I numeri reali

Note per il corso di Analisi Matematica 1

G. Mauceri

a.a. 2003-04

Contents

1 Introduzione

La nozione intuitiva del sistema dei numeri reali è legata al concetto di misura per classi di grandezze omogenee, come ad esempio la classe delle lunghezze, la classe delle aree, la classe dei tempi. Anche se questa nozione intuitiva è stata usata dai matematici almeno dai tempi degli antichi geometri Greci, soltanto verso la fine del diciannovesimo secolo si è arrivati a una costruzione formale rigorosa del sistema dei numeri reali a partire dai numeri razionali[1]

Dal punto di vista fondazionale un metodo abbastanza soddisfacente di introdurre i numeri reali consiste nel prendere i numeri naturali $0, 1, 2, 3 \dots$ come concetti primitivi, enunciando un sistema appropriato di assiomi per essi, e di usare poi i numeri naturali e la teoria degli insiemi per costruire il sistema dei numeri razionali. A loro volta i numeri razionali possono essere usati come base per la costruzione dei numeri reali. Poiché questo procedimento è piuttosto lungo e laborioso e noi siamo interessati esclusivamente nello sviluppo dell'analisi matematica a partire dalle proprietà dei numeri reali, seguiremo un procedimento diverso, che consiste nell'assumere i numeri reali come oggetti primitivi, indefiniti, che soddisfano certi assiomi. Supporremo quindi che esista un insieme $\mathbf{R}$, i cui elementi sono detti *numeri reali*, che soddisfa i nove assiomi enunciati nelle prossime sezioni. Gli assiomi possono essere riuniti in modo naturale in tre gruppi, che indicheremo con i nomi di *assiomi di campo*, *assiomi dell'ordine* e *assioma di completezza*. A partire da questi assiomi dedurremo tutte le altre proprietà dei numeri reali.

2 Gli assiomi di campo

Su $\mathbf{R}$ sono definite due operazioni[2] che ad ogni coppia di numeri reali (x, y) associano i numeri reali $x + y$ e xy, detti rispettivamente *somma* e *prodotto* di x e y, che soddisfano gli assiomi seguenti. Per ogni x, y e z in $\mathbf{R}$

Assioma 1 (proprietà associative) $(x + y) + z = x + (y + z)$, $(xy)z = x(yz)$

Assioma 2 (proprietà commutative) $x + y = y + x$, $xy = yx$

Assioma 3 (proprietà distributiva) $x(y + z) = xy + xz$

Assioma 4 (esistenza degli elementi neutri) *Esistono due numeri reali distinti, che indicheremo con 0 e 1, tali che per ogni x in $\mathbf{R}$, si ha $x + 0 = x$ e $1x = x$.*

Assioma 5 (esistenza dell'opposto) *Per ogni numero reale x esiste un numero reale y tale che $x + y = 0$.*

Assioma 6 (esistenza del reciproco) *Per ogni numero reale $x \neq 0$ esiste un numero reale y tale che $xy = 1$.*

[1]Due diverse costruzioni dei numeri reali vennero date da Richard Dedekind e George Cantor nel 1872.

[2]Il concetto di operazione su $\mathbf{R}$ puó essere ricondotto a quello di funzione definita sul prodotto cartesiano $\mathbf{R} \times \mathbf{R}$ a valori in $\mathbf{R}$.

Osserviamo che il numero reale y la cui esistenza è garantita dall'Assioma 5 è unico. Infatti, se $x+y=x+z=0$, allora $y=y+0=y+(x+z)=z+(x+y)=z+0=z$. Il numero reale y tale che $x+y=0$ si dice *l'opposto di* x e si denota con $-x$. La somma $x+(-y)$ si denota anche con $x-y$ ed è detta *la differenza* di x e y. Analogamente si dimostra l'unicità del reciproco di un numero reale $x \neq 0$. Il reciproco di x si denota con x^{-1} o con $1/x$. Il prodotto yx^{-1} si denota anche con y/x ed è detto anche *il rapporto* di y e x. Da questi assiomi possiamo dedurre tutte le abituali leggi dell'aritmetica; ad esempio: $-(-x)=x$, $(x^{-1})^{-1}=x$, $-(x-y)=y-x$, $x+(-y)=x-y$, $0x=x0=0$, $x/y+a/b=(xb+ya)/yb, \ldots$. Si noti anche che se xy=0 allora $x=0$ oppure $y=0$. La dimostrazione di tutte queste proprietà a partire dagli assiomi è un utile esercizio per il lettore.

3 Gli assiomi dell'ordine

Su $\mathbf{R}$ si introduce una relazione d'ordine a partire dal concetto non definito di *positività*.

Esiste un sottoinsieme $\mathbf{R}_+$ di $\mathbf{R}$, detto insieme dei numeri reali *positivi*, che soddisfa i due assiomi seguenti.

Assioma 7 *Per ogni x e y in $\mathbf{R}_+$ anche $x+y$ e $xy \in \mathbf{R}_+$.*

Assioma 8 *Per ogni numero reale x si verifica una e una sola delle tre alternative: $x=0$, oppure $x \in \mathbf{R}_+$, oppure $-x \in \mathbf{R}_+$.*

Definizione. Definiamo una relazione $<$ in $\mathbf{R}$ ponendo $x<y$ (leggi x *minore di* y) se e solo se $y-x \in \mathbf{R}_+$. Scriveremo anche $y>x$ (y *maggiore di* x) se $x<y$; $x \leq y$ (x *minore o uguale a* y) se $x<y$ oppure $x=y$; $y \geq x$ (y *maggiore o uguale di* x) se $x \leq y$. Se $x<0$ diciamo che x è *negativo.* Denoteremo con $\mathbf{R}_-$ l'insieme dei numeri reali negativi. Se $x \geq 0$ diremo anche che x è *non negativo.*

Teorema 3.1 *La relazione $\leq$ è una relazione d'ordine totale su $\mathbf{R}$. In altri termini essa soddisfa le seguenti proprietà:*

a) riflessività: per ogni x in $\mathbf{R}$ si ha $x \leq x$,

b) antisimmetria: per ogni x, y in $\mathbf{R}$, $x \leq y$ e $y \leq x$ implica $x=y$,

c) transitività: per ogni x, y e z in $\mathbf{R}$, $x \leq y$ e $y \leq z$ implica $x \leq z$,

d) totalità: per ogni coppia di numeri reali x e y vale sempre una delle relazioni $x \leq y$ oppure $y \leq x$.

La relazione $<$ soddisfa le seguenti proprietà di compatibilità con la somma e il prodotto:

e) monotonia rispetto alla somma: per ogni x, y e z in $\mathbf{R}$ se $x<y$ allora $x+z<y+z$,

f) monotonia rispetto al prodotto: per ogni x, y z in $\mathbf{R}$ *se $x < y$ e z è positivo allora $zx < zy$.*

Lasciamo al lettore la cura di dimostrare il Teorema 3.1 a partire dagli Assiomi 7 e 8. Elenchiamo alcune altre proprietà utili della relazione d'ordine.

- *Se $x \neq 0$ allora $x^2 > 0$.*
- *Per ogni x, y z in* $\mathbf{R}$ *se $x < y$ e z è negativo allora $zx > zy$.*
- *Se $x < y$ allora $-x > -y$.*
- *Se $xy > 0$ allora x e y sono entrambi positivi o entrambi negativi.*

Definizione. Siano a e b due numeri reali tali che $a < b$. L' *intervallo aperto di estremi* a e b è l'insieme $(a, b) = \{x \in R : a < x < b\}$; a è il primo estremo, b il secondo estremo. L'*intervallo chiuso* di estremi a e b è l'insieme $[a, b] = \{x \in R : a \leq x \leq b\}$. In maniera analoga si definiscono l'*intervallo semiaperto a destra* $[a, b)$ e l'*intervallo semiaperto a sinistra* $(a, b]$ mediante le disuguaglianze $a \leq x < b$ e $a < x \leq b$. Questi intervalli sono detti *limitati*. Gli intervalli semilitati sono gli insiemi

$$\begin{array}{rcll}
(a, +\infty): & = & \{x \in \mathbf{R} : a < x\} & \textit{intervallo aperto semilitato a sinistra} \\
{[a, +\infty)}: & = & \{x \in \mathbf{R} : a \leq x\} & \textit{intervallo chiuso semilitato a sinistra} \\
(-\infty, a): & = & \{x \in \mathbf{R} : x < a\} & \textit{intervallo aperto semilitato a destra} \\
(-\infty, a]: & = & \{x \in \mathbf{R} : x \leq a\} & \textit{intervallo chiuso semilitato a destra}
\end{array}$$

Sono intervalli anche l'insieme $\mathbf{R}$ (denotato talvolta con $(-\infty, +\infty)$), l'insieme vuoto $\emptyset$ e l'insieme costituito da un solo elemento $\{a\}$. Gli ultimi due sono detti *intervalli degeneri.*

4 Valore assoluto

Definizione. Sia x un numero reale. Si dice valore *assoluto* o *modulo* di x il numero reale $|x|$ definito da

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

Proposizione 4.1 *Il valore assoluto soddisfa le seguenti proprietà*

a) $|x| \geq 0$ per ogni x in $\mathbf{R}$ *e $|x| = 0$ se e solo se $x = 0$;*

b) $|x| = |-x|$;

c) $-|x| \leq x \leq |x|$*;*

d) se a *è un numero reale maggiore o uguale a* 0 *allora* $|x| \leq a$ *se e solo se* $-a \leq |x| \leq a$*.*

e) $|xy| = |x|\,|y|$*;*

f) $|x+y| \leq |x| + |y|$*;*

g) $||x| - |y|| \leq |x-y|$

per ogni x *e* y *in* $\mathbf{R}$*.*

Dimostrazione. Le prime quattro proprietà sono conseguenze immediate della definizione di valore assoluto. Per dimostrare la quarta si possono considerare separatamente i quattro casi $x \geq 0$ e $y \geq 0$; $x \geq 0$ e $y < 0$; $x < 0$ e $y \geq 0$; $x < 0$ e $y < 0$. Per dimostrare la f) si sommano le disuguaglianze $-|x| \leq x \leq |x|$ e $-|y| \leq x \leq |y|$ ottenendo

$$-(|x| + |y|) \leq x + y \leq |x| + |y|.$$

Quindi, per la d), $|x+y| \leq |x| + |y|$. Per dimostrare la g) osserviamo che

$$|x| = |(x-y) + y| \leq |x-y| + |y|$$

e quindi

$$|x| - |y| \leq |x-y|.$$

Scambiando x e y tra loro si ha anche

$$|y| - |x| \leq |y-x| = |x-y|.$$

La conclusione segue dalla d) perché $|x| - |y|$ e $|y| - |x|$ sono opposti l'uno dell'altro. □

Le disuguaglianze f) e g) sono dette *disuguaglianze triangolari*, perché quando vengono generalizzate ai vettori esprimono il fatto che la lunghezza di un lato di un triangolo è minore o uguale alla somma ed è maggiore o uguale alla differenza delle lunghezze degli altri due.

5 I numeri naturali e gli interi

In questa sezione descriviamo due sottoinsiemi particolari di $\mathbf{R}$, l'insieme $\mathbf{N}$ dei *numeri naturali* e l'insieme $\mathbf{Z}$ degli *interi*.

Definizione. Un sottoinsieme A di $\mathbf{R}$ si dice *induttivo* se ha le seguenti due proprietà:

a) $0 \in A$;

b) per ogni x, se $x \in A$ allora $x + 1 \in A$.

Sono esempi di insiemi induttivi $\mathbf{R}$ stesso e $\mathbf{R}_+ \cup \{0\}$.

Definizione. L'insieme $\mathbf{N}$ dei numeri naturali è l'intersezione di tutti i sottoinsiemi induttivi di $\mathbf{R}$.

L'insieme $\mathbf{N}$ è non vuoto, perché $0 \in \mathbf{N}$. Inoltre è facile vedere che $\mathbf{N}$ stesso è induttivo. Pertanto $1 = 0 + 1 \in \mathbf{N}$, $2 = 1 + 1 \in \mathbf{N}$, $3 = 2 + 1 \in \mathbf{N}$. Poichè $\mathbf{N}$ è contenuto in ogni insieme induttivo, esso è il più piccolo insieme induttivo. Precisamente si ha il seguente teorema.

Teorema 5.1 (teorema di induzione) *Sia A un sottoinsieme di $\mathbf{N}$ tale che*

a) $0 \in A$,

b) per ogni n in $\mathbf{N}$, $n \in A$ implica $n + 1 \in A$,

allora $A = \mathbf{N}$.

Dimostrazione. L'insieme A è induttivo. Quindi $\mathbf{N} \subseteq A$ e, poiché $A \subseteq \mathbf{N}$, si ha $A = \mathbf{N}$. □

Il Teorema di induzione è alla base di uno schema dimostrativo detto *principio di induzione*. Prima di enunciare il principio di induzione dobbiamo definire alcune nozioni logiche.

Definizione. Diremo *enunciato* o *formula* un'espressione sintatticamente ben formata, come ad esempio: "Parigi è in Inghilterra", "x è un uomo", "x+y=4", "se $x \in \mathbf{R}$ allora $x^2 \neq -1$". Denoteremo gli enunciati con lettere come P, Q, ecc.

Come si vede un enunciato può contenere delle variabili che possono assumere valori in un dato insieme. Le variabili che sono precedute dalle parole *per ogni* o *esiste* si dicono legate, le altre variabili si dicono libere. Così nell'enunciato "per ogni x in $\mathbf{R}$ esiste un y in $\mathbf{R}$ tale che $x + y = z$", le variabili x e y sono legate, mentre la variabile z è libera. Gli enunciati si dicono *aperti* se contengono delle variabili libere, *chiusi* se non contengono variabili o se tutte le variabili che appaiono in essi sono legate. Un *enunciato aperto* è detto anche un *predicato*. Se P è un predicato, scriveremo $P[x]$ tutte le volte che vorremo indicare che x è una delle variabili libere di P.

La negazione di un enunciato si ottiene premettendo la parola *non* all'enunciato stesso. Un enunciato P si dice *vero* se è un assioma o è deducibile dagli assiomi, si dice *falso* (o *refutabile*) se non–P è vero.[3] Si osservi che 'falso' non significa 'non vero'. Ad esempio l'enunciato "$x = 0$" non è né vero né falso nella teoria i cui assiomi sono A.1–A.8. Infatti in ogni campo vi sono due elementi distinti 0 e 1, uno solo dei quali soddisfa il predicato.

[3] Nel definire i termini 'vero' e 'falso' abbiamo seguito l'uso prevalente tra i matematici. Avvertiamo però il lettore che i logici matematici preferiscono dire P è dimostrabile e non–P è dimostrabile, riservando l'uso dei termini 'vero' e 'falso' ad un altro contesto.

Si noti che vi sono degli enunciati aperti che sono veri, come ad esempio "se $x \in \mathbf{R}$ allora $x^2 \geq 0$".[4]

Teorema 5.2 (principio di induzione) *Sia $P[n]$ un predicato in cui la variabile n è un numero naturale. Supponiamo che i seguenti due enunciati*

a) $P[0]$,

b) $P[n]$ *implica* $P[n+1]$,

siano veri. Allora $P[n]$ è vero per ogni n in $\mathbf{N}$.

Dimostrazione. Proviamo che l'insieme $A = \{n \in \mathbf{N} : P[n] \text{ è vero}\}$ è induttivo. Infatti $0 \in A$ perché $P[0]$ è vero. Se $n \in A$ allora $P[n]$ è vero e quindi per b) è vero anche $P[n+1]$. Quindi $n+1 \in A$. Poiché n è arbitrario, abbiamo dimostrato che, per ogni n, $n \in A$ implica $n+1 \in A$. [5] Pertanto A è induttivo e, quindi, $A = \mathbf{N}$ per il Teorema di induzione. Questo significa che $P[n]$ è vero per ogni $n \in \mathbf{N}$. $\square$

È essenziale che il lettore comprenda perfettamente il significato del principio di induzione. Essa afferma che, se vogliamo dimostrare che una proprietà vale per tutti i numeri naturali, non è necessario dimostrarla per ogni numero. Basta dimostrare che essa vale per 0 e che, **se** vale per un numero naturale n, vale anche per $n+1$. Il principio di induzione non è l'unico modo per dimostrare che una proprietà vale per tutti i numeri naturali. Per il principio di generalizzazione (vedi nota a pié di pagina), per dimostrare che $P[n]$ è vero per ogni n basta dimostrarlo per un n generico. Tuttavia in molti casi è più facile dimostrare che $P[0]$ è vero e che "$P[n]$ implica $P[n+1]$" è vero per un generico n, piuttosto che dimostrare direttamente che $P[n]$ è vero per un generico n.

Esaminiamo ora alcune proprietà dei numeri naturali.

Proposizione 5.3 *I numeri naturali sono maggiori o uguali a 0. Se m e n sono numeri naturali allora anche $m+n$ e mn sono numeri naturali. Se $m > n$ allora $m-n$ è un numero naturale.*

Dimostrazione. Tutte queste proprietà si dimostrano facilmente mediante il principio di induzione. A titolo d'esempio dimostriamo l'ultima, cioè che se $m > n$ allora $m-n$ è un numero naturale. Osserviamo dapprima che, poiché l'insieme $\{0\} \cup \{k \in \mathbf{N} : k = q+1, q \in \mathbf{N}\}$ è induttivo, per ogni numero naturale $k \neq 0$ esiste un numero naturale q tale $k = q+1$. Fissato un numero naturale arbitrario $m > 0$, indichiamo con $P[n]$ il predicato: "se $m > n$

[4] Si potrebbe credere che un enunciato chiuso debba sempre essere dimostrabile o refutabile. Tuttavia non è così: un risultato profondo di logica, dovuto a K. Gödel (1931), asserisce che, se l'aritmetica non è contradditoria, vi sono in essa enunciati chiusi P che sono *indecidibili*, cioè tali che P non è dimostrabile e non$-P$ non è dimostrabile.

[5] Questo è un esempio di applicazione di un metodo di dimostrazione detto *principio di generalizzazione*: sia $P[x]$ un enunciato che contiene la variabile libera x; se $P[x]$ è vero allora "per ogni x $P[x]$" è vero. In linguaggio meno formale: per dimostrare che $P[x]$ è vero per ogni x basta dimostrare che $P[x]$ è vero per un "generico" x.

allora $m-n$ è un numero naturale". Se $m > 0$ allora $m - 0 = m \in \mathbf{N}$. Quindi $P[0]$ è vero. Dimostriamo ora che $P[n]$ implica $P[n+1]$. Se $m > n+1$ allora si ha anche $m > n$ e quindi, per $P[n]$, si ha che $m - n \in \mathbf{N}$. Poiché $m - n > 1$, $m - n$ è un numero naturale diverso da 0 e quindi esiste un numero naturale q tale che $m-n = q+1$. Quindi $m-(n+1) = q \in \mathbf{N}$ e $P[n+1]$ è cosí dimostrato. $\square$

Proposizione 5.4 *Se n è un numero naturale non esistono numeri naturali maggiori di n e minori di $n+1$.*

Dimostrazione. Non vi sono numeri naturali maggiori di 0 e minori di 1, perché l'insieme $\{0\} \cup \{n \in \mathbf{N} : n \geq 1\}$ è induttivo. Se m e n fossero due numeri naturali tali che $n < m < n+1$, allora $m-n$ sarebbe un numero naturale maggiore di 0 e minore di 1. Ma questo contraddice quanto abbiamo appena provato. [6] $\square$

Una variante del principio di induzione che è utile in talune applicazioni è la seguente.

Corollario 5.5 (Principio di induzione generalizzato) *Siano $P[n]$ un predicato in cui la variabile n è un numero naturale e n_0 un numero naturale. Supponiamo che i seguenti due enunciati*

a) $P[n_0]$,

b) $P[n]$ *implica* $P[n+1]$,

siano veri. Allora $P[n]$ è vero per ogni $n \geq n_0$.

Dimostrazione. Se $n \geq n_0$ allora, per la Proposizione 5.3, esiste un numero naturale k tale che $n = n_0 + k$. Basta quindi osservare che l'insieme $\{k \in \mathbf{N} : P[k+n_0] \text{ è vero}\}$ coincide con $\mathbf{N}$ perché è induttivo. $\square$

Definizione. Sia X un insieme. Una *successioni a valori in X* è una funzione a definita su $\mathbf{N}$ a valori in X. Se $X = \mathbf{R}$ si dice che a è una successione *a valori reali.* Se $a : \mathbf{N} \to X$ è una successione è uso comune scrivere a_n per indicare il valore $a(n)$ di a in n. Si dice anche che a_n è *il termine n-esimo* della successione (a_n). Una successione può essere definita mediante una formula esplicita che permette di calcolare il valore a_n per ogni numero naturale n. Ad esempio $a_n = n^3 + 1$. Vi è però un altro modo di definire una successione mediante un procedimento noto come *definizione per ricorrenza.* Grosso modo il metodo di ricorrenza consiste nel definire una successione definendo a_0 e assegnando una procedura per calcolare a_{n+1}, dopo aver supposto che a_n sia già stato definito. La giustificazione di questo metodo si basa sul seguente *teorema di ricorrenza.*

Teorema 5.6 *Se x è un elemento di un insieme X e ϕ è una funzione da X in X, esiste un'unica successione (a_n) tale che $a_0 = x$ e $a_{n+1} = \phi(a_n)$, per ogni n in $\mathbf{N}$.*

[6] Questo è un primo esempio di *dimostrazione per contraddizione* o *per assurdo*: se aggiungendo l'enunciato non–Q agli assiomi si ottiene una contraddizione, cioè si dimostra sia R che non–R, allora Q è vero.

Dimostrazione. La dimostrazione del teorema di ricorrenza si basa sul principio di induzione. L'unicità della successione (a_n) è facile da dimostrare. Per dimostrare l'esistenza proviamo dapprima che per ogni intero $n \geq 1$ esiste una funzione g_n, definita su $\{0, 1, \ldots, n\}$ a valori in X, tale che

$$g_n(0) = x, \qquad g_n(k+1) = \phi(g_n(k)), \quad k = 0, 1, \ldots, n-1. \tag{5.1}$$

Se $n = 1$ poniamo $g_1(0) = x$, $g_1(1) = \phi(g_1(0))$. Supponiamo ora che l'assunto sia vero per un intero $n \geq 1$ arbitrario e definiamo g_{n+1} su $\{0, 1, \ldots, n+1\}$ ponendo

$$g_{n+1}(k) = g_n(k), \quad \text{se } k = 0, 1, \ldots, n, \qquad g_{n+1}(n+1) = \phi(g_{n+1}(n)).$$

È immediato verificare che g_{n+1} soddisfa la relazione

$$g_{n+1}(0) = x, \qquad g_{n+1}(k+1) = \phi(g_{n+1}(k)), \quad k = 0, 1, \ldots, n.$$

Quindi, per il principio di induzione, abbiamo dimostrato l'esistenza della funzione g_n per ogni intero $n \geq 1$. A questo punto è immediato verificare che la successione (a_n) definita da

$$a_0 = x, \qquad a_n = g_n(n), \quad n \geq 1,$$

soddisfa la relazione ricorsiva $a_{n+1} = \phi(a_n)$. □

Illustriamo ora l'uso del teorema di ricorrenza con un esempio. Consideriamo la funzione ϕ di $\mathbf{R}$ in $\mathbf{R}$, definita da $\phi(x) = x^3 + 1$. Per il teorema di ricorrenza, fissato un numero reale x, è possibile definire una successione $a : \mathbf{N} \to \mathbf{R}$ ponendo

$$a_0 = x, \qquad a_{n+1} = a_n^3 + 1.$$

Utilizzando la formula ricorsiva possiamo calcolare a_n qualunque sia il numero naturale n. Ad esempio, prendendo $x = 1$, si ha

$$a_0 = 1, \quad a_1 = a_0^3 + 1 = 2, \quad a_2 = a_1^3 + 1 = 9, \quad \ldots,$$

Si noti che il teorema di ricorrenza garantisce che la successione (a_n) è definita anche se non è data una formula esplicita per calcolare a_n a partire da n.

Non sempre il rapporto di due numeri naturali è un numero naturale. Tuttavia in $\mathbf{N}$ è possibile effettuare la divisione con resto, come dimostra il seguente teorema.

Teorema 5.7 *Siano n, d in $\mathbf{N}$, con $d > 0$. Esistono due numeri naturali q e r, univocamente determinati, tali che $n = qd + r$ e $0 \leq r < d$.*

Dimostrazione. Per dimostrare l'esistenza procediamo per induzione su n. Se $n = 0$ basta prendere $q = r = 0$. Supponiamo che per un numero naturale n arbitrario si abbia $n = qd + r$, con $0 \leq r < d$ e dimostriamo che esistono q' e r', con $0 \leq r' < d$, tali che $n + 1 = q'd + r'$. Se $r < d - 1$ allora $n + 1 = qd + r + 1$ e $0 \leq r + 1 < d$. Quindi $q' = q$ e $r' = r + 1$. Se $r = d - 1$ allora $n + 1 = qd + d = (q + 1)d$. Quindi $q' = q + 1$ e $r' = 0$.

Per dimostrare l'unicità supponiamo che $n = q_0 d + r_0 = q_1 d + r_1$ con $0 \leq r_0, r_1 < d$. Allora $(q_1 - q_0)d = r_1 - r_0$. Se, per assurdo, $q_0 \neq q_1$ possiamo supporre che $q_0 < q_1$. Allora si ottiene la contraddizione $d \leq (q_1 - q_0)d = r_1 - r_0 < d$. Pertanto $q_1 = q_0$ e $r_1 = r_0$. □

I numeri q e r si dicono il *quoziente* e il *resto* della divisione di n per d. Se $r = 0$ si dice che d è un *divisore* di n o che n è un *multiplo* di d e si scrive $d|n$ (leggi: d divide n).

Definizione. Un numero naturale $p > 1$ si dice *primo* se i suoi divisori sono solo p e 1. L'intero 1 non è un numero primo.

Un risultato fondamentale della teoria dei numeri interi è il seguente *teorema di fattorizzazione unica.*

Teorema 5.8 *Ogni numero naturale > 1 è primo o si fattorizza nel prodotto di numeri primi. La fattorizzazione è unica a parte l'ordine dei fattori.*

Dimostrazione. Ci limitiamo a dimostrare che ogni intero $n > 1$ è primo o si fattorizza nel prodotto di fattori primi, rinviando il lettore al corso di algebra per la dimostrazione dell'unicità della fattorizzazione. Sia $P[n]$ il predicato: tutti gli interi k tali che $2 \leq k \leq n$ sono primi o si fattorizzano nel prodotto di numeri primi. Allora $P[2]$ è vero. Supponiamo che $P[n]$ sia vero. Per dimostrare che anche $P[n+1]$ è vero è sufficiente provare che anche $n+1$ si fattorizza nel prodotto di numeri primi. Se $n+1$ stesso non è primo esistono due interi $k \leq n$ e $m \leq m$ tali che $n = km$. Poiché k e m sono entrambi minori o uguali di n, essi sono primi o si fattorizzano in prodotto di numeri primi; quindi anche $n+1$ è il prodotto di primi. □

Definizione. L'insieme $\mathbf{Z} = \{k \in \mathbf{R} : k \in \mathbf{N} \text{ oppure } -k \in \mathbf{N}\}$ è detto insieme degli *interi.* È facile vedere che se k è un intero anche $k-1$ e $k+1$ sono interi e che non vi sono interi maggiori di k e minori di $k+1$. Gli interi $k-1$ e $k+1$ sono detti rispettivamente *l'antecedente* e il *successivo* di k. L'insieme degli interi positivi si denota con $\mathbf{Z}_+$ o con $\mathbf{N}_+$.

6 I razionali

I quozienti di interi m/n, dove $n \neq 0$ sono detti *numeri razionali.* L'insieme dei numeri razionali si denota con $\mathbf{Q}$ e contiene l'insieme degli interi $\mathbf{Z}$. A differenza degli interi, dati due numeri razionali r e s con $r < s$, esiste sempre un altro numero razionale t tale che $r < t < s$: basta prendere per t la media $(r+s)/2$. Questa proprietà di $\mathbf{Q}$ si esprime dicendo che $\mathbf{Q}$ è *denso in sé.* Iterando il procedimento si può intuire che tra due numeri razionali vi sono sempre infiniti numeri razionali.[7] Non ha quindi senso parlare di antecedente o successivo di un numero razionale.

Il lettore può verificare facilmente che l'insieme $\mathbf{Q}$ soddisfa gli assiomi di campo e gli assiomi dell'ordine. Per questa ragione si dice che $\mathbf{Q}$ è un *campo ordinato.* L'insieme dei razionali positivi si denota con $\mathbf{Q}_+$.

[7]La definizione rigorosa di insieme infinito verrà precisata in seguito.

7 La rappresentazione geometrica dei razionali

I numeri razionali si possono rappresentare geometricamente come punti su una retta euclidea. Sia $\mathcal{R}$ una retta orientata. Scegliamo su di essa un punto O, detto *origine*, un punto U distinto da O sulla semiretta positiva e assumiamo il segmento $\overline{OU}$ come unità di misura delle lunghezze. Con semplici operazioni geometriche è possibile costruire multipli e sottomultipli del segmento $\overline{OU}$. Quindi assegnamo al numero razionale $r = m/n$ il punto P sulla semiretta positiva tale che $\overline{OP} = m/n\,\overline{OU})$ se $m, n > 0$, il punto P sulla semiretta negativa tale che $\overline{PO} = -m/n\,\overline{OU})$ se $m < 0,\ n > 0$. Al numero 0 assegnamo il punto O. Il numero razionale r si dice *ascissa* del punto P. L'applicazione di $\mathbf{Q}$ in $\mathcal{R}$ così definita è iniettiva ma non surgettiva. L'iniettività segue dal fatto che se $r < s$ l'immagine di r sulla retta precede l'immagine di s nell'orientazione fissata. Per dimostrare che non tutti i punti della retta hanno un'ascissa razionale premettiamo il seguente lemma.

Lemma 7.1 *Non esiste alcun numero razionale r tale che $r^2 = 2$.*

Dimostrazione. Supponiamo per assurdo che esista un numero razionale r tale che $r^2 = 2$. Poiché $r^2 = (-r)^2$, possiamo supporre che r sia positivo. Sia quindi $r = m/n$ con $m, n > 0$. Allora $m^2 = 2n^2$ e questo contraddice l'unicità della decomposizione dei numeri naturali in fattori primi, perché il fattore 2 compare con un esponente pari nel primo membro e con un esponente dispari nel secondo membro. $\square$

Proposizione 7.2 *Sia $\overline{OP}$ il segmento di lunghezza uguale alla diagonale del quadrato di lato $\overline{OU}$. Allora il punto P non corrisponde ad alcun numero razionale.*

Dimostrazione. Se r fosse un numero razionale tale che $\overline{OP} = r\,\overline{OU}$, per il teorema di Pitagora si avrebbe $r^2 = 2$. Ma questo contraddice il Lemma 7.1. $\square$

L'insieme dei numeri razionali si rivela quindi insufficiente per risolvere il problema della misura delle grandezze omogenee. Infatti i numeri razionali permettono di misurare solo quelle grandezze che sono *commensurabili* con l'unità di misura scelta. Vedremo invece che questo inconveniente non si verica con l'insieme dei numeri reali perchè $\mathbf{R}$ soddisfa un ulteriore assioma: l'assioma di completezza.

8 L'assioma di completezza

Prima di enunciare l'assioma di completezza è necessario introdurre alcune definizioni e notazioni. Sia X un insieme totalmente ordinato, cioè un insieme su cui è definita una relazione $\leq$ riflessiva, antisimmetrica, transitiva e che soddisfa la condizione di totalità del Teorema 3.1.

Definizione. Sia S un sottoinsieme non vuoto di X. Diremo che un elemento a di X é un *minorante* di S se $a \leq x$ per ogni $x \in S$. Analogamente diremo che elemento b di X è un *maggiorante* di S se $x \leq b$ per ogni $x \in S$. Un insieme S si dice *inferiormente limitato* se esiste almeno un minorante di S, *inferiormente illimitato* se l'insieme dei minoranti di

S è vuoto. Le definizioni di insieme *superiormente limitato*, *superiormente illimitato* sono analoghe. Un insieme si dice *limitato* se è superiormente e inferiormente limitato. Un minorante di S che appartiene a S si dice *minimo* di S; un maggiorante di S che appartiene a S si dice *massimo* di S. Un insieme può avere al più un minimo e al più un massimo. Infatti, se a e a' sono minoranti di S e appartengono entrambi a S, si ha $a \leq a'$ e $a' \leq a$ e quindi $a = a'$. L'unicità del massimo si prova in modo analogo. Le notazioni $\min S$ e $\max S$ denoteranno il minimo e il massimo di S.

Diamo alcuni esempi per illustrare questi concetti.

Esempio 1. Sia $X = \mathbf{R}$. L'intervallo $[0, 1)$ è limitato. L'insieme dei minoranti è l'intervallo $(-\infty, 0]$. L'insieme dei maggioranti è l'intervallo $[1, +\infty)$. Poichè 0 è un minorante e appartiene all'insieme $[0, 1)$ si ha $0 = \min[0, 1)$. L'insieme è privo di massimo.

Esempio 2. Sia $X = \mathbf{Q}$, $S = \{1/n : n \in \mathbf{Z}_+\}$. Allora l'insieme dei maggioranti di S è l'insieme dei razionali maggiori o uguali a 1. Poiché $1 \in S$ si ha che $1 = \max S$. Ogni numero razionale ≤ 0 è un minorante di S e non vi sono altri minoranti, perché, se $r = m/n$ è un numero razionale positivo, $1/(n+1) < r$ e quindi r non è un minorante di S. Pertanto 0 è il massimo dell'insieme dei minoranti di S, ma S è privo di minimo.

Definizione. Se l'insieme dei minoranti di S ha massimo a si dice che a è *l'estremo inferiore* di S. Analogamente, se l'insieme dei maggioranti di S ha minimo b si dice che b è *l'estremo superiore* di S.

L'estremo inferiore e l'estremo superiore di un insieme, se esistono, sono necessariamente unici. Essi si denotano rispettivamente con $\inf S$ e $\sup S$. Si noti che se S ha minimo esso coincide con l'estremo inferiore. Tuttavia, come mostra l'Esempio 2, un insieme può avere estremo inferiore senza avere minimo. Viceversa se l'estremo inferiore di S appartiene a S, esso è il minimo di S. Considerazioni analoghe valgono per estremo superiore e massimo.
Possiamo ora formulare l'assioma di completezza.

Assioma 9 *Ogni sottoinsieme non vuoto superiormente limitato di* $\mathbf{R}$ *ha estremo superiore.*

Il fatto che ogni sottoinsieme non vuoto e inferiormente limitato di $\mathbf{R}$ ha estremo inferiore è una conseguenza del seguente risultato generale valido in ogni insieme totalmente ordinato.

Proposizione 8.1 *Sia* X *un insieme totalmente ordinato. Ogni sottoinsieme non vuoto inferiormente limitato di* X *ha estremo inferiore se e solo se ogni sottoinsieme non vuoto superiormente limitato di* X *ha estremo superiore.*

Dimostrazione. Proviamo la sufficienza della condizione, lasciando la dimostrazione della necessità al lettore per esercizio. Sia S un sottoinsieme non vuoto inferiormente limitato di X e sia S_* l'insieme dei minoranti di S. Allora S_* è non vuoto e superiormente limitato (tutti gli elementi di S sono maggioranti di S_*). Pertanto per l'assioma di completezza S_* ha estremo superiore a. Poiché a è il minimo dei maggioranti di S_* e gli elementi di S sono maggioranti di S_*, si ha che $a \leq x$ per ogni x in S. Quindi a è un minorante di S e perciò $a \in S_*$. Questo prova che $a = \max S_* = \inf S$. $\square$

Il lettore può verificare facilmente che, se S è un sottoinsieme non vuoto e superiormente limitato di $\mathbf{R}$ e $a = \sup S$, allora l'insieme dei maggioranti di S è l'intervallo chiuso semilimitato a sinistra $[a, +\infty)$. Analogamente, se S è un sottoinsieme non vuoto e inferiormente limitato di $\mathbf{R}$ e $b = \inf S$, allora l'insieme dei minoranti di S è l'intervallo chiuso semilimitato a destra $(-\infty, b]$. Queste osservazioni forniscono un criterio utile per determinare l'estremo superiore e l'estremo inferiore degli insiemi. Ad esempio per determinare l'estremo superiore di un insieme S si determina dapprima l'insieme dei maggioranti di S risolvendo le disequazioni $x \geq s$ per ogni s in S. L'insieme delle soluzioni è un intervallo chiuso semilitato a sinistra $[a, +\infty)$. Quindi $\sup S = \min [a, +\infty) = a$.

Un altro criterio utile per determinare l'estremo inferiore e l'estremo superiore di un insieme si basa sulla seguente proprietà: se l'insieme S ha estremo superiore vi sono elementi in S "arbitrariamente vicini" a $\sup S$; se S ha estremo inferiore vi sono in S elementi "arbitrariamente" vicini a $\inf S$.

Proposizione 8.2 *Sia S un sottoinsieme non vuoto di $\mathbf{R}$. Un numero reale a è l'estremo superiore di S se e solo se a è un maggiorante di S e per ogni $\epsilon > 0$ esiste un elemento s in S tale che $a - \epsilon < s$. Analogamente a è l'estremo inferiore di S se e solo se a è un minorante di S e per ogni $\epsilon > 0$ esiste un elemento s in S tale che $s < a + \epsilon$.*

Dimostrazione. . Sia $a = \sup S$. Se esistesse un $\epsilon > 0$ tale che per ogni s in S si avesse $s \leq a - \epsilon$, allora $a - \epsilon$ sarebbe un maggiorante di S minore di a. Questo contraddice il fatto che a è il minimo dei maggioranti. Viceversa, supponiamo che a sia un maggiorante di S e che che per ogni $\epsilon > 0$ esista un s in S tale che $a - \epsilon < s$. Dimostriamo che a è il minimo dei maggioranti di S. Se $b < a$, posto $\epsilon = b - a > 0$, si avrebbe che esiste un elemento s in S tale che $a - \epsilon = b < s$. Pertanto b non sarebbe un maggiorante di S. La dimostrazione della caratterizzazione dell'estremo inferiore è simile. □

9 Conseguenze della completezza

In questa sezione esponiamo alcune proprietà dei numeri reli che derivano dall'assioma di completezza. Cominciamo con il dimostrare che l'insieme dei numeri reali soddisfa una proprietà analoga al *postulato di continuità della retta.*[8]

Definizione. Una coppia (A, B) di sottoinsiemi non vuoti di $\mathbf{R}$ si dice *separata* se per ogni a in A e b in B si ha $a \leq b$. Una coppia separata si dice *contigua* se per ogni numero reale $\epsilon > 0$ esistono due elementi a in A e b in B tali che $b - a < \epsilon$. Un numero reale x si dice un *elemento di separazione* della coppia (A, B) se $a \leq x \leq b$ per ogni a in A e b in B.

[8] Il postulato di continuità della retta, nella formulazione di Cantor, è il seguente: siano $\mathcal{A}$ e $\mathcal{B}$ sono due sottoinsiemi della retta orientata tali che:

(i) ogni punto di $\mathcal{A}$ precede ogni punto di $\mathcal{B}$ nell'orientazione fissata;

(ii) comunque fissato un numero razionale $r > 0$ esistono due punti P in $\mathcal{A}$ e Q in $\mathcal{B}$ tali che la lunghezza del segmento $\overline{PQ}$ è minore di r.

Allora esiste uno e un solo punto della retta compreso tra $\mathcal{A}$ e $\mathcal{B}$.

Teorema 9.1 *Se (A, B) è una coppia separata di sottoinsiemi non vuoti di* $\mathbf{R}$ *esiste almeno un elemento di separazione. Se la coppia è contigua l'elemento di separazione è unico.*

Dimostrazione. Ogni elemento di B è un maggiorante di A. Quindi A è superiormente limitato e, per l'assioma di completezza, esiste $\sup A$. Poiché $\sup A$ è il minimo dei maggioranti di A, si ha $\sup A \leq b$ per ogni b in B. Quindi $\sup A$ è un minorante di B e pertanto $\sup A \leq \inf B$. Tutti gli elementi dell'intervallo $[\sup A, \inf B]$ sono elementi di separazione della coppia (A, B). Supponiamo ora che (A, B) sia contigua. Osserviamo che se x è un elemento di separazione allora deve essere $\sup A \leq x \leq \inf B$. Quindi, per dimostrare l'unicità dell'elemento di separazione, basta provare che $\sup A = \inf B$. Se, per assurdo, fosse $\sup A < \inf B$, preso $\epsilon = (\inf B - \sup A)/2 > 0$ esisterebbero due elementi a in A e b in B, tali che $b - a < (\inf B - \sup A)/2$. Ma questo è impossibile perché $a \leq \sup A < \inf B \leq b$ e quindi $\inf B - \sup A \leq b - a$. Pertanto $\sup A = \inf B$ e il teorema è dimostrato. □

Utilizzando il Teorema 9.1 e il postulato di continuità della retta, si ottiene la rappresentazione geometrica dei numeri reali. Precisamente si può dimostrare il seguente teorema.

Teorema 9.2 *La corrispondenza che ad ogni numero razionale associa un punto sulla retta $\mathcal{R}$, definita nella Sezione 6, si estende in modo unico a una corrispondenza biunivoca di* $\mathbf{R}$ *su $\mathcal{R}$ che preserva l'ordine. In altri termini esiste un'unica funzione bigettiva $\phi : \mathbf{R} \to \mathcal{R}$ tale che*

- $\phi(r) = r\overline{OU}$ *per ogni r in* $\mathbf{Q}$,
- *se x e y sono due numeri reali tali che $x < y$ allora $\phi(x)$ precede $\phi(y)$ nell'orientamento fissato sulla retta.*

La corrispondenza tra $\mathbf{R}$ e la retta euclidea risulta univocamente determinata, una volta che siano stati fissati un orientamento sulla retta, un'origine e un'unità di misura. Essa viene detta un *riferimento cartesiano su $\mathcal{R}$*. Il numero reale x che corrisponde al punto P è detto *ascissa* di P. L'insieme dei numeri reali viene quindi rappresentato geometricamente come l'insieme dei punti della retta. Questa rappresentazione geometrica ci consente di utilizzare un linguaggio geometrico nel parlare dei numeri reali. Così spesso parleremo del punto x anziché del punto di ascissa x; il valore assoluto $|x - y|$ verrà detto *distanza* dei punti x e y, e diremo che il punto x *si trova tra* a e b se $a \leq x \leq b$. Conseguentemente le espressioni *retta reale* o *asse reale* verranno utilizzati indifferentemente per denotare l'insieme dei numeri reali o una retta dotata di un riferimento cartesiano. Tuttavia noi utilizzeremo questa identificazione dell'insieme dei numeri reali con la retta reale soltanto come stampella per la nostra intuizione, senza mai fare riferimento a considerazioni geometriche per la dimostrazione delle proprietà di $\mathbf{R}$, che verranno dedotte esclusivamente dagli assiomi.[9]

[9] L'identificazione dei numeri reali con i punti della retta euclidea orientata, dopo aver scelto un'origine e un'unità di misura delle lunghezze, è alla base della costruzione geometrica del campo dei numeri reali data nel XVI secolo da R. Bombelli nel IV libro della sua *Algebra*. L'operazione di somma di due punti P e Q "positivi" (cioè che seguono l'origine nell'orientazione della retta) è definita geometricamente come somma dei segmenti $\overline{OP}$ e $\overline{OQ}$. Per definire il prodotto di P e Q si utilizza l'assioma di esistenza e unicità del

10 Archimedeità dei reali

In questa sezione esaminiamo alcune altre proprietà dei numeri reali che derivano dalla completezza.

Proposizione 10.1 *Ogni sottoinsieme non vuoto e superiormente limitato di* $\mathbf{Z}$ *ha massimo.*

Dimostrazione. Sia A un sottoinsieme non vuoto e superiormente limitato di $\mathbf{Z}$. Per l'assioma di completezza esiste $a \in \mathbf{R}$ tale che $a = \sup A$. Supponiamo, per assurdo, che a non sia il massimo di A, cioè che $a \notin A$. Per la caratterizzazione dell'estremo superiore (Proposizione 8.2) dovrebbe esistere un elemento k di A tale che $a - 1 < k < a$. Poiché abbiamo supposto che A non ha massimo, esiste un altro elemento h in A tale che $a - 1 < k < h < a$. Pertanto $k - h$ sarebbe un intero strettamente compreso tra 0 e 1. Questo contraddice la Proposizione 5.4. □

In modo analogo si dimostra che ogni sottoinsieme non vuoto inferiormente limitato di $\mathbf{Z}$ ha minimo. In particolare ogni sottoinsieme non vuoto di $\mathbf{N}$ ha minimo. Un insieme ordinato che gode della proprietà che ogni sottoinsieme non vuoto ha minimo si dice *bene ordinato.*

Corollario 10.2 *L'insieme dei numeri naturali è illimitato superiormente.*[10]

Dimostrazione. Se, per assurdo, $\mathbf{N}$ fosse superiormente limitato esso avrebbe massimo m per la Proposizione 10.1. Poiché $m + 1$ è un numero naturale maggiore di m si ha una contraddizione. □

Definizione. Un campo ordinato $\mathbf{K}$ si dice *archimedeo* [11] se per ogni coppia di elementi positivi ϵ e a esiste un intero positivo n tale che $n\epsilon > a$.

Teorema 10.3 *Il campo reale è archimedeo.*

Dimostrazione. Se $n\epsilon \leq a$ per ogni intero positivo n, l'insieme dei numeri naturali sarebbe superiormente limitato da a/ϵ, in contraddizione con il Corollario 10.2. □

Osservazione. Anche il campo $\mathbf{Q}$, pur non essendo completo, è archimedeo. Lasciamo al lettore la facile verifica di questo fatto. Tuttavia la proprietà archimedea non è una conseguenza dei soli assiomi di campo, perchè esistono dei campi ordinati non archimedei [12] (necessariamente non completi).

---

quarto proporzionale: il prodotto è il punto T tale che $\overline{OP} : \overline{OU} = \overline{OT} : \overline{OQ}$. L'estensione delle operazione anche ai punti "negativi" non presenta difficoltà. Per dimostrare che questa costruzione soddisfa gli assiomi di campo ordinato occorre utilizzare l'assiomatica della teoria dei rapporti di grandezze omogenee, sviluppata dal matematico greco Eudosso (III sec. A.C.) ed esposta nel V libro degli *Elementi* di Euclide.

[10] È opportuno osservare che questo corollario enuncia anche una proprietà di $\mathbf{R}$, che possiamo esprimere in modo vago e impreciso, ma suggestivo, dicendo che non esistono numeri reali "infiniti".

[11] In termini geometrici la proprietà archimedea significa che, date due grandezze, esiste sempre un multiplo della prima che è maggiore della seconda. In questa forma esso venne enunciato da Archimede, che ne fece uno degli assiomi della geometria e che lo utilizzò per il calcolo delle aree e dei volumi. In realtà Archimede stesso afferma che questo assioma era già stato impiegato dai suoi predecessori.

[12] Ad esempio il campo dei numeri reali non standard costruito da A. Robinson nel 1960.

Proposizione 10.4 *Siano a e x due numeri reali tali che*

$$a \leq x \leq a + \frac{1}{n} \tag{10.1}$$

per ogni intero positivo n. Allora $a = x$.

Dimostrazione. Se $a < x$ allora, per l' archimedeità dei reali esisterebbe un intero positivo n tale che $n(x-a) > 1$. Quindi $a + \frac{1}{n} < x$, contraddicendo la (10.1). Ne segue che non può essere $a < x$ e quindi $a = x$. □

Definizione. Un sottoinsieme A di $\mathbf{R}$ si dice *denso in* $\mathbf{R}$ se per ogni coppia di numeri reali x e y con $x < y$ esiste un elemento a in A tale che $x < a < y$.

Proposizione 10.5 *L'insieme dei numeri razionali $\mathbf{Q}$ è denso in $\mathbf{R}$.*

Dimostrazione. Siano x e y numeri reali con $x < y$. Poniamo $\epsilon = y - x$. Allora per l'archimedeità di $\mathbf{R}$ esiste un intero positivo n tale che $n\epsilon > 1$, cioè $1/n < \epsilon$. Per la Proposizione 10.1 esiste $m = \max\{k \in \mathbf{Z} : k \leq nx\}$. Allora $m \leq nx < m+1$ e $m/n \leq x < (m+1)/n = m/n + 1/n < x + \epsilon = y$. □

11 Altre conseguenze della completezza

Esaminiamo ora un'altra conseguenza importante dell'assioma di completezza.

Definizione. Una successione di intervalli (I_n) si dice *monotona* se $I_n \supseteq I_{n+1}$ per ogni n.[13] Si ha quindi

$$I_0 \supseteq I_1 \supseteq \ldots \supseteq I_n \supseteq \ldots$$

Può accadere che l'intersezione $\cap_{n\in\mathbf{N}} I_n$ di una successione monotona di intervalli sia vuota. Ad esempio se $I_n = (0, 1/n)$ è facile verificare, usando la proprietà di archimedeità dei reali, che $\cap_{n\in\mathbf{N}} I_n = \emptyset$. Un altro esempio è dato dalla successione di intervalli illimitati $I_n = [n, +\infty)$. Tuttavia, l'intersezione di una successione monotona di intervalli chiusi e limitati non è mai vuota. Si ha infatti il seguente

Teorema 11.1 *Se (I_n) è una successione monotona di intervalli chiusi e limitati esiste un elemento comune a tutti gli intervalli. Tale elemento è unico se l'estremo inferiore delle lunghezze degli intervalli è 0.*

Dimostrazione. Sia $I_n = [a_n, b_n]$. La lunghezza di I_n è allora $\ell(I_n) = b_n - a_n$. Consideriamo gli insiemi $A = \{a_n : n \text{ in } \mathbf{N}\}$ e $B = \{b_n : n \text{ in } \mathbf{N}\}$. Dimostriamo che la coppia (A, B) è separata. Si ha che $a_n \leq b_n$ per ogni n, perché a_n e b_n sono, rispettivamente, primo e secondo estremo dello stesso intervallo. Sia $n \leq m$; allora poiché $I_m \subseteq I_n$ si ha che $a_n \leq a_m$ e $b_m \leq b_n$. Siano ora a_k un generico elemento di A e b_h un generico elemento di B. Se $k \leq h$ si ha $a_k \leq a_h \leq b_h$. Se $h \leq k$ si ha $a_h \leq a_k \leq b_k$. In ogni caso $a_k \leq b_h$ e, quindi,

[13] Se (I_n) è una successione monotona di intervalli si dice anche che gli intervalli sono *incapsulati*.

(A, B) è separata. Per il Teorema 9.1 esiste un numero reale x tale che $a_n \leq x \leq b_n$ per ogni n. Pertanto $x \in I_n$ per ogni n.
Per dimostrare l'unicità osserviamo che un numero reale appartiene a tutti gli intervalli I_n se e solo se è un elemento di separazione della coppia (A, B). L'elemento di separazione è unico se la coppia (A, B) è contigua e questo avviene se $\inf\{b_n - a_n : n \text{ in } \mathbf{N}\} = \inf\{\ell(I_n) : n \text{ in } \mathbf{N}\} = 0$. □

Il Teorema 11.1 può essere utilizzato per dimostrare l'esistenza delle radici n-esime dei numeri reali positivi.

Teorema 11.2 *Sia y un numero reale positivo. Per ogni intero $n \geq 2$ esiste un unico numero reale positivo x tale che $x^n = y$.*

Dimostrazione. Dimostriamo dapprima l'unicità di x. Siano x_1 e x_2 sono due numeri reali positivi distinti. Supponiamo che $x_1 < x_2$. Allora $x_1^n < x_2^n$ e quindi non può essere $x_1^n = x_2^n$. Dimostriamo ora l'esistenza di x. Se $y = 1$ si ha $x = 1$. Supponiamo quindi che $y < 1$. Costruiremo una successione monotona di intervalli chiusi e limitati (I_k) tali che, posto $I_k = [a_k, b_k]$, si ha

a) $a_k^n \leq y \leq b_k^n$,

b) $\ell(I_k) = b_k - a_k \leq 2^{-k}(1 - y)$.

La successione (I_n) è definita ricorsivamente nel modo seguente. Definiamo $I_0 = [y, 1]$. Supponendo quindi di aver già definito I_k, consideriamo il punto medio $c = (a_k + b_k)/2$ di I_k. Se $c^n < y$ definiamo $I_{k+1} = [c, b_k]$, cioè $a_{k+1} = c$, $b_{k+1} = b_k$; altrimenti definiamo $I_{k+1} = [a_k, c]$, cioè $a_{k+1} = a_k$, $b_{k+1} = c$. Pertanto $I_{k+1} \subset I_k$ e $\ell(I_{k+1}) = \ell(I_k)/2$. La successione (I_k) è quindi monotona ed è facile dimostrare per induzione che essa soddisfa le condizioni a) e b). Per il Teorema 11.1 esiste un elemento x comune a tutti gli intervalli I_k. Dimostriamo che $x^n = y$. Per la condizione a) si ha $a_k^n \leq y \leq b_k^n$ per ogni n in $\mathbf{N}$. Inoltre, poiché $a_k \leq x \leq b_k$ per ogni k, si ha anche $a_k^n \leq x^n \leq b_k^n$ per ogni k in $\mathbf{N}$. Quindi

$$|y - x^n| \leq b_k^n - a_k^n.$$

Poiché a_k e b_k sono minori o uguali a 1,

$$\begin{aligned} b_k^n - a_k^n &= (b_k - a_k)(b_k^{n-1} + a_k b_k^{n-2} + \cdots + b_k a_k^{n-2} + a_k^{n-1}) \\ &\leq n(b_k - a_k) \\ &= \frac{n(1-y)}{2^k} \end{aligned}$$

per ogni k in $\mathbf{N}$. Pertanto

$$|y - x^n| \leq \inf\{\frac{n(1-y)}{2^k} : k \text{ in } \mathbf{N}\} = 0.$$

Questo dimostra che $x^n = y$ nel caso $0 < y < 1$. Se $y > 1$ si consideri $z = 1/y$. Allora $0 < z < 1$ e, per quanto abbiamo appena dimostrato, esiste un numero reale positivo u tale che $u^n = z$. Ma allora basta porre $x = 1/u$ per avere $x^n = y$. □

Definizione. Se y è un numero reale positivo, l'unico numero reale positivo x tale che $x^n = y$ si dice *radice n-esima di y* e si denota con $\sqrt[n]{y}$ ($\sqrt{y}$ se $n = 2$).

In particolare in $\mathbf{R}$ esiste un numero x tale che $x^2 = 2$. Poiché $x \notin \mathbf{Q}$ per il Lemma 7.1, l'insieme $\mathbf{R} \setminus \mathbf{Q}$ è non vuoto. Gli elementi di $\mathbf{R} \setminus \mathbf{Q}$ si dicono numeri *irrazionali.*

Proposizione 11.3 *Il campo* $\mathbf{Q}$ *non è completo.*

Dimostrazione. Se $\mathbf{Q}$ fosse completo, potremmo ripetere le dimostrazioni dei Teoremi 11.1 e 11.2 in $\mathbf{Q}$ anziché in $\mathbf{R}$, giungendo alla conclusione che l'equazione $x^2 = 2$ ha soluzione in $\mathbf{Q}$. Ma questo contraddice il Lemma 7.1. $\square$

Proposizione 11.4 *L'insieme dei numeri irrazionali* $\mathbf{R} \setminus \mathbf{Q}$ *è denso in* $\mathbf{R}$.

Dimostrazione. Siano x e y numeri reali con $x < y$. Per la Proposizione 10.5 esiste un numero razionale r tale che $x - \sqrt{2} < r < y - \sqrt{2}$. Allora $x < r + \sqrt{2} < y$ e $r + \sqrt{2}$ è irrazionale. $\square$

12 Allineamenti decimali

In questa sezione dimostreremo che a ogni numero reale è possibile associare un allineamento decimale limitato o illimitato. I numeri razionali sono esattamente quei numeri che hanno allineamenti decimali limitati o periodici. Anche se gli allineamenti decimali non giocheranno alcun ruolo nel resto del corso, abbiamo voluto trattare questo argomento per convincere il lettore che fosse rimasto scettico di fronte a una presentazione assiomatica, in cui il concetto di numero reale rimane indefinito, che gli assiomi di campo ordinato completo conducono alla rappresentazione dei numeri reali che gli è più familiare.

Ad ogni numero razionale maggiore o uguale a 0 è possibile associare un allineamento decimale nel modo seguente. Sia $r = p/q$ con p e q interi, $p \geq 0$ e $q > 0$. Effettuando successivamente la divisione (Teorema 5.7) si definiscono per ricorrenza due successioni di numeri naturali (p_n) e (r_n) tali che

$$\begin{aligned} p &= p_0 q + r_0, \qquad 0 \leq r_0 < q, \\ 10 r_0 &= p_1 q + r_1, \qquad 0 \leq r_1 < q, \\ &\dots \\ 10 r_n &= p_{n+1} q + r_{n+1}, \qquad 0 \leq r_{n+1} < q \\ &\dots \end{aligned} \tag{12.1}$$

Il numero naturale p_0 è detto *parte intera* del numero razionale r e i numeri naturali $p_1, p_2, p_3, \dots$ sono le *cifre decimali.* Le cifre decimali sono numeri naturali ≤ 9. Infatti dalla (12.1) si vede che

$$p_{n+1} = \frac{10 r_n - r_{n+1}}{q} < 10,$$

perché $r_n < q$ e $r_{n+1} \geq 0$. Poiché i resti delle divisioni successive sono numeri naturali compresi tra 0 e $q-1$, dopo q divisioni al massimo uno dei resti r_k si presenterà per la seconda volta. Ma, allora, tutti i resti seguenti si ripeteranno nello stesso ordine in cui si presentavano dopo la prima apparizione di r_k. Questo mostra che la successione delle cifre decimali di un numero razionale è *periodica*, cioè esiste una cifra o un gruppo di cifre che, dopo essere apparso la prima volta, si ripete infinite volte. [14] Questo gruppo di cifre è detto *periodo* del numero razionale r. Le cifre decimali che precedono il periodo sono dette *antiperiodo*. La successione (p_n) viene detta *allineamento decimale* di r. Per indicare che (p_n) è l'allineamento decimale di r si scrive

$$r = p_0.p_1p_2p_3\dots p_n\dots$$

Se il periodo è 0 l'allineamento si dice *limitato* e il periodo non si scrive (ad esempio 3/5=0.6). In caso contrario l'allineamento si dice *illimitato periodico* e si scrivono soltanto le cifre decimali fino al periodo, che viene segnalato con una sopralineatura (ad esempio $3422/990 = 3.4\overline{56}$). Diamo ora una diversa caratterizzazione dell'allineamento decimale dei numeri razionali.

Proposizione 12.1 *Una successione (p_n) di numeri naturali tale che $p_n \leq 9$ per $n \geq 1$ è l'allineamento decimale del numero razionale r se e solo se per ogni n essa soddisfa le disuguaglianze*

$$p_0 + \frac{p_1}{10} + \frac{p_2}{10^2} + \frac{p_3}{10^3} + \dots + \frac{p_n}{10^n} \leq r < p_0 + \frac{p_1}{10} + \frac{p_2}{10^2} + \frac{p_3}{10^3} + \dots + \frac{p_n}{10^n} + \frac{1}{10^n}. \tag{12.2}$$

.

Dimostrazione. È facile dimostrare per induzione che per ogni n in $\mathbf{N}$

$$r = p_0 + \frac{p_1}{10} + \frac{p_2}{10^2} + \frac{p_3}{10^3} + \dots + \frac{p_n}{10^n} + \frac{r_n}{10^n q}. \tag{12.3}$$

Pertanto, tenendo conto del fatto che $0 \leq r_n < q$, si vede che le diseguaglianze (12.2) sono soddisfatte. Viceversa, sia $r = p/q$ un razionale maggiore o uguale a 0 e supponiamo che le (12.2) siano soddisfatte per ogni n. Allora $p_0 \leq p/q < p_0 + 1$. Pertanto $p_0 q \leq p < (p_0+1)q$ e quindi, posto $r_0 = p - p_0 q$, si ha che $p = p_0 q + r_0$ con $0 \leq r_0 < q$. Analogamente, se

$$p_0 + \frac{p_1}{10} \leq p/q < p_0 + \frac{p_1}{10} + \frac{1}{10},$$

posto $r_1 = p - p_0 q - p_1 q/10$, si ha che $10 r_0 = p_1 q + r_1$ e $0 \leq r_1 < q$. Lasciamo al lettore il compito di completare la dimostrazione provando per induzione che $10 r^n = p_{n+1} q + r_{n+1}$ con $0 \leq r_{n+1} < q$. □

[14] Per rendere questa argomentazione rigorosa basta osservare che, se i resti r_n e r_{n+k} sono uguali, le due successioni dei quozienti e dei resti definite ricorsivamente a partire da r_n e r_{n+k} sono uguali per il teorema di ricorrenza (Teorema 5.6).

Le disuguaglianze (12.2) hanno una semplice interpretazione geometrica. Poiché la retta reale è l'unione degli intervalli disgiunti $[n, n+1)$, n in $\mathbf{Z}$, il punto r appartiene a uno e uno solo di tali intervalli, diciamo $[x_0, x_0+1)$. Questo determina la parte intera x_0 di r. Successivamente dividiamo l'intervallo $[x_0, x_0+1)$ nei dieci sottointervalli disgiunti

$$[x_0, x_0+\frac{1}{10}), [x_0+\frac{1}{10}, x_0+\frac{2}{10}), \ldots, [x_0+\frac{9}{10}, x_0+1),$$

ciascuno dei quali ha lunghezza $1/10$. Scegliamo l'intervallo $[x_0+\frac{x_1}{10}, x_0+\frac{x_1+1}{10})$ in cui cade r. Questo determina la prima cifra decimale x_1 di r. Le cifre decimali successive vengono determinate ricorsivamente, suddividendo ogni volta l'intervallo precedente in dieci sottointervalli semichiusi a sinistra di uguale ampiezza e scegliendo tra essi quello in cui cade il punto r. L'allineamento decimale è limitato se e solo se r cade in uno degli estremi degli intervalli semichiusi cosí costruiti. Lo stesso procedimento può essere utilizzato per generare l'allineamento decimale di un qualunque numero reale.

Sia x un numero reale maggiore o uguale a 0. La rappresentazione decimale (x_n) di x è definita ricorsivamente come segue. Si pone

$$x_0 = \max\{k \in \mathbf{Z} : k \leq x\}.$$

Si noti che il massimo esiste per il Lemma 10.1, perché l'insieme è non vuoto $(0 \leq x)$ e superiormente limitato da x. Successivamente si definisce

$$\begin{aligned} x_1 &= \max\{k \in \mathbf{Z} : x_0 + \frac{k}{10} \leq x\} \\ x_2 &= \max\{k \in \mathbf{Z} : x_0 + \frac{x_1}{10} + \frac{k}{10^2} \leq x\} \\ \ldots \end{aligned}$$

In generale, supposto di aver già definito $x_0, x_1, x_2, \cdots, x_n$ si definisce

$$x_{n+1} = \max\{k \in \mathbf{Z} : x_0 + \frac{x_1}{10} + \cdots + \frac{x_n}{10^n} + \frac{k}{10^{n+1}} \leq x\}.$$

Dalla definizione della successione (x_n) discende immediatamente che $0 \leq x_n \leq 9$ se $n \geq 1$ e

$$x_0 + \frac{x_1}{10} + \frac{x_2}{10^2} + \frac{x_3}{10^3} + \cdots + \frac{x_n}{10^n} \leq x < x_0 + \frac{x_1}{10} + \frac{x_2}{10^2} + \frac{x_3}{10^3} + \cdots + \frac{x_n}{10^n} + \frac{1}{10^n}. \quad (12.4)$$

per ogni n in $\mathbf{N}$. Pertanto, se x è razionale, la successione (x_n) coincide con l'allineamento decimale di x ottenuto mediante divisioni successive, per la Proposizione 12.1.

Abbiamo così definito un'applicazione $x \mapsto (x_n)$ dell'insieme dei numeri reali maggiori o uguali a 0 nell'insieme degli allineamenti decimali. L'applicazione è iniettiva, perché, se x e x' sono due numeri reali che generano lo stesso allineamento decimale (x_n), per le disuguaglianze (12.4), si ha $|x - x'| < 1/10^n$ per ogni n in $\mathbf{N}$. Pertanto $x = x'$. È naturale chiedersi se questa applicazione è surgettiva. La risposta è negativa.

Proposizione 12.2 [15] *Nessun numero reale genera un allineamento decimale con periodo* 9.

Dimostrazione. Dimostriamo dapprima che non esiste un numero reale che abbia $0.\overline{9}$ come allineamento decimale. Infatti, se $0.\overline{9}$ fosse l'allineamento decimale del numero reale x, per la (12.4) si avrebbe per ogni n

$$\frac{9}{10}\left(1+\frac{1}{10}+\cdots+\frac{1}{10^{n-1}}\right) \leq x < \frac{9}{10}\left(1+\frac{1}{10}+\cdots+\frac{1}{10^{n-1}}\right)+\frac{1}{10^n}. \tag{12.5}$$

Dalla 12.5, utilizzando l'identità $1+t+t^2+\cdots+t^{n-1}=(1-t^n)/(1-t)$ per $t=1/10$, si ottiene

$$1-\frac{1}{10^n} \leq x < 1.$$

Pertanto $0 \leq 1-x < 1/10^n$ per ogni n. Poiché $\inf\{1/10^n : n \in \mathbf{N}\} = 0$, ne segue che $x=1$ e questo contraddice la disuguaglianza $x<1$.
Per passare al caso generale osserviamo che è facile dimostrare per induzione che, se $y_0.y_1y_2\cdots y_n\cdots$ è l'allineamento decimale del numero reale y, allora l'allineamento decimale di $10^n y$ è

$$10^n y_0 + 10^{n-1}y_1 + \cdots + y_n.y_{n+1}y_{n+2}\cdots$$

Pertanto, se $x_0.x_1x_2\cdots x_n\overline{9}$ fosse l'allineamento decimale di un numero reale x, il numero reale $10^n x - (10^n x_0 + 10^{n-1}x_1 + \cdots + 10x_{n-1} + x_n)$ avrebbe allineamento decimale $0.\overline{9}$, ma questo è impossibile, come abbiamo appena dimostrato. $\square$

Tuttavia, se si escludono gli allineamenti decimali con periodo 9, tutti gli altri allineamenti decimali, periodici o no, sono generati da un numero reale maggiore o uguale a 0.

Proposizione 12.3 *Ogni allineamento decimale che non ha periodo* 9 *è generato da un numero reale maggiore o uguale a* 0.

Dimostrazione. Sia (x_n) una allineamento decimale che non ha periodo 9. la successione di intervalli $I_n=[a_n,b_n]$, dove

$$\begin{aligned} a_n &= x_0+\frac{x_1}{10}+\frac{x_2}{10^2}+\frac{x_3}{10^3}+\cdots+\frac{x_n}{10^n} \\ b_n &= x_0+\frac{x_1}{10}+\frac{x_2}{10^2}+\frac{x_3}{10^3}+\cdots+\frac{x_n}{10^n}+\frac{1}{10^n} \end{aligned}$$

è monotona e l'ampiezza di I_n è 10^{-n}. Pertanto, per la Proposizione 11.1, esiste un unico numero reale x comune a tutti gli I_n. Il punto x soddisfa le disuguaglianze $a_n \leq x \leq b_n$ per ogni n. Per dimostrare che (x_n) è l'allineamento decimale generato da x basta provare che si ha $x<b_n$ per ogni n. Se, per assurdo, esistesse un numero naturale m tale che

$$x=b_m=x_0+\frac{x_1}{10}+\frac{x_2}{10^2}+\frac{x_3}{10^3}+\cdots+\frac{x_m}{10^m}+\frac{1}{10^m},$$

[15] Il lettore può verificare che l'impossibilità di allineamenti decimali con periodo 9 è una conseguenza dell'aver scelto il segno $\leq$ a sinistra e il segno $<$ a destra nelle diseguaglianze (12.4). Se scambiamo tra loro i due segni $\leq$ e $<$ si ottiene una definizione diversa di allineamento decimale, per cui gli allineamenti con periodo 9 sono consentiti, ma non quelli con periodo 0.

si avrebbe che $b_m = x \leq b_{m+1}$. Pertanto

$$\frac{1}{10^m} \leq \frac{x_{m+1}}{10^{m+1}} + \frac{1}{10^{m+1}}$$

e quindi $x_{m+1} \geq 1/10^m - 1/10^{m+1} = 9$. In modo analogo si dimostra che, se $x_{m+k} = 9$ per $k = 1, 2, 3, \cdots, n$, allora anche $x_{m+n+1} = 9$. Ne consegue, per induzione, che tutte le cifre a partire da x_{m+1} sono uguali a 9. Pertanto il periodo di (x_n) sarebbe 9. □

Definizione. Diciamo che un allineamento decimale è *ammissibile* se non ha periodo 9. Indichiamo con $\mathcal{D}$ l'insieme degli allineamenti decimali ammissibili. Abbiamo visto che l'applicazione $x \mapsto (x_n)$ è una corrispondenza biunivoca dell'insieme $\mathbf{R}_+ \cup \{0\}$ sull'insieme $\mathcal{D}$. Questa corrispondenza ci permette di trasportare su $\mathcal{D}$ la struttura algebrica di $\mathbf{R}_+ \cup \{0\}$, definendo la somma e il prodotto di allineamenti decimali nel modo seguente: se (x_n) e (y_n) sono gli allineamenti associati ai numeri reali x e y rispettivamente, la loro somma è l'allineamento associato al numero $x + y$. Il prodotto di due decimali si definisce in modo analogo come l'allineamento associato al prodotto dei numeri reali corrispondenti. Possiamo quindi identificare l'insieme dei numeri reali maggiori o uguali a 0 con i loro allineamenti decimali e scrivere

$$x = x_0.x_1x_2x_3 \cdots x_n \cdots$$

per indicare che (x_n) è l'allineamento decimale che corrisponde al numero reale x.

In generale non è possibile dare una formula esplicita per il calcolo delle cifre della somma e del prodotto di due decimali illimitati. Tuttavia, usando la (12.4) si può facilmente dimostrare per induzione che, se uno dei decimali è limitato e ha solo n cifre non nulle dopo il punto, mentre le prime n cifre decimali dell'altro sono nulle, la loro somma si ottiene aggiungendo le cifre del secondo subito dopo quelle del primo. In simboli:

$$\begin{aligned} & x_0.x_1x_2 \cdots x_n \ + \ 0.\underbrace{0 \cdots 0}_{n \text{ cifre}}\, y_{n+1} \quad y_{n+2} \quad \cdots y_{n+k} \cdots \\ & \qquad = \quad x_0.x_1x_2 \cdots x_n y_{n+1} y_{n+2} \cdots y_{n+k} \cdots \end{aligned} \tag{12.6}$$

Inoltre, le cifre del prodotto di un decimale $0.x_1x_2\cdots$ per 10^{-m} si ottengono spostando a destra di m posti le cifre del primo fattore e inserendo m zeri dopo il punto:

$$10^{-m}\, 0.x_1x_2x_3 \cdots x_n \cdots \ = \ 0.\underbrace{0 \cdots 0}_{m \text{ cifre}}\, x_1 \cdots x_n \cdots \tag{12.7}$$

Possiamo ora dimostrare che un allineamento decimale periodico corrisponde sempre a un numero razionale.

Proposizione 12.4 *L'allineamento decimale periodico* $c.a_1a_2 \ldots a_k\overline{b_1b_2\cdots b_m}$ *corrisponde al numero razionale*

$$c + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_k}{10^k} + \frac{1}{1 - 10^{-m}}\left(\frac{b_1}{10^{k+1}} + \frac{b_2}{10^{k+2}} + \cdots + \frac{b_m}{10^{k+m}}\right).$$

Dimostrazione. Sia $d = c.a_1a_2 \dots a_k\overline{b_1b_2\cdots b_m}$. Allora, per la (12.6)

$$d = c.a_1a_2\cdots a_k + 0.\underbrace{0\cdots0}_{k\text{ cifre}}\overline{b_1b_2\cdots b_m}$$

Il decimale limitato $c.a_1a_2\cdots a_k$ corrisponde al numero razionale

$$a = c + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_k}{10^k}.$$

Inoltre

$$\begin{aligned} 0.\underbrace{0\cdots0}_{k\text{ cifre}}\overline{b_1b_2\cdots b_m} &= 0.\underbrace{0\cdots0}_{k\text{ cifre}}b_1\cdots b_m\overline{b_1b_2\cdots b_m} \\ &= 0.\underbrace{0\cdots0}_{k\text{ cifre}}b_1\cdots b_m + 0.\underbrace{0\cdots0}_{k\text{ cifre}}\underbrace{0\cdots0}_{m\text{ cifre}}\overline{b_1b_2\cdots b_m} \qquad (12.8) \end{aligned}$$

Siano

$$\begin{aligned} x &= 0.\underbrace{0\cdots0}_{k\text{ cifre}}\overline{b_1b_2\cdots b_m} \\ b &= 0.\underbrace{0\cdots0}_{k\text{ cifre}}b_1\cdots b_m. \end{aligned}$$

Poiché l'allineamento decimale di b è limitato, b è il numero razionale

$$\frac{b_1}{10^{k+1}} + \frac{b_2}{10^{k+2}} + \cdots + \frac{b_m}{10^{k+m}}.$$

Per la (12.8) si ha che $x = b + 10^{-m}x$ e, quindi, risolvendo rispetto a x si ottiene

$$x = \frac{1}{1-10^{-m}}b.$$

Pertanto $d = a + \frac{1}{1-10^{-m}}b$, come volevamo dimostrare. □

Per estendere la rappresentazione decimale ai numeri negativi si associa a ogni numero reale negativo l'allineamento decimale del suo valore assoluto preceduto dal segno $-$. In questo modo si ottiene una corrispondenza biunivoca di tutto $\mathbf{R}$ sull'insieme degli *allineamenti decimali ammissibili con segno* $\mathcal{D}_\pm$.

13 Esistenza e unicità del campo reale

In un approccio costruttivo alla teoria dei numeri reali, partendo dall'insieme $\mathbf{N}$ dei numeri naturali si può definire l'insieme dei numeri reali come l'insieme di tutti gli allineamenti decimali ammissibili con segno. Questo approccio però si scontra con una difficoltà tecnica: è difficile definire la somma e il prodotto di decimali illimitati, perché vi è la possibilità di infiniti "riporti". Anche se questa difficoltà può essere superata, definendo prima la somma e il prodotto di allineamenti limitati e estendendo poi le definizioni ai decimali illimitati con un procedimento di approssimazione, rimane la necessità di dimostrare che le operazioni così definite soddisfano gli assiomi di campo ordinato. La trattazione risulta così decisamente più laboriosa e pesante dell'approccio assiomatico. D'altra parte la trattazione assiomatica lascia aperto il problema dell'"esistenza" di $\mathbf{R}$, cioè di un insieme che verifica gli assiomi di campo ordinato completo. La questione dell'esistenza, ossia, in linguaggio moderno, la non-contradditorietà della teoria, viene risolta costruendo un "modello" di $\mathbf{R}$, come ad esempio la retta reale, con le operazione definite geometricamente, o l'insieme degli allineamenti decimali o ancora l'insieme dei "tagli" di Dedekind, a cui accenneremo brevemente nella sezione 14. Naturalmente la costruzione di un modello non fa altro che spostare la questione, riconducendola alla non-contradditorietà degli assiomi della geometria euclidea o dei numeri naturali (e a quelli della teoria degli insiemi).

L'esistenza di diversi modelli per gli assiomi di campo ordinato completo pone il problema dell'unicità del sistema dei numeri reali. In altri termini ci si chiede: il modello basato sugli allineamenti decimali è "sostanzialmente diverso" da quello basato sulla retta reale o da quello basato sui tagli di Dedekind? La questione viene risolta mediante la nozione di *isomorfismo di campi ordinati*.

Siano K e K' due campi ordinati.

Definizione. Un *isomorfismo* tra K e K' è un'applicazione iniettiva e surgettiva $\phi : K \to K'$, che preserva la struttura: per ogni x e y in K si ha $\phi(x + y) = \phi(x) + \phi(y)$ e $\phi(xy) = \phi(x)\phi(y)$. Inoltre se $x < y$ allora $\phi(x) < \phi(y)$.

Teorema 13.1 *Se K e K' sono due campi ordinati completi esiste un unico isomorfismo di campi ordinati $\phi : K \to K'$.*

Il Teorema 13.1 ci dice che esiste sostanzialmente un unico campo ordinato completo, perché tutti i modelli che soddisfano gli assiomi A1–A9 sono tra loro isomorfi. In questo senso si può parlare di unicità dei numeri reali. Rinviamo il lettore a [Bu, Capitolo 7] per la dimostrazione del Teorema 13.1.

14 I tagli di Dedekind

In questa sezione descriviamo per sommi capi la costruzione di Dedekind di un campo ordinato completo a partire dal campo dei numeri razionali. Supponendo di aver già costruito l'insieme dei numeri reali, osserviamo che ogni numero reale x individua un "taglio" dell'insieme $\mathbf{Q}$ dei numeri razionali in due sottoinsiemi: l'insieme dei numeri razionali maggiori di x e l'insieme dei numeri razionali minori di x. Denotiamo con $S(x) = \{r \in \mathbf{Q} : r > x\}$ l'insieme dei numeri razionali maggiori di x.

L'insieme $S(x)$ gode delle seguenti proprietà: è non vuoto e diverso da $\mathbf{Q}$; se r è un numero razionale in $S(x)$ ogni numero razionale maggiore di r è ancora in $S(x)$. Inoltre $S(x)$ è privo di minimo. Viceversa, ogni sottoinsieme S di $\mathbf{Q}$ tale che

1. $\emptyset \neq S \neq \mathbf{Q}$;
2. se $r \in S$ e $q > r$ allora $q \in S$;
3. S non ha minimo,

è della forma $S = S(x)$ per qualche numero reale x (basta prendere per x l'estremo inferiore di S). È evidente che l'insieme $S(x)$ è sufficiente per individuare il numero reale x. Dedekind ebbe l'idea di definire *numero reale* un qualunque sottoinsieme S di $\mathbf{Q}$ che soddisfa le proprietà 1.–3.

In altri termini, supponiamo di conoscere solamente l'insieme dei numeri razionali $\mathbf{Q}$. Diremo che un sottoinsieme S di $\mathbf{Q}$ che soddisfa le proprietà 1.–3. è un *taglio di Dedekind.* Definiamo l'insieme $\mathbf{T}$ dei numeri reali di Dedekind come l'insieme dei tagli di Dedekind.

Per ogni numero numero razionale r l'insieme $S(r) = \{q \in \mathbf{Q} : q > r\}$ è un taglio di Dedekind e quindi è un elemento di $\mathbf{T}$. L'applicazione $r \mapsto S(r)$ è chiaramente iniettiva. Quindi l'insieme dei numeri razionali si immerge in $\mathbf{T}$. Chiameremo i tagli di questo tipo *tagli razionali.* In particolare sono razionali il *taglio zero* $S(0)$ e il *taglio unità* $S(1)$.

Ci proponiamo ora di definire su $\mathbf{T}$ una struttura di campo ordinato completo. Cominciamo dalla relazione d'ordine ponendo $S_1 \leq S_2$ se S_2 è un sottoinsieme di S_1. Per definire la somma di due tagli di Dedekind S_1 e S_2 osserviamo che anche l'insieme $S_1 + S_2 = \{r + q : r \in S_1,\ q \in S_2\}$ è un taglio di Dedekind. Definiamo ora l'opposto del taglio S. Sia S' l'insieme dei minoranti di S in $\mathbf{Q}$, da cui è stato tolto l'estremo inferiore di S se S è un taglio razionale. Allora $-S = \{-r : r \in S'\}$ è un taglio, che chiameremo l'opposto di S. È facile vedere che $S \leq S(0)$ se e solo se $S(0) \leq -S$. Diremo che il taglio S è non negativo se $S(0) \leq S$. Per definire il prodotto in $\mathbf{T}$ consideriamo dapprima il caso di due tagli non negativi. Se S_1 e S_2 sono due tagli non negativi il loro prodotto è l'insieme $S_1S_2 = \{rq : r \in S_1,\ q \in S_2\}$. Naturalmente occorre verificare che l'insieme S_1S_2 è un taglio. Se S_1 è non negativo e S_2 è negativo, poniamo $S_1S_2 = -S_1(-S_2)$. Se S_1 e S_2 sono entrambi negativi il loro prodotto è $S_1S_2 = (-S_1)(-S_2)$. Non è difficile verificare che sui tagli razionali le operazioni di somma e prodotto e la relazione d'ordine così definite coincidono con la somma e il prodotto in $\mathbf{Q}$. In altri termini, se $S(r)$ e $S(q)$ sono due tagli razionali, si ha $S(r) + S(q) = S(r + q)$ e $S(r)S(q) = S(rq)$. Inoltre $S(r) \leq S(q)$ se e solo se $r \leq q$.

Teorema 14.1 *Con le operazioni e la relazione d'ordine definite sopra l'insieme* $\mathbf{T}$ *è un campo ordinato completo.*

Omettiamo la dimostrazione che è piuttosto lunga e laboriosa (vedi [Bu, Capitolo 8]). Lasciamo al lettore come esercizio il compito di verificare che alcune delle proprietà che definiscono la struttura di campo ordinato completo sono soddisfatte. Ci limitiamo a osservare che la completezza di $\mathbf{T}$ discende dal fatto che, se A è un sottoinsieme inferiormente limitato di $\mathbf{T}$, il taglio $\cup_{S \in A} S$ è l'estremo inferiore di A.

References

[Ha] P. R. Halmos, *Teoria elementare degli insiemi*, Feltrinelli Editore, Milano, 1970.

[Bu] C. W. Burrill, *Foundations of Real Numbers*, McGraw-Hill Book Company, New York St. Louis San Francisco Toronto London Sydney, 1967.