Fondamenti della Matematica

a.a. 2011/12

La struttura dei numeri reali: costruzione e proprietà

Alberto Zanardo

Dip. Matematica P. A. - Università di Padova

Marzo 2012

Indice

Avvertenza

In questa dispensa verranno considerate le costruzioni tradizionali dell'insieme $\mathbb{R}$ dei numeri reali sulla base dei numeri razionali (o di un arbitrario campo ordinato archimedeo). Per alcuni risultati di algebra ci si riferirà a [Piacentini Cattaneo, 1996]. Verranno invece ridimostrati in dettaglio teoremi sui campi ordinati che possiamo trovare anche in [De Marco, 1996, Cap. 0 e App. B] o in [Cohen and Ehrlich, 1963], o nelle prime sezioni di [Guiotto, 2008]. Si suggerisce anche la lettura di [Fiori and Invernizzi, 2009] per un più approfondito inquadramento storico e un maggiore approfondimento di alcune argomenti di queste dispense.

1 Campi Ordinati Archimedei

Ricordiamo che un *campo* è una struttura $\mathbb{K} = \langle K, +, \cdot, 0_\mathbb{K}, 1_\mathbb{K} \rangle$ dove K è un insieme, $+$ e $\cdot$ sono operazioni binarie su K, $0_\mathbb{K}$ e $1_\mathbb{K}$ sono elementi distinti di K, e in cui valgono le seguenti proprietà:

1. *Associatività di + e ·*: $\forall x, y, z\, [x + (y + z) = (x + y) + z \ \text{ e } \ x \cdot (y \cdot z) = (x \cdot y) \cdot z]$;
2. *Commutatività di + e ·*: $\forall x, y\, [x + y = y + x \ \text{ e } \ x \cdot y = y \cdot x]$;
3. *Distributività di · rispetto a +*: $\forall x, y, z\, (x \cdot (y + z) = x \cdot y + y \cdot z)$;
4. *Proprietà degli elementi neutri*: (i) $\forall x(x + 0_\mathbb{K} = x)$, (ii) $\forall x(x \cdot 1_\mathbb{K} = x)$;
5. *Esistenza dell'opposto e del reciproco*: (i) $\forall x \exists y(x + y = 0_\mathbb{K})$,

   (ii) $\forall x \neq 0_\mathbb{K}, \exists y(x \cdot y = 1_\mathbb{K})$.

Un *campo totalmente ordinato* è una struttura $\mathbb{K} = \langle K, +, \cdot, \leq, 0_\mathbb{K}, 1_\mathbb{K} \rangle$ in cui $\langle K, +, \cdot, 0_\mathbb{K}, 1_\mathbb{K} \rangle$ è un campo e $\leq$ è una relazione binaria su K che verifica le seguenti proprietà.

6. *Riflessività:* $\forall x(x \leq x)$;
7. *Antisimmetria:* $\forall x, y\, (x \leq y \land y \leq x \to x = y)$;
8. *Transitività:* $\forall x, y, z\, (x \leq y \land y \leq z \to x \leq z)$;
9. *Totalità:* $\forall x, y\, (x \leq y \lor y \leq x)$;
10. *Compatibilità dell'ordine con l'addizione:* $\forall x, y, z\, (x \leq y \to x + z \leq y + z)$;
11. *Compatibilità dell'ordine con la moltiplicazione:* $\forall x, y, \forall z \geq 0_\mathbb{K}\, (x \leq y \to x \cdot z \leq y \cdot z)$.

Le proprietà 6.-8. definiscono le *relazioni d'ordine* e assieme a 9. definiscono le *relazioni d'ordine totale*. Nel caso dei campi si parlerà spesso di campi ordinati, sottintendendo 'totalmente'. Useremo le solite notazioni $-x$ e x^{-1} o $\frac{1}{x}$, per l'opposto ed il reciproco di x.

Dall'uguaglianza $k \geq 0_{\mathbb{K}}$ in un campo ordinato, per la proprietà 10, sommando $-k$ a destra e a sinistra, otteniamo $0_{\mathbb{K}} \geq -k$. Elementi opposti hanno quindi segno opposto. Supponendo quindi per assurdo $1_{\mathbb{K}} < 0_{\mathbb{K}}$, cioè $-1_{\mathbb{K}} > 0_{\mathbb{K}}$, moltiplicando per $-1_{\mathbb{K}}$ otteniamo, per la proprietà 11, $1_{\mathbb{K}} = (-1_{\mathbb{K}}) \cdot (-1_{\mathbb{K}}) > 0_{\mathbb{K}}$. Possiamo dunque concludere $1_{\mathbb{K}} > 0_{\mathbb{K}}$. Da ciò segue che ogni somma $1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}$ è diversa da 0, e quindi i campi ordinati hanno caratteristica 0. In base al Teorema 4.10.4 in [Piacentini Cattaneo, 1996] abbiamo quindi il seguente teorema che dice che l'insieme $\mathbb{Q}$ dei numeri razionali è il 'più piccolo' campo ordinato.

Teorema 1.1 *Sia $\mathbb{K} = \langle K, +, \cdot, \leq, 0_{\mathbb{K}}, 1_{\mathbb{K}} \rangle$ un campo ordinato, e per ogni naturale $n > 0$ indichiamo con $n_{\mathbb{K}}$ la somma di n addendi $1_{\mathbb{K}} + 1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}$. Allora la funzione f definita da*

$$f\left(\frac{m}{n}\right) = \frac{m_{\mathbb{K}}}{n_{\mathbb{K}}} \qquad f\left(\frac{-m}{n}\right) = -\frac{m_{\mathbb{K}}}{n_{\mathbb{K}}} \qquad f(0) = 0_{\mathbb{K}}$$

è un isomorfismo da $\mathbb{Q}$ su un sottocampo ordinato di $\mathbb{K}$.

In base questo teorema, possiamo identificare $f(q)$ con q per ogni razionale q, per cui avrà senso scrivere $\mathbb{Q} \subseteq \mathbb{K}$. In particolare scriveremo 1 e 0 al posto di $1_{\mathbb{K}}$ e $0_{\mathbb{K}}$, e $\frac{n}{m}$ al posto di $\frac{n_{\mathbb{K}}}{m_{\mathbb{K}}}$. Dati inoltre $k, k' \in \mathbb{K}$,[1] come al solito scriveremo spesso kk' invece di $k \cdot k'$. Conviene inoltre usare la seguente notazione

$$\mathbb{K}^+ \;=\; \{k \in \mathbb{K} : 0 < k\} \tag{1.1}$$

Ogni campo ordinato è *denso*; dati cioè due elementi $a < b$, esiste un altro elemento c tale che $a < c < b$. Dalle proprietà della relazione d'ordine segue infatti che

$$a < b \;\Rightarrow\; a + a < a + b < b + b \;\Rightarrow\; \frac{a+a}{2} < \frac{a+b}{2} < \frac{b+b}{2} \;\Rightarrow\; a < \frac{a+b}{2} < b$$

Definizione 1.2 *Un campo ordinato è* archimedeo *se dati due suoi elementi a e b, con $a > 0$, esiste un numero naturale n tale che $na > b$.*[2]

Esercizio 1.1 *Dimostrare che, in ogni campo ordinato $\mathbb{K}$, le seguenti proprietà sono equivalenti all'archimedeità:*

(i) *per ogni $a \in \mathbb{K}^+$ esiste un naturale n tale che $\frac{1}{n} < a$;*

[1] Se $\mathbb{K}$ è $\langle K, +, \cdot, \leq, 0_{\mathbb{K}}, 1_{\mathbb{K}} \rangle$, a rigore si dovrebbe scrivere $k \in K$, per distinguere la struttura dall'insieme su cui è basata. Ciò tuttavia appesantisce il discorso specialmente considerando gli insiemi numerici dei naturali, degli interi, ecc. che usiamo abitualmente. Non ci sarà comunque pericolo di confusione scrivendo $k \in \mathbb{K}$ anziché $k \in K$.

[2] In base all'identificazione di $\mathbb{Q}$ con un sottocampo ordinato dell'arbitrario campo ordinato $\mathbb{K}$ (Teorema 1.1), con na intendiamo la somma $a + \cdots + a$ di n addendi, cioè $n_{\mathbb{K}} \cdot a$.

(ii) *per ogni $b \in \mathbb{K}$, esiste un naturale n tale che $n > b$.*

Vale inoltre il seguente risultato

Proposizione 1.3 *Un campo ordinato $\mathbb{K}$ è archimedeo se e solo se $\mathbb{Q}$ è denso in $\mathbb{K}$.*
Dimostrazione. Se $\mathbb{Q}$ è denso in $\mathbb{K}$, allora, per ogni $a \in K$ esiste un razionale $q > a$, e quindi, per (ii) nell'Esercizio 1.1, dall'archimedeità di $\mathbb{Q}$ segue l'archimedeità di $\mathbb{K}$.

Supponiamo inversamente che $\mathbb{K}$ sia archimedeo e consideriamo due suoi elementi $a < b$. Esiste quindi un naturale n tale che $\frac{1}{n} < b - a$. Consideriamo l'insieme $A = \{m \in \mathbb{Z} : b \leq \frac{m}{n}\}$. Per l'archimedeità di $\mathbb{K}$, A non è vuoto. Per lo stesso motivo esiste un intero k tale che $-b < \frac{k}{n}$, cioè $\frac{-k}{n} < b$ da cui segue $-k < m$ per ogni $m \in A$. Questo insieme è dunque limitato inferiormente e possiamo considerare il suo minimo m_0. Abbiamo quindi $\frac{m_0 - 1}{n} < b$, $\frac{m_0-1}{n} + \frac{1}{n} \geq b$ e $\frac{m_0-1}{n} \geq b - \frac{1}{n}$, da cui segue $\frac{m_0-1}{n} > a$ per la disuguaglianza $\frac{1}{n} < b - a$. ■

Proposizione 1.4 *Sia $\mathbb{K}$ un campo ordinato archimedeo e sia φ una funzione crescente da $\mathbb{K}$ in $\mathbb{K}$ la cui restrizione a $\mathbb{Q}$ sia l'identità. Allora φ è l'dentità su $\mathbb{K}$.*
Dimostrazione. Dato $x \in \mathbb{K}$ ed $\varepsilon \in \mathbb{K}^+$, per la densità di $\mathbb{Q}$ in $\mathbb{K}$ esistono due razionali p e q tali che $x - \varepsilon < p < x < q < x + \varepsilon$. Poiché φ è crescente ed è l'identità su $\mathbb{Q}$, abbiamo anche $p = \varphi(p) \leq \varphi(x) \leq \varphi(q) = q$ e dunque $x - \varepsilon < \varphi(x) < x + \varepsilon$. La tesi segue dal fatto che queste disuguaglianze valgono per ogni $\varepsilon \in \mathbb{K}^+$. ■

Nel seguito di queste note si verdrà che l'insieme dei reali è archimedeo. In [De Marco, 1996, Esempio B.2.9] viene dato un esempio di campo ordinato non archimedeo.

2 Sezioni

Definizione 2.1 *Dato il campo ordinato $\mathbb{K}$ e due suoi sottoinsiemi X e Y, diciamo che la coppia (X, Y) è una* sezione *(o un* taglio di Dedekind*) su $\mathbb{K}$ se sono verificate le seguenti condizioni.*

$$\begin{aligned} &\text{(a)} \quad X \neq \emptyset,\ Y \neq \emptyset \\ &\text{(b)} \quad X \cup Y = \mathbb{K} \\ &\text{(c)} \quad \forall x \in X, \forall y \in Y, x < y \end{aligned} \tag{2.1}$$

L'insieme delle sezioni su $\mathbb{K}$ verrà indicato con $\mathcal{S}(\mathbb{K})$.

Si osservi che dalla proprietà (c) segue che $X \cap Y = \emptyset$.

Una sezione (X, Y) è di *prima specie* se X ha massimo o Y ha minimo, di *seconda specie*, o *lacuna*, altrimenti. Poiché ogni campo ordinato è denso, non può succedere che X abbia massimo e Y abbia minimo.

Ogni sezione di prima specie (X, Y) su $\mathbb{K}$ individua un elemento di $\mathbb{K}$: il massimo di X o il minimo di Y.

Convenzione 2.2 *Verranno identificate le sezioni di prima specie* (X,Y) *e* (X',Y') *ogniqualvolta* X *ha massimo* x_0, Y' *ha minimo* y'_0, *e* $x_0 = y'_0$. *In tal caso,* x_0 *viene chiamato* elemento separatore *della sezione.*[3]

Dalla definizione di sezione segue immediatamente che l'elemento separatore è unico. È banale osservare che in ogni campo ordinato ci sono sezioni di prima specie: dato $a \in \mathbb{K}$, basta porre $X = \{k \in \mathbb{K} : k \leq a\}$ e $Y = \{k \in \mathbb{K} : k > a\}$. Meno banale è mostrare alcuni campi ordinati hanno lacune.

Lemma 2.3 *Sia* $\mathbb{K}$ *un campo ordinato e sia:*

$$X = \{k \in K : k \leq 0 \text{ o } k^2 < 2\} \qquad Y = \{k \in K : k > 0 \text{ e } k^2 \geq 2\}$$

Allora (i) $(X,Y) \in \mathcal{S}(\mathbb{K})$, *e* (ii) *se* (X,Y) *è di prima specie e* a *è il suo elemento separatore, allora* $a^2 = 2$.

Dimostrazione. Segue immediatamente dalla definizione che $X \neq \emptyset$, $Y \neq \emptyset$ e $X \cup Y = \mathbb{K}$. Dati $x \in X$ e $y \in Y$, se $x < 0$ allora banalmente $x < y$. Se invece $x \geq 0$, abbiamo $x^2 < 2 < y^2$, da cui segue $x < y$ (*Esercizio*).

Mostriamo innanzitutto che X non ha massimo. Consideriamo un elemento $x \geq 1$ di X (ogni elemento di X minore di 1 non può essere il massimo perché $1 \in X$). Per la densità di $\mathbb{K}$ possiamo considerare un suo elemento $b > 0$ tale che $2 - x^2 > b$. In particolare abbiamo $b < 1$. Si verifica facilmente che $(x + \frac{b}{4x})^2 < 2$ perché dalle ipotesi segue $\frac{b^2}{16x^2} < \frac{b}{2}$.

L'eventuale elemento separatore di (X,Y) è quindi il minimo y_0 di Y. Se $y_0^2 > 2$, ragionando come nel caso precedente, consideriamo un elemento b di K tale che $0 < b < y_0^2 - 2$, da cui segue $\left(y_0 - \frac{b}{2y_0}\right)^2 > 2$, contro la minimalità di y_0. ■

Dal fatto che l'equazione $x^2 = 2$ non ha soluzioni in $\mathbb{Q}$ e dal lemma precendente segue:

Corollario 2.4 *Il campo ordinato* $\mathbb{Q}$ *ha lacune.*

Osservazione. È chiaro che la dimostrazione precedente può essere ripetuta per ogni razionale positivo che non sia un quadrato di un altro razionale. Inoltre il discorso vale anche per potenze diverse da 2. Le lacune su $\mathbb{Q}$ sono quindi infinite. Con nozioni abbastanza semplici di teoria degli insiemi non è difficile dimostrare che di fatto le lacune sono 'molte di più' delle sezioni di prima specie, nel senso che non esiste nessuna funzione suriettiva dall'insieme di queste ultime nell'insieme delle lacune.

[3] Esistono altre definizioni delle sezioni sui razionali per le quali non c'è bisogno di questa convenzione. Alcuni autori per esempio richiedono che in ogni caso X non abbia massimo e Y non abbia minimo, e che l'unione $X \cup Y$ sia $\mathbb{Q}$ oppure $\mathbb{Q}$ privato di un numero razionale. Oppure si potrebbe escludere dall'insieme di tutte le sezioni quelle in cui Y ha minimo. Queste definizioni diverse presentano tuttavia altri problemi.

Esercizio 2.1 *Date le sezioni* (X,Y) *e* (X',Y') *su* $\mathbb{Q}$*, definiamo la* somma $(X,Y)+(X',Y')$ *come la coppia* (X'',Y'') *dove* $X''=\{x+x' : x\in X \text{ e } x'\in X'\}$ *e* $Y''=\{y+y' : y\in X \text{ e } y'\in X'\}$*. Determinare le condizioni affiché* $(X,Y)+(X',Y')$ *sia una sezione su* $\mathbb{Q}$*.*

Esercizio 2.2 *Definiamo la relazione* $\prec$ *su* $\mathcal{S}(\mathbb{Q})$ *tramite* $(X,Y)\prec(X',Y') \Leftrightarrow X\subset X'$*. Descrivere le proprietà di* $\prec$ *in assenza della* Convenzione 2.2*.*

Avvertenza 2.5 *Nei prossimi tre paragrafi, salvo avviso contrario, considereremo esclusivamente il campo ordinato* $\mathbb{Q}$*. Tutte le dimostrazioni possono essere tuttavia ripetute, senza essenziali cambiamenti, per un arbitrario campo ordinato archimedeo* $\mathbb{K}$*: è sufficiente tenere presente che* $\mathbb{Q}$ *è denso in* $\mathbb{K}$ (Proposizione 1.3)*.*

3 Successioni di Cauchy su $\mathbb{Q}$

Una "successione a valori nell'insieme A" è una funzione f dall'insieme $\mathbb{N}$ dei numeri naturali in A. Come al solito, i valori $f(0), f(1), \ldots,$ verranno indicati con $a_0, a_1, \ldots$ e scriveremo spesso (a_n) invece di f.

Definizione 3.1 *Una successione* (a_n) *a valori in* $\mathbb{Q}$ *è di* Cauchy*, o* fondamentale*, se*

$$\forall\varepsilon>0\,,\exists n_\varepsilon : m,n\geq n_\varepsilon \Rightarrow |a_m-a_n|<\varepsilon \tag{3.1}$$

L'insieme delle successioni di Cauchy su $\mathbb{Q}$ *verrà indicato con* $\mathcal{C}(\mathbb{Q})$*.*

Le successioni di Cauchy sono quelle che "si addensano sempre più". Se immaginiamo di rappresentare su una retta gli elementi di una successione di Cauchy, abbiamo che, comunque preso un numero $\varepsilon>0$, da un certo valore dell'indice n in avanti, tutti i punti si trovano in un intervallo I_ε di ampiezza ε. Basta infatti considerare un naturale n_0 tale che, in base a (3.1), $|a_m-a_n|<\frac{\varepsilon}{2}$ per tutti gli $m,n\geq n_0$. Se I_ε ha (ampiezza ε e) centro in a_{n_0}, allora $a_n\in I_\varepsilon$ per ogni $n\geq n_0$.

Osserviamo inoltre che, dati due intervalli I_ε e $I_{\varepsilon'}$ del tipo appena descritto, la loro intersezione contiene tutti gli a_n per n maggiore di un opportuno n^*. L'intuizione geometrica vorrebbe che l'intersezione di tutti gli intervalli I_ε fosse costituita da un solo punto, a cui dovrebbe corrispondere una coordinata nel sistema numerico che si sta considerando. Nell'insieme dei razionali una tale coordinata non sempre esiste, mentre nei reali esiste. Questo è un altro modo per descrivere il tipo di chiusura che porta dai razionali ai reali.

Esercizio 3.1 *Dimostrare che ogni successione di Cauchy è limitata.*

Somma e prodotto di successioni sono definite nel modo usuale:

$$(a_n) + (b_n) = (a_n + b_n) \qquad (a_n) \cdot (b_n) = (a_n b_n) \tag{3.2}$$

Rispetto a queste operazioni, l'insieme $\mathbb{Q}^{\mathbb{N}}$ di tutte le successioni a valori in $\mathbb{Q}$ è un anello commutativo con identità, prodotto diretto di una famiglia numerabile di copie di $\mathbb{Q}$. La seguente proposizione stabilisce che $\mathcal{C}(\mathbb{Q})$ è chiuso per somma e prodotto, e quindi è un sottoanello di $\mathbb{Q}^{\mathbb{N}}$.

Proposizione 3.2 *Se* (a_n) *e* (b_n) *sono successioni di Cauchy, allora anche* $(a_n + b_n)$ *e* $(a_n b_n)$ *sono successioni di Cauchy.*

Dimostrazione. Dato $\varepsilon > 0$, scegliamo n_ε tale che (3.1) risulti verificata da entrambe le successioni con $\frac{\varepsilon}{2}$ al posto di ε. In tal modo (3.1) viene verificata dalla somma.

Per quanto riguarda il prodotto, usiamo l'Esercizio 3.1 e consideriamo un numero razionale A tale che, per ogni n, $|a_n| < A$ e $|b_n| < A$. Sia n^* un numero naturale tale che, per $n, m \geq n^*$, $|a_m - a_n| < \frac{\varepsilon}{2A}$ e $|b_m - b_n| < \frac{\varepsilon}{2A}$. Per tali m, n abbiamo anche

$$\begin{aligned}
&|a_m b_m - a_n b_n| = |a_m b_m - a_m b_n + a_m b_n - a_n b_n| = |a_m(b_m - b_n) + b_n(a_m - a_n)| \leq \\
&\leq |a_m|\,|b_m - b_n| + |b_n|\,|a_m - a_n| < A\frac{\varepsilon}{2A} + A\frac{\varepsilon}{2A} = \varepsilon
\end{aligned}$$

■

Abbiamo quindi che $\langle \mathcal{C}(\mathbb{Q}), +, \cdot, (0), (1) \rangle$ è un anello commutativo con unità, dove, per ogni razionale a, (a) indica la successione costantemente uguale ad a.

Definizione 3.3 *Diciamo che la successione* (a_n) *a valori in* $\mathbb{Q}$ ha limite $a \in \mathbb{Q}$ *(o* converge *ad a), e scriviamo* $L(a_n) = a$*, se*

$$\forall \varepsilon > 0, \exists n_\varepsilon \,:\, \forall n \geq n_\varepsilon,\ |a_n - a| < \varepsilon$$

Se la successione (a_n) ha limite a, allora, per ogni $\varepsilon > 0$, esiste un indice n_ε tale che $|a_n - a| < \frac{\varepsilon}{2}$ per ogni $n > n_\varepsilon$. Dati quindi $m, n > n_\varepsilon$, abbiamo $|a_m - a_n| \leq |a_n - a| + |a - a_m| < \varepsilon$. Le successioni convergenti in $\mathbb{Q}$ costituiscono dunque un sottoinsieme di $\mathcal{C}(\mathbb{Q})$. Vedremo che si tratta di un sottoinsieme proprio.[4]

Definizione 3.4 *Diremo che una successione* (a_n) *è una* zero-successione*, o* infinitesima*, se* $L(a_n) = 0$*. L'insieme delle zero-successioni in* $\mathbb{Q}$ *viene indicato da* $Z(\mathbb{Q})$*.*

Esercizio 3.2 *Dimostrare che* $Z(\mathbb{Q})$ *è un ideale in* $\mathcal{C}(\mathbb{Q})$*.*

[4] Questo risultato non vale per tutti i campi ordinati archimedei, ma solo per quelli che, come $\mathbb{Q}$, hanno lacune (v. Avvertenza 2.5).

Da questo risultato, per la Proposizione 4.3.3 in [Piacentini Cattaneo, 1996], segue che la relazione $\equiv$ definita da $(a_n) \equiv (b_n)$ se e solo se $L(a_n - b_n) = 0$ è una congruenza su $\mathcal{C}(\mathbb{Q})$. Diremo che (a_n) e (b_n) sono *equivalenti* se $(a_n) \equiv (b_n)$. Indicheremo con $[a_n]_\equiv$ la classe di equivalenza di (a). Sull'insieme quoziente $\mathcal{C}(\mathbb{Q})/\equiv$ possiamo dunque definire le operazioni di somma e prodotto:

$$[a_n]_\equiv + [b_n]_\equiv = [a_n + b_n]_\equiv \qquad [a_n]_\equiv \cdot [b_n]_\equiv = [a_n b_n]_\equiv \tag{3.3}$$

L'insieme $\mathcal{C}(\mathbb{Q})/\equiv$ diventa così un anello, usualmente indicato con $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$.

Esercizio 3.3 *La successione (b_n) è una* sottosuccessione *di (a_n) se esiste una funzione $f : \mathbb{N} \to \mathbb{N}$, strettamente crescente, tale che, per ogni n, $b_n = a_{f(n)}$. Dimostrare che ogni successione di Cauchy è equivalente ad ogni sua sottosuccessione.*

Definizione 3.5 *Diremo che una successione (a_n) è* positiva *se esistono $q > 0$ e n^* tali che $a_n > q$ per ogni $n \geq n^*$. Diremo che (a_n) è* negativa *se $(-a_n)$ è positiva.*

Esercizio 3.4 *Dimostrare che se (a_n) è positiva (risp. negativa) e $(a_n) \equiv (b_n)$, allora (b_n) è positiva (risp. negativa).*

Proposizione 3.6 *Una qualsiasi successione (a_n) di Cauchy è positiva, oppure è negativa, oppure è una zero-successione.*

Dimostrazione. Supponiamo che (a_n) non sia una zero-successione. Allora esiste un ε tale che, per ogni naturale h, $|a_k| \geq \varepsilon$ per qualche $k > h$. Per la condizione (3.1), esiste un n^* tale che, per ogni $n, m \geq n^*$, $|a_n - a_m| < \frac{\varepsilon}{2}$. Fissiamo un $m^* > n^*$ tale che $|a_{m^*}| \geq \varepsilon$. Per ogni $n > n^*$ abbiamo quindi

$$|a_n| = |a_n - a_{m^*} + a_{m^*}| > |a_{m^*}| - |a_n - a_{m^*}| > \frac{\varepsilon}{2}$$

da cui segue che, per ogni $n > n^*$, $a_n > \frac{\varepsilon}{2}$ oppure $a_n < -\frac{\varepsilon}{2}$. Ma la condizione $|a_n - a_m| < \frac{\varepsilon}{2}$ per $m, n \geq n^*$ implica che $a_n > \frac{\varepsilon}{2}$ per ogni $n > n^*$, oppure $a_n < -\frac{\varepsilon}{2}$ per ogni $n > n^*$. ■

Lemma 3.7 *Per ogni successione di Cauchy (a_n) non infinitesima, esistono una successione di Cauchy (b_n) e un naturale n^* tali che $a_n b_n = 1$ per ogni $n \geq n^*$.*

Dimostrazione. Supponiamo che (a_n) sia positiva (per (a_n) negativa la dimostrazione è identica). Allora esiste un $\delta > 0$ tale che $a_n > \delta$ per ogni n maggiore o uguale ad un opportuno n^*. Poniamo $b_n = 1$ per $n < n^*$, e $b_n = \frac{1}{a_n}$ per $n \geq n^*$. La successione (b_n) verifica dunque la seconda condizione dell'enunciato. Dato $\varepsilon > 0$, sia n_1 tale che $|a_m - a_n| < \delta^2 \varepsilon$ per ogni $m, n \geq n_1$. Per $m, n > \max\{n^*, n_1\}$ abbiamo quindi

$$|b_m - b_n| \;=\; \frac{|a_n - a_m|}{|a_m a_n|} \;<\; \frac{\delta^2 \varepsilon}{\delta^2} \;=\; \varepsilon$$

che prova che (b_n) è di Cauchy. ■

Proposizione 3.8 *L'ideale $Z(\mathbb{Q})$ è massimale in $\mathcal{C}(\mathbb{Q})$.*

Dimostrazione. Sia I un ideale in $\mathcal{C}(\mathbb{Q})$ contenente propriamente $Z(\mathbb{Q})$, e sia (a_n) un elemento di $I \setminus Z(\mathbb{Q})$. Per il lemma precedente esiste una successione (b_n) tale che $a_n b_n = 1$ per ogni n maggiore o uguale ad un opportuno n^*. Il prodotto $(a_n b_n)$ appartiene ad I. Abbiamo inoltre $(a_n b_n) \equiv (1)$. Per concludere basta osservare che I è chiuso per la relazione $\equiv$. Se infatti $(c_n) \equiv (c'_n)$, la differenza $(c_n - c'_n) \in Z(\mathbb{Q})$, ma $Z(\mathbb{Q}) \subseteq I$. ∎

Su $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ possiamo inoltre definire la relazione $\leq$ tramite:

$$[a_n]_\equiv \leq [b_n]_\equiv \quad \text{se e solo se} \quad (b_n - a_n) \text{ è positiva oppure è una zero-successione} \tag{3.4}$$

Esercizio 3.5 *Dimostrare che* (3.4) *è un a buona definizione.*

Esercizio 3.6 *Dimostrare che la relazione $\leq$ in $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ è una relazione d'ordine totale.*

Esercizio 3.7 *Dimostrare che per ogni $(a_n) \in \mathcal{C}(\mathbb{Q})$, $[|a_n|]_\equiv = |[a_n]_\equiv|$.*

Lemma 3.9 *La relazione d'ordine definita in* (3.4) *è compatibile con le operazioni di somma e prodotto.*

Dimostrazione. Lasciamo la dimostrazione della compatibilità con la somma come esercizio. Per la moltiplicazione, consideriamo solo il caso delle disuguaglianze strette, essendo banali i casi in cui compare qualche uguaglianza.

Supponiamo $[a_n]_\equiv < [b_n]_\equiv$ e $[c_n]_\equiv > [0]$. Dalla definizione (3.4) segue che anche $(b_n - a_n)$ e (c_n) sono successioni positive. Esistono quindi due numeri razionali positivi p e q, ed un naturale n^* tali che $c_n > p$ e $b_n - a_n > q$ per ogni $n \geq n^*$. Da ciò segue che, per tali n, $c_n(b_n - a_n) > p\,q$. Dunque $(c_n b_n - c_n a_n)$ è positiva e $[c_n]_\equiv \cdot [a_n]_\equiv = [c_n a_n]_\equiv < [c_n b_n]_\equiv = [c_n]_\equiv \cdot [b_n]_\equiv$. ∎

Da questi ultimi risultati, assieme al Teorema 4.5.11 in [Piacentini Cattaneo, 1996] e alla Proposizione 3.8, segue quindi:

Teorema 3.10 *L'insieme $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ con le operazioni di somma e prodotto definite in* (3.3) *e la relazione $\leq$ definita in* (3.4) *è un campo ordinato in cui $[0]_\equiv$ e $[1]_\equiv$ sono rispettivamente l'elemento neutro per somma e prodotto.*

4 Corrispondenza tra sezioni e successioni di Cauchy

Proposizione 4.1 *Data una sezione (X, Y) in $\mathbb{Q}$, esistono due successioni (x_n) e (y_n) di Cauchy tali che, per ogni $n \in \mathbb{N}^+$, $x_n \in X$, $y_n \in Y$, e $y_n - x_n = \dfrac{1}{n}$.*

Dimostrazione. Possiamo scegliere arbitrariamente x_0 e y_0. Sia x_1 il più grande numero intero appartenente a X. Tale numero esiste per l'archimedeità di $\mathbb{Q}$ (e perché Y non è vuoto). Poniamo $y_1 = x_1 + 1$. Dati x_n e $y_n = x_n + \frac{1}{n}$ abbiamo due possibilità: (1) $x_n + \frac{1}{n+1} \in Y$ e (2) $x_n + \frac{1}{n+1} \in X$. Nel primo caso poniamo $x_{n+1} = x_n$ e $y_{n+1} = x_{n+1} + \frac{1}{n+1}$. Nel secondo caso poniamo $y_{n+1} = y_n$ e $x_{n+1} = y_{n+1} - \frac{1}{n+1}$. Quest'ultimo numero appartiene a X per le seguenti uguaglianze e disuguaglianze: $y_{n+1} - \frac{1}{n+1} = y_n - \frac{1}{n+1} = x_n + \frac{1}{n} - \frac{1}{n+1} = x_n + \frac{1}{n(n+1)} \leq x_n + \frac{1}{n+1} \in X$.

Resta da dimostrare che (x_n) e (y_n) sono di Cauchy; lo facciamo solo per (x_n) essendo simile la dimostrazione per (y_n). Dato $\varepsilon > 0$, sia n_ε un naturale tale che $\frac{1}{n_\varepsilon} < \varepsilon$. Dati $n, m \geq n_\varepsilon$, sia $x_n \leq x_m$. Allora $|x_m - x_n| = x_m - x_n < y_n - x_n = \frac{1}{n} \leq \frac{1}{n_\varepsilon} < \varepsilon$. ■

Le successioni (x_n) e (y_n) che verificano la precedente proposizioni non sono uniche. Data per esempio una tale coppia di successioni, possiamo porre: $x'_n = x_n + \frac{1}{2n}$ se $x_n + \frac{1}{2n} \in X$, e $x'_n = x_n - \frac{1}{2n}$ altrimenti, e porre $y'_n = x'_n + \frac{1}{n}$. Le successioni (x'_n) e (y'_n) verificano ancora le condizioni della proposizione. In generale abbiamo il seguente risultato.

Esercizio 4.1 *Dimostrare che, data una sezione (X, Y) su $\mathbb{Q}$, esistono infinite coppie di successioni (x_n) e (y_n) che verificano la* Proposizione 4.1.

Non è particolarmente importante che nella Proposizione 4.1 si abbia $y_n - x_n = \frac{1}{n}$: ciò che conta è che $L(y_n - x_n) = 0$. Il senso di quella proposizione è che, per ogni sezione (X, Y), esistono coppie di successioni $(x_n) \equiv (y_n)$, tali che $x_i \in X$ e $y_i \in Y$ per ogni naturale i.

Proposizione 4.2 *Siano (X, Y) e (X', Y') sezioni su $\mathbb{Q}$ e siano (x_n) e (y_n), e (x'_n) e (y'_n) successioni che, rispettivamente, verificano la* Proposizione 4.1. *Allora $(X, Y) = (X', Y')$ se e solo se $(x_n) \equiv (x'_n)$.*

Dimostrazione. Supponiamo $(X, Y) = (X', Y')$. Per ogni $n \in \mathbb{N}^+$, abbiamo $x'_n \leq x_n \leq y'_n$ oppure $x_n \leq x'_n \leq y_n$, e quindi, in entrambi i casi, $|x_n - x'_n| < \frac{1}{n}$, da cui segue la tesi.

Supponiamo ora $(X, Y) \neq (X', Y')$ e $X \subset X'$. Per la definizione di sezione, l'insieme $X' \setminus X$ è un intervallo su $\mathbb{Q}$ e, per la Convenzione 2.2, non può essere un intervallo degenere della forma $[a, a]$. Possiamo quindi considerare due razionali $a < b$ appartenenti a $X' \setminus X$. Per ogni n abbiamo quindi $y'_n - x_n > b - a$ e dunque $(x_n) \not\equiv (y'_n) \equiv (x'_n)$. ■

La Proposizione 4.1 permette di determinare successioni di Cauchy partendo da sezioni. Il passaggio da successioni di Cauchy a sezioni viene stabilito dalla seguente proposizione.

Proposizione 4.3 *Sia (a_n) una successione di Cauchy su $\mathbb{Q}$ e sia*

$$X = \{x \in \mathbb{Q} : \{n : x > a_n\} \text{ è finito}\} \tag{4.1}$$

Allora la coppia $(X, \mathbb{Q} \setminus X)$ è una sezione su $\mathbb{Q}$.

Dimostrazione. Dalla definizione di X segue che, se $x' < x \in X$, allora $x' \in X$. Quindi $x < y$ per ogni $x \in X$ e $y \in \mathbb{Q} \setminus X$. Risulta banalmente $X \cup (\mathbb{Q} \setminus X) = \mathbb{Q}$. Per dimostrare che X e $\mathbb{Q} \setminus X$ sono entrambi non vuoti basta osservare che (a_n) è limitata: se $|a_n| < M$ per ogni n, allora ogni $q < -M$ appartiene a X e ogni $q > M$ appartiene a $\mathbb{Q} \setminus X$. ■

Le due precedenti proposizioni permettono di passare $\mathcal{S}(\mathbb{Q})$ a $\mathcal{C}(\mathbb{Q})$, e viceversa. I seguenti risultati mostrano che i due passaggi sono sostanzialmente l'uno l'inverso dell'altro.

Proposizione 4.4 *Sia (a_n) una successione di Cauchy, sia (X, Y) la sezione determinata da (a_n) in base a* (4.1)*, e siano (x_n) e (y_n) due successioni che verificano le condizioni della* Proposizione 4.1. *Allora $(a_n) \equiv (x_n)$.*

Dimostrazione. Dato $\varepsilon > 0$ sia n^* un numero naturale tale che $\frac{1}{n^*} < \frac{\varepsilon}{2}$ e $|a_m - a_n| < \frac{\varepsilon}{2}$ per $m, n \geq n^*$. Ogni intervallo $]x_n, y_n[$ contiene infiniti elementi della successione (a_n); sia $a_{n'}$ un arbitrario elemento di tale intervallo con $n' \geq n^*$. Per ogni $n \geq n^*$ abbiamo quindi

$$|a_n - x_n| = |a_n - a_{n'} + a_{n'} - x_n| \leq |a_n - a_{n'}| + |a_{n'} - x_n| < \frac{\varepsilon}{2} + (y_n - x_n) < \varepsilon$$

■

Corollario 4.5 *Le successioni di Cauchy (a_n) e (b_n) sono equivalenti se e solo se determinano la stessa sezione in base a* (4.1).

Dimostrazione. Per la Proposizione 4.4, due successioni che determinano la stessa sezione sono equivalenti. Usando anche la Proposizione 4.2 abbiamo l'implicazione inversa. ■

In base alle proposizioni precedenti abbiamo che (4.1) determina una corrispondenza biunivoca tra $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ e $\mathcal{S}(\mathbb{Q})$. Questa corrispondenza viene resa più precisa dalla seguente proposizione.

Teorema 4.6 *Sia (X, Y) la sezione determinata dalla successione di Cauchy (a_n) in base a* (4.1)*. Allora (a_n) ha limite se e solo se (X, Y) è di prima specie e tale limite è l'elemento separatore di (X, Y).*

Dimostrazione. Per la Propozizione 4.4 possiamo dimostrare il teorema per due successioni (x_n) e (y_n) che verificano la Proposizione 4.1 per la sezione (X, Y).

Se (X, Y) è di prima specie con elemento separatore a, allora, per ogni $n \in \mathbb{N}^+$, $|a - x_n| \leq y_n - x_n = \frac{1}{n}$ e $L(x_n) = a$.

Supponiamo ora $L(x_n) = a = L(y_n)$ e supponiamo per assurdo $a < x$ per qualche $x \in X$. Dalla definizione di limite segue che infiniti elementi della successione (y_n) appartengono all'intervallo $]a, x[$, contro l'ipotesi che (X, Y) sia una sezione. Possiamo dunque concludere che $x \leq a$ per ogni $x \in X$ e, con lo stesso ragionamento, $a \leq y$ per ogni $y \in Y$. ■

Abbiamo già osservato che i numeri razionali corrispondono in modo naturale alle sezioni di prima specie su $\mathbb{Q}$ ed alle classi di equivalenza in $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ in cui ogni successione ha limite. In base al risultato precendente abbiamo che queste corrispondenze vengono conservate dalla corrispondenza tra sezioni e classi di equivalenza di successioni di Cauchy.

Esercizio 4.2 *La corrispondenza tra classi di equivalenza di successioni di Cauchy e sezioni su $\mathbb{Q}$, assieme a* (3.3)*, induce un'operazione di somma sull'insieme delle sezioni. Confrontare questa operazione con quella definita nell'*Esercizio 2.1.

Esercizio 4.3 *La corrispondenza tra classi di equivalenza di successioni di Cauchy e sezioni su $\mathbb{Q}$, assieme alla definizione* (3.4)*, induce un ordinamento sull'insieme delle sezioni. Confrontare questo ordinamento con la relazione $\prec$ considerata nell'*Esercizio 2.2.

5 Allineamenti decimali

Definizione 5.1 *Un* allineamento decimale *è una funzione f da $\mathbb{N}$ nell'insieme $\mathbb{Z}$ degli interi tale che, per $n \in \mathbb{N}^+$, $f(n) \in \{0, 1, \ldots, 9\}$. Il numero intero $f(0)$ viene chiamato* parte intera *di f, mentre la successione $f(1), f(2), \ldots$ viene chiamata* parte decimale.[5]

L'insieme degli allineamenti decimali (su $\mathbb{Z}$) verrà indicato con $\mathcal{A}_{10}(\mathbb{Z})$. La nozione di allineamento decimale formalizza l'idea di *numero decimale* che usiamo abitualmente. Per questo motivo l'allineamento decimale f viene anche indicato con $f(0).f(1)f(2)\ldots$, che corrisponde all'usuale notazione quando $f(0) \geq 0$.

Esercizio 5.1 *A quale numero decimale corrisponde l'allineamento f se $f(0) < 0$?*

Ad ogni allineamento decimale f possiamo associare la successione (monotòna crescente) (a_n) in $\mathbb{Q}$ definita da

$$a_n = \sum_{i=0}^{n} \frac{f(i)}{10^i} \tag{5.1}$$

Diremo che la successione (a_n) è *generata* dall'allineamento decimale f. Osserviamo che, per $m > n$ in una tale successione,

$$a_m - a_n = \sum_{i=n+1}^{m} \frac{f(i)}{10^i} \leq \frac{9}{10^{n+1}} \sum_{i=0}^{m-n-1} \frac{1}{10^i} = \frac{9}{10^{n+1}} \cdot \frac{1 - (\frac{1}{10})^{n-m}}{1 - \frac{1}{10}} < \frac{1}{10^n} \tag{5.2}$$

[5]Tutto quanto detto riguardo agli allineamenti decimali può essere ripetuto e continua a valere per qualsiasi base del sistema di numerazione, con le ovvie modifiche (v. per esempio [Facchini, 2000, Cap.1, App.4.1]).

dove abbiamo usato l'uguaglianza $1+p+\cdots+p^n = \frac{1-p^{n+1}}{1-p}$ con $p = \frac{1}{10}$. Dato quindi $\varepsilon > 0$, se n_ε è tale che $\dfrac{1}{10^{n_\varepsilon}} < \varepsilon$, allora $|a_m - a_n| = a_m - a_n < \varepsilon$ per ogni $m, n \geq n_\varepsilon$. Le successioni generate da allineamenti decimali sono dunque successioni di Cauchy.

Ogni successione generata da un allineamento decimale appartiene ad una classe in $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$. Per la seguente Proposizione 5.2, il caso in cui due allineamenti diversi generano due successioni equivalenti è molto particolare.

Proposizione 5.2 *Siano* (a_n) *e* (b_n) *le successioni di Cauchy generate dagli allineamenti decimali* $f \neq g$. *Allora* $(a_n) \equiv (b_n)$ *se e solo se esiste* $k \in \mathbb{N}$ *tale che*

$$\begin{array}{ll} \text{(i)} & f(n) = g(n) \text{ per ogni } n < k \\ \text{(ii)} & f(k) = 1 + g(k) \\ \text{(iii)} & f(n) = 0 \text{ e } g(n) = 9 \text{ per ogni } n > k \end{array} \tag{5.3}$$

oppure se valgono le (i)-(iii) *scambiando* f *con* g.

Dimostrazione. Supponiamo che gli allineamenti decimali f e g verifichino la condizione (5.3). Allora $a_n - b_n = 0$ per $n < k$ e $a_n - b_n = \dfrac{1}{10^n}$ per $n \geq k$. Quindi $L(a_n - b_n) = 0$.

Se inversamente f e g non verificano la condizione (5.3), possiamo supporre $f(k) > g(k)$ per il primo naturale k tale che $f(k) \neq g(k)$. Allore esiste un naturale n tale che $a_n - b_n \geq \dfrac{2}{10^n}$. Quindi, tenendo presente (5.2) e che (a_n) è monotona crescente, per ogni $m > n$ abbiamo: $a_m - b_m \geq a_n - b_m > a_n - (b_n + \dfrac{1}{10^n}) \geq \dfrac{1}{10^n}$. Il limite $L(a_n - b_n)$, se esiste, non può quindi essere 0. ■

Questo risultato giustifica l'usuale identificazione, per esempio, di 1 con $0.\overline{9}$. In generale, possiamo, come nel caso delle sezioni, adottare la seguente convenzione.

Convenzione 5.3 *Nel seguito verranno identificati gli allineamenti decimali* f *e* g *aventi le proprietà* (i)-(iii) *della* Proposizione 5.2.

Per la Proposizione 5.2 e la precedente convenzione, ogni classe di equivalenza $[(a_n)]_\equiv$ contiene al più una successione di Cauchy associata ad un allineamento decimale. Vale anche il risultato opposto.

Proposizione 5.4 *Ogni successione di Cauchy è equivalente alla successione associata ad un allineamento decimale.*

Dimostrazione. Data una successione di Cauchy (a_n), definiamo l'allineamento decimale f in modo analogo a (4.1). Si osservi che in questo caso si tratta di una definizione induttiva.

$$f(n) = \text{ il massimo intero } m \text{ tale che } \{a_k : a_k < \sum_{i=0}^{n-1} \frac{f(i)}{10^i} + \frac{m}{10^n}\} \text{ è finito} \tag{5.4}$$

L'esistenza della funzione f è garantita dal fatto che (a_n) è limitata (Esercizio 3.1) e dall'archimedeità di $\mathbb{Q}$.

Mostriamo che f è un allineamento decimale, cioè che $0 \leq f(n) \leq 9$ per ogni $n > 0$. Dalla massimalità richiesta in (5.4) segue che la disuguaglianza $0 \leq f(n)$ è verificata da ogni n. Supponiamo per assurdo $f(n^*) > 9$. Dalle uguaglianze:

$$\sum_{i=0}^{n^*} \frac{f(i)}{10^i} = \sum_{i=0}^{n^*-1} \frac{f(i)}{10^i} + \frac{f(n^*)}{10^{n^*}} - \frac{1}{10^{n^*-1}} + \frac{1}{10^{n^*-1}} = \sum_{i=0}^{n^*-1} \frac{f(i)}{10^i} + \frac{f(n^*) - 10}{10^{n^*}} + \frac{1}{10^{n^*-1}}$$

e da (5.4) con $n = n^*$, segue che la disuguaglianza $a_k < \displaystyle\sum_{i=0}^{n^*-1} \frac{f(i)}{10^i} + \frac{1}{10^{n^*-1}}$ è verificata da un insieme finito di k perché $f(n^*) - 10 \geq 0$. Ma ciò contraddice la massimalità di $f(n^* - 1)$.

Sia (b_n) la successione associata all'allineamento decimale f. Resta da dimostrare che $L(a_n - b_n) = 0$. Dato $\varepsilon > 0$ scegliamo n^* tale che $\dfrac{1}{10^{n^*}} < \dfrac{\varepsilon}{2}$ e, per ogni $m, n \geq n^*$, $|a_m - a_n| < \dfrac{\varepsilon}{2}$. Per 5.4, ogni intervallo $[b_n, b_n + \dfrac{1}{10^n}[$ contiene infiniti termini della successione (a_n); sia $a_{n'}$ un arbitrario elemento di tale intervallo con $n' > n^*$. Per ogni $n > n^*$ valgono quindi le disuguaglianze

$$|a_n - b_n| = |(a_n - a_{n'}) + (a_{n'} - b_n)| \leq |(a_n - a_{n'})| + |(a_{n'} - b_n)| < \frac{\varepsilon}{2} + \frac{1}{10^n} < \varepsilon$$

■

Esiste dunque una corrispondenza biunivoca tra $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ ed allineamenti decimali. Anche in questo caso, è possibile rendere più precisa la corrispondenza.

Teorema 5.5 *L'allineamento decimale f è periodico se e solo se la successione generata ha limite in $\mathbb{Q}$.*

Dimostrazione. Un allineamento decimale f è periodico se esistono un $n_0, k > 0$ tali che $f(n) = f(n + k)$ per ogni $n \geq n_0$. Ai fini di questa dimostrazione, non è restrittivo supporre $n_0 = 1$ e $f(0) = 0$; altrimenti ci possiamo riportare in questa situazione con una moltiplicazione per un'opportuna potenza di 10 e con la somma con un opportuno intero.[6] Con tali ulteriori ipotesi non restrittive, nella notazione usuale f verrebbe dunque scritto come $0.\overline{c_1 \dots c_k}$.

[6] L'uguaglianza $n_0 = 1$ viene generalmente espressa dicendo che l'*antiperiodo* è nullo.

Sia (a_n) la successione di Cauchy generata da f. Poniamo $q = \frac{c_1}{10^1} + \frac{c_2}{10^2} + \cdots + \frac{c_k}{10^k}$. Per ogni $n > 0$, abbiamo $a_{kn} = \sum_{i=0}^{n-1} \left(\frac{1}{10^k}\right)^i q = q \, \frac{1 - \left(\frac{1}{10^k}\right)^n}{1 - \frac{1}{10^k}}$. La successione (a_{kn}) converge quindi a $\frac{q}{1 - \frac{1}{10^k}}$ e, per l'Esercizio 3.3, tale valore è anche il limite di (a_n).[7]

Inversamente, dato il numero razionale $\frac{m}{k}$, mostriamo che esiste una successione (a_n) associata ad un allineamento decimale periodico, e tale che $L(a_n) = \frac{m}{k}$. La tesi seguirà a quel punto dalla Proposizione 5.2. Non è restrittivo supporre $m, k > 0$.

Indichiamo $Q(a, b)$ e $R(a, b)$ $(a, b \in \mathbb{Z})$ rispettivamente il quoziente e il resto della divisione intera di a per b. Abbrevieremo inoltre $Q(10^n m, k)$ e $R(10^n m, k)$ con rispettivamente q_n e r_n. Valgono le seguenti uguaglianze:

(1) $10^n m = k\, q_n + r_n \quad (0 \leq r_n < k)$

(2) $\frac{m}{k} = \frac{q_n}{10^n} + \frac{r_n}{10^n k}$

(3) $10^{n+1} m = 10k\, q_n + k\, Q(10r_n, k) + R(10r_n, k) \quad (0 \leq R(10r_n, k) < k)$

(4) $q_{n+1} = 10q_n + Q(10r_n, k)$

(5) $r_{n+1} = R(10r_n, k)$

L'uguaglianza (1) segue dalla definizione di q_n e r_n per le proprietà della divisione in $\mathbb{Z}$. La (2) segue dalla (1) dividendo per $10^n k$. La (3) segue dalla (1) moltiplicando per 10 ed esprimendo $10r_n$ come $k\, Q(10r_n, k) + R(10r_n, k)$. (4) e (5) seguono da (3).

Poniamo $a_n = \frac{q_n}{10^n}$. Dall'uguaglianza (2) segue che $L(a_n) = \frac{m}{k}$ perché (r_n) è limitata. Da (4) seguono le uguaglianze

$$a_{n+1} - a_n = \frac{q_{n+1}}{10^{n+1}} - \frac{q_n}{10^n} = \frac{10q_n + Q(10r_n, k)}{10^{n+1}} - \frac{q_n}{10^n} = \frac{Q(10r_n, k)}{10^{n+1}}$$

Dalle disuguaglianze $0 \leq r_n < k$ segue che $Q(10r_n, k) \in \{0, 1, \ldots, 9\}$. Per (5.1) possiamo dunque concludere che (a_n) è generata dall'allineamento decimale f definito da: $f(0) = Q(m, k)$ e, per ogni $n \in \mathbb{N}$, $f(n + 1) = Q(10r_n, k)$.

I resti r_n possono assumere solo un numero finito di valori. Quindi esistono $n_0, \lambda \in \mathbb{N}$ tali che $r_{n_0} = r_{n_0+\lambda}$. Osservando poi che, per ogni naturale n, $f(n + 1) = Q(10r_n, k)$ è univocamente determinato da r_n, così come r_{n+1}, possiamo concludere che, per ogni $n \geq n_0$, $f(n) = f(n + \lambda)$. ■

[7] Il limite appena determinato può essere scritto come $\frac{10^k q}{10^k - 1} = \frac{c_1 \ldots c_k}{9 \ldots 9}$, dove a denominatore la cifra 9 è ripetuta k volte. Questo è un caso particolare della formula che viene insegnata alla scuola media per trasformare un numero decimale periodico in frazione. Nella seconda parte della dimostrazione non sarà poi difficile riconoscere l'usuale algoritmo per la divisione. Converrà anzi aver presente quell'algoritmo per capire meglio la dimostrazione stessa.

Esercizio 5.2 *La corrispondenza tra $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ e $A_{10}(\mathbb{Z})$, assieme a (3.4), determina una relazione d'ordine su $A_{10}(\mathbb{Z})$. Definire la stessa relazione senza usare le successioni di Cauchy.*

Possiamo ora riassumere i risultati visti nei precedenti paragrafi: (1) c'è corrispondenza biunivoca tra $\mathcal{S}(\mathbb{Q})$, $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ e $\mathcal{A}_{10}(\mathbb{Z})$; (2) le sezioni di prima specie corrispondono alle successioni di Cauchy che hanno limite, che a loro volta corrispondono agli allineamenti decimali periodici; (3) le sezioni, o successioni, o allineamenti viste al punto precedente sono in corrispondenza biunivoca con l'insieme dei numeri razionali. Tutte queste strutture quindi possono essere viste come estensioni dell'insieme dei numeri razionali e costituire un nuovo sistema numerico.

Allineamenti decimali finiti

Alla scuola media si distingue spesso tra numeri decimali finiti, e numeri decimali periodici. In queste note non abbiamo questa distinzione, essendo tutti gli allineamenti decimali particolari successioni di interi. È tuttavia naturale definire gli *allineamenti decimali finiti* come gli allineamenti f tali che $f(n) = 0$ per ogni n maggiori di un opportuno n_0.

Data una qualsiasi coppia a, b di interi, dall'uguaglianza $b - R(b,k) = k\,Q(b,k)$ segue che anche la differenza $ab - aR(b,k)$ è multiplo di k, e quindi $R(ab,k) = R(aR(b,k),k)$. Da questa uguaglianza, usando n volte l'uguaglianza (5) nella dimostrazione del Teorema 5.5, otteniamo

$$r_n = R(10r_{n-1},k) = R(10R(10r_{n-2},k),k) = R(100r_{n-2},k) = \ \dots \ = R(10^n r_0,k)$$

e possiamo concludere che l'allineamento decimale f corrispondente al numero razionale $\frac{m}{k}$ è finito ogniqualvolta k è prodotto di potenze di 2 e 5, i divisori primi della base 10.

Supponiamo inversamente che m e k siano primi tra loro e che p sia un fattore primo di k diverso da 2 e da 5. Il resto r_0 non ha p come fattore primo (altrimenti p sarebbe fattore primo anche di m) e quindi $r_n = R(10^n r_0, k)$ è diverso da 0 per ogni naturale n. L'allineamento decimale f non è dunque finito.

Abbiamo quindi il noto risultato che l'allineamento decimale corrispondente al numero razionale $\frac{m}{k}$ (con m e k primi fra loro) è finito se e solo se i fattori primi di k sono 2 e 5, i divisori primi della base del sistema di numerazione.

6 Campi ordinati completi

Definizione 6.1 *Il campo ordinato $\mathbb{K}$ è* completo*, (o* completo per l'ordine*, o* completo alla Dedekind*) se, per ogni coppia X, Y di sottoinsiemi non vuoti di K,*

$$(\forall x \in X, \forall y \in Y, x \le y) \to \exists z : \forall x \in X, \forall y \in Y, x \le z \le y \tag{6.1}$$

Esercizio 6.1 *Dimostrare che un campo ordinato è completo se e solo se non ha lacune.*

Ricordiamo che in un insieme ordinato $(X, \leq)$ un *maggiorante* (risp. *minorante*) dell'insieme $A \subseteq X$ è un elemento $x \in X$ tale che $a \leq x$ (risp. $x \leq a$) per ogni $a \in A$. L'*estremo superiore* (risp. *inferiore*) di A (in simboli: $\sup_X(A)$ (risp. $\inf_X(A)$)) è, se esiste, il minimo (risp. massimo) dei suoi maggioranti (risp. minoranti).

Teorema 6.2 *In ogni campo ordinato $\mathbb{K}$ sono equivalenti le seguenti asserzioni:*

(a) *$\mathbb{K}$ è completo;*

(b) *per ogni sottoinsieme non vuoto X di K, se X ha un maggiorante, allora X ha estremo superiore;*

(c) *per ogni sottoinsieme non vuoto X di K, se X ha un minorante, allora X ha estremo inferiore.*

Dimostrazione. (a) $\Rightarrow$ (b). Sia $X \subseteq K$, $X \neq \emptyset$, e supponiamo che l'insieme Y dei maggioranti di X non sia vuoto. Quindi $x \leq y$ per ogni $x \in X$ e $y \in Y$, e per (6.1) esiste quindi uno $z \in K$ tale che $x \leq z \leq y$ per ogni $x \in X$ e $y \in Y$. Osserviamo che $z \in Y$ perché $x \leq z$ per ogni $x \in X$. Ma per (6.1) $z \leq y$ per ogni $y \in Y$ e quindi z è il minimo dei maggioranti di X.

(b) $\Rightarrow$ (a). Supponiamo che X e Y verifichino l'antecedente di (6.1). Ogni elemento di Y è un maggiorante di X e quindi, per (b), possiamo considerare l'estremo superiore z di questo insieme. Poiché z è il minimo maggiorante abbiamo $z \leq y$ per ogni $y \in Y$ e $x \leq z$ per ogni $x \in X$. Il conseguente di (6.1) è dunque verificato da z.

(b) $\Leftrightarrow$ (c). L'applicazione $f : \mathbb{K} \to \mathbb{K}$ definita da $f(x) = -x$, è un automorfismo di $\mathbb{K}$ come insieme ordinato. ∎

Proposizione 6.3 *Ogni campo ordinato completo è archimedeo.*

Dimostrazione. Sia $\mathbb{K}$ un campo ordinato completo e supponiamo per assurdo che esistano due suoi elementi a, b, con $a > 0$, tali che $na \leq b$ per ogni naturale n. Poniamo $X = \{na : n \in \mathbb{N}\}$ e $Y = \{y : \forall n \in \mathbb{N}, na \leq y\}$. Gli insiemi X e Y sono non vuoti (perché $b \in Y$) e verificano l'antecedente di (6.1). Sia z un elemento di K che verifica il conseguente di (6.1). Consideriamo $z - a$; poiché $a > 0$, abbiamo $z - a < z$ e quindi $z - a \notin Y$. Dalla definizione di Y segue che $z - a < na$ per qualche naturale n e quindi $z < na + a = (n+1)\,a \in X$, contro l'ipotesi che z verifichi il conseguente di (6.1). ∎

Ricordiamo ora che i risultati del §4 valgono per qualsiasi campo ordinato archimedeo (v. Nota 2.5). Sulla base di quei risultati possiamo dunque enunciare il seguente teorema.

Teorema 6.4 *Un campo ordinato $\mathbb{K}$ è completo se e solo se è archimedeo e tutte le successioni di Cauchy su $\mathbb{K}$ hanno limite.*

Il fatto che ogni successione di Cauchy converga in $\mathbb{K}$ viene espresso dicendo che $\mathbb{K}$ è *sequenzialmente completo*, o *completo alla Cauchy.* Il precedente teorema può dunque essere espresso dicendo che la completezza (alla Dedekind) è equivalente all'archimedeità più la completezza alla Cauchy.

Teorema 6.5 *Tutti i campi ordinati completi sono isomorfi.*

Dimostrazione. Siano $\mathbb{K}_1$ e $\mathbb{K}_2$ campi ordinati completi. Per ogni $x \in \mathbb{K}_1$ possiamo considerare l'insieme $A(x) = \{q \in \mathbb{Q} : q \leq x\}$. Per l'archimedeità di $\mathbb{K}_1$, $A(x)$ è limitato superiormente in $\mathbb{Q}$ e quindi è limitato superiormente anche in $\mathbb{K}_2$. Per la completezza di $\mathbb{K}_2$ possiamo definire $\varphi : \mathbb{K}_1 \to \mathbb{K}_2$ ponendo

$$\varphi(x) = \sup_{\mathbb{K}_2} A(x)$$

Per la densità di $\mathbb{Q}$ in $\mathbb{K}_1$ (Prop. 6.3 e 1.3), se $x < y$ allora $A(x)$ è contenuto propriamente in $A(y)$ e quindi φ è crescente. Inoltre, se $x \in \mathbb{Q}$ allora x è il massimo di $A(x)$ e $\varphi(x) = x$.

In modo analogo possiamo definire una funzione $\psi : \mathbb{K}_2 \to \mathbb{K}_1$, crescente, e tale che la sua restrizione a $\mathbb{Q}$ sia l'identità. Le due funzioni composte $\psi \circ \varphi$ e $\varphi \circ \psi$ sono dunque funzioni crescenti rispettivamente da $\mathbb{K}_1$ in sé e da $\mathbb{K}_2$ in sé, e tali che la loro restrizione a $\mathbb{Q}$ è l'identità. Per la Proposizione 1.4 $\psi \circ \varphi$ e $\varphi \circ \psi$ sono rispettivamente l'identià su $\mathbb{K}_1$ e l'identià su $\mathbb{K}_2$. Dunque φ è una biiezione che conserva l'ordine.

Resta da dimostrare che φ è conserva le operazioni. Usando la densità di $\mathbb{Q}$ in $\mathbb{K}_1$ e in $\mathbb{K}_2$, mostreremo che, per ogni $\varepsilon \in \mathbb{Q}^+$ e $x, y \in \mathbb{K}_1$,

$$\begin{aligned} &\varphi(x) + \varphi(y) - \varepsilon < \varphi(x+y) < \varphi(x) + \varphi(y) + \varepsilon \quad \text{e} \\ &\varphi(x)\varphi(y) - \varepsilon < \varphi(xy) < \varphi(x)\varphi(y) + \varepsilon \end{aligned} \tag{6.2}$$

da cui segue $\varphi(x) + \varphi(y) = \varphi(x+y)$ e $\varphi(x)\,\varphi(y) = \varphi(xy)$.

Per la densità di $\mathbb{Q}$ in $\mathbb{K}_1$ possiamo considerare i numeri razionali p_1, p_2, q_1, q_2 tali che

$$x - \frac{\varepsilon}{2} < p_1 < x < p_2 < x + \frac{\varepsilon}{2} \qquad y - \frac{\varepsilon}{2} < q_1 < y < q_2 < y + \frac{\varepsilon}{2} \tag{6.3}$$

In queste disuguaglianze possiamo sostituire x, y e $x+y$ rispettivamente con $\varphi(x)$, $\varphi(y)$ e $\varphi(x+y)$, perché φ è iniettiva, crescente, ed è l'identità su $\mathbb{Q}$. Ovviamente, la sostituzione, per esempio nella prima disuguaglianza, si ottiene in questo modo: $x < p_1 + \dfrac{\varepsilon}{2} \;\Rightarrow\; \varphi(x) < \varphi(p_1 + \dfrac{\varepsilon}{2}) \;\Rightarrow\; \varphi(x) < p_1 + \dfrac{\varepsilon}{2}$. Dalle disuguaglianze più esterne otteniamo in particolare

$$\varphi(x) - \frac{\varepsilon}{2} < p_1 \qquad p_2 < \varphi(x) + \frac{\varepsilon}{2} \qquad \varphi(y) - \frac{\varepsilon}{2} < q_1 \qquad q_2 < \varphi(y) + \frac{\varepsilon}{2}$$

da cui segue

$$\varphi(x) + \varphi(y) - \varepsilon < p_1 + q_1 \quad \text{e} \quad p_2 + q_2 < \varphi(x) + \varphi(y) + \varepsilon$$

A questo punto la prima riga in (6.2) segue osservando che, per le disuguaglianze più interne in (6.3), $p_1 + q_1 < \varphi(x + y) < p_2 + q_2$.

Per quanto riguarda il prodotto, non è restrittivo supporre x e y positivi. Sia δ un numero razionale tale che

$$\delta > 0 \qquad \delta < x \qquad \delta < y \qquad \delta < \frac{\varepsilon}{2(x+y)} \qquad \delta^2 < \frac{\varepsilon}{2}$$

La densità di $\mathbb{Q}$ in $\mathbb{K}_1$ ci garantisce che δ esiste. Scegliamo $p_1, p_2, q_1, q_2 \in \mathbb{Q}$ in modo che le seguenti disuguaglianze (analoghe alle (6.3)) siano verificate.

$$x - \delta < p_1 < x < p_2 < x + \delta \qquad y - \delta < q_1 < y < q_2 < y + \delta \tag{6.4}$$

Osserviamo che i razionali p_i, q_i, $p_2 - \delta$ e $q_2 - \delta$ sono tutti positivi. Moltiplicando, e sommando o sottraendo opportunamente δ, da queste disuguaglianze ricaviamo

$$p_1 q_1 < xy < p_2 q_2 \qquad p_2 - \delta < x < p_1 + \delta \qquad q_2 - \delta < y < q_1 + \delta \tag{6.5}$$

Per le proprietà di φ, queste disuguaglianze valgono anche sostituendo x, y e xy con, rispettivamente, $\varphi(x)$, $\varphi(y)$ e $\varphi(xy)$. Dalle ultime due disuguaglianze, possiamo ricavare

$$(p_2 - \delta)(q_2 - \delta) < \varphi(x)\varphi(y) < (p_1 + \delta)(q_1 + \delta)$$

e combinando con $p_1 q_1 < \varphi(xy) < p_2 q_2$ otteniamo

$$\begin{aligned}
\varphi(xy) - \varphi(x)\varphi(y) &< p_2 q_2 - (p_2 - \delta)(q_2 - \delta) = \delta(p_2 + q_2 - \delta) < \delta(x + y + \delta) \\
\varphi(xy) - \varphi(x)\varphi(y) &> p_1 q_1 - (p_1 + \delta)(q_1 + \delta) = -\delta(p_1 + q_1 + \delta) > -\delta(x + y + \delta)
\end{aligned}$$

cioè, tenendo presente che $\delta < \frac{\varepsilon}{2(x+y)}$ e $\delta^2 < \frac{\varepsilon}{2}$,

$$|\varphi(xy) - \varphi(x)\varphi(y)| < \delta(x + y) + \delta^2 < \varepsilon$$

che equivale alla seconda disuguaglianza in (6.2). ∎

7 Numeri Reali

Una possibile definizione della struttura $\mathbb{R}$ dei *numeri reali* è la seguente:

$$\mathbb{R} \stackrel{\text{def}}{=} \mathcal{C}(\mathbb{Q})/Z(\mathbb{Q}) \tag{7.1}$$

Un numero reale è quindi una classe di equivalenza di successioni di Cauchy in $\mathbb{Q}$, e le operazioni e l'ordine su $\mathbb{R}$ sono quelle considerate nel §3. In base ai risultati precedenti abbiamo che l'insieme $\mathbb{R}$ può essere identificato anche con l'insieme dei tagli di Dedekind su $\mathbb{Q}$ o con l'insieme degli allineamenti decimali (accettando le identificazioni date dalle Convenzioni 2.2 e 5.3).

Le operazioni e la relazione d'ordine su $\mathbb{R}$ sono quelle definite in (3.3) e (3.4). Per il Teorema 3.10 abbiamo che $\mathbb{R}$ è un campo ordinato. Lo zero e l'unità in $\mathbb{Q}$ sono rispettivamente le classi $[0]_\equiv$ e $[1]_\equiv$ delle successioni costanti (0) e (1). Il sottocampo ordinato di $\mathbb{R}$ isomorfo a $\mathbb{Q}$, la cui esistenza è stabilita dal Teorema 1.1, coincide quindi con l'immagine della funzione $\eta : Q \to R$ definita da $\eta(q) = [q]_\equiv$. Vengono chiamati *irrazionali* i numeri reali che non appartengono all'immagine di η.

Lemma 7.1 $\mathbb{R}$ *è archimedeo.*

Dimostrazione. Sia $[a_n]_\equiv \in \mathbb{R}$. Per l'Esercizio 3.1, esiste un q tale che $a_n < q$ per ogni n. Quindi $(q - a_n)$ è una successione positiva o una zero-successione e $[q]_\equiv \geq [a_n]_\equiv$. Dall''archimedeità di $\mathbb{Q}$ segue dunque la tesi. ■

Anche se possiamo identificare $\mathbb{Q}$ con l'immagine di η nel seguito converrà tenere distinti i due insiemi numerici (continueremo quindi a scrivere $\eta(q)$ anziché q). Verrà poi spesso precisato se l'ambiente del discorso sia $\mathbb{Q}$ o $\mathbb{R}$. Nel caso dei limiti, scriveremo poi $L_\mathbb{Q}$ o $L_\mathbb{R}$ per specificare in quale campo i limiti vengono considerati.

Lemma 7.2 *Ogni successione di Cauchy di razionali converge in* $\mathbb{R}$ *e il limite è la classe di equivalenza della successione stessa. Cioè: data una successione* $(a_n) \in \mathcal{C}(\mathbb{Q})$ *la successione* $(\eta(a_n))$ *converge in* $\mathbb{R}$ *e* $L_\mathbb{R}(\eta(a_n)) = [a_n]_\equiv$.

Dimostrazione. Dato $\varepsilon \in \mathbb{R}^+$, per il Lemma 7.1 possiamo considerare $\delta \in \mathbb{Q}^+$ tale che $\eta(\delta) < \varepsilon$ in $\mathbb{R}$. Poiché (a_n) è di Cauchy in $\mathbb{Q}$, esiste un n_δ tale che, per tutti gli $m, n \geq n_\delta$, $|a_m - a_n| < \frac{\delta}{2}$, da cui segue $\delta - |a_m - a_n| > \frac{\delta}{2}$. Quindi, per ogni $m_0 \geq n_\delta$, la successione $(b_n) = (\delta - |a_{m_0} - a_n|)$ è positiva in $\mathcal{C}(\mathbb{Q})$ e dunque $[b_n]_\equiv = [\delta - |a_{m_0} - a_n|]_\equiv > 0$ in $\mathbb{R}$. Per l'Esercizio 3.7, questa disuguaglianza può essere scritta come

$$[\delta]_\equiv - [|a_{m_0} - a_n|]_\equiv = \eta(\delta) - |[a_{m_0}]_\equiv - [a_n]_\equiv| = \eta(\delta) - |\eta(a_{m_0}) - [a_n]_\equiv| > 0$$

Abbiamo quindi che, per ogni $m_0 \geq n_\delta$,

$$|\eta(a_{m_0}) - [a_n]_\equiv| < \eta(\delta) < \varepsilon$$

cioè $L_\mathbb{R}(\eta(a_n)) = [a_n]_\equiv$. ■

Teorema 7.3 $\mathbb{R}$ *è un campo ordinato completo.*

Dimostrazione. In base ai risultati precedenti, dobbiamo dimostrare che ogni successione di Cauchy in $\mathbb{R}$ ha limite in $\mathbb{R}$. L'idea è ovviamente quella di usare il lemma precedente e la densità di $\mathbb{Q}$ in $\mathbb{R}$.

Sia (ξ_n) una successione di Cauchy in $\mathbb{R}$. Per ogni naturale n scegliamo un razionale a_n tale che $|\xi_n - \eta(a_n)| < \eta(\frac{1}{n+1})$. Mostriamo che (a_n) è di Cauchy in $\mathbb{Q}$. Dato $\varepsilon \in \mathbb{Q}^+$, esiste un n^* tale che, per $m, n \geq n^*$, $|\xi_m - \xi_n| < \eta(\frac{\varepsilon}{3})$; non è poi restrittivo supporre $\frac{1}{n^*+1} < \frac{\varepsilon}{3}$. Per $m, n \geq n^*$, abbiamo dunque

$$
\begin{aligned}
|\eta(a_m) - \eta(a_n)| &= |\eta(a_m) - \xi_m + \xi_m - \xi_n + \xi_n - \eta(a_n)| \leq \\
&\leq |\eta(a_m) - \xi_m| + |\xi_m - \xi_n| + |\xi_n - \eta(a_n)| < \eta(\varepsilon)
\end{aligned}
$$

da cui segue $|a_m - a_n| < \varepsilon$. Possiamo dunque concludere che (a_n) è di Cauchy in $\mathbb{Q}$ e che, per il Lemma 7.2, $L_{\mathbb{R}}(\eta(a_n)) = [a_n]_{\equiv}$. Ma la successione $(\xi_n - \eta(a_n))$ è una zero-successione in $\mathbb{R}$ e quindi $L_{\mathbb{R}}(\xi_n) = [a_n]_{\equiv}$. ∎

Corollario 7.4 *$\mathbb{R}$ contiene ogni campo ordinato archimedeo.*

Dimostrazione. Abbiamo osservato (Avvertenza 2.5) che i risultati del Paragrafo 3 valgono per un qualsiasi campo ordinato archimedeo $\mathbb{K}$. In particolare possiamo considerare l'estensione $\mathcal{C}(\mathbb{K})/Z(\mathbb{K})$ di $\mathbb{K}$ e, con una dimostrazione analoga a quella del Teorema 7.3, concludere che $\mathcal{C}(\mathbb{K})/Z(\mathbb{K})$ è un campo ordinato completo. Per il Teorema 6.5, $\mathcal{C}(\mathbb{K})/Z(\mathbb{K})$ è isomorfo a $\mathbb{R}$. ∎

7.1 Osservazioni conclusive

Il Teorema 6.5 ci garantisce che possiamo parlare de *il* campo ordinato completo. Per questo motivo i numeri reali vengono spesso presentati in modo *assiomatico*: essi possono essere visti come una qualsia struttura che verifica gli *assiomi* 1.-11. in § 1 e (6.1), e le loro proprietà sono quelle deducibili da quegli assiomi. Poco importa quindi se vediamo i reali come classi di equivalenza su $\mathcal{C}(\mathbb{Q})$, o come un qualsiasi altro campo ordinato completo: il Teorema 6.5 ci assicura che le proprietà della somma, del prodotto, e della relazione d'ordine restano sempre le stesse. Dobbiamo però osservare che quel teorema asserisce l'unicità, a meno di isomorfismi, del campo ordinato completo, ma non dice nulla riguardo all'esistenza. Il senso delle costruzioni viste in queste note è appunto mostrare che esiste almeno un campo ordinato completo.

Un'altra osservazione sui risultati di queste note è il carattere 'conclusivo' della costruzione dei reali. Abbiamo visto che $\mathbb{R}$ è un campo ordinato archimedeo, e quindi possiamo considerare le sezioni, o le successioni di Cauchy, su $\mathbb{R}$ stesso. I risultati del §7 ci dicono che con queste operazioni non otteniamo niente di nuovo: otteniamo un campo ordinato isomorfo ad $\mathbb{R}$.

La costruzione della struttura dei numeri reali sulla base dei numeri razionali costituisce la conclusione del processo noto come *Aritmetizzazione dell'Analisi.* Tale processo mirava alla definizione della struttura dei numeri reali attraverso operazioni insiemistiche sulla struttura dei numeri naturali. La costruzione degli interi e poi dei razionali come quozienti rispettivamente di $\mathbb{N} \times \mathbb{N}$ e $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ è abbastanza semplice (v. [Piacentini Cattaneo, 1996, Cap. 2]). Il passo cruciale è quello finale: da $\mathbb{Q}$ a $\mathbb{R}$. Storicamente, le ricerche in questo settore della matematica ebbero luogo nella seconda metà del XIX secolo. Iniziate con il lavori Karl Weierstrass (1815-1897), si conclusero con le costruzioni dei reali come sezioni su $\mathbb{Q}$ (Richard Dedekind (1831-1916)) successioni di Cauchy su $\mathbb{Q}$ (Georg Cantor (1845-1918)). È interessante osservare come ben tre soluzioni del problema della definizione dei numeri reali siano comparse in stampa nello stesso anno, il 1872 (v. [Lolli, 2008, p.79], [Bottazzini, 1981, §6.2]).

Le sezioni di Dedekind sono forse il primo esempio di uso di insiemi come singole entità numeriche: un insieme viene visto come un unico oggetto. Anche se attualmente operazioni di questo tipo ci sembrano abbastanza naturali, è evidente la forte astrazione su cui esse sono basate. Non è certo più semplice e intuitivo considerare singole entità numeriche le classi di equivalenza di successioni di Cauchy (per le quali, oltre ad operazioni insiemistiche, dobbiamo ricorrere anche alla nozione di funzione). È invece apparentemente più semplice vedere, come viene fatto alla scuola media, i numeri reali come numeri decimali, finiti, o periodici, o non periodici. In questo caso infatti si tratta di estendere una nozione che siamo già abituati ad usare: sappiamo trattare i numeri decimali periodici, per cui possiamo andare 'leggermente' oltre considerando numeri decimali anche non periodici. La semplicità di questa estensione è tuttavia solo apparente; per rendercene conto basta considerare operazioni elementari come la somma o il prodotto. Cosa significa sommare o moltiplicare due numeri decimali infiniti e non periodici? Se $\sqrt{2} = 1.41421\ldots$ e $\sqrt{3} = 1.73205\ldots$, quanto fa, in termini di numeri decimali, $\sqrt{2} + \sqrt{3}$? È chiaro che non possiamo ricorrere all'usuale algoritmo per la somma di due numeri decimali, né trasformare i numeri in frazioni. Una possibile risposta passa attraverso le successioni di Cauchy. Dette (a_n) e (b_n) le successioni di Cauchy generate dagli allineamenti decimali di $\sqrt{2}$ e $\sqrt{3}$ sappiamo che $(a_n + b_n)$ è ancora una successione di Cauchy e che, per la Proposizione 5.4, $(a_n + b_n)$ è equivalente ad un'unica successione generata da un allineamento decimale: l'allineamento decimale di $\sqrt{2} + \sqrt{3}$.

L'operazione di somma su $\mathcal{A}_{10}(\mathbb{Z})$ vista sopra è dunque indotta da quella su $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ tramite la corrispondenza tra $\mathcal{A}_{10}(\mathbb{Z})$ e $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ vista nel §5. In modo analogo si possono definire il prodotto e la relazione d'ordine su $\mathcal{A}_{10}(\mathbb{Z})$ e, per la corrispondenza tra $\mathcal{S}(\mathbb{Q})$ e $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ studiata nel § 4, possiamo fare lo stesso con i tagli di Dedekind.

Nella presentazione originale della costruzione dei reali come sezioni su $\mathbb{Q}$, tuttavia, Dedekind definisce direttamente le operazioni e la relazione d'ordine su $\mathcal{S}(\mathbb{Q})$. Per quanto riguarda l'ordine la definizione è in effetti più semplice di quella in $\mathcal{C}(\mathbb{Q})/Z(\mathbb{Q})$ (v. Esercizio 4.3). La definizione di prodotto è invece più laboriosa. La costruzione di $\mathbb{R}$ come insieme delle sezioni su $\mathbb{Q}$ può essere vista in molti testi di analisi.

In [Burrill, 1967] vengono riportate le costruzioni di $\mathbb{R}$ nei tre modi visti in queste note, in cui, in ogni costruzione, le operazioni e la relazione d'ordine sono definite indipendentemente dalle altre (v. per esempio gli Esercizi 2.1 e 2.2). Per quanto riguarda gli allineamenti decimali, tuttavia, non dobbiamo aspettarci che la somma ed il prodotto vengano definite in modo analogo alla somma ed al prodotto di due numeri decimali finiti. La definizione è molto più complessa. Viene innanzitutto definita, in modo abbastanza ovvio (v. Esercizio 5.2), la relazione d'ordine su $\mathcal{A}_{10}(\mathbb{Z})$, poi viene mostrato che ogni insieme superiormente limitato di allineamenti decimali ha estremo superiore, infine, somma e prodotto di allineamenti decimali vengono definiti come l'estremo superiore di un opportuno insiemi di allineamenti decimali finiti.

A Questioni di cardinalità. L'Ipotesi del Continuo. Reali algebrici e reali trascendenti.

In questa sezione verranno usate alcune definizioni e risultati classici di Teoria degli Insiemi che riassumiamo qui brevemente senza dimostrazioni.

TI1 Diciamo che l'insieme A ha *cardinalità* minore o uguale all'insieme B (in simboli: $|A| \leq |B|$) se esiste un funzione iniettiva da A in B. A ha cardinalità uguale a B ($|A| = |B|$) se esiste un funzione biiettiva da A in B. A ha cardinalità minore di B ($|A| < |B|$) se $|A| \leq |B|$ e $|A| \neq |B|$. Se $|A| = |B|$ diciamo che A e B sono *equipotenti*.

TI2 Teorema di Cantor-Schöder-Bernstein: se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$.

TI3 Diciamo che A è infinito se $|\mathbb{N}| \leq |A|$ o, equivalentemente, se esiste un sottoinsieme proprio B di A tale che $|A| = |B|$.

TI4 Un insieme A è *numerabile* se $|A| = |\mathbb{N}|$. Ogni sottoinsieme infinito di un insieme numerabile è numerabile (e dunque il numerabile è l'infinito "più piccolo").

TI5 Il prodotto cartesiano di insiemi numerabili è numerabile. Gli insiemi $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili.

TI6 Se gli insiemi $A_i : i \in I$ sono finiti o numerabili e I è finito o numerabile, allora $\bigcup_{i \in I} A_i$ è finito o numerabile.

TI7 Teorema di Cantor: per ogni insieme A, $|A| < |\wp(A)|$, dove $\wp(A)$ indica l'insieme di tutti i sottoinsiemi di A (l'*insieme potenza* di A).

TI8 Se l'insieme B è infinito e $|A| \leq |B|$, allora $|A \cup B| = |A \times B| = |B|$.

TI9 Se l'insieme B è infinito e $|A| < |B|$, allora $|B \setminus A| = |B|$.

Nel seguito i numeri reali verranno visti come *allineamenti binari*, definiti in modo analogo agli allineamenti decimali del §5. Indicheremo poi con $S_{\{0,1\}}$ l'insieme delle successioni (s_n) ad elementi in $\{0, 1\}$.

Lemma A.1 $|S_{\{0,1\}}| = |\wp(\mathbb{N})|$.

Dimostrazione. Ad ogni $(s_n) \in S_{\{0,1\}}$ possiamo associare l'insieme $A_{(s_n)} \subseteq \mathbb{N}$ definito da $A_{(s_n)} = \{m \in \mathbb{N} : s_m = 1\}$. Se $(s_n) \neq (s'_n)$, allora, per qualche m, $s_m \neq s'_m$ e il numero naturale m appartiene ad uno dei due insiemi $A_{(s_n)}$ e $A_{(s'_n)}$, ma non appartiene all'altro. La corrispondenza $(s_n) \to A_{(s_n)}$ è dunque iniettiva. Dato $A \subseteq \mathbb{N}$, possiamo considerare la successione $(s_n) \in S_{\{0,1\}}$ definita da $s_m = \begin{cases} 1 & \text{se } m \in A \\ 0 & \text{se } m \notin A \end{cases}$. Si verifica immediatamente che $A_{(s_n)} = A$ e dunque la corrispondenza $(s_n) \to A_{(s_n)}$ è anche suriettiva. ■

Ad ogni $(s_n) \in S_{\{0,1\}}$ possiamo associare il numero reale $r_{(s_n)} \in [0,1]$ il cui allineamento binario f viene definito da $f(0) = 0$ e $f(m) = s_{m-1}$ per ogni $m > 0$. In notazione binaria r_σ viene scritto come $0.s_0s_1s_2\ldots$. Per la Proposizione 5.4 la corrispondenza $(s_n) \to r_{(s_n)}$ è suriettiva (sull'intervallo $[0,1]$) ma, per Proposizione 5.2, non è iniettiva. Per renderla tale basta ridurre opportunamente l'insieme $S_{\{0,1\}}$. Poniamo

$$S_{\bar{1}} = \{(s_n) \in S_{\{0,1\}} : \exists n_0(s_m = 1 \text{ per ogni } m \geq n_0)\} \quad \text{e} \quad S^*_{\{0,1\}} = S_{\{0,1\}} \setminus S_{\bar{1}}$$

Per la Proposizione 5.2 la corrispondenza $(s_n) \to r_{(s_n)}$ è una biiezione tra $S^*_{\{0,1\}}$ e $[0,1[$. Si osservi che ora l'intervallo non contiene 1 che corrisponde all'allineamento binario $0.\bar{1} \in S_{\bar{1}}$.

Teorema A.2 $|\mathbb{R}| = |\wp(\mathbb{N})|$.

Dimostrazione. Osserviamo preliminarmente che $S_{\bar{1}}$ è numerabile. Infatti, per il Teorema 5.5, i numeri reali della forma $r_{(s_n)}$ con $(s_n) \in S_{\bar{1}}$ sono razionali, e l'insieme $S_{\bar{1}}$ è infinito. Possiamo dunque concludere $|S_{\bar{1}}| = |\mathbb{N}|$ per **TI4,5**. Per il Lemma A.1 e **TI9** abbiamo quindi $|S^*_{\{0,1\}}| = |\wp(\mathbb{N})|$. Ma $S^*_{\{0,1\}}$ è in corrispondenza biunivoca con $[0,1[$ che dunque ha pure cardinalità uguale a $\wp(\mathbb{N})$. Per concludere basta osservare che $|\mathbb{R}| = |\mathbb{Z} \times [0,1[\,|$ e usare **TI8**. ■

Per questo risultato la cardinalità di $\wp(\mathbb{N})$ viene anche chiamata *Cardinalità del Continuo*. Osserviamo in particolare che l'insieme dei numeri reali ha cardinalità strettamente maggiore a $\mathbb{N}$, e quindi a $\mathbb{Q}$, anche se i razionali sono densi in $\mathbb{R}$.

Un famoso problema sorto dopo la scoperta che $|\mathbb{N}| < |\wp(\mathbb{N})|$ è se esistano insiemi X tali che $|\mathbb{N}| < |X| < |\wp(\mathbb{N})|$, e in generale se, dato un insieme Y esistano insiemi X tali che $|Y| < |X| < |\wp(Y)|$. Il fatto che le usuali operazioni insiemistiche non producano variazioni nella cardinalità (v. **TI5,6,8,9**) portò a formulare l'*Ipotesi del Continuo* e l'*Ipotesi Generalizzata del Continuo* che rispondono negativamente alle questioni poste sopra:

Ipotesi del Continuo (CH) *Non esistono insiemi con cardinalità strettamente compresa tra la cardinalità di $\mathbb{N}$ e quella di $\wp(\mathbb{N})$.*

Ipotesi Generalizzata del Continuo (GCH) *Per ogni insieme X non esistono insiemi con cardinalità strettamente compresa tra la cardinalità di X e quella di $\wp(X)$.*

Una conseguenza dell'Ipotesi del Continuo e dell'uguaglianza $|\mathbb{R}| = |\wp(\mathbb{N})|$, è che i sottoinsiemi di $\mathbb{R}$ sono finiti, oppure numerabili, oppure hanno la stessa cardinalità di $\mathbb{R}$.

Nel 1940 Kurt Gödel (1906-1978) dimostrò la *coerenza relativa* dell'Ipotesi (generalizzata) del Continuo: se la Teoria degli Insiemi non porta a contraddizioni, allora non si ottengono contraddizioni anche assumendo l'Ipotesi (generalizzata) del Continuo. Restava il problema dell'*indipendenza*, cioè la questione se l'Ipotesi del Continuo sia o non sia deducibile dagli altri assiomi della Teoria degli Insiemi. La risposta a tale questione venne data nel 1963 da Paul Cohen (1934-2007) che dimostrò che l'Ipotesi (generalizzata) del Continuo non è conseguenza degli altri assiomi.

Funzioni a valori in $\mathbb{R}$

Nella sezione precedente abbiamo considerato solo *confronti* di cardinalità. Abbiamo cioè dato un significato alle espressioni $|X| \leq |Y|$ e $|X| = |Y|$, ma non abbiamo attribuito nessun significato all'espressione $|X|$. In teoria degli insiemi con questo simbolo si indica un particolare insieme equipotente ad X, il *cardinale* o *numero cardinale* di X[8]. Non rientra negli scopi di queste dispense studiare i dettagli della teoria dei numeri cardinali. Ci limitiamo a riassumere alcuni risultati principali che ci consentiranno di trattare la cardinalità di particolari insiemi.

Nella classe dei numeri cardinali sono definibili una relazione d'ordine (che risulta essere un buon ordinamento) e le usuali operazioni aritmetiche di somma, prodotto, potenza. In particolare, se X è finito allora $|X|$ è proprio il numero - definito in teoria degli insiemi - dei suoi elementi, e la relazione d'ordine e le operazioni aritmetiche coincidono con quelle usuali tra numeri naturali. Inoltre, per tutti i numeri cardinali finiti o infiniti, la relazione d'ordine coincide con la relazione definita in **TI1**. Ha senso quindi usare lo stesso simbolo $\leq$ per entrambe.

Dati due cardinali h e k, la somma $h+k$ viene definita come il cardinale dell'insieme $X \cup Y$, dove $|X| = h$, $|Y| = k$ e $X \cap Y = \emptyset$. Si dimostra che il risultato non dipende dalla scelta di X e Y. Da **TI8** segue che, se $h \leq k$ e k è infinito, allora $h + k = k$. Equivalentemente, se h o k è infinito, allora $h + k = \max\{h, k\}$. Il prodotto $h \cdot k$ dei cardinali h e k viene definito come il cardinale del prodotto cartesiano $h \times k$. Anche in questo caso possiamo usare **TI8**, per concludere che, se se h o k è infinito, allora $h \cdot k = \max\{h, k\}$.

Infine, la potenza h^k viene definita come il cardinale dell'insieme ${}^k h$ delle funzioni da k in h. Dati gli insiemi X, Y e Z, sia F una funzione da Z in ${}^Y X$: per ogni $z \in Z$, $F(z)$ è una funzione da Y in X. Definiamo una funzione $\varphi_F : Z \times Y \to X$ tramite $\varphi_F(z, y) = F(z)(y)$. La corrispondenza $\chi : F \to \varphi_F$ è iniettiva: se $F \neq F'$ allora esiste z tale che $F(z) \neq F'(z)$ e quindi esiste y tale che $F(z)(y) \neq F'(z)(y)$, cioè $\varphi_F(z, y) \neq \varphi_{F'}(z, y)$. La corrispondenza χ è

[8] In [Lolli, 1994], per evitare di confondere le due nozioni, viene usata la scrittura $\mathrm{card}(X)$ nel primo caso, cioè nel confronto di cardinalità, e $\mathrm{Card}(X)$ nel secondo.

anche suriettiva: data $\varphi : Z \times Y \to X$, possiamo definire la funzione F_φ che a ogni z associa la restrizione di φ a $\{z\} \times Y$. Si verifica immediatamente che $\varphi = \chi(F_\varphi)$. Esiste dunque una corrispondenza biunivoca tra ${}^{Z}({}^{Y}X)$ e ${}^{Z\times Y}X$ e quindi i due insiemi sono equipotenti. Per la potenza cardinale vale dunque l'usuale uguaglianza $(h^k)^{k'} = h^{k\cdot k'}$.

Il cardinale dell'insieme dei numeri naturali, che per **TI4** è il minimo cardinale infinito, viene indicato con $\aleph_0$. Abbiamo dunque $|\mathbb{N}| = \aleph_0$. I cardinali finiti vengono indicati con il corrispondente numero naturale, usando il grassetto per ricordare stiamo considerando la definizione insiemistica di numero naturale. In base a questa definizione abbiamo che ogni naturale è costituito dai naturali che lo precedono. In particolare abbiamo $\mathbf{2} = \{\mathbf{0}, \mathbf{1}\}$. Abbiamo già osservato che ad ogni sottoinsieme X di un dato insieme Y possiamo associare la sua funzione caratteristica $f_X : Y \to \{0, 1\}$ che vale 1 su tutti e soli gli elementi di X. Gli insiemi $\wp(Y)$ e ${}^{Y}\{0, 1\}$ hanno dunque la stessa cardinalità. Usando la potenza cardinale possiamo concludere che $|\wp(\mathbb{N})| = |\mathbb{R}| = \mathbf{2}^{\aleph_0}$. Il cardinale $\mathbf{2}^{\aleph_0}$ è dunque la cardinalità del continuo e per questo motivo viene anche indicato con c.[9]

Possiamo ora usare le proprietà delle operazioni tra cardinali viste sopra per studiare la cardinalità di particolari insiemi di funzioni. Partiamo da ${}^{\mathbb{N}}\mathbb{R}$. La cardinalità di questo insieme è data da

$$c^{\aleph_0} \;=\; (\mathbf{2}^{\aleph_0})^{\aleph_0} \;=\; \mathbf{2}^{\aleph_0\cdot\aleph_0} \;=\; \mathbf{2}^{\aleph_0} \;=\; c$$

Le funzioni da $\mathbb{N}$ in $\mathbb{R}$ sono quindi "tante quante" le funzioni da $\mathbb{N}$ in $\{0, 1\}$, cioè tante quante i numeri reali. Non è quindi strano che abbia la stessa cardinalità l'insieme delle funzioni da $\mathbb{N}$ in $\mathbb{N}$, come è dimostrato dalle seguenti disuguaglianze, usando **TI2**.

$$c \;=\; \mathbf{2}^{\aleph_0} \;\leq\; \aleph_0^{\aleph_0} \;\leq\; c^{\aleph_0} \;=\; c$$

L'insieme delle funzioni da $\mathbb{R}$ in $\mathbb{R}$ ha cardinalità

$$c^c \;=\; (\mathbf{2}^{\aleph_0})^{\mathbf{2}^{\aleph_0}} \;=\; \mathbf{2}^{\aleph_0\cdot\mathbf{2}^{\aleph_0}} \;=\; \mathbf{2}^{(\mathbf{2}^{\aleph_0})} \;=\; \mathbf{2}^c$$

L'insieme ${}^{\mathbb{R}}\mathbb{R}$ è dunque equipotente all'insieme delle funzioni da $\mathbb{R}$ in $\{0, 1\}$ e quindi a $\wp(\mathbb{R})$.

Se invece consideriamo l'insieme C^0 delle funzioni continue da $\mathbb{R}$ in $\mathbb{R}$, possiamo osservare che ognuna di queste funzioni è univocamente determinata dai suoi valori in $\mathbb{Q}$ che ha cardinalità $\aleph_0$. L'insieme C^0 ha dunque cardinalità minore o uguale a $c^{\aleph_0} = c$. Poiché tutte le funzioni costanti sono continue, possiamo concludere $|C^0| = c$.

Reali algebrici e reali trascendenti

Un numero reale è *algebrico* se è soluzione di un'equazione polinomiale a coefficienti in $\mathbb{Z}$. I reali non algebrici vengono detti *trascendenti*. Ogni razionale è un reale algebrico in quanto soluzione di un'equazione di primo grado a coefficienti in $\mathbb{Z}$. I reali algebrici

[9] Il minimo cardinale maggiore di $\aleph_0$ viene indicato con $\aleph_1$. L'Ipotesi del Continuo viene quindi espressa dall'uguaglianza $\mathbf{2}^{\aleph_0} = \aleph_1$

costituiscono un sottocampo ordinato di $\mathbb{R}$. Non siamo però qui interessati alla struttura numerica dell'insieme dei reali algebrici, bensì alla sua cardinalità. Iniziamo con un lemma

Lemma A.3 *L'insieme delle equazioni polinomiali a coefficienti in $\mathbb{Z}$ è numerabile.*

Dimostrazione. Osserviamo che da **TI5** segue che per ogni naturale $n > 0$ il prodotto cartesiano $\mathbb{Z}^n$ è numerabile. Ad ogni polinomio di grado k a coefficienti in $\mathbb{Z}$ possiamo far corrispondere la $(k+1)$-upla $\langle a_k, a_{k-1}, \ldots, a_0\rangle$ dei suoi coefficienti. L'insieme delle equazioni di grado k è dunque numerabile essendo in corrispondenza biunivoca con un sottoinsieme infinito di $\mathbb{Z}^{k+1}$: l'insieme delle $(k+1)$-uple $\langle a_k, a_{k-1}, \ldots, a_0\rangle$ con $a_k \neq 0$. Da **TI6** segue che l'insieme di tutti i polinomi a coefficienti in $\mathbb{Z}$ è numerabile. ■

Teorema A.4 *L'insieme dei reali algebrici è numerabile.*

Dimostrazione. Per il lemma precedente, possiamo considerare una successione $E_0, E_1, \ldots$ delle equazioni polinomiali a coefficienti in $\mathbb{Z}$, e quindi anche la successione $S_0, S_1, \ldots$ in cui S_i è l'insieme delle soluzioni in $\mathbb{R}$ di E_i. L'insieme dei reali algebrici è dunque $\bigcup_{i\in\mathbb{N}} S_i$. Ogni insieme S_i è finito e quindi, per **TI6**, l'insieme dei reali algebrici è finito o numerabile. Tale insieme non è ovviamente finito. ■

Corollario A.5 *L'insieme dei reali trascendenti ha cardinalità uguale a quella di $\mathbb{R}$.*

Dimostrazione. Usare il teorema precedente e **TI9**. ■

B Irrazionalità di e e π. Trascendenza di e. Numeri di Liouville

Fino alla prima metà del XIX secolo non era stata dimostrata l'esistenza di numeri trascendenti. Attorno al 1850 Joseph Liouville (1809-1882) diede la prima dimostrazione della trascendenza di particolari numeri reali. Per quanto riguarda i numeri reali che incontriamo più spesso bisogna aspettare ancora qualche anno: nel 1873 Charles Hermite (1822-1901) dimostra che il numero e è trascendente, mentre la trascendenza di π è stata dimostrata da Ferdinand von Lindemann (1852-1939) nel 1882.

La dimostrazione del Teorema di Cantor, da cui segue abbastanza facilmente il Corollario A.5, è stata pubblicata nel 1891. È chiaro che in quel periodo il risultato che l'insieme dei reali trascendenti abbia cardinalità strettamente maggiore dell'insieme degli algebrici diventava particolarmente significativo. Il rovescio della medaglia è che la dimostrazione di Cantor non esibisce nessun numero trascendente, mentre le dimostrazioni che un dato numero reale è trascendente mettono in luce importanti proprietà di questi numeri e degli algebrici.

In questo capitolo, tratto essenzialmente da [Scimemi, 2008], vedremo la dimostrazione della trascendenza di e ed i numeri di Liouville, considerando prima l'irrazionalità di e e di π. Non vedremo invece la dimostrazione della trascendenza di π che è molto complicata.

Teorema B.1 *Il numero e è irrazionale.*

Dimostrazione. Se consideriamo l'espressione di e^x con polinomio di MacLaurin di grado n con resto di Lagrange abbiamo

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + \frac{e^{\xi} \cdot x^{n+1}}{(n+1)!}$$

dove ξ è compreso tra 0 e x. In particolare, per $x = 1$, abbiamo

$$\frac{1}{(n+1)!} \leq e - \sum_{k=0}^{n} \frac{1}{k!} \leq \frac{3}{(n+1)!}$$

e, moltiplicando per $n!$,

$$\frac{1}{n+1} \leq e\, n! - \sum_{k=0}^{n} \frac{n!}{k!} \leq \frac{3}{n+1} \qquad (*)$$

Se e fosse il numero razionale $\frac{h}{m}$, allora il termine intermedio risulterebbe intero positivo per ogni $n > m$, ma al tempo stesso questo termine tende a 0 per $n \to \infty$. ■

La prima dimostrazione dell'irrazionalità di π, attorno al 1770, è dovuta a Johann Heinrich Lambert (1728-1777). Successivamente furono date altre dimostrazioni. Quella che vedremo sembra attualmente la più semplice ed è stata data nel 1946 da Ivan Niven (1915-1999).

Teorema B.2 *Il numero π è irrazionale.*

Dimostrazione. Supponiamo per assurdo $\pi = \frac{a}{b}$ con a e b numeri naturali. Dato $n > 0$ consideriamo il polinomio di grado $2n$

$$f(x) = \frac{x^n(a-bx)^n}{n!} = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} a^k (-b)^{n-k} x^{2n-k} \qquad (*)$$

Mostriamo preliminarmente che tutte le derivate di $f(x)$ sono numeri interi per $x = 0$. Per $j > 2n$, $f^{(j)}(x)$ è identicamente nulla. Per $j < n$, ogni addendo in $f^{(j)}(x)$ contiene una potenza positiva di x, e quindi $f^{(j)}(0) = 0$. Per $j \in \{n, n+1, \ldots, 2n\}$

$$f^{(j)}(x) = \frac{1}{n!} \sum_{k=0}^{2n-j} \binom{n}{k} a^k (-b)^{n-k} \frac{(2n-k)!}{(2n-k-j)!} x^{2n-k-j} \qquad (**)$$

dove possiamo limitare la sommatoria a $2n-j$, perché la derivata j-esima di x^{2n-k} è nulla per $j > 2n-k$, cioè $k > 2n-j$. L'esponente k-esimo nella sommatoria $(**)$ è positivo quando $k < 2n-j$ e quindi l'unico addendo che non si annulla in $f^{(j)}(0)$ è quello in cui $k = 2n-j$:

$$f^{(j)}(0) \;=\; \frac{1}{n!}\binom{n}{2n-j} a^{2n-j}(-b)^{j-n}\frac{j!}{0!}$$

Poiché $n \le j \le 2n$ abbiamo $f^{(j)}(0) \in \mathbb{Z}$.

Osserviamo infine che $f(x) = f(\pi - x)$ da cui segue $f^{(j)}(\pi) = (-1)^j f^{(j)}(0)$. Sia

$$F(x) \;=\; f(x) - f''(x) + f^{(4)}(x) + \cdots + (-1)^n f^{(2n)}(x) \;=\; \sum_{j=0}^{n}(-1)^j f^{(2j)}(x)$$

Per i risultati precedenti abbiamo $F(0) = F(\pi) \in \mathbb{Z}$. Dalla definizione di $F(x)$ segue inoltre $F''(x) + F(x) = f(x)$. Moltiplicando questa uguaglianza per $\sin x$ ricaviamo

$$\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) = f(x)\sin x \quad \text{e}$$

$$\int_0^\pi f(x)\sin x\,dx \;=\; [F'(x)\sin x - F(x)\cos x]_0^\pi \;=\; F(0) + F(\pi) \qquad (***)$$

Nell'intervallo $]0,\pi[$, tenendo presente l'ipotesi $\pi = \frac{a}{b}$, abbiamo $0 < f(x) < \frac{(\pi a)^n}{n!}$ e quindi $0 < \int_0^\pi f(x)\sin x\,dx < \pi\,\frac{(\pi a)^n}{n!}$. In particolare, poiché la successione $(\frac{(\pi a)^n}{n!})$ è infinitesima, per n sufficientemente grande $0 < \int_0^\pi f(x)\sin x\,dx < 1$. Ma ciò contraddice $(***)$ perché $F(0) + F(\pi)$ è intero. ■

Questo risultato è stato dimostrato costruendo un particolare polinomio e poi integrando un'opportuna equazione differenziale. Non è sorprendente che ad un certo punto siano intervenute le funzioni trigonometriche perché in qualche modo si dovevano usare le proprietà di π. La seguente dimostrazione della trascendenza di e segue un percorso analogo.

Teorema B.3 *Il numero e è trascendente.*

Dimostrazione. Supponiamo per assurdo $\sum_{k=0}^m a_k e^k = 0$, dove ogni a_k è intero e $a_0, a_m \neq 0$. Fissato un numero primo p (per ora arbitrario), consideriamo preliminarmente il polinomio

$$f(x) \;=\; \frac{1}{(p-1)!}\,x^{p-1}(x-1)^p(x-2)^p\ldots(x-m)^p$$

Tale polinomio appartiene a $\mathbb{Q}[x]$ e ha grado $n = p-1+mp$. Sia $F(x) = \sum_{j=0}^{n} f^{(j)}(x)$. Allora $F'(x) = \sum_{j=0}^{n} f^{(j+1)}(x) = \sum_{j=1}^{n} f^{(j)}(x)$, e quindi $F'(x) - F(x) = -f(x)$. Moltiplicando per e^{-x}

(fattore integrante) e integrando da 0 a $k \in \{1, \ldots, m\}$, otteniamo

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x) \quad \text{e} \quad e^{-k}F(k) - F(0) \;=\; \int_0^k -e^{-t}f(t)\,dt \tag{$*$}$$

Moltiplicando la seconda delle uguaglianze in $(*)$ per $a_k e^k$ e sommando su k abbiamo

$$\sum_{k=0}^{m} a_k F(k) \;=\; \sum_{k=0}^{m} a_k e^k \int_0^k -e^{-t}f(t)\,dt \tag{$**$}$$

Arriveremo ad un assurdo mostrando che per p sufficientemente grande il primo termine di questa uguaglianza è un intero non nullo, mentre il secondo può essere reso arbitrariamente piccolo in valore assoluto.

I valori di $F(k)$ sono determinati dai valori delle derivate $f^{(j)}(x)$ in k. Osserviamo che per $j = 0, 1, \ldots, p-2$ le derivate $f^{(j)}(x)$ sono somme in cui ogni addendo è prodotto di x, $(x-1), \ldots, (x-m)$ dove ogni fattore ha un esponente positivo. Tutte queste derivate quindi sono nulle per $x = 0, 1, \ldots, m$. La derivata $f^{(p-1)}(x)$ invece si annulla per $x = 1, \ldots, m$, mentre $f^{(p-1)}(0) = (-1)^m(m!)^p$.

Per $j = p, p+1, \ldots, n$, tutti gli addendi di $f^{(j)}(x)$ che non si annullano per ogni x in $\{0, 1, \ldots, m\}$ sono il risultato di p derivazioni di (almeno) una potenza $(x-i)^p$, o di $p-1$ derivazioni di x^{p-1} e una derivazione di qualche $(x-i)^p$. In definitiva troviamo sempre il fattore $p!$ che, semplificato con il denominatore $(p-1)!$, dà un numero intero multiplo di p. Esiste dunque $z \in \mathbb{Z}$ tale che

$$\sum_{k=0}^{m} a_k F(k) \;=\; (-1)^m a_0 (m!)^p + pz$$

Se $p > m$ e $p > |a_0|$, allora il primo addendo non è multiplo di p e quindi la somma è un intero non nullo.

Serve ora un'opportuna maggiorazione dell'integrale a destra in $(**)$. Per x nell'intervallo $[0, m]$, abbiamo $|x-k| \le m$ e $|-e^{-x}| \le 1$. Quindi $\left|-e^{-x}f(x)\right| \le \dfrac{m^{p-1+mp}}{(p-1)!}$ e

$$\left|\int_0^k -e^{-t}f(t)\,dt\right| \;\le\; k\frac{m^{p-1+mp}}{(p-1)!} \;=\; k\frac{m^m(m^{m+1})^{p-1}}{(p-1)!}$$

Possiamo ora arrivare alla conclusione osservando che la successione $a^s/s!$ è infinitesima. Ciò significa infatti che, al crescere di p, $\int_0^k -e^{-t}f(t)\,dt$ tende zero, e lo stesso quindi succede per la sommatoria destra in $(**)$. ∎

Come si vedrà in seguito, il problema della distinzione tra reali algebrici e reali trascendenti è strettamente legato alla possibilità di approssimare con precisione prefissata un numero reale con numeri razionali. Alla lettera, questa espressione non dice niente perché i razionali sono densi nei reali e quindi ogni reale può essere approssimato con precisione arbitraria con un numero razionale. Ci poniamo però il problema di approssimare un numero reale γ con frazioni $\frac{h}{k}$ dove la precisione è una funzione $F(k)$, per ora non precisata, del denominatore k che riterremo sempre maggiore di 0. Cerchiamo cioè soluzioni $\frac{h}{k}$ della disequazione

$$\left|\gamma - \frac{h}{k}\right| \; < \; F(k) \tag{B.2}$$

Esercizio B.1 *Dimostrare che, per ogni irrazionale* γ *e ogni naturale* n*,* (B.2) *ha infinite soluzioni per* $F(k) = \dfrac{1}{2k}$*.*

Suggerimento: osserviamo che, per ogni naturale m, esiste h tale che $\frac{h-1}{m} < \gamma < \frac{h}{m}$. ■

Teorema B.4 Teorema di Dirichlet (1805-1859) *Se* $\gamma \in \mathbb{Q}$ *allora è finito il numero di razionali* $\frac{h}{k}$ *che verificano la disuguaglianza*

$$\left|\gamma - \frac{h}{k}\right| < \frac{1}{k^2} \tag{$*$}$$

Se invece $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ *la disuguaglianza* $(*)$ *è verificata da infinite frazioni* $\frac{h}{k}$*.*

Dimostrazione. Se $\gamma = \frac{r}{s} \neq \frac{h}{k}$, risulta $\left|\gamma - \frac{h}{k}\right| = \left|\frac{kr-hs}{sk}\right| \geq \frac{1}{sk}$. La disuguaglianza $\left|\gamma - \frac{h}{k}\right| < \frac{1}{k^2}$ può dunque valere solo se $\frac{1}{sk} < \frac{1}{k^2}$, cioè per $k < s$.

Sia ora γ irrazionale e supponiamo per assurdo che l'insieme delle soluzioni di $(*)$ sia finito: $\left\{\frac{h_1}{k_1}, \ldots, \frac{h_m}{k_m}\right\}$. Sia n un numero naturale tale che, per ogni i, $\frac{1}{n} < \left|\gamma - \frac{h_i}{k_i}\right|$. Arriveremo ad un assurdo mostrando che esiste una soluzione di $(*)$ tale che $\left|\gamma - \frac{h}{k}\right| < \frac{1}{n}$.

Indichiamo con $[a]$ la parte intera del numero reale a e consideriamo gli n numeri reali $\gamma - [\gamma]$, $2\gamma - [2\gamma], \ldots, n\gamma - [n\gamma]$. Poiché γ irrazionale, questi numeri appartengono all'intervallo aperto $(0,1)$ e, per lo stesso motivo, appartengono all'unione degli n intervalli aperti $(0, \frac{1}{n}), (\frac{1}{n}, \frac{2}{n}), \ldots, (\frac{n-1}{n}, 1)$. Possiamo considerare due casi.

Caso 1: per qualche $k \leq n$, $k\gamma - [k\gamma]$ appartiene all'intervallo $(0, \frac{1}{n})$. Abbiamo quindi

$$\left|\gamma - \frac{[k\gamma]}{k}\right| \; < \; \frac{1}{nk} \; \leq \; \frac{1}{k^2}$$

Vale poi banalmente $\left|\gamma - \frac{[k\gamma]}{k}\right| \; < \; \frac{1}{n}$.

Caso 2: non è verificato il caso 1 e quindi esistono $r < s \leq n$ tali che i numeri $r\gamma - [r\gamma]$ e $s\gamma - [s\gamma]$ appartengono allo stesso intervallo di ampiezza $\frac{1}{n}$. Abbiamo quindi $|(s-r)\gamma - ([s\gamma] - [r\gamma])| < \frac{1}{n}$ e, posto $k = s - r$, otteniamo $\left|\gamma - \dfrac{[s\gamma] - [r\gamma]}{k}\right| < \dfrac{1}{nk}$. Possiamo quindi procedere come nel caso precedente. ■

Teorema B.5 Teorema di Liouville *Sia γ un irrazionale algebrico, zero del polinomio irriducibile $f(x) \in \mathbb{Z}[x]$. Allora, se n è il grado di f, per ogni reale $\beta > 1$ è finito il numero delle frazioni $\frac{h}{k}$ che verificano la disuguaglianza*

$$\left|\gamma - \frac{h}{k}\right| \;\le\; \frac{1}{\beta|f'(\gamma)|k^n} \tag{$*$}$$

Dimostrazione. Sia $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Per ogni frazione $\frac{h}{k}$, tenendo presente che $f(x)$ non ha radici razionali, abbiamo

$$\left|f\left(\frac{h}{k}\right)\right| \;=\; \frac{|a_n h^n + a_{n-1}h^{n-1}k + \cdots + a_1 h k^{n-1} + a_0 k^n|}{k^n} \;\ge\; \frac{1}{k^n}$$

Per il Teorema del Valor Medio abbiamo inoltre che esiste ξ tale che $|\gamma - \xi| \le \left|\gamma - \frac{h}{k}\right|$ e

$$f\left(\frac{h}{k}\right) = f(\gamma) + \left(\frac{h}{k} - \gamma\right) f'(\xi)$$

e dunque, poiché $f(\gamma) = 0$,

$$\frac{1}{k^n} \;\le\; \left|f\left(\frac{h}{k}\right)\right| \;=\; \left|\gamma - \frac{h}{k}\right| |f'(\xi)| \tag{$**$}$$

Scelto $\beta > 1$, per la continuità della funzione $|f'(x)|$ esiste un intorno $\Delta = [\gamma - \epsilon, \gamma + \epsilon]$ di γ, tale che $|f'(x)| < \beta|f'(\gamma)|$ per ogni $x \in \Delta$. Osserviamo ora che, se $\frac{h}{k}$ risolve $(*)$, allora il valore ξ in $(**)$ non appartiene a Δ. Infatti in tal caso avremmo

$$\frac{1}{k^n} \;\le\; \left|\gamma - \frac{h}{k}\right| |f'(\xi)| \;<\; \left|\gamma - \frac{h}{k}\right| \beta|f'(\gamma)| \;\le\; \frac{1}{k^n}$$

Abbiamo quindi

$$\epsilon \;<\; |\gamma - \xi| \;\le\; \left|\gamma - \frac{h}{k}\right| \;\le\; \frac{1}{\beta|f'(\gamma)|k^n}$$

da cui segue $k^n < \dfrac{1}{\epsilon\beta|f'(\gamma)|}$ che è verificato da un insieme finito di k. ∎

Corollario B.6 *Il numero $\gamma = \sum_{i=1}^{\infty} 10^{-i!}$ è trascendente.*

Dimostrazione. Per ogni naturale $n > 0$ abbiamo

$$\begin{aligned} \gamma - \sum_{i=1}^{n} 10^{-i!} \;&=\; \sum_{i=n+1}^{\infty} 10^{-i!} \;=\; 10^{-(n+1)!} \sum_{i=0}^{\infty} \frac{10^{(n+1)!}}{10^{(n+1+i)!}} \;< \\ &<\; 10^{-(n+1)!} \cdot 2 \;=\; \frac{2}{10^{(n+1)n!}} \;=\; \frac{2}{10^{n!}} \cdot \left(\frac{1}{10^{n!}}\right)^n \end{aligned} \tag{$*$}$$

Se $\sum_{i=1}^{n} 10^{-i!} = \frac{h}{k}$ abbiamo $k = 10^{n!}$ e quindi la disuguaglianza $(*)$ può essere scritta come $(**)$ $\gamma - \frac{h}{k} < \frac{2}{10^{n!}} \cdot \frac{1}{k^n}$.

Supponiamo ora per assurdo che γ sia algebrico con polinomio minimo $f(x)$ di grado m e sia $\beta > 1$. Sia $n > m$ tale che $10^{n!} > 2\beta|f'(\gamma)|$. Dalla disuguaglianza $(**)$ segue

$$\left|\gamma - \frac{h}{k}\right| \; < \; \frac{1}{\beta|f'(\gamma)|k^n} \; < \; \frac{1}{\beta|f'(\gamma)|k^m}$$

Ma esistono infiniti n con quelle proprietà e ciò contrasta con il Teorema di Liouville. ■

Riferimenti bibliografici

[Bottazzini, 1981] Bottazzini, U. (1981). *Il calcolo sublime: storia dell'analisi matematica da Euler a Weierstrass*. Boringhieri.

[Burrill, 1967] Burrill, C. W. (1967). *Foundations of real numbers*. McGraw-Hill.

[Cohen and Ehrlich, 1963] Cohen, L. and Ehrlich, G. (1963). *The Structure of the Real Number System*. van Nostrand.

[De Marco, 1996] De Marco, G. (1996). *Analisi Uno*. Decibel. Seconda edizione.

[Facchini, 2000] Facchini, A. (2000). *Algebra e Matematica Discreta*. Decibel.

[Fiori and Invernizzi, 2009] Fiori, C. and Invernizzi, S. (2009). *Numeri Reali*. Pitagora.

[Guiotto, 2008] Guiotto, P. (2008). Complementi di analisi matematica. Dispense per la Scuola Galileiana.

[Lolli, 1994] Lolli, G. (1994). *Dagli insiemi ai numeri*. Boringhieri.

[Lolli, 2008] Lolli, G. (2008). Dispense per il Corso di *Storia e Filosofia della Teoria degli Insiemi*. Scuola Normale Superiore di Pisa, a.a. 2008/09, `http://homepage.sns.it/lolli/dispense08/corso08-3.pdf`.

[Piacentini Cattaneo, 1996] Piacentini Cattaneo, G. M. (1996). *Algebra - Un approccio algoritmico*. Decibel.

[Scimemi, 2008] Scimemi, B. (2008). Appunti per il corso di *Matematica e Classica 1*. Dip. Matematica P.A. Univ. Padova, a.a. 2008/09, `http://www.cissm.unipd.it/dispense/scimemi/` (Matematica Classica).

Indice analitico