1 Numeri reali

Definizione 1.1 *Un* campo ordinato *è un campo* $\mathbb{K}$ *munito di una relazione d'ordine totale* $\leq$*, compatibile con le operazioni di somma e prodotto nel senso seguente:*

1. $\forall a, b, c \in \mathbb{K}$, $a \leq b \implies a + c \leq b + c$;
2. $\forall a, b, c \in \mathbb{K}$, $c \geq 0$, $a \leq b \implies c \cdot a \leq c \cdot b$.

Il campo $\mathbb{Q}$ dei numeri razionali è un campo ordinato.

Osservazione 1.1 *Si verifica facilmente che esiste un'unica relazione d'ordine totale su* $\mathbb{Q}$ *che lo renda un campo ordinato.*

L'esercizio seguente mostra che esistono moltissimi campi ordinati (in effetti, infiniti).

Esercizio 1.1 *Se* $\mathbb{K}$ *è un campo ordinato, si consideri l'anello dei polinomi*

$$\mathbb{K}[t] = \left\{ \sum_{k=0}^{n} a_k t^k \mid n \in \mathbb{N},\ a_1, \dots, a_n \in \mathbb{K} \right\}$$

e il corrispondente campo delle frazioni

$$\mathbb{F} = \{p/q \mid p, q \in \mathbb{K}[t],\ q \neq 0\}.$$

Si dimostri che $\mathbb{F}$ *è un campo ordinato (si ponga* $t \geq a$ *per ogni* $a \in \mathbb{K}$*).*

Definizione 1.2 *Diciamo che il campo* $\mathbb{K}$ *ha* caratteristica zero *se per ogni* $n \in \mathbb{Z}^+$ *si ha* $n \cdot 1 \neq 0$*. Qui* $n \cdot 1$ *indica la somma* $1 + 1 + \cdots + 1$ *con* n *termini.*

Proposizione 1.1 *Ogni campo ordinato ha caratteristica zero.*

Il campo $\mathbb{Q}$ dei numeri razionali ha caratteristica zero. In effetti, $\mathbb{Q}$ è il più piccolo campo con caratteristica zero. Questo è il senso della seguente:

Proposizione 1.2 *Sia* $\mathbb{K}$ *un campo di caratteristica zero. Allora esiste un unico omomorfismo si campi* $\varphi : \mathbb{Q} \to \mathbb{K}$*, e tale omomorfismo risulta iniettivo.*

In altre parole, *ogni campo con caratteristica zero contiene un unico sottocampo isomorfo a* $\mathbb{Q}$. In particolare, questo vale per i campi ordinati. Nel seguito, dato un campo ordinato $\mathbb{K}$ identificheremo il suo sottocampo isomofo a $\mathbb{Q}$ con $\mathbb{Q}$ stesso.

Definizione 1.3 *Un campo ordinato* $\mathbb{K}$ *si dice* Archimedeo *se per ogni* $a, b \in \mathbb{K}$*,* $a > 0$*,* $b > 0$*, esiste* $n \in \mathbb{N}$ *tale che* $n \cdot a > b$*.*

Il campo $\mathbb{Q}$ dei numeri razionali è Archimedeo. Il campo $\mathbb{F}$ dell'Esercizio 1.1 non è Archimedeo.

Proposizione 1.3 *Sia $\mathbb{K}$ un campo ordinato Archimedeo. Ogni intervallo aperto $]a, b[$, $a, b \in \mathbb{K}$, $a < b$, contiene almeno un numero razionale.*

Un sottoinsieme di un insieme ordinato che ha intersezione non vuota con ogni intervallo aperto si dice *denso*. Quindi la proposizione precedente afferma che $\mathbb{Q}$ è denso in ogni campo Archimedeo. Iterando questa proposizione, si verifica facilmente che ogni intervallo aperto di un campo Archimedeo contiene infiniti numeri razionali.

Dimostrazione. Supponiamo inizialmente $b > a > 0$. Dato che $b - a > 0$ la proprietà di Archimede implica che esiste $n \in \mathbb{Z}^+$ tale che $n \cdot (b - a) > 1$, ossia $b - a > 1/n$. L'insieme

$$A = \left\{ k \in \mathbb{N} \mid k \in \mathbb{N},\ \frac{k}{n} > a \right\} \subset \mathbb{Z}^+$$

è non vuoto: questo segue dalla proprietà di Archimede applicata ai numeri positivi $1/n$ e a. Sia $m = \min A$ (ogni sottoinsieme non vuoto di $\mathbb{N}$ ha minimo). Dato che $m \in A$, $m/n > a$. Dato che m è il minimo di A, $m - 1$ non appartiene ad A. Quindi $(m - 1)/n \leq a$, da cui, usando anche il fatto che $1/n < b - a$,

$$\frac{m}{n} = \frac{m-1}{n} + \frac{1}{n} \leq a + \frac{1}{n} < a + (b - a) = b.$$

Quindi $m/n \in]a, b[$, come richiesto.

Possiamo ricondurre il caso di un intervallo qualsiasi $]a, b[$ al caso $a > 0$ traslando l'intervallo di una traslazione intera: per la proprietà di Archimede possiamo trovare un intero n tale che $a + n > 0$, e si considera l'intervallo $]a + n, b + n[$. □

Osservazione 1.2 *E' anche facile verificare che se $\mathbb{K}$ è Archimedeo, $a \in \mathbb{K}$ e per ogni $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, risulta $|a| \leq \epsilon$, allora $a = 0$.*

Definizione 1.4 *Un campo ordinato $\mathbb{K}$ si dice* completo *se per ogni sottoinsieme $A \subset \mathbb{K}$ limitato superiormente esiste l'estremo superiore di A.*

Come conseguenza, per ogni sottoinsieme $A \subset \mathbb{K}$ limitato inferiormente esiste l'estremo inferiore di A: infatti $-A = \{a \in \mathbb{K} \mid -a \in A\}$ è limitato superiormente e si verifica facilmente che

$$\inf A = -\sup(-A).$$

Proposizione 1.4 *Ogni campo ordinato completo è Archimedeo.*

Dimostrazione. Supponiamo per assurdo che esistano $a, b \in \mathbb{K}$, $a > 0$, $b > 0$, tali che per ogni $n \in \mathbb{N}$ vale $n \cdot a \leq b$. Allora l'insieme

$$A = \{n \cdot a \mid n \in \mathbb{N}\}$$

è limitato superiormente (b è un maggiorante). Sia $s = \sup A$. Dato che $s - a < s = \sup A$, esiste un $n \in \mathbb{N}$ tale che $n \cdot a > s - a$, ossia $(n+1) \cdot a > s$. Ma $(n+1) \cdot a$ è ancora un elemento di A, e l'ultima disuguaglinza contraddice il fatto che s sia un maggiorante di A. □

Definizione 1.5 *Definiamo assiomaticamente il campo* $\mathbb{R}$ *dei* numeri reali *come un* campo ordinato completo.

Il seguente risultato mostra che queste proprietà caratterizzano $\mathbb{R}$ in modo univoco.

Teorema 1.5 *Siano* $\mathbb{K}_1$ *e* $\mathbb{K}_2$ *campi ordinati completi. Allora esiste un isomorfismo di campi* $\varphi : \mathbb{K}_1 \to \mathbb{K}_2$ *strettamente crescente.*

Premettiamo alla dimostrazione di questo teorema il seguente:

Lemma 1.6 *Sia* $\mathbb{K}$ *una campo Archimedeo e sia* $\varphi : \mathbb{K} \to \mathbb{K}$ *una funzione crescente la cui restrizione a* $\mathbb{Q}$ *sia l'identità (per ogni* $q \in \mathbb{Q}$, $\varphi(q) = q$*). Allora* φ *è l'identità su* $\mathbb{K}$.

Dimostrazione. Sia $x \in \mathbb{K}$. Per la densità dei razionali nei campi Archimedei, dato $\epsilon \in \mathbb{K}$, $\epsilon > 0$, possiamo trovare due razionali p, q tali che

$$x - \epsilon < p < x < q < x + \epsilon.$$

Dalle proprietà di φ deduciamo che

$$p = \varphi(p) \leq \varphi(x) \leq \varphi(q) = q,$$

e sfruttando la prima disuguaglianza troviamo

$$x - \epsilon < \varphi(x) < x + \epsilon,$$

ossia $|\varphi(x) - x| < \epsilon$. Dato che questa disuguaglinza vale per ogni $\epsilon > 0$, concludiamo che $\varphi(x) = x$. □

Dimostriamo ora il Teorema di unicità 1.5. Vogliamo costruire l'isomorfismo $\varphi : \mathbb{K}_1 \to \mathbb{K}_2$. Dato $x \in \mathbb{K}_1$, consideriamo il sottoinsieme di $\mathbb{Q}$,

$$A(x) = \{q \in \mathbb{Q} \mid q \leq x\},$$

dove $\leq$ è la relazione d'ordine in $\mathbb{K}_1$. L'insieme $A(x)$ è limitato superiormente in $\mathbb{K}_1$ (x è un maggiorante). Per la proprietà di Archimede esistono razionali maggiori di x, dunque $A(x)$ è limitato superiormente anche in $\mathbb{Q}$.

Vediamo adesso $A(x)$ come sottoinsieme di $\mathbb{K}_2$. Essendo $A(x)$ limitato superiormente in $\mathbb{Q}$, è a maggior ragione limitato superiormente in $\mathbb{K}_2$. Per la completezza di $\mathbb{K}_2$ possiamo porre

$$\varphi(x) = \sup A(x) \in \mathbb{K}_2,$$

dove sup indica l'estremo superiore in $\mathbb{K}_2$.

Se $x \in \mathbb{Q}$, l'insieme $A(x)$ ha massimo x, dunque $\varphi(x) = x$. Inoltre, se $x, y \in \mathbb{K}_1$, $x < y$, si ha $A(x) \subset A(y)$, da cui

$$\varphi(x) = \sup A(x) \leq \sup A(y) = \varphi(y),$$

e quindi la funzione φ è crescente.

Scambiando i ruoli di $\mathbb{K}_1$ e $\mathbb{K}_2$ troviamo una funzione $\psi : \mathbb{K}_2 \to \mathbb{K}_1$ che vale l'identità su $\mathbb{Q}$ e che risulta crescente. Allora le funzioni

$$\psi \circ \varphi : \mathbb{K}_1 \to \mathbb{K}_1, \quad \varphi \circ \psi : \mathbb{K}_2 \to \mathbb{K}_2,$$

sono entrambe crescenti (composizioni di funzioni crescenti) e valgono l'identità su $\mathbb{Q}$. Per il Lemma 1.6, $\psi \circ \varphi$ coincide con l'identità su $\mathbb{K}_1$ e $\varphi \circ \psi$ coincide con l'identità su $\mathbb{K}_2$. Quindi φ è bigettiva e ψ è la sua inversa. In particolare, φ è strettamente crescente (una funzione crescente ed iniettiva è strettamente crescente).

Rimane da verificare che φ è un isomorfismo di campi. Questo seguirà dal fatto che φ è l'identità su $\mathbb{Q}$ ed è crescente, sfruttando la densità dei razionali.

Iniziamo con il dimostrare che φ conserva la somma. Siano $x, y \in \mathbb{K}_1$. Dato $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, esistono $p_1, p_2, q_1, q_1 \in \mathbb{Q}$ tali che

$$x - \epsilon < p_1 < x < p_2 < x + \epsilon, \quad y - \epsilon < q_1 < y < q_2 < y + \epsilon.$$

Quindi

$$p_1 + q_1 < x + y < p_2 + q_2, \quad p_2 - \epsilon < x < p_1 + \epsilon, \quad q_2 - \epsilon < y < q_1 + \epsilon.$$

Dato che φ è crescente e vale l'identità su $\mathbb{Q}$, troviamo le disuguaglianze

$$p_1 + q_1 \leq \varphi(x + y) \leq p_2 + q_2, \quad p_2 - \epsilon \leq \varphi(x) \leq p_1 + \epsilon, \quad q_2 - \epsilon \leq \varphi(y) \leq q_1 + \epsilon,$$

dove abbiamo sfruttato il fatto che anche ϵ è un razionale. Combinate assieme queste disuguaglianze implicano

$$\varphi(x) + \varphi(y) - 2\epsilon \leq \varphi(x + y) \leq \varphi(x) + \varphi(y) + 2\epsilon,$$

e dato che ciò vale per ogni ϵ razionale positivo concludiamo che $\varphi(x + y) = \varphi(x) + \varphi(y)$ (vedi Osservazione 1.2).

Verifichiamo ora che $\varphi(xy) = \varphi(x)\varphi(y)$. Possiamo ridurci facilmente al caso $x > 0$, $y > 0$. Siano $\epsilon, p_1, p_2, q_1, q_2$ come sopra, con ϵ cosí piccolo che $x - \epsilon > 0$ e $y - \epsilon > 0$. Allora

$$p_1 q_1 < xy < p_2 q_2, \quad p_2 - \epsilon < x < p_1 + \epsilon, \quad q_2 - \epsilon < y < q_1 + \epsilon,$$

e per le proprietà di φ,

$$p_1 q_1 \leq \varphi(xy) \leq p_2 q_2, \quad p_2 - \epsilon \leq \varphi(x) \leq p_1 + \epsilon, \quad q_2 - \epsilon \leq \varphi(y) \leq q_1 + \epsilon.$$

dato che $p_2 - \epsilon > x - \epsilon > 0$ e $q_2 - \epsilon > y - \epsilon > 0$, dalle ultime due disuguaglianze segue che

$$(p_2 - \epsilon)(q_2 - \epsilon) \leq \varphi(x)\varphi(y) \leq (p_1 + \epsilon)(q_1 + \epsilon).$$

Si ottiene quindi

$$\begin{aligned} \varphi(xy) - \varphi(x)\varphi(y) &\leq p_2 q_2 - (p_2 - \epsilon)(q_2 - \epsilon) = \epsilon(p_2 + q_2 - \epsilon) < \epsilon(x + y + \epsilon), \\ \varphi(xy) - \varphi(x)\varphi(y) &\geq p_1 q_1 - (p_1 + \epsilon)(q_1 + \epsilon) = -\epsilon(p_1 + q_1 - \epsilon) < -\epsilon(x + y + \epsilon), \end{aligned}$$

da cui

$$|\varphi(xy) - \varphi(x)\varphi(y)| < \epsilon|x + y| + \epsilon^2.$$

Per l'arbitrarietà del razionale positivo ϵ si deduce $\varphi(xy) = \varphi(x)\varphi(y)$. $\square$

Osservazione 1.3 *L'argomento sopra mostra anche che l'isomorfismo strettamente crescente* $\varphi : \mathbb{K}_1 \to \mathbb{K}_2$ *è unico.*

Osservazione 1.4 *L'argomento sopra mostra anche che ogni campo Archimedeo è un sottocampo di* $\mathbb{R}$*: se* $\mathbb{K}$ *è un campo Archimedeo, esiste (unico) un omomorfismo iniettivo strettamente crescente* $\varphi : \mathbb{K} \to \mathbb{R}$.