Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

CAMPI REALMENTE CHIUSI E IL TEOREMA FONDAMENTALE DELL'ALGEBRA

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Monica Idà

Presentata da:
Alessandro Liane

Anno Accademico 2021-2022

"In fondo, la vita è tutta una seria di rimpianti.
E vivere consiste proprio nel trasformare quei rimpianti
in opportunità, ciascuno a modo proprio."

Indice

Introduzione

L'idea all'origine di questa tesi è nata inizialmente durante un corso del terzo anno, quando è scaturito il mio interesse su cosa rendesse o meno un campo, o più in generale un anello, ordinato. Con lo scopo di approfondire questa particolare tipo di struttura matematica ho poi finito con l'imbattermi in una dimostrazione di natura puramente algebrica di una generalizzazione del Teorema Fondamentale dell'Algebra per una particolare tipologia di campi, detti *campi formalmente reali*: la teoria di questi oggetti è stata sviluppata negli anni 20 del '900 dai matematici Emil Artin e Otto Schreier, i quali, studiandone le proprietà, in seguito sono stati in grado di dimostrare tale generalizzazione mediante il solo utilizzo di strumenti provenienti dall'algebra, osservando come l'impossibilità di trovare estensioni algebriche che estendessero l'ordine di tali campi implicasse che la loro chiusura algebrica fosse analoga a quella dei numeri reali. Come affermò il matematico tedesco Hans Zassenhaus ([6]):

"*O. Schreier's and Artin's ingenious characterization of formally real fields as fields in which -1 is not the sum of squares and the ensueing deduction of the existence of an algebraic ordering of such fields started the discipline of real algebra. Really, Artin and his congenial friend and colleague Schreier set out on the daring and successful construction of a bridge between algebra and analysis. In the light of Artin-Schreier's theory the fundamental theorem of algebra truly is an algebraic theorem inasmuch as it states that irreducible polynomials over really closed fields only can be linear or quadratic.*"

Il presente elaborato ha lo scopo di studiare i campi ordinati e le loro proprietà caratterizzanti, per arrivare alla dimostrazione del teorema di Artin-Schreier. In seguito mostriamo una costruzione del completamento di un campo ordinato mediante successioni di Cauchy, che applicata a $\mathbb{Q}$ dà una costruzione dei numeri reali e ci permette di

dedurre come corollario del Teorema di Artin-Schreier il Teorema Fondamentale dell'Algebra. È bene precisare che, nonostante alcuni concetti richiamino metodi provenienti dall'analisi reale e dalla topologia, gli oggetti usati durante l'intera trattazione sono definiti in maniera puramente algebrica.

Nel primo capitolo vengono introdotte le nozioni di base sugli anelli ordinati che verranno utilizzate nel resto della trattazione, tra cui gli omomorfismi d'ordine tra anelli ordinati, le estensioni dell'ordine di un sottoanello all'anello che lo contiene, il valore assoluto e le sue proprietà.

Nel secondo capitolo l'attenzione viene posta sui campi ordinati, provando che un campo può essere dotato della struttura di campo ordinato se e solo se è un campo formalmente reale, il che significa che -1 non può essere scritto come somma di quadrati.

Nel terzo capitolo vengono introdotti i campi realmente chiusi e i campi euclidei, per poi dimostrare il Teorema di Artin-Schreier (Teorema 3.3.1).

Per concludere, nel quarto capitolo si introduce il concetto di completamento di un campo ordinato e si definiscono le proprietà di un campo ordinato quali l'essere archimedeo, la proprietà dell'estremo superiore e la proprietà del valore intermedio per i polinomi: si ottiene quindi $\mathbb{R}$ come completamento del campo ordinato $\mathbb{Q}$ e si vede che $\mathbb{R}$ è realmente chiuso. Come corollario si ottiene il Teorema Fondamentale dell'Algebra.

Per la comprensione del testo vi è un unico requisito non banale: la conoscenza dei fatti basilari della teoria di Galois. Nella dimostrazione del Teorema di Artin-Schreier si usano infatti la teoria di Galois e i Sylow p-sottogruppi, per i quali si rimanda a dei testi di algebra.

Per la stesura dei risultati si è fatto principalmente riferimento al testo di Paul M. Cohn [3], con alcuni spunti utilizzati nel quarto capitolo dovuti al testo di Pete L. Clark [2].

Va osservato che nel Teorema 8.7.1 di [3] la proprietà universale dei completamenti manca di un'ipotesi, senza la quale la dimostrazione non funziona; per tale motivo, all'interno di questa tesi suddetta ipotesi è stata aggiunta (Teorema 4.2.6).

Capitolo 1

Anelli ordinati

In questo primo capitolo introduciamo la nozione di anello (commutativo) ordinato, uno dei principali concetti che verranno utilizzati nel corso della tesi, illustrandone alcune delle proprietà caratterizzanti. Con "anello" intenderemo sempre "anello commutativo non banale".

1.1 Le prime definizioni

Notazione: Nel seguito, se x, y sono elementi di un anello $\mathfrak{R}$, denoteremo il loro prodotto sia con $x \cdot y$ che con xy, a seconda dei casi. Se $a \in \mathfrak{R}$, diremo che a è un *quadrato* se esiste $x \in \mathfrak{R}$ se esiste $x \in \mathfrak{R}$ tale che $x^2 = a$. Infine se $\mathbb{K}$ è un campo, poniamo $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$.

Definizione 1.1.1. Sia $\mathfrak{R}$ un anello e sia '$<$' una relazione d'ordine totale stretto definita su di esso. Si dice che $(\mathfrak{R}, <)$ è un *anello ordinato* se l'ordinamento è compatibile con le operazioni binarie definite sull'anello, ossia per ogni $x, y, z \in \mathfrak{R}$ valgono le seguenti proprietà:

O.1 $x > y \ \Rightarrow \ x + z > y + z$,

O.2 $x > 0, \ y > 0 \ \Rightarrow \ xy > 0$.

Un elemento $x \in \mathfrak{R}$ è detto *positivo* se $x > 0$, *negativo* se $x < 0$. Inoltre quando ogni volta scriveremo "$x \leq y$", come al solito, si intenderà "$x < y$ oppure $x = y$".

Se $\mathfrak{R}$ è un dominio d'integrità, rispettivamente un campo, $(\mathfrak{R}, <)$ viene detto *dominio d'integrità ordinato*, rispettivamente *campo ordinato*.
Nel seguito, per semplicità di notazione, un anello ordinato $(\mathfrak{R}, <)$ verrà denotato semplicemente con $\mathfrak{R}$.

Esempio 1. Gli anelli $\mathbb{Z}$ e $\mathbb{Q}$ dotati del classico ordinamento sono degli anelli ordinati. Vedremo come per ognuno di questi anelli tale ordinamento è anche l'unico possibile.

Definizione 1.1.2. Siano $\mathfrak{R}$, $\mathfrak{S}$ anelli ordinati e sia $\Phi : \mathfrak{R} \to \mathfrak{S}$ un omorfismo iniettivo di anelli. Si dice che Φ è un *omomorfismo d'ordine* di $\mathfrak{R}$ in $\mathfrak{S}$ se preserva l'ordine, ossia se $x < y$ in $\mathfrak{R}$, $\Phi(x) < \Phi(y)$ in $\mathfrak{S}$. Diciamo che $\mathfrak{R}$ e $\mathfrak{S}$ sono *ordinatamente isomorfi* se Φ è un isomorfismo.

Nota bene:. Non si può fare a meno di chiedere Φ iniettivo. Infatti, se così non fosse esisterebbe $x \in \ker(\Phi)$ non nullo quindi $x > 0$ (oppure $x < 0$). Tuttavia $\Phi(x) = 0 \not> 0$ (oppure $\Phi(x) = 0 \not< 0$) e perciò Φ non preserverebbe l'ordine.

Proposizione 1.1.3. *La composizione di due omomorfismi d'ordine è a sua volta un omomorfismo d'ordine. In particolare, se $\mathfrak{R}$ e $\mathfrak{S}$ sono ordinatamente isomorfi e $\mathfrak{S}$ e $\mathfrak{T}$ sono ordinatamente isomorfi, allora $\mathfrak{R}$ e $\mathfrak{T}$ sono ordinatamente isomorfi.*

Dimostrazione. Siano $\mathfrak{R}$, $\mathfrak{S}$, $\mathfrak{T}$ degli anelli ordinati e siano f,g con $\mathfrak{R} \xrightarrow{f} \mathfrak{S}$, $\mathfrak{S} \xrightarrow{g} \mathfrak{T}$ degli omomorfismi d'ordine. Per definizione f e g sono omomorfismi iniettivi di anelli, per cui anche $h := g \circ f : \mathfrak{R} \to \mathfrak{T}$ è un omomorfismo iniettivo di anelli. Bisogna solamente mostrare che h preserva l'ordine. Siano $x < y$ in $\mathfrak{R}$; essendo f un omomorfismo d'ordine abbiamo $f(x) < f(y)$ in $\mathfrak{S}$, dunque essendo anche g un omomorfismo d'ordine abbiamo $h(x) = g(f(x)) < g(f(y)) = h(y)$ in $\mathfrak{T}$. □

1.2 Alcune proprietà

Vediamo alcune delle proprietà degli anelli ordinati che utilizzeremo.

Osservazione 1.2.1. In $\mathfrak{R}$ anello ordinato se $x \in \mathfrak{R}$ con $x > 0$ allora $-x < 0$, e se $y \in \mathfrak{R}$ con $y < 0$ allora $-y > 0$. Inoltre se $x > 0, y < 0$ si ha $xy < 0$. Infatti, supponiamo

$x > 0$; allora per la proprietà **O.1** si ha:

$$0 \;=\; x \;-\; x \;>\; 0 \;-\; x \;=\; -x.$$

Il caso $y < 0$ si dimostra in modo del tutto analogo. Utilizzando invece la proprietà **O.2**, se $x > 0$ e $y < 0$ si ha:

$$-\,x \cdot y \;=\; x \cdot (-y) \;>\; 0 \;\Rightarrow\; x \cdot y \;<\; 0.$$

Proposizione 1.2.2. *Ogni $\mathfrak{R}$ anello ordinato è un dominio d'integrità, e il quadrato di un elemento non nullo è positivo; in particolare $1 > 0$. Inoltre, $char(\mathfrak{R}) = 0$.*

Dimostrazione. Siano $x, y \in \mathfrak{R}$ entrambi non nulli. Analizziamo i vari casi utilizzando la proprietà **O.2** assieme all'Osservazione 1.2.1:

- *Se* $x > 0,\ y > 0$: $\Rightarrow\ xy > 0$;
- *Se* $x < 0,\ y < 0$: $\Rightarrow -x, -y > 0 \Rightarrow xy = (-x)(-y) > 0$;
- *Se* $x > 0 > y$: $\Rightarrow xy < 0$.

In ognuno di questi casi abbiamo perciò $xy \neq 0$. Ponendo poi $y = x$, per quanto visto nei primi due casi si ha $x^2 = x \cdot x > 0$. In particolare, siccome $1 = 1^2 > 0$, per la proprietà **O.1** segue che $n1 = 1 + \ldots + 1 > 0\ \forall n \in \mathbb{N}^*$ e dunque $char(\mathfrak{R}) = 0$. □

Osservazione 1.2.3. In $\mathfrak{R}$ anello ordinato se $x, y, z \in \mathfrak{R}$ sono tali che $x < y$ e $z > 0$, allora $xz < yz$. Infatti sia $y - x$ che z sono positivi, perciò:

$$yz \;-\; xz \;=\; (y-x)z \;>\; 0 \;\Rightarrow\; xz \;<\; yz.$$

Osservazione 1.2.4. Dati x, y invertibili in un anello ordinato $\mathfrak{R}$, se $x > 0$ e $0 < x < y$ allora $\frac{1}{x} > 0$ e $\frac{1}{x} > \frac{1}{y}$. Infatti se fosse $\frac{1}{x} < 0$ si avrebbe $1 = x \cdot \frac{1}{x} < 0$, giungendo a una contraddizione. Dato che $xy > 0$, è sufficiente moltiplicare per $\frac{1}{xy}$ entrambi i lati della disuguaglianza $x < y$.

Corollario 1.2.5. *Ogni anello finito $\mathfrak{F}$ non può essere dotato di un ordinamento tale da renderlo un anello ordinato.*

Dimostrazione. Per la Proposizione 1.2.2 un anello ordinato deve avere caratteristica nulla. Dato che un anello finito $\mathfrak{F}$ possiede sempre $char(\mathfrak{F}) \neq 0$, allora non può essere un anello ordinato. □

Osservazione 1.2.6. Sia $\mathfrak{R}$ un anello ordinato. L'insieme di tutti i suoi elementi positivi $P = \{x \in \mathfrak{R} \mid x > 0\}$ verifica $1 \in P,\ 0 \notin P$ e per ogni $x, y \in P$ si ha $x + y, xy \in P$. Inoltre, siccome $\mathfrak{R}$ è totalmente ordinato, l'ordinamento definisce una tripartizione di $\mathfrak{R}$ per cui per ogni $x \in \mathfrak{R}$ una e una sola delle seguenti è vera: $x \in P, -x \in P$ o $x = 0$.

Proposizione 1.2.7. *Sia $\mathfrak{R}$ un anello e sia $\mathrm{P} \subseteq \mathfrak{R}$ un suo sottoinsieme soddisfacente le condizioni seguenti:*

$$1 \in \mathrm{P},\ 0 \notin P \quad e \quad \forall x, y \in \mathrm{P} \quad si\ ha \quad x + y,\ x \cdot y \in \mathrm{P}, \tag{1.1}$$

$$\forall x \in \mathfrak{R} \textbf{ una e una sola } \textit{delle seguenti è vera: } x \in P, -x \in P, x = 0. \tag{1.2}$$

Allora $\mathfrak{R}$ è un anello ordinato, con '$<$' definita nel modo seguente:

$$per\ x, y \in \mathfrak{R}\ si\ ha\ x < y \Leftrightarrow\ y - x \in P;$$

e P è detto il positive order set dell'anello. Quindi, ogni ordine in un anello è caratterizzato dal proprio positive order set.

Dimostrazione. Per prima cosa verifichiamo che '$<$' definisce una relazione d'ordine totale stretto su $\mathfrak{R}$.
Antiriflessività: $\forall x \in \mathfrak{R}$ non si ha $x < x$ perché $0 \notin P$;
Transitività: $\forall x, y, z \in \mathfrak{R}$ con $x < y,\ y < z$ abbiamo $y - x, z - y \in P$, quindi per la (1.1) $z - x = (z - y) + (y - x) \in P$, il che vuol dire $x < z$;
Legge di tricotomia: Siccome P soddisfa (1.2), per ogni $x, y \in \mathfrak{R}$ si ha $x - y \in P$ o $y - x \in P$ o $x - y = 0$ e una sola di queste è vera, ovvero $y < x,\ x < y$ o $x = y$.
Abbiamo così dimostrato che '$<$' è una relazione d'ordine totale stretto su $\mathfrak{R}$ e osserviamo che $x > 0$ se e solo se $x \in P$.
Mostriamo infine che '$<$' rispetta **O.1** e **O.2**; infatti per $x, y, z \in \mathfrak{R}$:

- *Se* $x < y$: $\Rightarrow\ (y + z) - (x + z) = y + z - x - z = y - x \in P\ \Rightarrow\ x + z < y + z$;
- *Se* $0 < x, 0 < y$: $\Rightarrow\ x, y \in P\ \Rightarrow\ xy \in P\ \Rightarrow\ 0 < xy$.

Quindi $(\mathfrak{R}, <)$ soddisfa $\mathbf{O.1}, \mathbf{O.2}$ e P è il positive order set di questo ordinamento. □

1.3 Estensione di un ordinamento al campo dei quozienti

Definizione 1.3.1. Sia $\mathfrak{R}$ un anello e sia $\mathfrak{T} \subseteq \mathfrak{R}$ un suo sottoanello proprio con $\mathfrak{R}$, $\mathfrak{T}$ anelli ordinati. Diciamo che $\mathfrak{R}$ *estende l'ordine* di $\mathfrak{T}$ se l'immersione i: $\mathfrak{T} \to \mathfrak{R}$, $x \mapsto x$ è un omomorfismo d'ordine, ossia se $x < y$ in $\mathfrak{T}$ allora $x < y$ in $\mathfrak{R}$.

Osservazione 1.3.2. Siano $\mathfrak{R}_2 \subseteq \mathfrak{R}_1$ due anelli dotati di ordinamenti distinti tali che $\mathfrak{R}_1, \mathfrak{R}_2$ siano anelli ordinati. Siano poi P_1, P_2 rispettivamente i positive order set di $\mathfrak{R}_1, \mathfrak{R}_2$. Allora $\mathfrak{R}_1$ estende l'ordine di $\mathfrak{R}_2$ se e solo se $P_2 \subseteq P_1$. Infatti, supponiamo che $\mathfrak{R}_1$ estenda l'ordine di $\mathfrak{R}_2$; allora se $x \in \mathfrak{R}_2$ con $x > 0$ in $\mathfrak{R}_2$ abbiamo anche $x > 0$ in $\mathfrak{R}_1$. Ma per la definizione di positive order set di un anello ordinato questo equivale a dire se $x \in P_2$ allora $x \in P_1$, da cui abbiamo $P_2 \subseteq P_1$.
Supponiamo ora $P_2 \subseteq P_1$ e siano $x, y \in \mathfrak{R}_2$. Allora per la Proposizione 1.2.7 abbiamo:

$$x < y \text{ in } \mathfrak{R}_2 \;\Leftrightarrow\; y - x \in P_2 \;\Rightarrow\; y - x \in P_1 \;\Leftrightarrow\; x < y \text{ in } \mathfrak{R}_1.$$

Dunque $\mathfrak{R}_1$ estende l'ordine di $\mathfrak{R}_2$.

Abbiamo visto nella Proposizione 1.2.2 come un anello ordinato $\mathfrak{R}$ sia anche un dominio di integrità, per tale motivo è possibile definire il suo *campo dei quozienti* $\mathcal{Q}(\mathfrak{R})$. Il seguente teorema ci dice che anche tale campo ammette una struttura di campo ordinato, oltre a fornire un'importante informazione sul legame tra i due ordinamenti.

Teorema 1.3.3. *Sia $\mathfrak{R}$ un anello ordinato. L'ordine di $\mathfrak{R}$ può essere esteso al suo campo dei quozienti $\mathcal{Q}(\mathfrak{R})$ in maniera unica, ossia nel modo seguente:*

$$\forall x, y \in \mathfrak{R} \text{ con } y \neq 0 \text{ si ha } \frac{x}{y} > 0 \text{ in } \mathcal{Q}(\mathfrak{R}) \;\Leftrightarrow\; xy > 0 \text{ in } \mathfrak{R}. \tag{1.3}$$

Dimostrazione. Se $\mathcal{Q}(\mathfrak{R})$ estende l'ordine di $\mathfrak{R}$, l'ordinamento sul campo dei quozienti soddisfa (1.3); infatti per $x, y \in \mathfrak{R}$, $y \neq 0$ abbiamo visto che $y^2 > 0$, perciò $\frac{x}{y} > 0$ se e solo se $xy = \frac{x}{y} \cdot y^2 > 0$.
Mostriamo ora che effettivamente (1.3) definisce un ordinamento di $\mathcal{Q}(\mathfrak{R})$ tale da renderlo un campo ordinato. Per prima cosa mostriamo che la definizione è ben posta. Dati $\frac{a}{b}, \frac{c}{d} \in \mathcal{Q}(\mathfrak{R})$ abbiamo $\frac{a}{b} = \frac{c}{d}$ se e solo se $ad = cb$, cioè se e solo se $abd^2 = cdb^2$ con

$b^2, d^2 > 0$. Quindi la condizione (1.3) dà:

$$\frac{a}{b} > 0 \; in \; \mathcal{Q}(\mathfrak{R}) \Leftrightarrow ab > 0 \; in \; \mathfrak{R} \Leftrightarrow ab \cdot d^2 > 0 \; in \; \mathfrak{R} \Leftrightarrow cd \cdot b^2 > 0 \; in \; \mathfrak{R} \Leftrightarrow \frac{c}{d} > 0 \; in \; \mathcal{Q}(\mathfrak{R}).$$

Poniamo ora:

$$P = \left\{ f = \frac{x}{y} \in \mathcal{Q}(\mathfrak{R}) \mid xy > 0 \; in \; \mathfrak{R} \right\}.$$

Se tale insieme verifica (1.1), (1.2) allora per la Proposizione 1.2.7 abbiamo concluso la dimostrazione. Siano quindi $f_1, f_2 \in P$; per come sono definite le operazioni di somma e prodotto nel campo dei quozienti abbiamo:

$$f_1 + f_2 = \frac{x_1 \cdot y_2 + x_2 \cdot y_1}{y_1 \cdot y_2} \quad , \quad f_1 \cdot f_2 = \frac{x_1 \cdot x_2}{y_1 \cdot y_2}.$$

Ne segue dunque che $f_1 + f_2, f_1 \cdot f_2 \in P$ in quanto:

$$(x_1 \cdot y_2 + x_2 \cdot y_1) \cdot (y_1 \cdot y_2) = (x_1 \cdot y_1) \cdot y_2^2 + (x_2 \cdot y_2) \cdot y_1^2 > 0,$$

$$x_1 \cdot x_2 \cdot y_1 \cdot y_2 = (x_1 \cdot x_2) \cdot (y_1 \cdot y_2) > 0,$$

verificando così (1.1). Inoltre, anche la (1.2) è verificata; infatti se $\frac{x}{y} \in \mathcal{Q}(\mathfrak{R})$ una e una sola delle seguenti è vera in $\mathfrak{R}$: $xy > 0$, $xy < 0$, $xy = 0$. Da ciò segue che una e una sola delle seguenti è vera in $\mathcal{Q}(\mathfrak{R})$: $\frac{x}{y} > 0$, $\frac{x}{y} < 0$, $\frac{x}{y} = 0$. □

Corollario 1.3.4. *L'anello degli interi $\mathbb{Z}$ e il campo dei razionali $\mathbb{Q}$ ammettono un unico ordinamento, ovvero quello classico.*

Dimostrazione. Preso un ordinamento '$<$' qualsiasi che dia a $\mathbb{Z}$ la struttura di anello ordinato, necessariamente $1, 1+1, \ldots$ sono tutti positivi mentre $-1, -(1+1), \ldots$ sono tutti negativi; allora tale ordinamento coincide con quello usuale e ne segue che è l'unico possibile. Essendo infine $\mathbb{Q} = \mathcal{Q}(\mathbb{Z})$ per il teorema appena dimostrato esiste un unico modo per estendere l'ordine di $\mathbb{Z}$ a quello di $\mathbb{Q}$ ed esso è quello usuale. □

1.4 Valore assoluto

Definizione 1.4.1. Per ogni elemento $a \in \mathfrak{R}$ anello ordinato, si definisce il *valore assoluto*

$$|a| := \begin{cases} a & \text{se} \quad a \geq 0, \\ -a & \text{se} \quad a < 0. \end{cases}$$

Vediamo ora alcune proprietà importanti del valore assoluto.

Proposizione 1.4.2. *Sia $\mathfrak{R}$ un anello ordinato. Allora valgono le seguenti proprietà:*

Av.1 $|a| \geq 0 \ \ \forall a \in \mathfrak{R}$ *e si ha* $|a| = 0 \iff a = 0$,

Av.2 $|a \cdot b| = |a| \cdot |b| \ \ \forall a, b \in \mathfrak{R}$,

Av.3 $|a + b| \leq |a| + |b| \ \ \forall a, b \in \mathfrak{R}$.

Dimostrazione. Siano a, b due elementi qualsiasi di $\mathfrak{R}$. La **Av.1** segue direttamente dalla definizione del valore assoluto. La **Av.2** segue immediatamente esaminando i quattro casi possibili: $a \geq 0$ e $b \geq 0$, $a \geq 0$ e $b < 0$, $a < 0$ e $b \geq 0$, $a < 0$ e $b < 0$. Per dimostrare **Av.3** analizziamo nel dettaglio tutti i casi possibili. Se $a, b \geq 0$ abbiamo: $|a + b| = a + b = |a| + |b|$; se $a, b < 0$ allora: $|a+b| = -(a+b) = -a-b = |a| + |b|$. Supponiamo adesso $a \leq 0 \leq b$, e che quindi $-b \leq 0 \leq -a$. Ora utilizzando ciò osserviamo:

$$a + b \leq 0 + b \leq -a + b = |a| + |b|, \ -a - b \leq -a + 0 \leq -a + b = |a| + |b|.$$

Dunque si ha $|a + b| \leq |a| + |b|$. □

Osservazione 1.4.3. Se $\Phi : \mathfrak{R} \to \mathfrak{S}$ è un omomorfismo d'ordine allora per ogni $x \in \mathfrak{R}$ vale $\Phi(|x|) = |\Phi(x)|$. Infatti per definizione di omomorfismo d'ordine, se $x \geq 0$ in $\mathfrak{R}$ allora $\Phi(x) \geq 0$ in $\mathfrak{S}$, mentre se $x < 0$ in $\mathfrak{R}$ allora $\Phi(x) < 0$ in $\mathfrak{S}$.

Capitolo 2

Una caratterizzazione dei campi ordinati

In questo capitolo entriamo più nel dettaglio nello studio delle proprietà dei campi ordinati, mediante l'ausilio del concetto di campo formalmente reale: ciò ci permetterà di dimostrare una proprietà caratterizzante dei campi ordinati.

2.1 Core di un campo

Cominciamo col definire in un anello la nozione di cono, oltre a enunciare alcune delle sue proprietà.

Definizione 2.1.1. Sia $\mathfrak{R}$ un anello. Un sottoinsieme $V \subset \mathfrak{R}$ è definito *cono* se soddisfa le seguenti condizioni:

$$-1 \notin V, \quad x^2 \in V \ \ \forall\, x \in \mathfrak{R} \quad e \quad \forall y, z \in V \ si\ ha\ y+z, yz \in V. \tag{2.1}$$

Nota bene:. Può accadere che in un anello esista più di un cono o che non ce ne sia nemmeno uno.

Esempio 2. Il campo $\mathbb{F}_2$ formato dai soli elementi 0 e 1 non ammette alcun cono: infatti un cono $V \subset \mathbb{F}_2$ per definizione dovrebbe contenere $1^2 = 1$, tuttavia $1 = -1$ e per la definizione di cono $-1 \notin V$.

Di seguito sono elencate alcune delle proprietà dei coni utili ai nostri scopi.

Osservazione 2.1.2. Sia $\mathfrak{R}$ un anello e sia $V \subset \mathfrak{R}$ un cono. Allora per ogni $x \in V$ invertibile si ha $x^{-1} \in V$. Infatti, per definizione di cono abbiamo $(x^{-1})^2 \in V$. Basta dunque osservare per la chiusura rispetto alla moltiplicazione: $x^{-1} = x \cdot (x^{-1})^2 \in V$.

Osservazione 2.1.3. Sia $\mathfrak{R}$ un anello ordinato e sia Q il suo positive order set. Allora l'insieme $V := Q \cup \{0\}$ è un cono di $\mathfrak{R}$ e, posto $-V := \{-x \mid x \in V\}$, verifica:

$$\mathfrak{R} \;=\; V \;\cup\; -V \;,\; V \;\cap\; -V \;=\; \{0\}. \tag{2.2}$$

Infatti, siccome Q è un positive order set è chiuso rispetto alle operazioni di somma e prodotto. Grazie alla Proposizione 1.2.2, sappiamo che, eccetto l'elemento nullo, i quadrati di elementi di $\mathfrak{R}$ sono positivi perciò appartengono a Q, e $-1 < 0$ per cui $-1 \notin Q$. Quindi, attraverso l'aggiunta dell'elemento nullo, l'insieme V soddisfa sia la definizione di cono che la proprietà (2.2).

Viceversa in ogni dominio d'integrità $\mathfrak{D}$, se $V \subset \mathfrak{D}$ è un cono soddisfacente (2.2) allora $V \setminus \{0\}$ è il positive order set di un ordine totale stretto '$<$' che rende $\mathfrak{D}$ un anello ordinato. Infatti, posto $S := V \setminus \{0\}$, per la definizione di cono e la proprietà (2.2), tale insieme S soddisfa le ipotesi della Proposizione 1.2.7 e, dunque, la tesi è verificata.

Lemma 2.1.4. *Sia $\mathbb{K}$ un campo e $V \subset \mathbb{K}$ un cono. Se V verifica la condizione $\mathbb{K} = V \cup -V$, allora $V \setminus \{0\}$ è il positive order set di un ordinamento su $\mathbb{K}$.*

Dimostrazione. Basta osservare che in un campo la seconda condizione di (2.2) è ridondante, in quanto se esistesse $c \in V \cap -V$ non nullo avremmo $-c, c^{-1} \in V$, da cui seguirebbe $-1 = c \cdot (-c) \cdot (c^{-1})^2 \in V$ ma ciò andrebbe contro la definizione di cono. □

Definizione 2.1.5. Sia $\mathbb{K}$ un campo. Si definisce *core* di $\mathbb{K}$ l'insieme delle somme finite di quadrati

$$C = C(\mathbb{K}) := \left\{ \sum_i x_i^2 \mid x_i \in \mathbb{K} \right\}.$$

Sia $\mathbb{F} \subseteq \mathbb{K}$ un sottocampo e supponiamo $\mathbb{F}$ ordinato. Si definisce $\mathbb{F}$-*core* di $\mathbb{K}$ l'insieme delle somme finite di quadrati a coefficienti positivi in $\mathbb{F}$

$$\Gamma_{\mathbb{F}}(\mathbb{K}) := \left\{ \sum_i \lambda_i \cdot x_i^2 \mid x_i \in \mathbb{K},\ \lambda_i \in \mathbb{F},\ \lambda_i > 0 \right\}.$$

Si osservi che si ha $C(\mathbb{K}) \subseteq \Gamma_{\mathbb{F}}(\mathbb{K})$ e, posto $P_{\mathbb{F}}$ il positive order set di $\mathbb{F}$, si ha in particolare $P_{\mathbb{F}} \subseteq \Gamma_{\mathbb{F}}(\mathbb{K}) \setminus \{0\}$.

Vediamo una condizione necessaria e sufficiente affinché gli insiemi appena definiti siano coni.

Proposizione 2.1.6. *Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione di campi e sia $\mathbb{F}$ un campo ordinato. Allora gli insiemi $\Gamma_{\mathbb{F}}(\mathbb{K}), C(\mathbb{K})$ sono chiusi rispetto alle operazioni di somma e prodotto, e sono coni di $\mathbb{K}$ se e solo se non contengono -1.*

Dimostrazione. Per definizione si ha $x^2 \in C(\mathbb{K})$ per ogni $x \in \mathbb{K}$, per cui tutti i quadrati di $\mathbb{K}$ sono contenuti in $C(\mathbb{K})$ e quindi sono contenuti anche in $\Gamma_{\mathbb{F}}(\mathbb{K})$. Mostriamo adesso la chiusura di $\Gamma_{\mathbb{F}}(\mathbb{K})$ rispetto alle operazioni di somma e di prodotto (la dimostrazione per $C(\mathbb{K})$ è identica). Siano perciò $a = \sum_i a_i x_i^2,\ b = \sum_j b_j y_j^2$ con $a, b \in \Gamma_{\mathbb{F}}(\mathbb{K})$: per la somma si ha $a + b = \sum_i a_i x_i^2 + \sum_j b_j y_j^2$, dove se $x_{i_0} = y_{i_0}$ allora $a_{i_0} + b_{i_0}$ è il coefficiente di $x_{i_0}^2$ ed è positivo; per il prodotto invece si ha $ab = \sum_{i.j} a_i b_j x_i^2 y_j^2 = \sum_{i.j} (a_i b_j)(x_i y_j)^2$ con $a_i b_j > 0$. Per cui $a + b, ab \in \Gamma_{\mathbb{F}}(\mathbb{K})$. In conclusione sia $\Gamma_{\mathbb{F}}(\mathbb{K})$ che $C(\mathbb{K})$ soddisfano le condizioni (2.1) e sono dei coni se e solo se non contengono l'elemento -1. □

2.2 Campi formalmente reali

D'ora in avanti quando scriveremo "*un campo $\mathbb{K}$ può essere ordinato*" oppure "*un campo $\mathbb{K}$ è ordinabile*" si intenderà che esiste una relazione d'ordine totale stretto '$<$' su $\mathbb{K}$ per la quale $(\mathbb{K}, <)$ è un campo ordinato.

Definizione 2.2.1. Un campo $\mathbb{K}$ viene detto *formalmente reale* se il suo core $C(\mathbb{K})$ non contiene l'elemento -1.

Per quanto visto nella Proposizione 2.1.6, si ha:

un campo $\mathbb{K}$ è $formalmente\ reale$ se e solo se $C(\mathbb{K})$ è un cono.

Proposizione 2.2.2. *Ogni campo formalmente reale $\mathbb{K}$ è di caratteristica zero.*

Dimostrazione. Supponiamo per assurdo che $char(\mathbb{K}) = p \in \mathbb{N}^*$. Per la definizione di caratteristica di un anello abbiamo $p1 = 1 + \ldots + 1 = 0$, il che implica $-1 = (p-1)1$.

Sappiamo che $C(\mathbb{K})$ è chiuso rispetto alla somma, inoltre essendo 1 un quadrato per definizione di core abbiamo $1 \in C(\mathbb{K})$; di conseguenza $-1 = (p-1)1 = 1+\ldots+1 \in C(\mathbb{K})$ ma ciò è impossibile per definizione di campo formalmente reale. □

Teorema 2.2.3. *Ogni $\mathbb{K}$ campo ordinabile è un campo formalmente reale.*

Dimostrazione. Sia $(\mathbb{K}, <)$ un campo ordinato; tutti gli elementi di $C(\mathbb{K})$ sono somma finita di quadrati, perciò sono necessariamente tutti elementi positivi di $\mathbb{K}$, incluso 1. Dunque $-1 \notin C(\mathbb{K})$, essendo negativo, e $\mathbb{K}$ è formalmente reale. □

Lemma 2.2.4. *Siano $\mathbb{K}$ un campo, $V \subset \mathbb{K}$ un cono e siano $a, b \in \mathbb{K}$ tali che $ab \in V$. Posto $V + aV := \{x + ay | x, y \in V\}$, allora $V + aV$ è un cono oppure $V - bV$ è un cono.*

Dimostrazione. Osserviamo subito che ogni elemento $x \in V$ può essere scritto come $x = x + a \cdot 0 \in V + aV$ oppure come $x = x - b \cdot 0 \in V - bV$, per cui il cono V, e di conseguenza anche tutti i quadrati di $\mathbb{K}$, sono contenuti sia in $V + aV$ che in $V - bV$. Mostriamo ora la chiusura di $V+aV$, $V-bV$ rispetto alle operazioni di somma e prodotto. Siano $x_1, x_2, y_1, y_2 \in V$; osservando che $a^2, b^2 \in V$ si ha:

$$(x_1 + ax_2) + (y_1 + ay_2) = (x_1 + y_1) + a\,(x_2 + y_2) \in V + aV;$$

$$(x_1 + ax_2) \cdot (y_1 + ay_2) = (x_1y_1 + a^2x_2y_2) + a\,(x_1y_2 + x_2y_1) \in V + aV;$$

$$(x_1 - bx_2) + (y_1 - by_2) = (x_1 + y_1) - b\,(x_2 + y_2) \in V - bV;$$

$$(x_1 - bx_2) \cdot (y_1 - by_2) = \left(x_1y_1 + b^2x_2y_2\right) - b\,(x_1y_2 + x_2y_1) \in V - bV.$$

Adesso supponiamo che entrambi $V + aV$ e $V - bV$ contengano -1, ossia che esistano $x, y, u, v \in V$ tali che $-1 = x + au = y - bv$. Riscrivendo $au = -1 - x$, $-bv = -1 - y$ osserviamo:

$$-abuv = (au)(-bv) = (-1 - x)(-1 - y) = 1 + x + y + xy$$

da cui segue $-1 = x + y + xy + abuv \in V$, il che per la definizione di cono non può succedere. L'unica possibilità dunque è che -1 non appartenga almeno a uno tra $V+aV$ e $V - bV$, per cui tale insieme è un cono. □

Osservazione 2.2.5. Nella dimostrazione precedente abbiamo visto in particolare che $V + aV, V - bV$ non sono dei coni se e solo se contengono -1.

Lemma 2.2.6. *Sia $\mathbb{K}$ un campo. Allora ogni cono $V \subset \mathbb{K}$ è contenuto in un cono massimale di $\mathbb{K}$, ed ogni cono massimale $M \subset \mathbb{K}$ soddisfa la condizione $\mathbb{K} = M \cup -M$.*

Dimostrazione. L'esistenza di un cono massimale contenente V segue dal lemma di Zorn. Sia ora $M \subset \mathbb{K}$ un cono massimale e sia $a \in \mathbb{K}$; allora $a \cdot a = a^2 \in M$, quindi per il Lemma 2.2.4 almeno uno tra i due insiemi $M + aM,\ M - aM$ è un cono contenente M. Ma per ipotesi M è massimale, perciò $M = M + aM$ se $M = M + aM$ è un cono o $M = M - aM$ se $M = M - aM$ è un cono, ossia $a \in M$ oppure $a \in -M$. Dunque, essendo vero per ogni $a \in \mathbb{K}$, il cono massimale M soddisfa la condizione $\mathbb{K} = M \cup -M$. □

Teorema 2.2.7. *Sia $\mathbb{K}$ un campo e sia $\mathbb{F} \subseteq \mathbb{K}$ un sottocampo ordinato. Allora l'ordinamento di $\mathbb{F}$ può essere esteso ad un ordinamento di $\mathbb{K}$ se e solo se $\Gamma_{\mathbb{F}}(\mathbb{K})$ è un cono.*

Dimostrazione. Supponiamo che $\mathbb{K}$ sia ordinabile e che estenda l'ordine di $\mathbb{F}$. Tutti gli elementi di $\Gamma_{\mathbb{F}}(\mathbb{K})$ sono somme finite di quadrati di $\mathbb{K}$ con coefficienti positivi in $\mathbb{F}$ e, poiché l'ordine viene esteso, lo sono anche in $\mathbb{K}$. Quindi $\Gamma_{\mathbb{F}}(\mathbb{K})$ contiene solo elementi positivi di $\mathbb{K}$ (oltre a 0) e perciò non può contenere l'elemento -1 in quanto elemento negativo di $\mathbb{K}$; per la Proposizione 2.1.6 ciò equivale a dire che $\Gamma_{\mathbb{F}}(\mathbb{K})$ è un cono.
Supponiamo invece che $\Gamma_{\mathbb{F}}(\mathbb{K})$ sia un cono. Per il Lemma 2.2.6 esiste $M \subset \mathbb{K}$ cono massimale contenente $\Gamma_{\mathbb{F}}(\mathbb{K})$ e che soddisfa la condizione $\mathbb{K} = M \cup -M$, mentre per il Lemma 2.1.4 l'insieme $M \setminus \{0\}$ costituisce il positive order set di un qualche ordinamento $(\mathbb{K}, <)$. Allora, per costruzione, il positive order set di $\mathbb{F}$ è contenuto in $\Gamma_{\mathbb{F}}(\mathbb{K}) \setminus \{0\}$, inoltre $\Gamma_{\mathbb{F}}(\mathbb{K}) \setminus \{0\} \subseteq M \setminus \{0\}$; per cui, grazie a quanto visto nell'Osservazione 1.3.2, $\mathbb{K}$ estende l'ordinamento di $\mathbb{F}$. □

Vediamo ora come il viceversa del Teorema 2.2.3 sia vero a sua volta, ottenendo in questo modo una caratterizzazione dei campi ordinabili.

Proposizione 2.2.8. *Sia $\mathbb{K}$ un campo formalmente reale e sia $V \subset \mathbb{K}$ un cono. Allora V è l'intersezione di tutti i coni massimali di $\mathbb{K}$ contenenti V.*

Dimostrazione. Osserviamo innanzitutto che l'intersezione di coni massimali di $\mathbb{K}$ contenenti V è ancora un cono. Infatti sia $\{M_i\}_{i \in \mathcal{I}}$ una famiglia di coni massimali di $\mathbb{K}$ contenenti V:

- per definizione di cono $-1 \notin M_i \ \forall \ i \in \mathcal{I} \ \Rightarrow -1 \notin \bigcap_{i\in\mathcal{I}} M_i$;
- sempre per definizione di cono $x^2 \in M_i \ \forall \ i \in \mathcal{I}$ per ogni $x \in \mathbb{K} \Rightarrow \ x^2 \in \bigcap_{i\in\mathcal{I}} M_i$ per ogni $x \in \mathbb{K}$;
- siano $x, y \in \bigcap_{i\in\mathcal{I}} M_i \Rightarrow \ x, y \in M_i \ \forall i \in \mathcal{I}$. Essendo M_i coni, sono chiusi rispetto alla somma e al prodotto, per cui $x + y, xy \in M_i \ \forall i \in \mathcal{I} \Rightarrow x + y, xy \in \bigcap_{i\in\mathcal{I}} M_i$.

Sia perciò $P := \cap\{M \subseteq \mathbb{K} \text{ cono massimale} \mid V \subseteq M\}$; per quanto appena detto P è un cono di $\mathbb{K}$ e $V \subseteq P$. Per finire la dimostrazione non resta che mostrare la veridicità dell'inclusione opposta. Sia così $a \notin V$ e supponiamo che $V - aV$ non sia un cono; per quanto visto nella dimostrazione del Lemma 2.2.4 ciò succede se e solo se $-1 \in V - aV$ ossia se e solo se $-1 = x - ay$ per qualche $x, y \in V$ con $y \neq 0$. Sotto queste ipotesi si può scrivere $ay = x+1$ quindi $a = (x+1) \cdot y^{-1} \in V$, ma ciò non è possibile per le ipotesi su a. Ne consegue perciò che $V - aV$ è un cono e, per il Lemma 2.2.6, esiste $M \subseteq \mathbb{K}$ cono massimale che soddisfa (2.2) e inoltre $V \subseteq V - aV \subseteq M$. Osserviamo così che $-a = 0 - a \cdot 1 \in M$, da cui segue per (2.2) che $a \notin M$; dunque per la definizione di P (M è un ideale massimale contenente V) vale $a \notin P$ e così $P \subseteq V$. □

Teorema 2.2.9. *Ogni $\mathbb{K}$ campo formalmente reale è un campo ordinabile.*

Dimostrazione. Per l'ipotesi di campo formalmente reale il core $C(\mathbb{K})$ è un cono di $\mathbb{K}$, quindi per il Lemma 2.2.6 esiste un cono massimale M di $\mathbb{K}$ che lo contiene e tale che $\mathbb{K} = M \cup -M$. Ma per il Lemma 2.1.4 l'insieme $M \setminus \{0\}$ costituisce il positive order set di un qualche ordinamento su $\mathbb{K}$, perciò il campo è ordinabile. □

Mettendo assieme i risultati del Teorema 2.2.3 e del Teorema 2.2.9 otteniamo infine la seguente caratterizzazione.

Teorema 2.2.10. *Un campo $\mathbb{K}$ è ordinabile se e solo se $\mathbb{K}$ è formalmente reale.*

Osservazione 2.2.11. Osserviamo che il core di un campo è contenuto in ogni cono del campo. Inoltre, il core di un campo formalmente reale è un cono per la Proposizione 2.1.6 quindi, per la Proposizione 2.2.8, C è l'intersezione di tutti i coni massimali. Abbiamo visto nella dimostrazione del Teorema 2.2.9 che un cono massimale è il positive order set di un ordinamento del campo e, d'altra parte, il positive order set di un ordinamento è

un cono massimale; ne si può perciò dedurre che un elemento $x \in \mathbb{K}$ è positivo sotto ogni ordinamento di $\mathbb{K}$ se e solo se può essere scritto come somma di quadrati. In tal caso x viene detto *totally positive*.

Capitolo 3

Il Teorema di Artin-Schreier

Dato un campo $\mathbb{K}$ e detto 1 il suo elemento neutro moltiplicativo, indichiamo con i un elemento appartenente a una qualche estensione algebrica $\mathbb{L} \supseteq \mathbb{K}$ tale che $i^2 = -1$.

3.1 Chiusura reale di un campo

In questa prima parte analizziamo una condizione sufficiente affinché, dati $\mathbb{K}$ campo ordinato e $\mathbb{K} \subseteq \mathbb{L}$ estensione algebrica di campi, sia possibile estendere l'ordine di $\mathbb{K}$ a $\mathbb{L}$. Per prima cosa definiamo le nozioni di campo realmente chiuso e di chiusura reale di un campo formalmente reale.

Definizione 3.1.1. Un campo $\mathbb{K}$ è detto *realmente chiuso* se è formalmente reale e non esiste $\mathbb{K} \subseteq \mathbb{L}$ estensione algebrica con $\mathbb{L}$ formalmente reale. Pertanto, $\mathbb{K}$ è massimale come campo formalmente reale nella sua chiusura algebrica $\overline{\mathbb{K}}$.

Definizione 3.1.2. Sia $\mathbb{K}$ un campo formalmente reale. Si definisce *chiusura reale di* $\mathbb{K}$ un'estensione algebrica $\mathbb{K} \subseteq \mathbb{E}$ dove $\mathbb{E}$ realmente chiuso.

Teorema 3.1.3. *Ogni campo formalmente reale ammette una chiusura reale.*

Dimostrazione. Sia $\mathbb{K}$ un campo formalmente reale; grazie al Teorema 2.2.10 possiamo supporlo ordinato. Consideriamo allora il poset $(\mathcal{F}, \leq)$ costituito dall'insieme $\mathcal{F} :=$

$\{\mathbb{E}$ campo ordinato $\mid \mathbb{K} \subseteq \mathbb{E} \subseteq \overline{\mathbb{K}}\}$ e dalla relazione d'ordine '$\leq$' definita nel modo seguente:

$$\textit{per } \mathbb{E}, \mathbb{L} \in \mathcal{F} \textit{ si ha } \mathbb{E} \leq \mathbb{L} \Leftrightarrow \mathbb{E} \subseteq \mathbb{L}, \ \mathbb{L} \textit{ estende l'ordine di } \mathbb{E}.$$

Sia ora '$\mathbb{E}_1 \leq \mathbb{E}_2 \leq \dots$' una catena di $(\mathcal{F}, \leq)$; detto $\mathbb{F}$ il campo ottenuto dall'unione di tutti gli elementi della catena, notiamo che $\mathbb{F} \in \mathcal{F}$ e costituisce un maggiorante per la catena. Infatti ogni elemento $a \in \mathbb{F}$ appartiene a qualche campo $\mathbb{E}_i$ della catena ed è quindi algebrico su $\mathbb{K}$. Se poi avessimo $-1 \in \Gamma_{\mathbb{E}_i}(\mathbb{F})$, con $\mathbb{E}_i$ elemento della catena, sarebbe possibile scrivere $-1 = \sum_j \lambda_j x_j^2$ con $0 < \lambda_j$ in $\mathbb{E}_i$ per ogni j, ma in tal caso esisterebbe un campo $\mathbb{E}_k$ della catena tale che $\mathbb{E}_i \leq \mathbb{E}_k$ e $\lambda_j, x_j \in \mathbb{E}_k$ per ogni j; ne conseguirebbe perciò $0 < \lambda_j x_j^2$ in $\mathbb{E}_k$ da cui $0 < \sum_j \lambda_j \ x_j^2 = -1$ in $\mathbb{E}_k$, giungendo così a una contraddizione. Per cui $-1 \notin \Gamma_{\mathbb{E}_i}(\mathbb{F})$ e $\mathbb{F}$ estende l'ordine di $\mathbb{E}_i$ (e quindi di $\mathbb{K}$) per il Teorema 2.2.7 e per la Proposizione 2.1.6. In conclusione, grazie al lemma di Zorn esiste $\mathbb{L}$ elemento massimale di $\mathcal{F}$. Quindi $\mathbb{L}$ non ha estensioni algebriche contenute in $\overline{\mathbb{K}}$ che estendano l'ordine di $\mathbb{K}$; inoltre, essendo ordinato, $\mathbb{L}$ è formalmente reale. □

Enunciamo il teorema anche noto come 'Teorema dell'elemento primitivo'.

Teorema 3.1.4. *Sia $\mathbb{K} \subseteq \mathbb{L}$ un'estensione finita di campi. Allora esiste un elemento $\alpha \in \mathbb{L}$ tale che $\mathbb{L} = \mathbb{K}(\alpha)$; in particolare $deg(f) = [\mathbb{L} : \mathbb{K}]$, dove $f \in \mathbb{K}[x]$ è il polinomio minimo di α.*

Dimostrazione. Si veda di [1], Capitolo 14, Teorema (4.1) per la prima parte, mentre per la seconda si veda [1], Capitolo 13, Proposizione (3.2). □

Lemma 3.1.5. *Sia $\mathbb{K}$ un campo ordinato e sia $\mathbb{K} \subseteq \mathbb{L}$ un'estensione algebrica finita. Allora:*

i) Se $[\mathbb{L} : \mathbb{K}] = 2n - 1$ per $n \in \mathbb{N}^*$, l'ordine di $\mathbb{K}$ può essere esteso a $\mathbb{L}$;

ii) Se $\mathbb{L} = \mathbb{K}(\sqrt{a})$, dove $a > 0$ in $\mathbb{K}$, l'ordine di $\mathbb{K}$ può essere esteso a $\mathbb{L}$.

Dimostrazione. *i*) Per il Teorema 3.1.4 esiste $\alpha \in \mathbb{L}$ tale che $\mathbb{L} = \mathbb{K}(\alpha)$; quindi per ogni elemento $\beta \in \mathbb{K}(\alpha)$ esistono $a_0, \dots, a_{2n-2} \in \mathbb{K}$ tali che $\beta = a_{2n-2}\alpha^{2n-2} + \dots + a_0$. Sia poi $p \in \mathbb{K}[x]$ il polinomio minimo di α su $\mathbb{K}$. Dimostriamo la tesi per induzione su n. Per $n = 1$ è ovvio, in quanto se $[\mathbb{L} : \mathbb{K}] = 1$ allora $\mathbb{K} = \mathbb{L}$. Sia perciò $n > 1$ e supponiamo la

tesi vera fino a $n-1$. Per il Teorema 2.2.7 basta mostrare che $\Gamma_{\mathbb{K}}(\mathbb{L})$, il $\mathbb{K}$-core di $\mathbb{L}$, è un cono. Supponiamo ciò non sia vero, cioè che $-1 \in \Gamma_{\mathbb{K}}(\mathbb{L})$, ossia $-1 = \sum_i \lambda_i x_i^2$ dove $x_i \in \mathbb{K}(\alpha)$ e $\lambda_i > 0$ in $\mathbb{K}$. Allora per ogni i esiste $h_i \in \mathbb{K}[x]$, con $deg(h_i) \leq 2n-2$, tale che $h_i(\alpha) = x_i$. Osserviamo che:

$$-1 = \sum_i \lambda_i h_i(\alpha)^2 \Leftrightarrow -1 - \sum_i \lambda_i h_i(\alpha)^2 = 0;$$

quindi per la definizione di polinomio minimo esiste un polinomio $q \in \mathbb{K}[x]$ tale che $p(x)q(x) = -1 - \sum_i \lambda_i h_i(x)^2$, o equivalentemente, posto $h(x) = \sum_i \lambda_i h_i(x)^2$:

$$-1 = p(x)q(x) + h(x). \tag{3.1}$$

Poiché $\lambda_i > 0$, il grado di $h(x)$ è pari e $deg(h) \leq 2(2n-2)$. Quindi per l'identità (3.1) abbiamo $deg(p \cdot q) = deg(h) \leq 2(2n-2)$. Perciò, dato che per ipotesi $deg(p) = 2n-1$ è dispari, anche il grado di q è dispari e $deg(q) \leq 2n-3 = 2(n-1)-1$. Come conseguenza, esiste un fattore irriducibile di q di grado $2k-1$ con $k \leq n-1$, e se β è una sua radice allora l'estensione $\mathbb{K} \subseteq \mathbb{K}(\beta)$ ha grado $2k-1$: allora per ipotesi induttiva $\mathbb{K}(\beta)$ estende l'ordinamento di $\mathbb{K}$, inoltre $\Gamma_{\mathbb{K}}(\mathbb{K}(\beta))$ è un cono di $\mathbb{K}(\beta)$. Tuttavia calcolando (3.1) in β si ottiene:

$$-1 = p(\beta)q(\beta) + h(\beta) = \sum_i \lambda_i h_i(\beta)^2 \in \Gamma_{\mathbb{K}}(\mathbb{K}(\beta));$$

il che non è possibile per l'ipotesi sul $\mathbb{K}$-core di $\mathbb{K}(\beta)$. Tale contraddizione è nata dall'aver supposto inizialmente $-1 \in \Gamma_{\mathbb{K}}(\mathbb{K}(\alpha))$. Perciò il $\mathbb{K}$-core di $\mathbb{K}(\alpha)$ è un cono e $\mathbb{K}(\alpha)$ estende l'ordinamento di $\mathbb{K}$.

ii) Analogamente a quanto visto nel punto precedente supponiamo $\Gamma_{\mathbb{K}}(\mathbb{L})$ non sia un cono. Allora è possibile scrivere:

$$-1 = \sum_i \lambda_i (x_i + y_i\sqrt{a})^2 = \sum_i \lambda_i (x_i^2 + y_i^2 a) + \sqrt{a} \sum_i 2x_i y_i;$$

cioè, ponendo $x = \sum_i \lambda_i (x_i^2 + y_i^2 a) \in \mathbb{K}$ e $y = \sum_i 2x_i y_i \in \mathbb{K}$, si ha $-1 = x + \sqrt{a}y$. Dal momento che -1 e $\sqrt{a}$ costituiscono una base per $\mathbb{K}(\sqrt{\alpha})$ come spazio vettoriale su $\mathbb{K}$, necessariamente si ha $y = 0$. Per cui otteniamo il seguente risultato:

$$-1 \;=\; \sum_i \lambda_i (x_i^2 + y_i^2 a) \;=\; \sum_i \lambda_i x_i^2 \;+\; a \sum_i \lambda_i y_i^2 \;>\; 0;$$

giungendo in questo modo a una contraddizione. Dunque $\Gamma_{\mathbb{K}}(\mathbb{L})$ è un cono e la tesi segue dal Teorema 2.2.7. □

Nota bene:. Se il grado dell'estensione $[\mathbb{L} : \mathbb{K}]$ è pari o infinito non è detto sia possibile estendere l'ordinamento di $\mathbb{K}$ a $\mathbb{L}$.

3.2 Campi euclidei

Introduciamo ora il concetto di campo euclideo, illustrandone successivamente alcune proprietà fondamentali.

Definizione 3.2.1. Diciamo che un campo $\mathbb{K}$ è *euclideo* se è ordinato e se ogni suo elemento positivo è un quadrato.

Nella definizione appena data, la proprietà di campo euclideo a prima vista sembra dipendere dall'ordine '$<$' definito su $\mathbb{K}$. Tuttavia vediamo subito come tale ordinamento sia l'unico possibile:

Proposizione 3.2.2. *Un campo euclideo ammette un unico ordinamento.*

Dimostrazione. Sia $(\mathbb{K}, <)$ euclideo e sia $\ll$ un altro ordinamento su $\mathbb{K}$. Siano poi P, Q i positive order set rispettivamente di $(\mathbb{K}, <)$,$(\mathbb{K}, \ll)$; poiché abbiamo visto in precedenza che ogni ordine è caratterizzato dal suo positive set, se facciamo vedere che $P = Q$ abbiamo mostrato che i due ordinamenti sono il medesimo. Chiaramente $P \subseteq Q$ essendo i quadrati di elementi non nulli sempre positivi per ogni ordinamento. Sia perciò $a \in Q$ e supponiamo $a \notin P$; per la proprietà (1.2) ciò implica $-a \in P$, per cui per l'ipotesi di campo euclideo esiste $x \in \mathbb{K}$ tale che $-a = x^2 \gg 0$, il che però non è possibile dal momento che $-a \ll 0$, dato che $a \in Q$. Dunque $a \in P$, mostrando in questo modo $Q \subseteq P$ e così anche l'uguaglianza desiderata. □

Nota bene:. Non è detto che se un campo $\mathbb{K}$ ammette un unico ordinamento '$<$', allora $(\mathbb{K}, <)$ sia euclideo.

Esempio 3. Il campo $\mathbb{Q}$ dei razionali, come già visto nel Corollario 1.3.4, possiede un unico ordinamento ma non è euclideo, dal momento che $2 > 0$ ma $\sqrt{2} \notin \mathbb{Q}$.

Proposizione 3.2.3. *Sia $\mathbb{K}$ un campo euclideo. Allora $i \notin \mathbb{K}$ e ogni elemento di $\mathbb{K}(i)$ può essere scritto come quadrato in $\mathbb{K}(i)$.*

Dimostrazione. Un campo euclideo $\mathbb{K}$ è ordinato e quindi è formalmente reale per il Teorema 2.2.10, per cui $-1 \in C(\mathbb{K})$; ma se i appartenesse a $\mathbb{K}$ il suo quadrato dovrebbe stare in $C(\mathbb{K})$, quindi $i \in \mathbb{K}$.
Sia $\alpha = a + ib \in \mathbb{K}(i)$ con $a, b \in \mathbb{K}$; vogliamo mostrare l'esistenza di $x, y \in \mathbb{K}$ tali che $\alpha = (x + iy)^2$. Chiaramente se $\alpha = 0$ è sufficiente prendere $x, y = 0$; possiamo così supporre almeno uno tra a, b non nullo. In tal caso, osserviamo che $0 < a^2 + b^2 \in \mathbb{K}$ quindi, siccome $\mathbb{K}$ è euclideo, esiste $c \in \mathbb{K}^*$ tale che $c^2 = a^2 + b^2$ e per le proprietà del valore assoluto viste nella sezione 1.4 si ha:

$$b^2 = c^2 - a^2 = |c|^2 - a^2 = (|c| + a)(|c| - a) \ , \ |c| > 0. \tag{3.2}$$

Analizziamo i vari casi possibili al variare di a. Se $a \geq 0$ abbiamo $\frac{|c|+a}{2} \geq \frac{|c|}{2} > 0$, perciò esiste $x \in \mathbb{K}^*$ tale che $x^2 = \frac{|c|+a}{2}$ visto che $\mathbb{K}$ è euclideo per ipotesi. Per cui ponendo $y = \frac{b}{2x}$, se riscriviamo b^2 come in (3.2) otteniamo:

$$(x + iy)^2 = x^2 + i^2y^2 + 2ixy = \frac{(|c| + a)}{2} - \frac{(|c| - a)}{2} + 2ix\frac{b}{2x} = a + ib = \alpha.$$

Se invece $a < 0$ allora $-a > 0$, per cui in questo caso si ha $\frac{|c|-a}{2} > \frac{|c|}{2} > 0$. Sempre perché $\mathbb{K}$ è euclideo esiste $x \in \mathbb{K}^*$ tale che $x^2 = \frac{|c|-a}{2}$. Perciò ponendo di nuovo $y = \frac{b}{2x}$ e riscrivendo b^2 come in (3.2) si ottiene:

$$(x + iy)^2 = x^2 + i^2y^2 + 2ixy = \frac{(|c| - a)}{2} - \frac{(|c| + a)}{2} + 2ix\frac{b}{2x} = a + ib = \alpha.$$

In conclusione tali x, y esistono sempre e α è un quadrato in $\mathbb{K}(i)$. □

Corollario 3.2.4. *Se $\mathbb{K}$ è un campo euclideo, allora $\mathbb{K}(i)$ non ammette estensioni quadratiche.*

Dimostrazione. Si consideri un'estensione $\mathbb{K}(i) \subseteq \mathbb{L}$ finita di grado 2; grazie al Teorema 3.1.4 esiste $\alpha \in \mathbb{L}$ tale che $\mathbb{L} = \mathbb{K}(i)(\alpha)$ e il polinomio minimo $f \in \mathbb{K}(i)[x]$ di α ha grado 2. Perciò esistono $p, q \in \mathbb{K}(i)$ tali che $f(x) = x^2 + px + q$ e inoltre $p^2 - 4q \in \mathbb{K}(i)$: per la Proposizione 3.2.3 allora esiste $\beta \in \mathbb{K}(i)$ tale che $\beta^2 = p^2 - 4q$ e le radici di f sono rispettivamente $\frac{-p+\beta}{2}, \frac{-p-\beta}{2} \in \mathbb{K}(i)$. Dunque, essendo α una radice di f, ne consegue che $\alpha \in \mathbb{K}(i)$ e perciò $\mathbb{L} = \mathbb{K}(i)(\alpha) = \mathbb{K}(i)$. □

3.3 Il Teorema di Artin-Schreier

Nella dimostrazione del Teorema 3.3.1 si utilizza la teoria di Galois, per la quale rimandiamo il lettore per esempio a [4]. Utilizzeremo inoltre le notazioni seguenti, in accordo con [4]:

Notazione: Se $\mathbb{K} \subseteq \mathbb{L}$ è un'estensione di campi, il suo gruppo di Galois è denotato con $Gal(\mathbb{L}|\mathbb{K})$; se G è un sottogruppo di $Gal(\mathbb{L}|\mathbb{K})$, si definisce il campo fisso di G come $\mathbb{L}_G = \{x \in \mathbb{L} \mid \phi(x) = x \text{ per ogni } \phi \in G\}$.

Per i teoremi di Sylow si veda ad esempio [5], Sezione 1.13.

Enunciamo adesso il Teorema di Artin-Schreier.

Teorema 3.3.1. *Sia $\mathbb{K}$ un campo. Allora le seguenti condizioni sono tra loro equivalenti:*

a) $\mathbb{K}$ *è realmente chiuso;*

b) $\mathbb{K}$ *è euclideo e ogni* $f \in \mathbb{K}[x]$ *di grado dispari ammete una radice in* $\mathbb{K}$*;*

c) $\mathbb{K}$ *non è algebricamente chiuso mentre* $\mathbb{K}(i)$ *è algebricamente chiuso.*

Dimostrazione. $a) \Rightarrow b)$ Se un campo è realmente chiuso per definizione è formalmente reale e quindi è ordinabile, per il Teorema 2.2.10. Mostriamo per prima cosa che $\mathbb{K}$ è euclideo. Sia $a \in \mathbb{K}$ con $a > 0$ e supponiamo $\sqrt{a} \notin \mathbb{K}$; allora per il Lemma 3.1.5 l'estensione algebrica $\mathbb{K} \subseteq \mathbb{K}(\sqrt{a})$ estende anche l'ordine di $\mathbb{K}$, e $\mathbb{K}(\sqrt{a})$ è ancora formalmente reale, ma ciò va contro l'ipotesi che $\mathbb{K}$ sia realmente chiuso. Di conseguenza, l'unica possibilità è che $\sqrt{a} \in \mathbb{K}$.
Sia adesso $f \in \mathbb{K}[x]$ un polinomio irriducibile con $deg(f) = n$ dispari, sia α una sua radice in un qualche campo di spezzamento di f avente polinomio minimo $p \in \mathbb{K}[x]$. Essendo f irriducibile tale polinomio è associato a p, per cui si ha $deg(p) = deg(f) = n$ e l'estensione algebrica $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ ha grado $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ dispari. Per tale motivo l'ordine di $\mathbb{K}$ può essere esteso a $\mathbb{K}(\alpha)$ grazie al Lemma 3.1.5, e $\mathbb{K}(\alpha)$ è ancora formalmente reale; essendo $\mathbb{K}$ realmente chiuso questo è possibile solamente se $\mathbb{K} = \mathbb{K}(\alpha)$, cioè se $[\mathbb{K}(\alpha) : \mathbb{K}] = n = 1$. Ne si deduce così che f, e con lui tutti i polinomi irriducibili di grado dispari, è un polinomio di primo grado; dunque ogni polinomio $g \in \mathbb{K}[x]$ di grado dispari ammette una radice nel campo dal momento che almeno una sua componente

irriducibile è di grado dispari.

$b) \Rightarrow c)$ In virtù dell'ipotesi $\mathbb{K}$ euclideo segue che $\mathbb{K}$ è ordinato e quindi $\mathbb{K}$ formalmente reale: per questo motivo -1 non può essere scritto come quadrato in $\mathbb{K}$ con la conseguenza che $i \notin \mathbb{K}$ e $\mathbb{K} \subset \mathbb{K}(i)$. Perciò $\mathbb{K}$ non è algebricamente chiuso e il polinomio x^2+1 è irriducibile su $\mathbb{K}$ (è il polinomio minimo di i).

Vogliamo ora far vedere che $\mathbb{K}(i)$ non ammette estensioni algebriche proprie. A tal fine, sia α algebrico su $\mathbb{K}(i)$ e proviamo che $\alpha \in \mathbb{K}(i)$. Sia p_α il polinomio minimo di α su $\mathbb{K}$ e sia $\mathbb{L}$ un campo di spezzamento del polinomio $p_\alpha(x)(x^2+1) \in \mathbb{K}[x]$; l'estensione $\mathbb{K} \subseteq \mathbb{L}$ è di Galois perché $char(\mathbb{K}) = 0$, inoltre abbiamo:

$$\mathbb{K} \subset \mathbb{K}(i) \subseteq \mathbb{L}.$$

Quindi, per il Teorema della torre:

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(i)] \cdot [\mathbb{K}(i) : \mathbb{K}] = 2[\mathbb{L} : \mathbb{K}(i)]. \tag{3.3}$$

Sia $G = Gal(\mathbb{L}|\mathbb{K})$; poiché per (3.3) abbiamo che 2 divide $[\mathbb{L} : \mathbb{K}] = |G|$, allora $|G| = 2^r \cdot m$ con m dispari. Sia poi S un Sylow 2-sottogruppo di G e sia $\mathbb{L}_S$ il suo campo fisso. Allora considerando la torre di campi

$$\mathbb{K} \subseteq \mathbb{L}_S \subseteq \mathbb{L},$$

per il Teorema Fondamentale della Teoria di Galois si ha $Gal(\mathbb{L}|\mathbb{L}_S) = S$, $|S| = [\mathbb{L} : \mathbb{L}_S]$ e $[\mathbb{L}_S : \mathbb{K}] = (G : S) = m$. Di conseguenza ogni $\beta \in \mathbb{L}_S$ ha grado dispari su $\mathbb{K}$; se p_β poi è il polinomio minimo di β su $\mathbb{K}$, dato che p_β è di grado dispari, per ipotesi ha una radice in $\mathbb{K}$ ed essendo p_β irriducibile questo significa $deg(p_\beta) = 1$, quindi $\beta \in \mathbb{K}$. Allora $\mathbb{L}_S = \mathbb{K}$, per cui $S = G$ e $|G| = 2^r$. Se $r = 1$, cioè se $[\mathbb{L} : \mathbb{K}] = |G| = 2$, abbiamo $\mathbb{L} = \mathbb{K}(i)$ e $\alpha \in \mathbb{K}(i)$. Mostriamo come non possa essere $r \geq 2$. Supponiamo $r \geq 2$; per (3.3) abbiamo $2^r = [\mathbb{L} : \mathbb{K}] = 2[\mathbb{L} : \mathbb{K}(i)]$, da cui $[\mathbb{L} : \mathbb{K}(i)] = 2^{r-1}$. Perciò $Gal(\mathbb{L}|\mathbb{K}(i))$, avendo ordine 2^{r-1} con $r - 1 \geq 1$, possiede un sottogruppo T di ordine 2^{r-2} e indice 2, quindi, considerando la torre di campi

$$\mathbb{K}(i) \subseteq \mathbb{L}_T \subseteq \mathbb{L},$$

per il Teorema Fondamentale della Teoria di Galois si ha $2 = (Gal(\mathbb{L}|\mathbb{K}(i)) : Gal(\mathbb{L}|\mathbb{L}_T)) = = [\mathbb{L}_T : \mathbb{K}(i)]$. Abbiamo così trovato una estensione quadratica $\mathbb{L}_T$ di $\mathbb{K}(i)$, arrivando così a una contraddizione visto che per il Corollario 3.2.4 $\mathbb{K}(i)$ non ammette estensioni quadratiche.

$c) \Rightarrow a)$ Essendo $\mathbb{K}(i)$ algebricamente chiuso per ipotesi e $[\mathbb{K}(i) : \mathbb{K}] = 2$, l'unica estensione algebrica ammessa da $\mathbb{K}$ è $\mathbb{K} \subseteq \mathbb{K}(i)$. Dato che $-1 = i^2 \in C(\mathbb{K}(i))$ tale campo non è formalmente reale e quindi non è ordinabile per il Teorema 2.2.10, perciò per ottenere la tesi è sufficiente mostrare che $\mathbb{K}$ invece è formalmente reale. Mostriamo innanzitutto che per ogni $a, b \in \mathbb{K}$ si ha che $a^2 + b^2$ è un quadrato. Siccome $\mathbb{K}(i)$ è algebricamente chiuso, le radici del polinomio $f(x) = x^2 - (a + ib) \in \mathbb{K}(i)[x]$ appartengono a $\mathbb{K}(i)$, perciò esiste $c + id \in \mathbb{K}(i)$ con $c, d \in \mathbb{K}$ tale che:

$$a + ib = (c + id)^2 = c^2 - d^2 + 2cdi.$$

Quindi $a = c^2 - d^2, b = 2cd$ da cui:

$$a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2 = c^4 + 2c^2d^2 + d^4 = (c^2 + d^2)^2.$$

Supponiamo ora sia possibile scrivere $-1 = a_1^2 + \ldots + a_n^2$ con $a_i \in \mathbb{K}$ per $i = 1, \ldots, n$: per quanto appena dimostrato, sommando di volta in volta gli addenti a coppie, esiste $y \in \mathbb{K}$ tale che $-1 = a_1^2 + \cdots + a_n^2 = y^2$ e quindi $i = y \in \mathbb{K}$ oppure $i = -y \in \mathbb{K}$. Tuttavia questo non può succedere poiché dalle ipotesi iniziali abbiamo che $i \notin \mathbb{K}$; dunque $-1 \notin C(\mathbb{K})$ e $\mathbb{K}$ è formalmente reale. □

Abbiamo visto nell'Osservazione 3.2.2 che ogni campo euclideo è ordinabile solamente in un modo; se ne può dedurre quindi il seguente corollario:

Corollario 3.3.2. *Ogni campo realmente chiuso ammette un unico ordinamento, e in tale ordinamento ogni elemento positivo possiede una radice.*

Proposizione 3.3.3. *Sia $\mathbb{K}$ un campo ordinato. Allora $\mathbb{K}$ è realmente chiuso se e solo se $\mathbb{K}$ ha la proprietà seguente* (proprietà del valore intermedio per i polinomi):

dati un polinomio $f \in \mathbb{K}[x]$ e $\alpha, \beta \in \mathbb{K}$ con $\alpha < \beta$, se $f(\alpha)f(\beta) < 0$ allora esiste $\gamma \in \mathbb{K}$ tale che $\alpha < \gamma < \beta$ e $f(\gamma) = 0$.

Dimostrazione. Supponiamo $\mathbb{K}$ realmente chiuso e siano $f \in \mathbb{K}[x]$ monico e $\alpha, \beta \in \mathbb{K}$, $\alpha < \beta$,$f(\alpha)f(\beta) < 0$. Dato che, per il Teorema 3.3.1 c) abbiamo $[\overline{\mathbb{K}} : \mathbb{K}] = [\mathbb{K}(i) : \mathbb{K}] = 2$, è possibile scrivere f come prodotto di fattori monici irriducibili di primo e secondo grado. Osserviamo che tutti i fattori di secondo grado possono assumere solo valori positivi per ogni $x \in \mathbb{K}$. Infatti ognuno di essi può essere riscritto come:

$$x^2 + px + q = (x + \frac{p}{2})^2 + (q - \frac{p^2}{4}).$$

Visto che per il Teorema 3.3.1 b) si ha $\mathbb{K}$ euclideo, notiamo che $q-\frac{p^2}{4}$ non può essere nullo o negativo, altrimenti per quanto appena detto esisterebbe $z \in \mathbb{K}$ tale che $z^2 = -(q-\frac{p^2}{4})$ e il polinomio avrebbe due radici ($-\frac{p}{2}+z$ e $-\frac{p}{2}-z$) andando contro l'ipotesi che tale fattore sia irriducibile. Quindi al variare di $x \in \mathbb{K}$, $f(x)$ cambia segno solamente se uno dei suoi fattori lineari lo cambia, e questo avviene solo in corrispondenza della radice del polinomio lineare, che è una radice di f. Perciò una radice di f deve essere compresa tra α e β.

Mostriamo ora la condizione opposta, partendo col verificare che $\mathbb{K}$ è euclideo. Sia $a > 0$ e sia $f(x) = x^2 - a \in \mathbb{K}[x]$; posti $\alpha = 0, \beta = 1 + a$ osserviamo che:

$$f(\alpha)f(\beta) = (-a)((a+1)^2 - a) = -a^3 - a^2 - a < 0,$$

perciò per la proprietà del valore intermedio per i polinomi esiste $\gamma \in \mathbb{R}$ tale che $f(\gamma) = 0$. Ma ciò equivale a dire $\gamma^2 - a = 0$, ossia $\gamma^2 = a$, quindi a è un quadrato.

Sia ora $g(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ un polinomio di grado n dispari. Prendendo $\alpha > 0$ in $\mathbb{K}$ abbastanza grande il segno di $f(\alpha)$ è lo stesso di a_n, mentre se si prende $\beta < 0$ abbastanza piccolo $f(\beta)$ avrà segno opposto: quindi $f(\alpha)f(\beta) < 0$ e per la proprietà del valore intermedio per i polinomi esiste $\gamma \in \mathbb{K}$ radice di g. Dunque per il Teorema 3.3.1 $\mathbb{K}$ è un campo realmente chiuso. □

Capitolo 4

Il completamento di un campo ordinato

4.1 Successioni in un campo ordinato

D'ora in avanti $\mathbb{K}$ denoterà sempre un campo ordinato e '$<$' il suo ordine.
Nel seguito diamo alcune definizioni e proprietà relative alle successioni in $\mathbb{K}$, che ricalcano le analoghe proprietà in $\mathbb{R}$ e che possono venire dimostrate in modo analogo.

Una *successione* $\{x_n\}$ in $\mathbb{K}$ è una funzione $f : \mathbb{N} \to \mathbb{K}$ dove $f(n) = x_n$. Dato $x \in \mathbb{K}$, con $\underline{x}$ si denota la *successione costante* dove $f(n) = x$ per ogni $n \in \mathbb{N}$. L'insieme delle successioni in $\mathbb{K}$ si denota con $\mathbb{K}^{\mathbb{N}}$.
L'insieme $\mathbb{K}^{\mathbb{N}}$ dotato delle operazioni binarie così definite:

$$\{x_n\} + \{y_n\} := \{x_n + y_n\} \qquad \{x_n\} \cdot \{y_n\} := \{x_n \cdot y_n\} \qquad c\,\{x_n\} := \underline{c}\,\{x_n\} = \{cx_n\}$$

per ogni $\{x_n\}, \{y_n\} \in \mathbb{K}^{\mathbb{N}}$ e per ogni $c \in \mathbb{K}$, ha la struttura di anello commutativo e di $\mathbb{K}$-spazio vettoriale.

Definizione 4.1.1. Una successione $\{a_n\}$ in $\mathbb{K}$ è detta *convergente* se esiste un $a \in \mathbb{K}$ tale che:

$$\forall \epsilon \in \mathbb{K}, \epsilon > 0 \text{ esiste } \overline{n} \in \mathbb{N} \text{ tale che } |a_n - a| < \epsilon \ \forall n \geq \overline{n}. \tag{4.1}$$

Diremo che "*la successione* $\{a_n\}$ *converge ad* a per n che tende a $+\infty$", e scriveremo "$a_n \to a$" o "$\lim_{n \to +\infty} a_n = a$". Denotiamo $\mathcal{R}$ l'insieme delle successioni convergenti di $\mathbb{K}$.
Una successione $\{a_n\}$ in $\mathbb{K}$ è detta *infinitesima* se converge a 0. Denotiamo con $\mathcal{I}$ l'insieme delle successioni infinitesime di $\mathbb{K}$.

Una successione $\{a_n\}$ in $\mathbb{K}$ è detta *di Cauchy* se soddisfa:

$$\forall \epsilon \in \mathbb{K}, \epsilon > 0 \text{ esiste } \overline{n} \in \mathbb{N} \text{ tale che } |a_m - a_n| < \epsilon \ \forall m, n \geq \overline{n}. \tag{4.2}$$

Denotiamo con $\mathcal{C}$ l'insieme delle successioni di Cauchy di $\mathbb{K}$.

Osservazione 4.1.2. Se in una successione convergente, rispettivamente infinitesima, rispettivamente di Cauchy vengono modificati un numero finito di termini, la sua continua ad essere convergente, rispettivamente infinitesima, rispettivamente di Cauchy.

Proposizione 4.1.3. *Sia $\mathbb{K}$ un campo ordinato. Allora valgono le seguenti proprietà:*

i) Il limite di una successione convergente è unico;

ii) Ogni successione costante $\underline{c}$ in $\mathbb{K}$ converge a c;

iii) L'insieme $\mathcal{R}$ è un sottoanello di $\mathbb{K}^{\mathbb{N}}$. In particolare se $\{a_n\}, \{b_n\} \in \mathcal{R}$ con $a_n \to a$, $b_n \to b$ allora $\{a_n\} + \{b_n\}$,$\{a_n\} \cdot \{b_n\}$ convergono rispettivamente ad $a + b, a \cdot b$;

iv) Se $\{a_n\} \in \mathcal{R}$ con $a_n \to a$ ed esiste $N \in \mathbb{N}$ tale che $a_n > 0$, rispettivamente $a_n < 0$, per ogni $n \geq N$ allora $a \geq 0$, rispettivamente $a \leq 0$;

v) Se $\{a_n\} \in \mathbb{K}^{\mathbb{N}}$, $\{b_n\} \in \mathcal{I}$ sono tali che $0 \leq a_n \leq b_n \ \forall n \in \mathbb{N}$ allora $\{a_n\} \in \mathcal{I}$;

vi) L'insieme $\mathcal{I}$ è un ideale di $\mathbb{K}^{\mathbb{N}}$;

vii) L'insieme $\mathcal{C}$ è un sottoanello di $\mathbb{K}^N$.

Proposizione 4.1.4. *Sia $\{a_n\}$ una successione di Cauchy non infinitesima in $\mathbb{K}$. Allora esistono $\epsilon \in \mathbb{K}, \epsilon > 0$ ed $N \in \mathbb{N}$ tali che $|a_n| \geq \epsilon$ per ogni $n \geq N$ con $n \in \mathbb{N}$.*

Corollario 4.1.5. *Sia $\{a_n\}$ una successione di Cauchy non infinitesima in $\mathbb{K}$ tale che $a_n \neq 0$ per ogni $n \in \mathbb{N}$. Allora la successione $\left\{\frac{1}{a_n}\right\}$ è ancora di Cauchy.*

Corollario 4.1.6. *Per ogni $\{x_n\} \in \mathcal{C}$ vale una e una sola delle seguenti:*

i) *Esistono $\epsilon \in \mathbb{K}, \epsilon > 0$ ed $N \in \mathbb{N}$ tali che $x_n > \epsilon$ per ogni $n \geq N$;*

ii) *Esistono $\epsilon \in \mathbb{K}, \epsilon > 0$ ed $N \in \mathbb{N}$ tali che $x_n < -\epsilon$ per ogni $n \geq N$;*

iii) *La successione $\{x_n\}$ è infinitesima.*

Osservazione 4.1.7. Ogni successione convergente è una successione di Cauchy. Quindi si ha la seguente catena di inclusioni:

$$\mathcal{I} \subseteq \mathcal{R} \subseteq \mathcal{C} \subseteq \mathbb{K}^{\mathbb{N}}.$$

È importante osservare come il viceversa non sia sempre vero: ad esempio la successione in $\mathbb{Q}$ di numeri razionali $1,\ 1.4,\ 1.41,\ 1.414, \ldots$ che approssima in maniera sempre più precisa $\sqrt{2}$ è una successione di Cauchy, tuttavia questa non converge in $\mathbb{Q}$. Per tale motivo introduciamo la nozione di campo completo.

Definizione 4.1.8. Un campo ordinato $\mathbb{K}$ si dice *completo* se ogni sua successione $\{a_n\}$ di Cauchy è una successione convergente, ossia se soddisfa (4.1).

Esempio 4. Il campo dei numeri razionali $\mathbb{Q}$ non è un campo completo.

Nonostante non tutti i campi ordinati siano completi, è possibile ovviare a questo problema: infatti vedremo come ogni campo ordinato $\mathbb{K}$ non completo possa essere esteso a un campo ordinato completo $\hat{\mathbb{K}} \supset \mathbb{K}$ che estende l'ordine di $\mathbb{K}$.

A tal fine introduciamo due nozioni necessarie a definire quello che chiameremo completamento di un campo.

Definizione 4.1.9. Sia $\mathbb{K}$ un campo ordinato e sia $\mathbb{F} \subseteq \mathbb{K}$ un suo sottocampo. Diremo che $\mathbb{F}$ è *denso in* $\mathbb{K}$ se è soddisfatta la seguente condizione:

$$\text{per ogni } a, b \in \mathbb{K},\ a < b \text{ esiste } c \in \mathbb{F} \text{ tale che } a < c < b. \tag{4.3}$$

Sia $f : \mathbb{F} \to \mathbb{K}$ un omomorfismo d'ordine tra due campi ordinati. Diremo che f è una *immersione densa* di $\mathbb{F}$ in $\mathbb{K}$ se la sua immagine $f(\mathbb{F})$ è densa in $\mathbb{K}$.

4.2 Il Teorema del completamento

Definizione 4.2.1. Siano $\mathbb{K}, \hat{\mathbb{K}}$ due campi ordinati. Diremo che $\hat{\mathbb{K}}$ è un *completamento* di $\mathbb{K}$ se soddisfa le seguenti condizioni:

i) $\hat{\mathbb{K}}$ è completo; *ii*) Esiste un'immersione densa $\lambda : \mathbb{K} \to \hat{\mathbb{K}}$ di $\mathbb{K}$ in $\hat{\mathbb{K}}$.

In tal caso possiamo identificare $\mathbb{K}$ con la sua immagine $\lambda(\mathbb{K})$ in $\hat{\mathbb{K}}$; l'estensione di campi $\mathbb{K} \subseteq \hat{\mathbb{K}}$ estende perciò l'ordine di $\mathbb{K}$.

Osserviamo che se $\mathbb{K}$ è completo allora $\hat{\mathbb{K}} = \mathbb{K}$ è un suo completamento, scegliendo come immersione densa l'identità.

La dimostrazione del teorema sull'esistenza del completamento di un campo ordinato, proprio per la sua universalità, è particolarmente lunga: per tale motivo una buona parte è presentata di seguito sotto forma di lemmi che verranno richiamati durante la dimostrazione del teorema.

Lemma 4.2.2. *Sia $\mathbb{K}$ campo ordinato e sia $\mathcal{I} \subseteq \mathbb{K}^{\mathbb{N}}$ l'insieme delle successioni infinitesime in $\mathbb{K}$. Allora $\mathcal{I}$ è un ideale di $\mathcal{C}$, e $\hat{\mathbb{K}} := \mathcal{C}/\mathcal{I}$ è un campo i cui elementi sono le classi di equivalenza $[\{x_n\}]$ definite dalla seguente relazione d'equivalenza:*

$$\forall \{a_n\}, \{b_n\} \in \mathcal{C} \text{ si ha } \{a_n\} \sim \{b_n\} \Leftrightarrow \{a_n - b_n\} \in \mathcal{I} \text{ ossia } a_n - b_n \to 0.$$

La classe di una successione costante di conseguenza è denotata $[\underline{x}]$; 0 denota $[\underline{0}]$

Dimostrazione. Una successione infinitesima è di Cauchy, per cui $\mathcal{I} \subseteq \mathcal{C}$ e $\mathcal{C}$ è un sottoanello di $\mathbb{K}^{\mathbb{N}}$; allora $\mathcal{I}$ è un ideale di $\mathcal{C}$ per la Proposizione 4.1.3 e $\hat{\mathbb{K}}$ è ben definito come anello quoziente.
Dal momento che $\hat{\mathbb{K}}$ è commutativo (in quanto quoziente di un anello commutativo), resta solo da dimostrare che ogni suo elemento diverso da 0 è invertibile. Sia perciò $\{a_n\} \in \mathcal{C}$ non infinitesima: dalla Proposizione 4.1.4 sappiamo esiste un qualche $N \in \mathbb{K}$ tale che ogni termine a_n con $n \geq N$ è non nullo, per cui la successione $\{b_n\}$ il cui termine n-esimo è definito da

$$b_n := \begin{cases} 1 & \text{se } n < N, \\ a_n & \text{se } n \geq N, \end{cases}$$

è ancora di Cauchy grazie all'Osservazione 4.1.2 ed è a termini non nulli. Ma allora, per mezzo della Proposizione 4.1.5 anche $\left\{\frac{1}{b_n}\right\} \in \mathcal{C}$ e per costruzione $a_n \cdot \frac{1}{b_n} \to 1$. Perciò $[\{a_n\}] \cdot \left[\left\{\frac{1}{b_n}\right\}\right] = \left[\{a_n\} \cdot \left\{\frac{1}{b_n}\right\}\right] = [\underline{1}]$, da cui si deduce $[\{a_n\}]^{-1} = \left[\left\{\frac{1}{b_n}\right\}\right]$. □

Lemma 4.2.3. *Sia $\hat{\mathbb{K}}$ come nel Lemma 4.2.2. Allora $\hat{\mathbb{K}}$ è un campo ordinato definendo il positive order set nel modo seguente: se $\alpha \in \hat{\mathbb{K}}$ con $\alpha = [\{x_n\}]$, $\{x_n\} \in \mathcal{C}$*

$$\alpha > 0 \text{ in } \hat{\mathbb{K}} \Leftrightarrow \text{esistono } \epsilon \in \mathbb{K}, \epsilon > 0 \text{ ed } N \in \mathbb{N} \text{ tali che } x_n > \epsilon \ \forall n \geq N. \tag{4.4}$$

Dimostrazione. Per prima cosa è necessario verificare che la definizione (4.4) sia ben posta; sia perciò $\{x_n\} \in \mathcal{C}$ con $[\{x_n\}] > 0$ in $\hat{\mathbb{K}}$ e sia $\{y_n\} \in [\{x_n\}]$. Per ipotesi sappiamo esistono $\epsilon > 0$ in $\mathbb{K}$ ed $N_1 \in \mathbb{N}$ tali che $x_n > \epsilon$ per ogni $n \geq N_1$ perciò, dal momento che $\{x_n\} \sim \{y_n\}$ ossia $x_n - y_n \to 0$, dato $\frac{\epsilon}{2} > 0$ esiste $N_2 \in \mathbb{N}$ tale che $|x_n - y_n| < \frac{\epsilon}{2}$ per ogni $n \geq N_2$. Allora si ha:

$$\epsilon < x_n = x_n - y_n + y_n \leq |x_n - y_n| + y_n < \tfrac{\epsilon}{2} + y_n \quad \text{per ogni } n \geq \max(N_1, N_2);$$

per cui sottraendo $\frac{\epsilon}{2}$ da entrambi i lati si ottiene $0 < \frac{\epsilon}{2} \leq y_n$ per ogni $n \geq \max(N_1, N_2)$. Quindi $[\{y_n\}] > 0$ in $\hat{\mathbb{K}}$, mostrando così che (4.4) rispetta le classi di equivalenza.
Posto

$$P := \Big\{\ [\{x_n\}] \in \hat{\mathbb{K}} \mid\ [\{x_n\}] > 0 \Big\}$$

per mostrare che la relazione (4.4) dà a $(\hat{\mathbb{K}}, <)$ la struttura di campo ordinato è sufficiente verificare grazie alla Proposizione 1.2.7 che P soddisfi (1.1) e (1.2). La condizione (1.2) è una conseguenza diretta del corollario 4.1.6. Verifichiamo la condizione (1.1); siano $[\{a_n\}], [\{b_n\}] \in P$ e mostriamo che la somma e il prodotto di tali classi è ancora contenuto in P. Per come sono definiti gli elementi di P, esistono $\epsilon_1, \epsilon_2 > 0$ in $\mathbb{K}$ ed esistono $N_1, N_2 \in \mathbb{N}$ tali che $a_n > \epsilon_1$ per ogni $n \geq N_1$, $b_m > \epsilon_2$ per ogni $m \geq N_2$. Perciò per $n \geq \max(N_1, N_2)$ si ha:

$$0 < \epsilon_1 + \epsilon_2 < a_n + b_n \quad , \quad 0 < \epsilon_1 \cdot \epsilon_2 < a_n \cdot b_n.$$

Dunque $[\{a_n\}] + [\{b_n\}]$,$[\{a_n\}] \cdot [\{b_n\}] \in P$. □

Lemma 4.2.4. *Sia $\hat{\mathbb{K}}$ campo ordinato come nei lemmi* 4.2.2, 4.2.3 *e sia $\alpha \in \hat{\mathbb{K}}$ con $\alpha = [\{a_n\}]$. Allora la successione $\left\{\left[\underline{a_n}\right]\right\}$ di $\hat{\mathbb{K}}$ converge ad α.*

Dimostrazione. Vogliamo dimostrare che per ogni $\epsilon = [\{\epsilon_m\}] > 0$ in $\hat{\mathbb{K}}$ esiste un $\overline{n} \in \mathbb{N}$ tale che per ogni $n \geq \overline{n}$ si abbia $\left|[\underline{a_n}] - \alpha\right| < \epsilon$ cioè $\epsilon - \left|[\underline{a_n}] - \alpha\right| > 0$. Per tale motivo vogliamo provare che esistono $\eta > 0$ in $\mathbb{K}$ ed $N \in \mathbb{N}$ tali che:

$$\epsilon_m - |a_m - a_n| > \eta \text{ in } \mathbb{K} \quad \forall m \geq N, \forall n \geq \overline{n}$$

Per ipotesi $\epsilon > 0$ perciò esistono $u > 0$ in $\mathbb{K}$ ed $n_1 \in \mathbb{N}$ tali che $\epsilon_m > u$ per ogni $m \geq n_1$. Per ipotesi $\{a_n\}$ è di Cauchy, perciò esiste $n_2 \in \mathbb{N}$ tale che $|a_m - a_n| < \frac{u}{2}$ per ogni $m, n \geq n_2$. Ne segue dunque che $\epsilon_m - |a_m - a_n| > \frac{u}{2}$ per ogni $m, n \geq \max(n_1, n_2)$. □

Lemma 4.2.5. *Sia $f : \mathbb{K} \to \mathbb{L}$ un'immersione densa e sia $\{x_n\}$ una successione di Cauchy in $\mathbb{K}$. Allora $\{f(x_n)\}$ è una successione di Cauchy in $\mathbb{L}$. Se $\{x_n\}$ è infinitesima, allora anche $\{f(x_n)\}$ lo è.*

Dimostrazione. Sia $\epsilon > 0$ in $\mathbb{L}$: siccome f è un'immersione densa esiste $\eta > 0$ in $\mathbb{K}$ tale che $0 < f(\eta) < \epsilon$. Sia $\{x_n\}$ di Cauchy; per tale η esiste $\overline{n} \in \mathbb{N}$ tale che $|x_m - x_n| < \eta$ per ogni $m, n \geq \overline{n}$; applicando f otteniamo così:

$$|f(x_m) - f(x_n)| = |f(x_m - x_n)| = f\left(|x_m - x_n|\right) < f(\eta) < \epsilon \text{ in } \mathbb{L} \quad \forall m, n \geq \overline{n},$$

ossia $\{f(x_n)\}$ è una successione di Cauchy in $\mathbb{L}$.
Nel caso di $\{x_n\}$ infinitesima, presi $\epsilon > 0$ in $\mathbb{L}$ ed $\eta > 0$ in $\mathbb{K}$ come prima, esiste $\overline{m} \in \mathbb{N}$ tale che $|x_n| < \eta$ per ogni $n \geq \overline{m}$; quindi applicando sempre f otteniamo $|f(x_n)| = f(|x_n|) < f(\eta) < \epsilon$ in $\mathbb{L}$ $\forall n \geq \overline{m}$, ossia $f(x_n) \to 0$. □

Possiamo adesso enunciare il risultato sull'esistenza del completamento.

Teorema 4.2.6. *Sia $\mathbb{K}$ un campo ordinato. Allora:*

a) Esiste un'immersione densa $\lambda : \mathbb{K} \to \hat{\mathbb{K}}$ dove $\hat{\mathbb{K}}$ è campo completo;

b) Se $f : \mathbb{K} \to \mathbb{L}$ è un'immersione densa di $\mathbb{K}$ in $\mathbb{L}$ campo completo, allora esiste un unico omomorfismo d'ordine $\hat{f} : \hat{\mathbb{K}} \to \mathbb{L}$ che fattorizzi f, ossia tale che $f = \hat{f} \circ \lambda$.

Dimostrazione. *a)* Sia $\hat{\mathbb{K}}$ il campo ordinato definito a partire da $\mathbb{K}$ nei lemmi 4.2.2 e 4.2.3 e sia λ l'applicazione

$$\begin{array}{rccc} \lambda & : & \mathbb{K} & \to & \hat{\mathbb{K}} \\ & & x & \mapsto & [\underline{x}] \end{array}$$

È immediato come λ sia un omomorfismo di campi. Se $x > 0$ in $\mathbb{K}$ presi $0 < \epsilon < x$ ed $N = 0$ la successione costante $\underline{x}$ ha tutti i suoi termini $> \epsilon$, per cui $\lambda(x) > 0$, cioè λ è un omomorfismo d'ordine. Ora bisogna solamente mostrare che $\lambda(\mathbb{K})$ è denso in $\hat{\mathbb{K}}$. Siano perciò $\alpha = [\{a_n\}], \beta = [\{b_n\}] \in \hat{\mathbb{K}}$ con $\alpha < \beta$. Per il Lemma 4.2.4 le successioni $\left\{\left[\underline{a_n}\right]\right\}$ e $\left\{\left[\underline{b_n}\right]\right\}$ convergono in $\hat{\mathbb{K}}$ rispettivamente ad α e a β. Allora per ogni $\epsilon > 0$ in $\hat{\mathbb{K}}$ esistono $n_1, n_2 \in \mathbb{N}$ tali che si abbia in $\hat{\mathbb{K}}$:

$$\begin{array}{l} \left|\left[\underline{a_n}\right] - \alpha\right| < \epsilon \quad \text{per ogni} \quad n \geq n_1, \\ \left|\left[\underline{b_n}\right] - \beta\right| < \epsilon \quad \text{per ogni} \quad n \geq n_2. \end{array} \tag{4.5}$$

Inoltre $\alpha < \beta$ significa che esistono $\eta > 0$ in $\mathbb{K}$ ed $n_3 \in \mathbb{N}$ tali che:

$$b_n - a_n > \eta \text{ per ogni } n \geq n_3.$$

Perciò scegliendo $\epsilon = \left[\underline{\frac{\eta}{3}}\right]$ le condizioni in (4.5) diventano:

$$\begin{aligned} \left|\left[\underline{a_n}\right] - \alpha\right| &< \left[\underline{\frac{\eta}{3}}\right] \quad \text{per ogni} \quad n \geq n_1, \\ \left|\left[\underline{b_n}\right] - \beta\right| &< \left[\underline{\frac{\eta}{3}}\right] \quad \text{per ogni} \quad n \geq n_2. \end{aligned}$$

Sia $\overline{n} = max(n_1, n_2, n_3)$. Quindi per ogni $n \geq \overline{n}$:

$$\begin{cases} b_n - a_n > \eta, \\ \left[\underline{\frac{\eta}{3}}\right] < \left[\underline{a_n}\right] - \alpha < \left[\underline{\frac{\eta}{3}}\right], \\ \left[\underline{\frac{\eta}{3}}\right] < \left[\underline{b_n}\right] - \beta < \left[\underline{\frac{\eta}{3}}\right]. \end{cases} \iff \begin{cases} b_n - a_n > \eta, \\ \alpha - \left[\underline{\frac{\eta}{3}}\right] < \left[\underline{a_n}\right] < \alpha + \left[\underline{\frac{\eta}{3}}\right], \\ \beta - \left[\underline{\frac{\eta}{3}}\right] < \left[\underline{b_n}\right] < \beta + \left[\underline{\frac{\eta}{3}}\right]. \end{cases}$$

Risulta allora:

$$\alpha < \left[\underline{a_{\overline{n}} + \frac{\eta}{3}}\right] < \left[\underline{a_{\overline{n}} + \frac{\eta}{2}}\right] = \left[\underline{a_{\overline{n}} + \eta - \frac{\eta}{2}}\right] < \left[\underline{b_{\overline{n}} - \frac{\eta}{2}}\right] < \left[\underline{a_{\overline{n}} + \frac{\eta}{3}}\right] < \beta,$$

cioè $\left[\underline{a_{\overline{n}} + \frac{\eta}{2}}\right] = \lambda(a_{\overline{n}} + \frac{\eta}{2})$ è compreso tra α e β.

Non resta che dimostrare la completezza di $\hat{\mathbb{K}}$. Sia quindi $\{\alpha_n\}$ una successione di Cauchy in $\hat{\mathbb{K}}$; se assume solo un numero finito di valori distinti $\{\beta_1, \ldots, \beta_k\}$ è possibile definire ϵ come il più piccolo valore che $|\beta_i - \beta_j|$ può assumere per $i \neq j$ ed $\tilde{\epsilon} = [\underline{\epsilon}] \in \hat{\mathbb{K}}$. Dato però che $\{\alpha_n\}$ è di Cauchy, per tale ϵ esiste $\overline{n} \in \mathbb{N}$ tale che $|\alpha_m - \alpha_n| < \epsilon$ in $\hat{\mathbb{K}}$ per ogni $n \geq \overline{n}$: allora $\alpha_n = \alpha_m$ per ogni $m, n \geq \overline{n}$, da cui segue $\alpha_n \to \beta_j$ per un qualche j. Adesso supponiamo invece che $\{\alpha_n\}$ assuma infiniti valori che possiamo supporre distinti togliendo gli eventuali termini ripetuti: siccome λ è un'immersione densa per ogni $n \in \mathbb{N}$ esiste un $a_n \in \mathbb{K}$ con $\lambda(a_n)$ compreso tra α_n e α_{n+1}, e la successione $\{a_n\}$ ottenuta in $\mathbb{K}$ è per costruzione di Cauchy. Infatti: $\{\alpha_n\}$ è di Cauchy per ipotesi, perciò per ogni $\epsilon > 0$ in $\hat{\mathbb{K}}$ esiste $\overline{n} \in \mathbb{N}$ tale che $|\alpha_m - \alpha_n| < \frac{\epsilon}{2}$ per ogni $m, n \geq \overline{n}$. Supponiamo sia per esempio (negli altri casi si procede analogamente)

$$\alpha_m < \lambda(a_m) < \alpha_{m+1} < \alpha_n < \lambda(a_n) < \alpha_{n+1};$$

allora $|\lambda(a_m) - \lambda(a_n)| < \alpha_{n+1} - \alpha_m < \frac{\epsilon}{2}$ per ogni $m, n \geq \overline{n}$. Quindi se $\eta = \lambda(\tilde{\epsilon})$ con $\tilde{\epsilon} \in \mathbb{K}$, $\tilde{\epsilon} > 0$ si ha $|a_m - a_n| < \tilde{\epsilon}$ per ogni $m, n \geq \overline{n}$, per cui $\{a_n\}$ è di Cauchy. Per il

Lemma 4.2.4 la successione $\left\{\left[\underline{a_n}\right]\right\}$ converge ad $\alpha := [\{a_n\}]$. Allora $\{\alpha_n\}$ converge ad α anch'essa, dato che per ϵ ed $\overline{n}$ come prima:

$$|\alpha_n - \alpha| = \left|\alpha_n - \left[\underline{a_n}\right] + \left[\underline{a_n}\right] - \alpha\right| \leq \left|\alpha_n - \left[\underline{a_n}\right]\right| + \left|\left[\underline{a_n}\right] - \alpha\right| <$$

$$< |\alpha_{n+1} - \alpha| + \left|\left[\underline{a_n}\right] - \alpha\right| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \text{ per } n \text{ abbastanza grande.}$$

b) Siano $\mathbb{L}$ ed f come nell'enunciato: data una successione $\{x_n\}$ di Cauchy in $\mathbb{K}$, per il Lemma 4.2.5 anche la successione $\{f(x_n)\}$ è di Cauchy in $\mathbb{L}$ che è completo, per cui è convergente a un qualche $x \in \mathbb{L}$. Sia ora $\{y_n\} \sim \{x_n\}$ (cioè $x_n - y_n \to 0$) e sia $y = \lim_{n\to+\infty} f(y_n) \in \mathbb{L}$. Sempre per il Lemma 4.2.5 abbiamo $f(x_n) - f(y_n) = f(x_n - y_n) \to 0$, da cui si deduce $x - y = 0$ ossia $x = y$: ne consegue perciò che l'applicazione

$$\begin{aligned} \hat{f}: \quad \hat{\mathbb{K}} &\to \mathbb{L} \\ [\{x_n\}] &\mapsto \lim_{n\to+\infty} f(x_n) \end{aligned}$$

è ben posta, e in più soddisfa l'identità $f = \hat{f} \circ \lambda$. Il fatto che $\hat{f}$ così definito sia un omomorfismo di campi segue dai punti *ii*) e *iii*) della Proposizione 4.1.3. Proviamo che $\hat{f}$ è un omomorfismo d'ordine. Se $[\{a_n\}] > 0$ allora esistono $\epsilon > 0$ in $\mathbb{K}$, $N \in \mathbb{N}$ tali che $a_n > \epsilon$ per ogni $n \geq N$ e, dato che f è per ipotesi un omomorfismo d'ordine, ne segue che $f(a_n) > f(\epsilon) > 0$ per ogni $n \geq N$: allora $\lim_{n\to+\infty} f(a_n) \geq f(\epsilon) > 0$ in $\mathbb{L}$ per il punto *iv*) della Proposizione 4.1.3.
Sia infine $g : \hat{\mathbb{K}} \to \mathbb{L}$ un omomorfismo d'ordine tale che $f = g \circ \lambda$, perciò g è anche un'immersione densa. Per il Lemma 4.2.4 per ogni $x \in \hat{\mathbb{K}}$ esiste $\{x_n\}$ successione di Cauchy in $\mathbb{K}$ tale che $\left[\underline{x_n}\right] \to x$; per l'unicità del limite vista in 4.1.3 si ha

$$g(x) = \lim_{n\to+\infty} g([\underline{x_n}]) = \lim_{n\to+\infty} g(\lambda(x_n)) = \lim_{n\to+\infty} f(x_n) = \hat{f}(x),$$

da cui segue l'unicità di $\hat{f}$. □

Dalla proprietà universale del completamento (punto *b*) del Teorema 4.2.6) si deduce:

Corollario 4.2.7. *Il completamento di un campo ordinato è unico a meno di isomorfismo.*

Dimostrazione. Siano $f_1 : \mathbb{K} \to \mathbb{F}_1$, $f_2 : \mathbb{K} \to \mathbb{F}_2$ due completamenti di un campo ordinato $\mathbb{K}$. Applicando il Teorema 4.2.6 prima con $\lambda = f_1$ e $f = f_2$, poi con $\lambda = f_2$

e $f = f_1$, vediamo che esiste un unico omomorfismo d'ordine $\hat{f_2} : \mathbb{F}_1 \to \mathbb{F}_2$ tale che $f_2 = \hat{f_2} \circ f_1$ e un unico omomorfismo d'ordine $\hat{f_1} : \mathbb{F}_2 \to \mathbb{F}_1$ tale che $f_1 = \hat{f_1} \circ f_2$. Mostriamo che $\hat{f_2} \circ \hat{f_1} = Id_{\mathbb{F}_2}$: siccome $\mathbb{F}_2$ è completo, applicando di nuovo il teorema e prendendo questa volta $f = f_2$ l'unico omomorfismo d'ordine da $\mathbb{F}_2$ in se stesso è proprio $Id_{\mathbb{F}_2}$. Quindi $Id_{\mathbb{F}_2} = \hat{f_2} \circ \hat{f_1}$. Ripetendo lo stesso procedimento ma scambiando $\mathbb{F}_2$ con $\mathbb{F}_1$, $\hat{f_2}$ con $\hat{f_1}$ si dimostra così che $\hat{f_1} \circ \hat{f_2} = Id_{\mathbb{F}_1}$: dunque $\hat{f_1} = \hat{f_2}^{-1}$ e $\mathbb{K}_1 \cong \mathbb{K}_2$. □

È ora possibile definire il campo dei numeri reali $\mathbb{R}$.

Definizione 4.2.8. Il completamento del campo ordinato dei numeri razionali $\mathbb{Q}$ è detto *campo dei numeri reali* e si denota con $\mathbb{R}$. In particolare $\mathbb{R}$ è un campo ordinato e il suo ordine estende quello di $\mathbb{Q}$.

Il campo dei numeri complessi $\mathbb{C}$ è definito come $\mathbb{C} := \mathbb{R}(i)$. Si vede subito che $\mathbb{C}$ non è formalmente reale e quindi non è ordinabile, in quanto $-1 = i^2 \in C(\mathbb{C})$ (si veda il Teorema 2.2.10).

4.3 Campi archimedei

Ora che abbiamo definito il campo dei numeri reali $\mathbb{R}$ vediamo alcune proprietà che lo caratterizzano. La prima tra queste è la 'proprietà archimedea'.

Definizione 4.3.1. Un campo ordinato $\mathbb{K}$ è detto *archimedeo* se per ogni elemento $a \in \mathbb{K}$ esiste un $n \in \mathbb{N}$ tale che $n1 > a$.

Vediamo ora un'importante caratterizzazione dei campi archimedei. Ci occorre richiamare la nozione di sottocampo fondamentale di un campo di caratteristica zero.

Definizione 4.3.2. Dati un campo $\mathbb{K}$ con $char(\mathbb{K}) = 0$ e l'omomorfismo di campi $\varphi : \mathbb{Q} \to \mathbb{K}$, $\varphi(\mathbb{Q})$, $\varphi(\frac{n}{s}) = \frac{n1}{s1}$, è detto il *sottocampo fondamentale* di $\mathbb{K}$.

Dal momento che ogni omomorfismo di campi è iniettivo, è possibile identificare $\mathbb{Q}$ con $\varphi(\mathbb{Q})$: per tale motivo d'ora in avanti, dato un campo ordinato $\mathbb{K}$, indicheremo con

$\mathbb{Q}$ il suo sottocampo fondamentale. Inoltre, sempre in virtù di tale identificazione, da questo momento in poi indicheremo con $\mathbb{N}$ il sottoinsieme $\{n1 \mid n \in \mathbb{N}\}$. Visto che per il Corollario 1.3.4 l'ordine sui numeri razionali (e quindi sui numeri naturali) è quello classico, osserviamo che ogni sottoinsieme $N \subseteq \mathbb{N}$ pensato come sottoinsieme di $\mathbb{K}$ possiede un elemento minimale.

Proposizione 4.3.3. *Un campo ordinato $\mathbb{K}$ è archimedeo se e solo se $\mathbb{Q}$ è denso in $\mathbb{K}$.*

Dimostrazione. Sia $\mathbb{K}$ un campo archimedeo e siano $a, b \in \mathbb{K}$ due elementi distinti tali che $a < b$: l'obbiettivo è di trovare un elemento $c \in \mathbb{Q}$ tale che $a < c < b$. Studiamo allora i diversi casi possibili per a, b:

- *Se $a < 0 < b$:* è sufficiente prendere $c = 0 \in \mathbb{Q}$;
- *Se $0 < a < b$:* poiché $\mathbb{K}$ è archimedeo esiste $n \in \mathbb{N}$ tale che $0 < \frac{1}{b-a} < n$, da cui segue $\frac{1}{n} < b - a$. Sia S l'insieme degli $r \in \mathbb{N}$ tali che $na < r$; tale insieme sarà non vuoto dato che $\mathbb{K}$ è archimedeo. Sia perciò $m = \min S$; avremo allora $na < m$, ossia $a < \frac{m}{n}$, e $m - 1 \leq na$, da cui deriva $\frac{m-1}{n} \leq a$ e quindi $\frac{m}{n} \leq a + \frac{1}{n}$. Preso perciò $c = \frac{m}{n} \in \mathbb{Q}$:
$$a < \frac{m}{n} \leq a + \frac{1}{n} < a + (b - a) = b;$$
- *Se $a < b < 0$:* abbiamo $0 < -b < -a$, ma allora per il punto precedente esiste $d \in \mathbb{Q}$ tale che $-b < d < -a$. Ponendo $c = -d$ si ha $a < c < d$.

Supponiamo adesso che $\mathbb{Q}$ sia denso in $\mathbb{K}$ e sia $a \in \mathbb{K}$. Se $a \leq 0$ basta prendere $n = 1$ in quanto $a \leq 0 < 1$. Invece se $a > 0$, allora $0 < a < 2a$ e quindi $0 < \frac{1}{2a} < \frac{1}{a}$: poiché $\mathbb{Q}$ è denso in $\mathbb{K}$ esistono $n, m \in \mathbb{N}$ tali che $\frac{1}{2a} < \frac{n}{m} < \frac{1}{a}$ da cui infine si ottiene $a < \frac{m}{n} \leq m$. □

Osservazione 4.3.4. In virtù della definizione del campo dei numeri reali come completamento di $\mathbb{Q}$ quest'ultimo è denso in $\mathbb{R}$; quindi per la Proposizione 4.3.3 appena vista $\mathbb{R}$ è un campo archimedeo.

Lemma 4.3.5. *Sia $\mathbb{K}$ campo ordinato e sia $\mathbb{F} \subseteq \mathbb{K}$ un sottocampo archimedeo denso in $\mathbb{K}$. Allora $\mathbb{K}$ è archimedeo.*

Dimostrazione. Siano $a, b \in \mathbb{K}$ con $a < b$; per la densità di $\mathbb{F}$ in $\mathbb{K}$ esiste $x \in \mathbb{F} \subseteq \mathbb{K}$ tale che $a < x < b$ e quindi esiste anche $y \in \mathbb{F}$ tale che $a < x < y < b$. Ma allora per la Proposizione 4.3.3 esiste $c \in \mathbb{Q}$ tale che $x < c < y$, per cui si ha $a < c < b$. Dunque $\mathbb{Q}$ è denso anche in $\mathbb{K}$ e, sempre per la Proposizione 4.3.6, ciò implica che $\mathbb{K}$ è archimedeo. □

Teorema 4.3.6. *Ogni sottocampo di $\mathbb{R}$, dotato dell'ordinamento indotto da quello di $\mathbb{R}$, è archimedeo. Viceversa, ogni campo ordinato archimedeo è ordinatamente isomorfo a un sottocampo di $\mathbb{R}$.*

Dimostrazione. Sia $\mathbb{F}$ un sottocampo di $\mathbb{R}$, e sia $a \in \mathbb{F}$. Allora $a \in \mathbb{R}$ e quindi esiste $n \in \mathbb{N}$ tale che $a < n$.
Supponiamo adesso $\mathbb{K}$ sia un campo archimedeo e sia $\hat{\mathbb{K}}$ il suo completamento: allora per il Lemma 4.3.5 abbiamo $\mathbb{Q}$ denso in $\hat{\mathbb{K}}$. Inoltre, siccome $\hat{\mathbb{K}}$ estende l'ordine di $\mathbb{K}$, $\hat{\mathbb{K}}$ estende anche l'ordine di $\mathbb{Q}$ ed è quindi anche un suo completamento. Per il Corollario 4.2.7 esiste dunque un omorfismo d'ordine $\varphi : \hat{\mathbb{K}} \to \mathbb{R}$, mostrando così che $\mathbb{K}$ è ordinatamente isomorfo a $\varphi(\mathbb{K}) \subseteq \mathbb{R}$. □

Corollario 4.3.7. *Ogni campo ordinato archimedeo completo è isomorfo a $\mathbb{R}$.*

4.4 Il Teorema Fondamentale dell'Algebra

Definizione 4.4.1. Sia $\mathbb{K}$ un campo ordinato e sia U un suo sottoinsieme non vuoto. Un elemento $\gamma \in \mathbb{K}$ è detto *maggiorante* di U se $\gamma \geq x$ per ogni $x \in U$.

Diciamo che U è *superiormente limitato* se ha un maggiorante.

Posto $X := \{\gamma \in \mathbb{K} \mid \gamma \text{ maggiorante di } U\}$, se X è non vuoto e se possiede un minimo (che quindi è unico) $\tilde{\gamma}$ diciamo che $\tilde{\gamma}$ è l'estremo superiore di U e scriviamo $\tilde{\gamma} = \sup U$.

Diciamo che $\mathbb{K}$ ha la *proprietà dell'estremo superiore* se vale:

per ogni sottoinsieme $U \subset \mathbb{K}$ non vuoto e superiormente limitato esiste $\sup U$.

È importante notare come non tutti i campi ordinati siano dotati della proprietà dell'estremo superiore.

Esempio 5. Consideriamo in $\mathbb{Q}$ il sottoinsieme $U = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$: tale insieme possiede dei maggioranti in $\mathbb{Q}$ (ad esempio 2) e, visto come sottocampo ordinato di $\mathbb{R}$, il suo estremo superiore è $\sqrt{2}$. Tuttavia $\sqrt{2}$ non appartiene a $\mathbb{Q}$, perciò $\mathbb{Q}$ non ha la proprietà dell'estremo superiore.

Per poter vedere che $\mathbb{R}$ è dotato della proprietà dell'estremo superiore è necessario introdurre alcuni lemmi.

Lemma 4.4.2. *La successione $\{2^{-n}\}$ in $\mathbb{R}$ è una successione infinitesima.*

Dimostrazione. Sia $\epsilon > 0$ in $\mathbb{R}$: per l'Osservazione 4.3.4 sappiamo che $\mathbb{R}$ è archimedeo, quindi esiste $\overline{n} \in \mathbb{N}$ tale che $\epsilon^{-1} < \overline{n}$ ossia $\overline{n}^{-1} < \epsilon$. Allora per ogni $n \in \mathbb{N}$ con $n \geq \overline{n}$ si ha $n^{-1} < \overline{n}^{-1} < \epsilon$. È facile provare per induzione che $n \leq 2^n$, da cui $2^{-n} \leq n^{-1}$, perciò concludiamo che $2^{-n} < \epsilon$ per ogni $n \geq \overline{n}$. □

Lemma 4.4.3. *Siano $\{a_n\}, \{b_n\}$ due successioni in $\mathbb{R}$ tali che:*

i) $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ per ogni $n \in \mathbb{N}$;

ii) la successione $\{b_n - a_n\}$ è infinitesima.

Allora sia $\{a_n\}$ che $\{b_n\}$ sono delle successioni di Cauchy in $\mathbb{R}$.

Dimostrazione. Sia $\epsilon > 0$ in $\mathbb{R}$ fissato: essendo $\{b_n - a_n\}$ convergente e quindi di Cauchy, esiste $\overline{n} \in \mathbb{N}$ che soddisfa (4.2). Siano $n, m \in \mathbb{N}$ tali che $n, m \geq \overline{n}$: possiamo supporre $\overline{n} \leq n \leq m$ (altrimenti basta scambiare n con m). Allora:

$$|a_m - a_n| + |b_n - b_m| = a_m - a_n + b_n - b_m = |a_m - b_m - (a_n - b_n)| < \epsilon. \tag{4.6}$$

Osservando in particolare che $|a_m - a_n|, |b_n - b_m| \geq 0$ per la disuguaglianza (4.6) si ha $|a_m - a_n| \leq |a_m - a_n| + |b_n - b_m| < \epsilon$, mostrando che la successione $\{a_n\}$ è di Cauchy, e analogamente per $\{b_n\}$. □

Teorema 4.4.4. *Il campo dei numeri reali $\mathbb{R}$ ha la proprietà dell'estremo superiore.*

Dimostrazione. Sia $U \subset \mathbb{R}$ un sottoinsieme non vuoto e superiormente limitato e sia X l'insieme dei suoi maggioranti in $\mathbb{R}$. Se U ha massimo, tale massimo è $\sup U$. Supponiamo

perciò U non abbia massimo e quindi $U \cap X = \varnothing$. Poiché per ipotesi X non è vuoto (U ammette almeno un maggiorante) esiste un $b_0 \in X$. Sia $a_0 \in U$; osserviamo come per il valore $\frac{a_0+b_0}{2}$ ci siano due possibilità:

- *Se* $\frac{a_0+b_0}{2} \in X$: posto b_1 tale valore e posto $a_1 = a_0$, si ha $a_1 \leq b_1$ e:
$$b_1 - a_1 = \frac{a_0 + b_0}{2} - a_0 = \frac{b_0 - a_0}{2} = (b_0 - a_0) \cdot 2^{-1};$$
- *Se* $\frac{a_0+b_0}{2} \notin X$: non essendo un maggiorante di U esiste un qualche $y \in U$ tale che $\frac{a_0+b_0}{2} \leq y$. Posti questa volta $a_1 = y, b_1 = b_0$ si ha $a_1 \leq b_1$ e in particolare:
$$b_1 - a_1 = b_0 - y \leq b_0 - \frac{a_0 + b_0}{2} = \frac{b_0 - a_0}{2} = (b_0 - a_0) \cdot 2^{-1}.$$

In entrambi i casi siamo riusciti a trovare $a_1 \in U$, $b_1 \in X$ tali che $a_0 \leq a_1 \leq b_1 \leq b_0$ e $b_1 - a_1 \leq (b_0 - a_0) \cdot 2^{-1}$, ritornando in una situazione identica al caso iniziale di a_0, b_0. Proseguendo in questo modo si costruiscono due successioni $\{a_n\}$,$\{b_n\}$ in $\mathbb{R}$ tali che per ogni $n \in \mathbb{N}$ si ha:

i) $a_n \in U$, $b_n \in X$ e $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$;

ii) $|b_n - a_n| = b_n - a_n \leq (b_{n-1} - a_{n-1}) \cdot 2^{-1} \leq \ldots \leq (b_0 - a_0) \cdot 2^{-n}$.

Ora, grazie alla Proposizione 4.1.3 e il Lemma 4.4.2, osserviamo come la successione $\{b_n - a_n\}$ sia infinitesima: allora, per il Lemma 4.4.3, le successioni $\{a_n\}, \{b_n\}$ sono di Cauchy in $\mathbb{R}$ e per la sua completezza sono convergenti necessariamente a uno stesso valore $\gamma \in \mathbb{R}$.
Notiamo adesso che $\gamma \in X$; infatti se esistesse $y \in U$ tale che $\gamma < y$, per la convergenza di $\{b_n\}$ esisterebbe $p \in \mathbb{N}$ tale che:

$$b_p - \gamma = |b_p - \gamma| < \gamma - y \;\Rightarrow\; b_p < y - \gamma + \gamma = y.$$

Ma $b_p \in X$ e $y \in U$, quindi questo non può accadere.
Mostriamo infine che γ è il minimo dei maggioranti di U. Supponiamo esista $x \in X$ tale che $x < \gamma$; questa volta per la convergenza di $\{a_n\}$ esiste $q \in \mathbb{N}$ tale che $a_q \in U$ e:

$$\gamma - a_q = |a_q - \gamma| < \gamma - x \;\Rightarrow\; x = \gamma - (x - \gamma) < a_q.$$

Ma $a_q \in U$ e $x \in X$, quindi questo non può accadere. Dunque per ogni $x \in X$ necessariamente si ha $\gamma \leq x$. □

Dalla dimostrazione del teorema è possibile evincere il seguente corollario.

Corollario 4.4.5. *Sia $U \subset \mathbb{R}$ sottoinsieme non vuoto e superiormente limitato e sia X l'insieme dei suoi maggioranti in $\mathbb{R}$. Allora U possiede un estremo superiore γ ed esistono due successioni $\{a_n\}, \{b_n\}$ convergenti ad γ tali che:*

i) $a_n \in U$ e $b_n \in X \setminus U$ per ogni $n \in \mathbb{N}$;

ii) $a_n \leq a_{n+1} \leq \gamma \leq b_{n+1} \leq b_n$ per ogni $n \in \mathbb{N}$.

Dimostrazione. Se $\gamma \in U$ basta prendere come $\{a_n\}$ la successione costante $\underline{\gamma}$, mentre per $\{b_n\}$ si può prendere per esempio la successione $\{\gamma + 2^{-n}\}$. Se $\gamma \notin U$ è sufficiente ripercorrere la dimostrazione del Teorema 4.4.4. □

Ricordiamo che (si veda la Proposizione 3.3.3) un campo ordinato $\mathbb{K}$ ha la proprietà del valore intermedio per i polinomi se, dati un polinomio $f \in \mathbb{K}[x]$ e $\alpha, \beta \in \mathbb{K}$ con $\alpha < \beta$, se $f(\alpha)f(\beta) < 0$ allora esiste $\gamma \in \mathbb{K}$ tale che $\alpha < \gamma < \beta$ e $f(\gamma) = 0$. Osserviamo che non tutti i campi ordinati hanno questa proprietà: ad esempio per il campo dei numeri razionali, presi $\alpha = 0, \beta = 2$ ed $f(x) = x^3 - 2$ si ha $f(\alpha)f(\beta) < 0$, ma il polinomio f non ammette radici in $\mathbb{Q}$.

Prima di poter dimostrare che $\mathbb{R}$ è dotato della proprietà del valore intermedio per i polinomi è necessario enunciare il seguente lemma:

Lemma 4.4.6. *Sia $\mathbb{K}$ un campo ordinato, sia $f \in \mathbb{K}[x]$ un polinomio e sia $\{a_n\}$ una successione in $\mathbb{K}$ convergente ad $a \in \mathbb{K}$. Allora la successione $\{f(a_n)\}$ in $\mathbb{K}$ converge ad $f(a)$.*

Dimostrazione. Sia $f(x) = c_n x^n + \cdots + c_0$, con $c_p \in \mathbb{K}$ per $p = 0, \ldots, n$. È sufficiente verificare l'enunciato per i polinomi della forma $g_p(x) := x^p$: infatti, una volta fatto ciò, la tesi seguirà direttamente dalla Proposizione 4.1.3 dato che:

$$f(a_n) \;=\; \sum_{p=0}^{n} c_p g_p(a_n) \to \sum_{p=0}^{n} c_p g_p(a) \;=\; f(a).$$

Mostriamo perciò l'enunciato per i polinomi g_p ragionando per induzione sul grado p. Poniamo come ipotesi induttiva:

I(k): *la successione* $\{g_k(a_n)\}$ *in* $\mathbb{K}$ *converge a* $g_k(a)$.

Per $k = 0$ banalmente $g_0(a_n) = g_0(a) = 1$ per ogni $n \in \mathbb{N}$. Supponiamo adesso **I(k)** vera per $k \leq p$ e verifichiamolo per $p+1$. Per far ciò basta riscrivere $g_{p+1}(x) = x^{p+1} = x^p \cdot x = = g_p(x) \cdot g_1(x)$: abbiamo per ipotesi $g_p(a_n) \to g_p(a)$ e $g_1(a_n) \to g_1(a)$ e, per la Proposizione 4.1.3 infine $g_{p+1}(a_n) = g_p(a_n) \cdot g_1(a_n) \to g_p(a) \cdot g_1(a) = g_{p+1}(a)$. □

Teorema 4.4.7. *Il campo* $\mathbb{R}$ *dei numeri reali possiede la proprietà del valore intermedio per i polinomi.*

Dimostrazione. Siano $f \in \mathbb{R}[x]$ e $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$, $f(\alpha)f(\beta) < 0$. Non è restrittivo chiedere $f(\alpha) < 0 < f(\beta)$ (altrimenti è sufficiente sostituire f con $-f$). Definito l'insieme $U := \{x \in \mathbb{R} \mid x < \beta,\ f(x) < 0\}$ abbiamo $U \neq \varnothing$ perché $\alpha \in U$ e inoltre U è superiormente limitato da β: allora per il Corollario 4.4.5 esiste $\gamma \in \mathbb{R}$ estremo superiore di U. Si ha $\alpha \leq \gamma \leq \beta$ e, posto X l'insieme dei maggioranti di U, esistono due successioni $\{a_n\}, \{b_n\}$ come nell'enunciato di tale corollario, perciò per il Lemma 4.4.6 abbiamo $\{f(a_n)\}, \{f(b_n)\}$ convergono a $f(\gamma)$. Osserviamo che $\beta \neq \gamma$: infatti, dato che $f(a_n) < 0$ per ogni $n \in \mathbb{N}$, per il punto v) della Proposizione 4.1.3 abbiamo $f(\gamma) \leq 0 < f(\beta)$. Inoltre, preso $\epsilon = \beta - \gamma > 0$, dato che $b_n \to \gamma$ esiste $\overline{n} \in \mathbb{N}$ tale che $0 \leq b_n - \gamma = |b_n - \gamma| < \beta - \gamma$ per ogni $n \geq \overline{n}$, ossia $\gamma \leq b_n < \beta$ per ogni $n \geq \overline{n}$: quindi la successione $\{c_n\} := \{b_{n+\overline{n}}\}$ è interamente compresa tra γ e β e $f(c_n) \to f(\gamma)$. Ora, se esiste $p \in \mathbb{N}$ tale che $f(c_p) = 0$ la dimostrazione è terminata dato che $\alpha \leq \gamma \leq c_p < \beta$. Altrimenti, se $f(c_n) \neq 0$ per ogni $n \in \mathbb{N}$, abbiamo che $f(c_n) > 0$ per il Corollario 4.4.5; quindi per il punto iv) della Proposizione 4.1.3 possiamo dedurre $f(\gamma) \geq 0$, mentre prima avevamo visto che $f(\gamma) \leq 0$. Dunque $f(\gamma) = 0$, mostrando così l'enunciato. □

È arrivato infine il momento di dimostrare il Teorema Fondamentale dell'Algebra.

Teorema 4.4.8. *Ogni polinomio* h *a coefficienti in* $\mathbb{C}$ *avente grado* $deg(h) \geq 1$ *possiede almeno una radice in* $\mathbb{C}$.

Dimostrazione. Abbiamo appena visto come $\mathbb{R}$ sia un campo ordinato che soddisfa la proprietà del valore intermedio. Perciò $\mathbb{R}$ è un campo realmente chiuso per la Proposizione 3.3.3 e $\overline{\mathbb{R}} = \mathbb{R}(i) = \mathbb{C}$ per il Teorema 3.3.1, ottenendo dunque la tesi per la definizione di chiusura algebrica di un campo. □

Bibliografia

[1] Michael Artin: *Algebra*, Bollati Boringhieri 1997.

[2] Pete L. Clark: *Honors Calculus*, 2014.
`http://alpha.math.uga.edu/~pete/2400full.pdf`

[3] Paul M. Cohn: *Basic Algebra - Groups, Rings and Fields*, Springer 2005.

[4] David A. Cox: *Galois Theory*, John Wiley & Sons, Inc. 2012.

[5] Nathan Jacobson: *Basic Algebra I: Second Edition*, Dover Publications, Inc. 2009.

[6] Hans Zassenhaus: *Emil Artin, his life and his work*, Notre Dame Journal of Formal Logic., Volume V, Number 1, January 1964.

Ringraziamenti

In questa sezione voglio ringraziare tutte le persone che mi sono state affianco, in un modo o nell'altro, durante tutto il mio percorso universitario. C'è da dire però che il momento in cui mi ritrovo a scrivere questa parte non mi lascia molto tempo per riflettere correttamente su chi nello specifico io abbia intenzione di ringraziare, dato che le persone sono tante: per tale motivo sono sicuro mi dimenticherò di più di una persona, per cui spero comunque che chi a fine ringraziamenti senta di non essere stato chiamato non sia indignato per la sua assenza. Nel dubbio, spero queste righe possano essere lo stesso un valido ringraziamento.

La prima persona che mi trovo a ringraziare non può che essere la mia relatrice, la Professoressa Monica Idà, la quale con estrema disponibilità (e pazienza) mi ha seguito in quest'ultimo periodo, dandomi consigli oltre che sulla stesura di questa tesi sul modo di scrivere ed esporre articoli in campo accademico.

Non posso poi che ringraziare tutti i miei amici, tra chi conosco da una vita e chi invece da meno: ringrazio ognuno di voi per la vostra presenza e compagnia in tutti questi anni, oltre che per avermi sopportato ogni qualvolta io mi sia messo a parlare di matematica senza il vostro consenso, e per tutte le volte che sono finito con l'abusare dell'utilizzo di parole come 'ipoteticamente', 'comunque', 'piango' e la lista potrebbe andare avanti all'infinito.

Ringrazio poi i miei genitori per tutto il supporto che mi hanno fornito in questi anni di università, a livello economico come a livello emotivo, e che mi hanno sopportato durante tutte le sessioni d'esame ed in questi mesi di stesura della tesi. Per ultima ci tengo a ringraziare mia sorella Rebecca per tutto il suo supporto e per essere stata la mia principale fonte di riferimento per ogni dubbio di tipo linguistico (e non solo) che

ho avuto ben più di un paio di volte mentre mi ritrovavo a scrivere la tesi.

Per quanto i travagli non siano stati pochi in questi ultimi quattro anni, non posso che ritenermi grato di tutte le esperienze vissute durante la triennale: sono riuscito ad approfondire qualcosa che da sempre suscita in me forte fascino e interesse, riscoprendo ulteriormente il piacere di fare matematica e tutte le soddisfazioni che questa disciplina porta con sé anche nei momenti di dubbio e incomprensione.