1

Ordered and real-closed fields

The field of real numbers $\mathbb{R}$ comes with a canonical ordering which is compatible with its field operations. This means, for example, that if $a \geq 0$ then $a + b \geq b$ for all b and $a \cdot b \geq 0$ provided that also $b \geq 0$. In this chapter we introduce *ordered fields* and capture their orderings algebraically using the notion of a *cone*. Classical algebraic geometry works best over algebraically closed fields. The analogue of this in the ordered setting is a *real-closed* field. We prove that every ordered field can be embedded into a real-closed one and that real closures are unique up to unique isomorphism. The presentation closely follows [BCR98, Chapter 1].

1.1 Ordered fields and cones

Recall that a binary relation $\leq$ on a set X is a *partial order* of X if it is reflexive, transitive and antisymmetric. A partial order can have incomparable elements, i.e., $x, y \in X$ such that neither $x \leq y$ nor $y \leq x$ holds. If any two elements are comparable, the ordering is *total* or *linear*. As usual, a partial order defines an opposite partial order $x \geq y :\Leftrightarrow y \leq x$ and a strict (irreflexive) ordering $x < y :\Leftrightarrow x \leq y \wedge x \neq y$.

Definition 1.1. An *ordered field* $(\mathbb{F}, \leq)$ consists of a field $\mathbb{F}$ equipped with a total order $\leq$ on its elements which is compatible with the field operations:

1. if $x \leq y$ then $x + z \leq y + z$ for every z;
2. if $x, y \geq 0$ then $xy \geq 0$.

To reduce notational load we will often refer to an ordered field $(\mathbb{F}, \leq)$ simply as $\mathbb{F}$ in contexts where the ordering is clear from context or arbitrary.

Remark 1.2. We will have occasions to talk about ordered rings as well using the defining properties of Definition 1.1 verbatim. However, the rings we are interested in are integral domains and then Exercise 1.4 shows that its orderings are determined by the orderings of its field of fractions, so there is no loss of generality in treating ordered fields only.

Example 1.3. The fields $\mathbb{Q}$ and $\mathbb{R}$ come equipped with their usual order. For both of them, this order is at the same time the only possible order relation that turns them into ordered fields. For $\mathbb{Q}$ this follows from Exercise 1.4 because it is the fraction field of $\mathbb{Z}$ which clearly has a unique ordering induced by $n < n + 1$, which is mandated by the definition of an ordered ring. A more specific proof is Exercise 1.3. For the real numbers, this follows from the existence of square roots for all positive numbers, as will be seen in Exercise 1.7. △

Example 1.4: Infinitesimals. The field $\mathbb{R}(x)$ generated by one transcendental x over $\mathbb{R}$ is the field of fractions of the polynomial ring $\mathbb{R}[x]$. Since x satisfies no non-trivial algebraic relations over $\mathbb{R}$, we are free to insert it at any point on the (extended) real line. This extends the ordering of $\mathbb{R}$ to $\mathbb{R} \cup \{ x \}$. The axioms of an ordered ring then automatically prescribe the ordering of every polynomial in $\mathbb{R}[x]$, hence $\mathbb{R}[x]$ becomes an ordered ring and $\mathbb{R}(x)$ an ordered field by Remark 1.2.

Conversely, fix an ordering of $\mathbb{R}(x)$. The element x defines a partition of $\mathbb{R}$ into two blocks $A = \{ a < x \}$ and $B = \{ b > x \}$; such a partition is called a *cut* and denoted as $A < x < B$. The possible cuts are

— $\emptyset < x < \mathbb{R}$ when x is negatively infinite.
— $(-\infty, a) < x < [a, \infty)$ when x is infinitesimally smaller than a,
— $(-\infty, a] < x < (a, \infty)$ when x is infinitesimally greater than a,
— $\mathbb{R} < x < \emptyset$ when x is positively infinite.

All of these orderings are related by rational coordinate changes of $\mathbb{R}$. Of special importance is the cut $(-\infty, 0] < x < (0, \infty)$ where x is a *(positive) infinitesimal*. We usually use the letter ε instead of x to suggest this. △

The first property of the ordering implies that it can be recovered from the non-negative elements alone because $x \leq y$ if and only if $0 \leq y - x$. The next definition captures basic properties of non-negativity algebraically:

Definition 1.5. Let $\mathbb{F}$ be a field. A *cone* is a subset $\mathcal{P} \subseteq \mathbb{F}$ such that (1) $\mathcal{P} + \mathcal{P} \subseteq \mathcal{P}$, (2) $\mathcal{P} \cdot \mathcal{P} \subseteq \mathcal{P}$, and (3) $x^2 \in \mathcal{P}$ for all $x \in \mathbb{F}$. A cone is *proper* if it does not contain -1.

Lemma 1.6. A cone $\mathcal{P}$ over $\mathbb{F}$ (of characteristic not 2) is proper if and only if it is a proper subset of $\mathbb{F}$.

Proof. One direction is obvious. For the other direction suppose that $-1 \in \mathcal{P}$ and let $a \in \mathbb{F}$ be arbitrary. Since $\mathbb{F}$ has characteristic $\neq 2$ we can write $a = \left(\frac{a+1}{2}\right)^2 + (-1) \cdot \left(\frac{a-1}{2}\right)^2 \in \mathcal{P}$ and thus $\mathcal{P} = \mathbb{F}$. □

Every field $\mathbb{F}$ has a smallst cone which is generated from the squares in $\mathbb{F}$ by finite sums and products. Since products of squares are again squares, we see immediately that every element in this cone can be written in the form $\sum_i a_i^2$ for finitely many $a_i \in \mathbb{F}$. This is the *sums of squares cone* $\sum \mathbb{F}^2$.

Proposition 1.7. The subset $\mathcal{P} = \{ x \in \mathbb{F} : x \geq 0 \}$ of an ordered field $(\mathbb{F}, \leq)$ is a proper cone satisfying $\mathcal{P} \cup -\mathcal{P} = \mathbb{F}$. Conversely, every proper cone with this property defines an ordering of $\mathbb{F}$.

Proof. That the set of non-negative elements $\mathcal{P}$ is a cone is obvious from the two properties of $\leq$ in Definition 1.1. In particular for every $a \in \mathbb{F}$ we have $a^2 = (-a)^2 \geq 0$ since $a \geq 0$ or $-a \geq 0$. Because every element is comparable to zero, we have $x \leq 0$ or $x \geq 0$ for each x, and hence $\mathcal{P} \cup -\mathcal{P} = \mathbb{F}$. If $\mathcal{P}$ is not proper, then $\mathcal{P} = \mathbb{F}$ by Lemma 1.6.

But then $0 \leq x$ for all x which implies $-x \leq 0$ by Exercise 1.1. But we also have $0 \leq -x$ for all x. Since $\leq$ is antisymmetric, $\mathbb{F} = \{ 0 \}$ — a contradiction.

In the opposite direction, we define an ordering by $x \leq y :\Leftrightarrow y - x \in \mathcal{P}$. Reflexivity, transitivity and compatibility with field arithmetic follow from cone properties. For antisymmetry one needs $\mathcal{P} \cap -\mathcal{P} = \{ 0 \}$ which is derived from properness analogously to Lemma 1.6. The condition $\mathcal{P} \cup -\mathcal{P} = \mathbb{F}$ shows that $\leq$ is total. □

Some authors refer to cones as *preorders*. Proposition 1.7 gives the additional features that make a preorder into an order. As the pairs $(\mathbb{F}, \leq)$ and $(\mathbb{F}, \mathcal{P})$ are equivalent descriptions of an ordered field, we freely mix and switch between the two.

Definition 1.8. The cone $\mathcal{P}(\mathbb{F}, \leq) := \{ x \in \mathbb{F} : x \geq 0 \}$ is the *non-negative cone* or *order cone* of the ordered field $\mathbb{F}$.

Example 1.9. The sums of squares are the smallest preorder but not necessarily an order. This can be seen in the function field $\mathbb{R}(\varepsilon)$ with an infinitesimal $\varepsilon > 0$. This ε is positive but not a sum of squares. Suppose otherwise, so that $\varepsilon = \sum f_i^2$ for rational functions $f_i = {}^{g_i}/_{h} \in \mathbb{R}(\varepsilon)$ with common denominator h. After clearing denominators, ε is seen to satisfy a non-zero(!) polynomial equation $\varepsilon \cdot h^2 = \sum_i g_i^2$ over $\mathbb{R}[\varepsilon]$. But this cannot happen because ε is transcendental over $\mathbb{R}$. △

Lemma 1.10. Let $\mathcal{P}$ be a proper cone in a field $\mathbb{F}$ and $-a \notin \mathcal{P}$. Then the set $\mathcal{P}[a] := \{ x + ay : x, y \in \mathcal{P} \}$ is a proper cone.

Proof. Closedness under addition and multiplication are obvious. Suppose $\mathcal{P}[a]$ is not proper, so that $-1 = x + ay$ for $x, y \in \mathcal{P}$. If $y = 0$, we have an immediate contradiction to $\mathcal{P}$ being proper. Otherwise we can write $-a = \frac{1+x}{y} \in \mathcal{P}$, which is also a contradiction. □

Theorem 1.11. Every proper cone $\mathcal{P}$ in $\mathbb{F}$ can be extended to an ordering of $\mathbb{F}$. Conversely, $\mathcal{P}$ is the intersection of all orderings of $\mathbb{F}$ extending it.

Proof. If $\mathcal{P}$ is a proper cone but not an order cone, then there exists $a \in \mathbb{F}$ such that $a \notin \mathcal{P} \cup -\mathcal{P}$. By Lemma 1.10 we may extend $\mathcal{P}$ to a proper cone including a. Hence, using Zorn's lemma on the poset of proper cones containing $\mathcal{P}$, we obtain a maximal proper cone $\mathcal{P}^* \supseteq \mathcal{P}$. Since it is maximal it satisfies $\mathcal{P}^* \cup -\mathcal{P}^* = \mathbb{F}$ and hence is an ordering.

Clearly the intersection $\mathcal{P}'$ of all orderings of $\mathbb{F}$ extending $\mathcal{P}$ is a proper cone extending $\mathcal{P}$. Suppose there exists $a \in \mathcal{P}' \setminus \mathcal{P}$. Then $\mathcal{P}[-a]$ is a proper cone above $\mathcal{P}$ which can be extended to an ordering of $\mathbb{F}$ by the first part of the proof. But $a \notin \mathcal{P}[-a]$ which contradicts $a \in \mathcal{P}'$. □

Corollary 1.12. Let $\mathbb{F}$ be a field. The following are equivalent: (a) $\mathbb{F}$ can be ordered, (b) $\mathbb{F}$ has a proper cone, (c) $-1 \notin \sum \mathbb{F}^2$, (d) whenever $\sum_i x_i^2 = 0$ in $\mathbb{F}$ then all $x_i = 0$.

Definition 1.13. A field which can be ordered, and hence satisfies any of the above equivalent conditions, is called *(formally) real*.

1.2 Extensions and real closure

Definition 1.14. (1) Let $(\mathbb{F}_1, \leq_1)$ and $(\mathbb{F}_2, \leq_2)$ be two ordered fields. A function $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ is a *homomorphism* of ordered fields (or *order-preserving homomorphism*) if φ is a field homomorphism such that $\varphi(a) \geq_2 0$ whenever $a \geq_1 0$.

(2) If φ is an injective order-preserving homomorphism, then we may regard $\mathbb{F}_1$ as an *ordered subfield* of $\mathbb{F}_2$ and $\mathbb{F}_2$ as an *ordered extension* of $\mathbb{F}_1$.

(3) Given two extensions $\mathbb{F}_1/\mathbb{F}$ and $\mathbb{F}_2/\mathbb{F}$ (ordered or not) an $\mathbb{F}$-*homomorphism* $\mathbb{F}_1 \to \mathbb{F}_2$ is a homomorphism which is the identity on $\mathbb{F}$.

As the name suggests, an ordered extension extends not only the field as a set, but also the ordering. If $(\mathbb{F}_2, \mathcal{P}_2)/(\mathbb{F}_1, \mathcal{P}_1)$, then $\mathbb{F}_2 \supseteq \mathbb{F}_1$ and $\mathcal{P}_2 \supseteq \mathcal{P}_1$. Every order-preserving homomorphism fixes $\mathbb{Q}$ with its unique order pointwise.

Example 1.15: Quadratic extensions. Let $(\mathbb{F}, \leq)$ be an ordered field and suppose there is $0 < a \in \mathbb{F}$ which does not have a square root in $\mathbb{F}$. The algebraic closure of $\mathbb{F}$ has two square roots $\pm\sqrt{a}$ which yield a quadratic extension $\mathbb{F}(\sqrt{a})/\mathbb{F}$. Recall that every element in the extension can be written uniquely as $x + \sqrt{a}y$ for $x, y \in \mathbb{F}$. The smallest cone $\mathcal{P}'$ in $\mathbb{F}(\sqrt{a})$ which contains $\mathcal{P}$ consists of finite sums the form

$$\sum_{i=1}^{n} b_i (c_i + d_i \sqrt{a})^2,$$

where $b_i \in \mathcal{P}$ and $c_i, d_i \in \mathbb{F}$. Since a is positive, $\mathcal{P}'$ is proper(!) and contains neither $\sqrt{a}$ nor $-\sqrt{a}$. By Lemma 1.10 and Theorem 1.11 both extensions $\mathcal{P}'[\sqrt{a}]$ and $\mathcal{P}'[-\sqrt{a}]$ give rise to (distinct but isomorphic) orderings of $\mathbb{F}(\sqrt{a})$.

To solve a general quadratic equation $ax^2 + bx + c$ it is necessary and sufficient to adjoin the square root of its discriminant $\sqrt{b^2 - 4ac}$, which reduces the general case to the treatment of square roots. △

An algebraically closed field is a field without proper algebraic extensions (since every univariate polynomial splits into linear factors). The analogous concept for ordered fields is this:

Definition 1.16. A real field without proper real algebraic extensions is *real-closed*. A real algebraic extension $\mathbb{F}_2/\mathbb{F}_1$ in which $\mathbb{F}_2$ is real-closed is a *real closure* of $\mathbb{F}_1$.

From the maximality property and our treatment of quadratic extensions in Example 1.15 we see immediately that real-closed fields have a unique ordering:

Corollary 1.17. A real-closed field has a unique ordering given by its squares.

In establishing the uniqueness of the real closure of an ordered field below, we need the following lemmas; see [BCR98, Section 1.3] for a proof using the theory of *Sturm sequences*.

Lemma 1.18. Let $(\mathbb{F}, \leq)$ be an ordered field, $\mathbb{F}^*$ a real closed field and $\varphi : \mathbb{F} \to \mathbb{F}^*$ an order-preserving homomorphism. If $\mathbb{F}'/\mathbb{F}$ is an ordered extension of finite degree, then there is an order-preserving extension $\varphi' : \mathbb{F}' \to \mathbb{F}^*$ of φ.

Lemma 1.19. Let $(\mathbb{F}, \leq)$ be an ordered field, $f \in \mathbb{F}[x]$ and $\mathbb{F}_1$ and $\mathbb{F}_2$ two real-closed extensions of $\mathbb{F}$. Then f has the same number of roots in $\mathbb{F}_1$ and in $\mathbb{F}_2$.

Theorem 1.20. Let $(\mathbb{F}, \leq)$ be an ordered field. There exists a real closure $\mathsf{rcl}(\mathbb{F})$ of $\mathbb{F}$. The real closure is unique up to unique isomorphism, i.e., for every two real closures $\mathsf{rcl}(\mathbb{F})_1$ and $\mathsf{rcl}(\mathbb{F})_2$ there exists a unique order-preserving $\mathbb{F}$-isomorphism between them.

Proof. To prove existence, let $\mathsf{acl}(\mathbb{F})$ be an algebraic closure of $\mathbb{F}$. We consider the poset of ordered fields $(\mathbb{F}_1, \leq_1)$ extending $(\mathbb{F}, \leq)$ and lying below $\mathsf{acl}(\mathbb{F})$ ordered by extension (as ordered fields). Every chain $(\mathbb{F}_i, \mathcal{P}_i)$ in this poset has an upper bound $(\bigcup_i \mathbb{F}_i, \bigcup_i \mathcal{P}_i)$, so Zorn's lemma implies that there is a maximal element $(\mathbb{F}^*, \mathcal{P}^*)$. It follows easily from its maximality and Example 1.15 that $\mathcal{P}^*$ is the set of squares and therefore the unique ordering of $\mathbb{F}^*$. Thus if there is a proper real algebraic extension $\mathbb{F}'/\mathbb{F}^*$, then first $\mathbb{F}'$ must lie in $\mathsf{acl}(\mathbb{F})$ (up to an order-preserving isomorphism) because it is algebraic over $\mathbb{F}$ and furthermore any ordering of $\mathbb{F}'$ must extend that of $\mathbb{F}^*$. But then $(\mathbb{F}^*, \mathcal{P}^*)$ would not be maximal which in turn proves that $\mathbb{F}^*$ is real-closed.

Let now $\mathbb{F}_1 = \mathsf{rcl}(\mathbb{F})$ be a real closure of $\mathbb{F}$ and $\mathbb{F}_2$ some real-closed extension of $\mathbb{F}$. We prove that there is a unique order-preserving $\mathbb{F}$-homomorphism $\mathbb{F}_1 \to \mathbb{F}_2$. Consider the partially ordered set of all order-preserving homomorphisms $\varphi : \mathbb{K} \to \mathbb{F}_2$ for any intermediate field $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{F}_1$ equipped with its ordering induced by $\mathbb{F}_1$. Two such homomorphisms $\phi : \mathbb{K} \to \mathbb{F}_2$ and $\phi' : \mathbb{K}' \to \mathbb{F}_2$ are compared via $\phi \leq \phi'$ if and only if $\mathbb{K} \subseteq \mathbb{K}'$ and $\varphi = \varphi'|_{\mathbb{K}}$. Application of Zorn's lemma gives a maximal homomorphism $\varphi^* : \mathbb{K}^* \to \mathbb{F}_2$. By definition $\mathbb{K}^* \subseteq \mathbb{F}_1$. If there were $a \in \mathbb{F}_1 \setminus \mathbb{K}^*$, then Lemma 1.18 would show the existence of a strictly larger homomorphism $\varphi' : \mathbb{K}^*(a) \to \mathbb{F}_2$ contradicting the maximality of φ. Thus we have an order-preserving $\mathbb{F}$-homomorphism $\mathbb{F}_1 \to \mathbb{F}_2$.

To see that this homomorphism is unique, take any $a \in \mathbb{F}_1$ and consider its minimal polynomial f over $\mathbb{F}$. Since f is irreducible and $\mathbb{F}$ is perfect, all roots of f in any field extending $\mathbb{F}$ are distinct. Let $a_1 < \cdots < a_k$ be the ordered sequence of roots of f in $\mathbb{F}_1$ and let $a = a_j$. By Lemma 1.19, we have the same number of roots $a'_1 < \ldots a'_k$ of f in $\mathbb{F}_2$. Any $\mathbb{F}$-homomorphism $\psi : \mathbb{F}_1 \to \mathbb{F}_2$ leaves f unchanged and hence maps a root of f in $\mathbb{F}_1$ to a root in $\mathbb{F}_2$. Since field homomorphisms are injective this mapping between the finitely many roots is bijective and if ψ is also order-preserving, then $a = a_j$ must map to a'_j. This uniquely determines ψ.

This yields unique $\mathbb{F}$-homomorphisms between $\mathsf{rcl}(\mathbb{F})_1$ and $\mathsf{rcl}(\mathbb{F})_2$. Composing them yields the unique $\mathbb{F}$-homomorphisms on $\mathsf{rcl}(\mathbb{F})_1$ and $\mathsf{rcl}(\mathbb{F})_2$ which are the respective identity maps. Hence the two real closures are isomorphic. □

From the proof we can extract the following slightly more versatile result:

Corollary 1.21. Let $(\mathbb{F}, \leq)$ an ordered field, $\mathsf{rcl}(\mathbb{F})$ its real closure and $\varphi : \mathbb{F} \to \mathbb{F}^*$ an order-preserving homomorphism into a real-closed field. Then there is a unique order-preserving extension $\varphi' : \mathsf{rcl}(\mathbb{F}) \to \mathbb{F}^*$.

Theorem 1.22. For a real field $\mathbb{F}$ the following are equivalent:

(a) $\mathbb{F}$ is real-closed.
(b) $\mathbb{F}$ has a unique ordering given by its squares and every univariate polynomial of odd degree has a root in $\mathbb{F}$.
(c) $\mathbb{F}(\sqrt{-1})$ is algebraically closed.

Proof. **(a) ⇒ (b):** The first part is Corollary 1.17. Suppose $f \in \mathbb{F}[x]$ is a polynomial of odd degree without a root in $\mathbb{F}$. We may suppose f to have the lowest odd degree with this property and to be irreducible. Then $\mathbb{F}' = \mathbb{F}[x]/\langle f \rangle$ is a proper algebraic extension of $\mathbb{F}$ and thus cannot be real. According to Corollary 1.12 we must have $-1 \in \sum \mathbb{F}'^2$, say

$$-1 = \sum_{i=1}^{m} h_i^2 + fg \quad \text{for } h_i, g \in \mathbb{F}[x], \deg h_i < \deg f.$$

The sum of squares term has even degree $\leq 2d-2$, so necessarily $\deg g \leq d-2$ is odd. By minimality of $\deg f$, g has a root $a \in \mathbb{F}$ but then $-1 = \sum_{i=1}^{m} h_i^2(a) \in \sum \mathbb{F}^2$ contradicts Corollary 1.12.

(b) ⇒ (c): First let $f \in \mathbb{F}[x]$ of degree $d = 2^m n$ where n is odd. If $m = 0$, then f has a root in $\mathbb{F}$ by assumption. We now proceed by induction on m. Let $y_1, \ldots, y_d$ be the roots of f in an algebraic closure of $\mathbb{F}$ and consider the sequence of polynomials

$$g_h = \prod_{i<j} (x - y_i - y_j - h y_i y_j), \quad \text{for } h \in \mathbb{Z}.$$

Since g_h is invariant under permuting the roots y_i, Galois theory implies that $g_h \in \mathbb{F}[x]$. Its degree is $\binom{d}{2} = 2^{m-1}n'$ for an odd n' and hence g_h has a root $y_i + y_j + h y_i y_j \in \mathbb{F}(\sqrt{-1})$ by our induction hypothesis. With $h = 0$ and $h = 1$ we see that $y_i + y_j \in \mathbb{F}(\sqrt{-1})$ and $y_i y_j \in \mathbb{F}(\sqrt{-1})$. But these are the roots of the quadratic equation $x^2 + (y_i + y_j)x + y_i y_j$ which is solvable in $\mathbb{F}(\sqrt{-1})$. Hence f has a root.

This settles the case when $f \in \mathbb{F}[x]$. Let now $f \in \mathbb{F}(\sqrt{-1})[x]$ and $\overline{f}$ the conjugate polynomial obtained by replacing all $\sqrt{-1}$ in the coefficients by $-\sqrt{-1}$. Then $f\overline{f} \in \mathbb{F}[x]$ and has a root in $\mathbb{F}(\sqrt{-1})$ by the preceding part of the proof. The root is either one of f or of $\overline{f}$. In the first case we are done and in latter case, we have the conjugate root $\overline{x}$ as a root of f and are also done.

(c) ⇒ (a): Suppose $\mathbb{F}'/\mathbb{F}$ is an algebraic extension. By Theorem A.1, $\mathbb{F}' = \mathbb{F}(a)$ for some primitive element $a \in \mathbb{F}'$. But then $\mathbb{F}(a, \sqrt{-1})/\mathbb{F}(\sqrt{-1})$ is an algebraic extension of an algebraically closed field and must be trivial, showing $a \in \mathbb{F}(\sqrt{-1})$ and hence $\mathbb{F}' = \mathbb{F}$ or $\mathbb{F}' = \mathbb{F}(\sqrt{-1})$. In the latter case, the extension cannot be real. □

The following important corollary is left as Exercise 1.5:

Corollary 1.23: Intermediate value theorem. Let $\mathbb{F}$ be real-closed and $f \in \mathbb{F}[x]$. If there are $a < b$ in $\mathbb{F}$ such that $f(a) < 0 < f(b)$, then f has a root between a and b.

Example 1.24. The field $\mathbb{R}$ is real-closed because $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed. The real closure of $\mathbb{Q}$ is **not** $\mathbb{R}$ but the countable subset of $\mathbb{R}$ which contains the algebraic numbers over $\mathbb{Q}$. A real-closed extension of $\mathbb{R}(\varepsilon)$ is the field of *Puiseux series*; see [BPR06, Section 2.6] for more information. △

1.3 Exercises

Choose exercises to solve from the list below. The target value is 15 points. By solving more exercises, you can get up to 20 points this week. Solutions must be submitted on MyCourses by the end of **Thursday, May 4**.

1.1 Let $(\mathbb{F}, \leq)$ be an ordered field. Prove the following facts about non-negative elements: (1) If $x \leq 0 \leq y$ then $xy \leq 0$. (2) If $x > 0$ then ${}^1\!/_x > 0$. $\boxed{\text{2 points}}$

1.2 Let $\mathcal{P}$ be a cone in $\mathbb{F}$. Show that $\mathcal{P}$ is proper if and only if $\mathcal{P} \cap -\mathcal{P} = \{ 0 \}$. $\boxed{\text{1 point}}$

1.3 Prove that the unique ordering of $\mathbb{Q}$ is given by its sums of squares. $\boxed{\text{2 points}}$

1.4 An *ordered ring* $(\mathcal{R}, \leq)$ is a commutative ring with unity equipped with a total order obeying the same properties as in Definition 1.1. (1) Prove that an ordered ring has characteristic zero and that if $\mathcal{R}$ has no nilpotent elements, then it has no zero divisors. (2) Suppose that $\mathcal{R}$ is an integral domain. Show that there is a one-to-one correspondence between the orderings of $\mathcal{R}$ and its field of fractions. $\boxed{\text{5 points}}$

1.5 Prove the Intermediate Value Theorem for polynomials over a real-closed field, Corollary 1.23. *(Hint: factor f over the algebraic closure of $\mathbb{F}$.)* $\boxed{\text{4 points}}$

1.6 An ordered field $(\mathbb{F}, \leq)$ is *archimedean* if for any $x \in \mathbb{F}$ there is an integer n such that $n > x$ (under the canonical embedding $\mathbb{Z} \hookrightarrow \mathbb{F}$). (1) Show that $\mathbb{F}$ is archimedean if and only if the rational numbers are dense in $\mathbb{F}$ with its order topology, i.e., every non-empty interval in $\mathbb{F}$ contains a rational number. (2) Prove that $\mathbb{R}$ and all its subfields are archimedean. *(Hint: You may use that the order topology of $\mathbb{R}$ is the usual euclidean topology.)* (3) Conclude that $\mathbb{F}$ is archimedean if and only if it can be embedded as an ordered field into $\mathbb{R}$. (4) Give an example of a non-archimedean ordered field. $\boxed{\text{10 points}}$

1.7 An ordered field $(\mathbb{F}, \leq)$ is *euclidean* if for every $a \in \mathbb{F}$ with $a > 0$ there is $b \in \mathbb{F}$ such that $b^2 = a$. (1) Prove that a euclidean field has a unique ordering. (2) Prove that real-closed fields are euclidean. Hence, every ordered field $\mathbb{F}$ has a smallest euclidean extension in a real closure $\mathsf{rcl}(\mathbb{F})$, which is its *euclidean closure* with respect to $\mathsf{rcl}(\mathbb{F})$. (3) Prove that two euclidean closures of $\mathbb{F}$ (taken in different real closures) are equal up to a unique order-preserving $\mathbb{F}$-isomorphism. $\boxed{\text{5 points}}$

1.8 Let $\mathbb{F}$ be an ordered field, fix a real closure $\mathsf{rcl}(\mathbb{F})$ and consider the affine plane over it. A point $(x, y) \in \mathsf{rcl}(\mathbb{F})^2$ with $x, y \in \mathbb{F}$ is $\mathbb{F}$*-rational*. A point (x, y) in $\mathsf{rcl}(\mathbb{F})^2$ is a *ruler and compass point (rcp)* if it is $\mathbb{F}$-rational or if it can be constructed in one of the following ways:

(a) As the intersection point of two distinct lines through rcps (*rcp lines*);
(b) As an intersection point of an rcp line and a circle through an rcp and centered at an rcp (an *rcp circle*); or
(c) As an intersection point of two distinct rcp circles.

By definition, every rcp can be constructed from finitely many $\mathbb{F}$-rational points using finitely many rcp lines and circles. A *ruler and compass number* is an $x \in \mathsf{rcl}(\mathbb{F})$ such that $(x, 0)$ is an rcp. Let $\mathsf{rcn}(\mathbb{F})$ denote the set of all ruler and compass numbers over $\mathbb{F}$.

(1) Prove that $\mathsf{rcn}(\mathbb{F})$ is a field between $\mathbb{F}$ and $\mathsf{rcl}(\mathbb{F})$.

Hence $\mathsf{rcn}(\mathbb{F})$ inherits a canonical ordering from $\mathsf{rcl}(\mathbb{F})$ which extends that of $\mathbb{F}$.

(2) Prove that $\mathsf{rcn}(\mathbb{F})$ is the euclidean closure $\mathsf{eucl}(\mathbb{F})$.

(3) Let $\alpha \in \mathsf{rcn}(\mathbb{F})$. Show that $[\mathbb{F}(\alpha) : \mathbb{F}]$ is a power of two.

(4) Conclude from the trigonometric identity $\cos\theta = 4\cos^3 {}^{\theta}\!/\!_3 - 3\cos {}^{\theta}\!/\!_3$ that it is impossible to trisect an arbitrary given angle $\cos\theta$ using ruler and compass over $\mathbb{F} = \mathbb{Q}(\cos\theta)$.

Consult [Mar98] for the geometric constructions that prove closure properties of ruler and compass numbers. $\boxed{\text{15 points}}$