristica*

$$\chi_A : X \rightarrow \mathbf{2} := \{0, 1\}; \quad x \mapsto \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

è una corrispondenza biunivoca tra l'insieme  $\mathcal{P}(X)$  delle parti di  $X$  e l'insieme  $\mathbf{2}^X$  delle funzioni su  $X$  a valori in  $\mathbf{2}$ . Quindi l'insieme  $\mathbf{2}^{\mathbb{N}}$  delle successioni a valori in  $\mathbf{2}$  è equipotente all'insieme  $\mathcal{P}(\mathbb{N})$  delle parti di  $\mathbb{N}$ .

**Proposizione 5.15** *L'insieme  $\mathcal{P}(\mathbb{N})$  delle parti di  $\mathbb{N}$  ha la cardinalità del continuo.*

**Dimostrazione:** Tenuto conto che  $|\mathcal{P}(\mathbb{N})| = |\mathbf{2}^{\mathbb{N}}|$ , mostriamo che  $\mathbf{2}^{\mathbb{N}}$  ha la cardinalità del continuo. Scriviamo  $\mathbf{2}^{\mathbb{N}} = X \cup Y$ , dove  $X$  è il sottoinsieme delle successioni che non sono quasi ovunque nulle e  $Y$  è il sottoinsieme delle successioni quasi ovunque nulle. Poiché  $X$  è equipotente all'intervallo  $(0, 1]$  (Corollario 3.7), per il Corollario 5.7, basta mostrare che l'insieme  $Y$  ha la cardinalità del numerabile. Sia  $Y_n$  l'insieme delle successioni  $(a_i)$  a valori in  $\mathbf{2}$  tali che  $a_i = 0$  per  $i \geq n$ . Allora la corrispondenza  $Y_n \rightarrow \mathbf{2}^n$  definita da  $(a_i) \mapsto (a_0, a_1, \dots, a_{n-1})$  è biunivoca. Quindi  $Y_n$  ha  $2^n$  elementi e  $Y = \bigcup_{n \geq 0} Y_n$  è numerabile per il Teorema 5.5.

Il fatto che  $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$  (Teorema 5.13) è conseguenza di un teorema più generale.

**Teorema 5.16 (G. Cantor, 1890)** *Sia  $X$  un insieme. Allora l'insieme delle parti di  $X$  ha cardinalità strettamente maggiore di quella di  $X$ .*

**Dimostrazione:** L'applicazione iniettiva

$$X \rightarrow \mathcal{P}(X), \quad x \mapsto \{x\}$$

ci permette di affermare che  $|X| \leq |\mathcal{P}(X)|$ .

D'altra parte, nessuna applicazione  $\varphi : X \rightarrow \mathcal{P}(X)$  può essere suriettiva e quindi  $|X| < |\mathcal{P}(X)|$ . Infatti, sia  $\varphi : X \rightarrow \mathcal{P}(X)$  una qualsiasi applicazione, così che  $\varphi(x) \in \mathcal{P}(X)$  è il sottoinsieme di  $X$  corrispondente all'elemento  $x \in X$ . Consideriamo l'insieme  $Z := \{x \in X; x \notin \varphi(x)\}$ . Se  $Z = \varphi(z)$ , allora per definizione

$$z \in Z \Leftrightarrow z \notin \varphi(z) \Leftrightarrow z \notin Z.$$

Questa contraddizione mostra che  $Z \neq \varphi(z)$ , per ogni  $z \in X$ . Quindi l'applicazione  $\varphi$  non è suriettiva.

Per il teorema precedente è possibile costruire una catena di insiemi

$$\mathbb{N} \subsetneq \mathcal{P}(\mathbb{N}) \subsetneq \mathcal{P}(\mathcal{P}(\mathbb{N})) \subsetneq \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \subsetneq \dots$$

di cardinalità strettamente crescente.

Una famosa congettura, formulata da Cantor nel 1878, afferma che non esistono insiemi la cui cardinalità è strettamente compresa tra la cardinalità di  $\mathbb{N}$  (cardinalità del numerabile) e quella di  $\mathcal{P}(\mathbb{N})$  (cardinalità del continuo). Questa congettura va sotto il nome di *Ipotesi del Continuo*. L'*Ipotesi Generalizzata del Continuo* afferma poi che, dato un qualsiasi insieme  $X$ , non esiste alcun insieme  $Y$  di cardinalità strettamente compresa tra la cardinalità di  $X$  e quella dell'insieme delle parti  $\mathcal{P}(X)$ . Quindi, secondo questa congettura, le uniche cardinalità transfinitive possibili sarebbero

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| = |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \dots$$

Il primo dei *23 problemi di Hilbert* chiedeva di dimostrare l'Ipotesi del Continuo. K. Gödel ha dimostrato nel 1938 che l'Ipotesi del Continuo è consistente con la teoria assiomatica degli insiemi (se tale teoria è consistente), compreso l'Assioma della Scelta. Mentre P. Cohen ha dimostrato nel 1963 che essa è indipendente. Quindi l'Ipotesi del Continuo, come l'Assioma della Scelta, non può essere dimostrata o confutata usando gli altri assiomi della teoria degli insiemi. In realtà era opinione di Gödel che tale congettura fosse *indecidibile*.

Le cardinalità si possono sommare e moltiplicare. Precisamente, denotando con  $X \uplus Y$  l'*unione disgiunta* di due insiemi  $X$  e  $Y$  e con  $X^Y$  l'insieme delle funzioni  $f : X \rightarrow Y$ , si può (ben) definire

$$|X| + |Y| := |X \uplus Y|, \quad |X| \cdot |Y| := |X \times Y| \quad |X|^{|Y|} := |X^Y|.$$

Queste operazioni tra cardinalità coincidono nel caso delle cardinalità finite con le usuali operazioni tra numeri naturali ed hanno praticamente tutte le proprietà delle operazioni tra numeri. Tuttavia, nel caso infinito esse non producono insiemi di cardinalità superiore.

**Teorema 5.17** *Siano  $X, Y$  due insiemi infiniti. Allora*

$$|X| + |Y| = \max\{|X|, |Y|\}; \quad |X \times Y| = \max\{|X|, |Y|\}$$

Una dimostrazione si può trovare in [7, Paragrafi 1.8 e 2.9]. Nel caso numerabile, ne derivano i Corollari 5.7 e 5.9.

Una conseguenza importante di questo teorema è che il prodotto cartesiano di  $n$  copie di un insieme infinito  $X$  ha la stessa cardinalità di  $X$ .

Questo fatto è in realtà equivalente all'Assioma della Scelta (cf. [2, Appendice A1]) ed implica ad esempio che  $\mathbb{R}$  e  $\mathbb{R}^n$  hanno la stessa cardinalità, in contraddizione con la nostra percezione dello spazio, che ci porta a credere che se una figura geometrica ha *dimensione superiore* ad un'altra allora è comunque *più grande* di questa.

Diamo di seguito la dimostrazione di Cantor del fatto che i punti di un quadrato sono tanti quanti quelli di un suo lato, cioè che  $|\mathbb{R}^2| = |\mathbb{R}|$  (Proposizione 5.12). Comunicando questo suo risultato a R. Dedekind, Cantor scrisse *Je le vois, mais je ne le crois pas ! (Lo vedo, ma non ci credo!)*.

**Teorema 5.18 (G. Cantor, 1877)** *Esiste una corrispondenza biunivoca tra l'insieme dei punti di un quadrato e l'insieme dei punti di un suo lato. Quindi  $|\mathbb{R}^n| = |\mathbb{R}|$ .*

**Dimostrazione:** Poiché l'intervallo  $[0, 1]$  ha la cardinalità del continuo (Proposizione 5.12), fissato nel piano ordinario un riferimento cartesiano, basta considerare il quadrato costruito sul segmento  $OU$ , dove  $O = (0, 0)$  è l'origine e  $U = (0, 1)$ . Allora i punti del quadrato sono in corrispondenza biunivoca con le coppie di numeri reali  $(x, y)$ , con  $x, y \in [0, 1]$ . Sempre per la Proposizione 5.12, possiamo anche supporre che  $x, y \neq 0$ . Poiché ogni numero reale  $x$  si rappresenta in modo unico come un numero decimale non finito (Teorema 3.6), usando questa rappresentazione, se  $x = 0, x_1x_2x_3 \dots$  e  $y = 0, y_1y_2y_3 \dots \in (0, 1]$ , alla coppia  $(x, y)$  possiamo far corrispondere il ben definito numero reale  $z := 0, x_1y_1x_2y_2x_3y_3 \dots \in (0, 1]$ . In questo modo si ottiene una corrispondenza iniettiva

$$(0, 1] \times (0, 1] \rightarrow (0, 1].$$

D'altra parte, ogni insieme non vuoto  $A$  è equipotente ad un sottoinsieme di  $A \times A$ , ad esempio attraverso l'applicazione diagonale

$$A \rightarrow A \times A, \quad a \mapsto (a, a).$$

Ne segue che  $|\mathbb{R}| \leq |\mathbb{R}^2| \leq |\mathbb{R}|$  e dunque  $|\mathbb{R}^2| = |\mathbb{R}|$ . Per induzione su  $n \geq 2$ , si ottiene poi che  $|\mathbb{R}^n| = |\mathbb{R}|$ .

## Riferimenti bibliografici

- [1] H. Dörrie, *100 Great Problems of Elementary Mathematics, their history and solutions*, Dover, 1965.
- [2] M. Fontana, S. Gabelli, *Insiemi, Numeri e Polinomi*, CISU, 1989.
- [3] H.-D. Hebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers*, Springer GTM 123, 1990.
- [4] S. Lang, *Analysis I*, Addison-Wesley, 1968.
- [5] S. Lang, *Undergraduate Algebra*, Second Edition, Springer UTM, 1990.
- [6] J. Lipman, *Transcendental Numbers*, Queen's Papers in Pure and Appl. Mat. 7, 1969.
- [7] A. Shen, N. K. Vereshchagin, *Basic Set Theory*, AMS, Student Math. Library 17, 2002.
- [8] B. L. Van der Waerden, *Modern Algebra*, F. Ungar, 1949.