2 The real numbers as a complete ordered field

In this section are presented what can be thought of as "the rules of the game:" the axioms of the real numbers. In this work, we present these axioms as rules without justification. There are other approaches which can be used. For example, another standard technique is to begin with the Peano axioms—the axioms of the natural numbers—and build up to the real numbers through several "completions" of this system. In such a setup, our axioms are theorems.

2.1 Field Axioms

This first set of axioms are called the field axioms because any object satisfying them is called a *field*. They give the algebraic properties of the real numbers.

A *field* is a nonempty set $\mathbb{F}$ along with two functions, multiplication $\times : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and addition $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ satisfying the following axioms.[3]

Axiom 1 (Associative Laws). If $a, b, c \in \mathbb{F}$, then $(a + b) + c = a + (b + c)$ and $(a \times b) \times c = a \times (b \times c)$.

Axiom 2 (Commutative Laws). If $a, b \in \mathbb{F}$, then $a + b = b + a$ and $a \times b = b \times a$.

Axiom 3 (Distributive Law). If $a, b, c \in \mathbb{F}$, then $a \times (b + c) = a \times b + a \times c$.

Axiom 4 (Existence of identities). There are $0, 1 \in \mathbb{F}$ such that $a + 0 = a$ and $a \times 1 = a$, $\forall a \in \mathbb{F}$.

Axiom 5 (Existence of an additive inverse). For each $a \in \mathbb{F}$ there is $-a \in \mathbb{F}$ such that $a + (-a) = 0$.

Axiom 6 (Existence of a multiplicative inverse). For each $a \in \mathbb{F} \setminus \{0\}$ there is $a^{-1} \in \mathbb{F}$ such that $a \times a^{-1} = 1$.

Although these axioms seem to contain most of the properties of the real numbers we normally use, there are other fields besides the real numbers.

Example 2.1. From elementary algebra we know that the rational numbers, $\mathbb{Q}$, are a field.

Example 2.2. Let $\mathbb{F} = \{0, 1, 2\}$ with with addition and multiplication calculated modulo 3. It is easy to check that the field axioms are satisfied.

Theorem 2.1. *The additive and multiplicative identities of a field $\mathbb{F}$ are unique.*

Proof. Suppose e_1 and e_2 are both multiplicative identities in $\mathbb{F}$. Then

$$e_1 = e_1 \times e_2 = e_2,$$

so the multiplicative identity is unique. The proof for the additive identity is essentially the same. □

[3] The functions $+$ and $\times$ are often called *binary operations*. The standard notation of $+(a, b) = a + b$ and $\times(a, b) = a \times b$ is used here.

Theorem 2.2. *Let $\mathbb{F}$ be a field. If $a, b \in \mathbb{F}$ with $b \neq 0$, then $-a$ and b^{-1} are unique.*

Proof. Suppose b_1 and b_2 are both multiplicative inverses for $b \neq 0$. Then, using Axiom 1,

$$b_1 = b_1 \times 1 = b_1 \times (b \times b_2) = (b_1 \times b) \times b_2 = 1 \times b_2 = b_2.$$

This shows the multiplicative inverse in unique. The proof is essentially the same for the additive inverse. □

From now on we will assume the standard notations for algebra; e. g., we will write ab instead of $a \times b$ and a/b instead of $a \times b^{-1}$. There are many other properties of fields which could be proved here, but they correspond to the usual properties of the real numbers learned in beginning algebra, so we omit them.

Problem 8. Prove that if $a, b \in \mathbb{F}$, where $\mathbb{F}$ is a field, then $(-a)b = -(ab) = a(-b)$.

2.2 Order Axiom

The axiom of this section gives us the order properties of the real numbers.

Axiom 7 (Order axiom.). There is a set $P \subset \mathbb{F}$ such that

(i) If $a, b \in P$, then $a + b, ab \in P$.

(ii) If $a \in \mathbb{F}$, then exactly one of the following is true: $a \in P$, $-a \in P$ or $a = 0$.

Of course, the P is known as the set of *positive* elements of $\mathbb{F}$. Using Axiom 7(ii), we see that $\mathbb{F}$ is divided into three pairwise disjoint sets: P, $\{0\}$ and $\{-x : x \in P\}$. The latter of these is the set of *negative* elements of $\mathbb{F}$.

Definition 2.1. We write $a < b$ or $b > a$, if $b - a \in P$. The meanings of $a \leq b$ and $b \geq a$ are now as expected.

Example 2.3. The rational numbers $\mathbb{Q}$ are an ordered field. This example shows there are ordered fields which are not equal to $\mathbb{R}$.

Extra Credit 2. Prove there is no set $P \subset \mathbb{Z}_3$ which makes $\mathbb{Z}_3$ into an ordered field.

Following are a few standard properties of ordered fields.

Theorem 2.3. *$a \neq 0$ iff $a^2 > 0$.*

Proof. ($\Rightarrow$) If $a > 0$, then $a^2 > 0$ by Axiom 7(a). If $a < 0$, then $-a > 0$ by Axiom 7(b) and above, $a^2 = 1a^2 = (-1)(-1)a^2 = (-a)^2 > 0$.
($\Leftarrow$) Since $0^2 = 0$, this is obvious. □

Theorem 2.4. *If $\mathbb{F}$ is an ordered field and $a, b, c \in \mathbb{F}$, then*

(a) $a < b \iff a + c < b + c$,

(b) $a < b \wedge b < c \implies a < c$,

(c) $a < b \wedge c > 0 \implies ac < bc$,

(d) $a < b \wedge c < 0 \implies ac > bc$.

Proof. (a) $a < b \iff b - a \in P \iff (b + c) - (a + c) \in P \iff a + c < b + c$.
(b) By supposition, both $b - a, c - b \in P$. Using the fact that P is closed under addition, we see $(b - a) + (c - b) = c - a \in P$. Therefore, $c > a$.
(c) Since $b - a \in P$ and $c \in P$ and P is closed under multiplication, $c(b - a) = cb - ca \in P$ and, therefore, $ac < bc$.
(d) By assumption, $b - a, -c \in P$. Apply part (c) and Problem 8. □

Theorem 2.5 (Two out of three rule). *Let $\mathbb{F}$ be an ordered field and $a, b, c \in \mathbb{F}$. If $ab = c$ and any two of a, b or c are positive, then so is the third.*

Proof. If $a > 0$ and $b > 0$, then Axiom 7(a) implies $c > 0$. Next, suppose $a > 0$ and $c > 0$. In order to force a contradiction, suppose $b \leq 0$. In this case, Axiom 7(b) shows

$$0 \leq a(-b) = -(ab) = -c < 0,$$

which is impossible. □

Corollary 2.6. *Let $\mathbb{F}$ be an ordered field and $a \in \mathbb{F}$. If $a > 0$, then $a^{-1} > 0$. If $a < 0$, then $a^{-1} < 0$.*

Proof. The proof is Problem 9. □

Problem 9. Prove Corollary 2.6.

Suppose $a > 0$. Since $1a = a$, Theorem 2.5 implies $1 > 0$. Applying Theorem 2.4, we see that $1 + 1 > 1 > 0$. It's clear that by induction, we can find a copy of $\mathbb{N}$ in any ordered field. Similarly, $\mathbb{Z}$ and $\mathbb{Q}$ also have unique copies in any ordered field.

The standard notation for intervals will be used on an ordered field, $\mathbb{F}$; i. e., $(a, b) = \{x \in \mathbb{F} : a < x < b\}$, $(a, \infty) = \{x \in \mathbb{F} : a < x\}$, $[a, b] = \{x \in \mathbb{F} : a \leq x \leq b\}$, etc.

2.2.1 Metric Properties

The order axiom on a field $\mathbb{F}$ allows us to introduce the idea of a distance between points in $\mathbb{F}$. To do this, we begin with the following familiar definition.

Definition 2.2. Let $\mathbb{F}$ be an ordered field. The *absolute value function* on $\mathbb{F}$ is a function $|\cdot| : \mathbb{F} \to \mathbb{F}$ defined as

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

The most important properties of the absolute value function are contained in the following theorem.

Theorem 2.7. *Let $\mathbb{F}$ be an ordered field. Then*

(a) $|x| \geq 0$ for all $x \in \mathbb{F}$ and $|x| = 0 \iff x = 0$;

(b) $|x| = |-x|$ for all $x \in \mathbb{F}$;

(c) $-|x| \leq x \leq |x|$ for all $x \in \mathbb{F}$;

(d) $|x| \leq y \iff -y \leq x \leq y$; and,

(e) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{F}$.

Proof. (a) The fact that $|x| \geq 0$ for all $x \in \mathbb{F}$ follows from Axiom 7(b). Since $0 = -0$, the second part is clear.

(b) If $x \geq 0$, then $-x \leq 0$ so that $|-x| = -(-x) = x = |x|$. If $x < 0$, then $-x > 0$ and $|x| = -x = |-x|$.

(c) If $x \geq 0$, then $-|x| = -x \leq x = |x|$. If $x < 0$, then $-|x| = -(-x) = x < -x = |x|$.

(d) This is left as an exercise.

(e) Add the two sets of inequalities $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$ to see $-(|x| + |y|) \leq x + y \leq |x| + |y|$. Now apply (d).

□

Definition 2.3. Let S be a set and $d : S \times S \to \mathbb{R}$ satisfy

(a) for all $x, y \in S$, $d(x, y) \geq 0$ and $d(x, y) = 0 \iff x = y$,

(b) for all $x, y \in S$, $d(x, y) = d(y, x)$, and

(c) for all $x, y, z \in S$, $d(x, z) \leq d(x, y) + d(y, z)$.

Then the function d is a *metric* on S.

A metric is a function which defines the distance between any two points of a set.

Example 2.4. Let S be a set and define $d : S \times S \to S$ by

$$d(x, y) = \begin{cases} 1, & x \neq y \\ 0, & x = y \end{cases}.$$

It is easy to prove that d is a metric on S. This trivial metric is called the *discrete* metric.

Theorem 2.8. *If $\mathbb{F}$ is an ordered field, then $d(x, y) = |x - y|$ is a metric on $\mathbb{F}$.*

Proof. This easily follows from various parts of Theorem 2.7 □

Problem 10. Prove $|x| \leq y$ iff $-y \leq x \leq y$.

2.3 The Completeness Axiom

Definition 2.4. A subset S of an ordered field $\mathbb{F}$ is *bounded above*, if there exists $M \in \mathbb{F}$ such that $M \geq x$ for all $x \in S$. A subset S of an ordered field $\mathbb{F}$ is *bounded below*, if there exists $m \in \mathbb{F}$ such that $m \leq x$ for all $x \in S$. The elements M and m are called *upper and lower bounds* for S, respectively.

Definition 2.5. Suppose $\mathbb{F}$ is an ordered field and S is bounded above in $\mathbb{F}$. A number $B \in \mathbb{F}$ is called a *least upper bound* of S if

(a) B is an upper bound for S, and

(b) if α is any upper bound for S, then $B \leq \alpha$.

Generally, we denote $B = \operatorname{lub} S$.

Suppose $\mathbb{F}$ is an ordered field and S is bounded below in $\mathbb{F}$. A number $b \in \mathbb{F}$ is called a *greatest lower bound* of S if

(a) b is a lower bound for S, and

(b) if α is any lower bound for S, then $b \geq \alpha$.

Generally, we denote $b = \operatorname{glb} S$.

Axiom 8 (Completeness). Every set which is bounded above has a least upper bound.

This is the final axiom. Any set which satisfies all eight axioms is called a *complete ordered field*. We assume the existence of a complete ordered field, called the *real numbers*. The real numbers are denoted by $\mathbb{R}$.

It can be shown that if $\mathbb{F}_1$ and $\mathbb{F}_2$ are both complete ordered fields, then they are the same, in the following sense. There exists a unique bijective function $i : \mathbb{F}_1 \to \mathbb{F}_2$ such that $i(a+b) = i(a) + i(b)$, $i(ab) = i(a)i(b)$ and $a < b \iff i(a) < i(b)$. Such a function i is called an *order isomorphism*. The existence of such an order isomorphism shows that the real numbers are essentially unique. Further discussion of this would take us too far afield. More reading on this topic can be done in [2].

Theorem 2.9. *If $A \subset \mathbb{R}$ is bounded above, then it has a unique least upper bound. If $A \subset \mathbb{R}$ is bounded below, then it has a unique greatest lower bound.*

Proof. Suppose a_1 and a_2 are both least upper bounds for A. By the definition of least upper bound, $a_1 \leq a_2 \leq a_1$ implies $a_1 = a_2$. The proof is similar for the greatest lower bound. □

Theorem 2.10. *$\alpha = \operatorname{lub} A$ iff $(\alpha, \infty) \cap A = \emptyset$ and for all $\varepsilon > 0$, $(\alpha - \varepsilon, \alpha] \cap A \neq \emptyset$. Similarly, $\beta = \operatorname{glb} A$ iff $(-\infty, \beta) \cap A = \emptyset$ and for all $\varepsilon > 0$, $[\beta, \beta + \varepsilon) \cap A \neq \emptyset$.*

Proof. We will prove the first statement, concerning the least upper bound. The second statement, concerning the greatest lower bound, follows similarly.

($\Rightarrow$) If $x \in (\alpha, \infty) \cap A$, then α cannot be an upper bound of A, which is a contradiction. If there is an $\varepsilon > 0$ such that $(\alpha - \varepsilon, \alpha] \cap A = \emptyset$, then from above, we conclude $(\alpha - \varepsilon, \infty) \cap A = \emptyset$. This implies $\alpha - \varepsilon/2$ is an upper bound for A which is less than $\alpha = \operatorname{lub} A$. This contradiction shows $(\alpha - \varepsilon, \alpha] \cap A \neq \emptyset$.

($\Leftarrow$) The assumption that $(\alpha, \infty) \cap A = \emptyset$ implies $\alpha \geq \operatorname{lub} A$. On the other hand, suppose $\operatorname{lub} A < \alpha$. By assumption, there is an $x \in (\operatorname{lub} A, \alpha) \cap A$. This is clearly a contradiction, since $\operatorname{lub} A < x \in A$. Therefore, $\alpha = \operatorname{lub} A$. □

Corollary 2.11. *If $\alpha = \operatorname{lub} A$ and $\alpha \notin A$, then for all $\varepsilon > 0$, $(\alpha - \varepsilon, \alpha] \cap A$ is an infinite set. Similarly, if $\beta = \operatorname{lub} A$ and $\beta \notin A$, then for all $\varepsilon > 0$, $(\beta - \varepsilon, \beta] \cap A$ is an infinite set.*

Proof. For each $n \in \mathbb{N}$, use Theorem 2.10 to choose $x_n \in (\alpha - 1/n, \alpha] \cap A$. Given $\varepsilon > 0$ let $N \in \mathbb{N}$ be large enough so that $0 < 1/N < \varepsilon$. Then, $\{x_n : n \geq N\} \subset (\alpha - \varepsilon, \alpha] \cap A$, and the corollary is proved. □

Problem 11. Let $A \subset \mathbb{R}$ be bounded above and

$$B = \{x : x \text{ is an upper bound of } A\}.$$

Prove $\operatorname{lub} A = \operatorname{glb} B$.

If a set A is not bounded above, then it is usual to write $\operatorname{lub} A = \infty$. Notice that the symbol "∞" is not a number. It is really a short way to say that there is no number which is an upper bound for A. Similarly, if B has no lower bound, then $\operatorname{glb} B = -\infty$.

An interesting observation is that $\operatorname{lub} \emptyset = -\infty$ and $\operatorname{glb} \emptyset = \infty$. To see the first of these, notice that every $M \in \mathbb{R}$ is an upper bound for the empty set. This is because, given M, there is no $x \in A$ such that $x \geq M$. Thus, the set of upper bounds for A has no lower bound.

Theorem 2.12 (Archimedean Principle). *If $a \in \mathbb{R}$, then there exists $n_a \in \mathbb{N}$ such that $n_a > a$.*

Proof. If the theorem is false, then a is an upper bound for $\mathbb{N}$. Let $\alpha = \operatorname{lub} \mathbb{N}$. According to Theorem 2.10 there is an $m \in \mathbb{N}$ such that $m > \alpha - 1$. But, this is a contradiction because $\alpha = \operatorname{lub} \mathbb{N} < m + 1 \in \mathbb{N}$. □

Some other variations on this theme are in the following corollary.

Corollary 2.13. *Let $a, b \in \mathbb{R}$ with $a > 0$.*

(a) There is an $n \in \mathbb{N}$ such that $an > b$.

(b) There is an $n \in \mathbb{N}$ such that $0 < 1/n < a$.

(c) There is an $n \in \mathbb{N}$ such that $n - 1 \leq a < n$.

Proof. (a) Use Theorem 2.12 to find $n \in \mathbb{N}$ where $0 < b/a < n$.

(b) Let $b = 1$ in part (a).

(c) Theorem 2.12 guarantees that $S = \{n \in \mathbb{N} : n > a\} \neq \emptyset\}$. If n is the least element of this set, then $n - 1 \notin S$ and $n - 1 \leq a < n$. □

2.4 Existence of $\sqrt{2}$

All of the above still does not establish that $\mathbb{Q}$ is different from $\mathbb{R}$. Since $\mathbb{Q} \subset \mathbb{R}$, we must find a real number which is not rational. The following two propositions show that $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Theorem 2.14. *There is a positive $\alpha \in \mathbb{R}$ such that $\alpha^2 = 2$.*

Proof. Let $S = \{x > 0 : x^2 < 2\}$. Then $1 \in S$, so $S \neq \emptyset$. If $x \geq 2$, then Theorem 2.4(c) implies $x^2 \geq 4 > 2$, so S is bounded above. Let $\alpha = \operatorname{lub} S$. It will be shown that $\alpha^2 = 2$.

Suppose first that $\alpha^2 < 2$. This assumption implies $(2 - \alpha^2)/(2\alpha + 1) > 0$. According to Corollary 2.13, there is an $n \in \mathbb{N}$ large enough so that

$$0 < \frac{1}{n} < \frac{2 - \alpha^2}{2\alpha + 1} \implies 0 < \frac{2\alpha + 1}{n} < 2 - \alpha^2.$$

Therefore,

$$\begin{aligned}\left(\alpha + \frac{1}{n}\right)^2 &= \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n^2} = \alpha^2 + \frac{1}{n}\left(2\alpha + \frac{1}{n}\right) \\ &< \alpha^2 + \frac{(2\alpha + 1)}{n} < \alpha^2 + (2 - \alpha^2) = 2\end{aligned}$$

contradicts the fact that $\alpha = \operatorname{lub} S$.

Next, assume $\alpha^2 > 2$. In this case, choose $n \in \mathbb{N}$ so that

$$0 < \frac{1}{n} < \frac{\alpha^2 - 2}{2\alpha} \implies 0 < \frac{2\alpha}{n} < \alpha^2 - 2.$$

Then

$$\left(\alpha - \frac{1}{n}\right)^2 = \alpha^2 - \frac{2\alpha}{n} + \frac{1}{n^2} > \alpha^2 - \frac{2\alpha}{n} > \alpha^2 - (\alpha^2 - 2) = 2,$$

again contradicts that $\alpha = \operatorname{lub} S$.

Therefore, $\alpha^2 = 2$. □

Theorem 2.15. *There is no $\alpha \in \mathbb{Q}$ such that $\alpha^2 = 2$.*

Proof. Assume to the contrary that there is $\alpha \in \mathbb{Q}$ with $\alpha^2 = 2$. Then there are $p, q \in \mathbb{N}$ such that $\alpha = p/q$ and p and q are relatively prime. Now,

$$\left(\frac{p}{q}\right)^2 = 2 \implies p^2 = 2q^2 \tag{1}$$

shows p^2 is even. Since the square of an odd number is odd, p must be even; i. e., $p = 2r$ for some $f \in \mathbb{N}$. Substituting this into (1), shows $2r^2 = q^2$. The same argument as above establishes q is also even. This contradicts the assumption that p and q are relatively prime. Therefore, no such α exists. □