REAL AND RATIONAL NUMBERS

1. Axioms for the Real Numbers

The set of real nubers, denoted $\mathbb{R}$, has the following properties:

1. **(Operations)** There are binary operations $+$ (addition) and $\cdot$ (multiplication), which take pairs of elements of $\mathbb{R}$ to elements of $\mathbb{R}$,
2. **(Commutativity)** For all $a, b \in \mathbb{R}$,
$$a + b = b + a \qquad \text{and} \qquad a \cdot b = b \cdot a.$$
3. **(Associativity)** For all $a, b, c \in \mathbb{R}$,
$$a + (b + c) = (a + b) + c \qquad \text{and} \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
4. **(Distributive Law)** For all $a, b, c \in \mathbb{R}$,
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$
5. **(Identity)** There are elements $0, 1 \in \mathbb{R}$ such that for all $a \in \mathbb{R}$,
$$a + 0 = a \qquad \text{and} \qquad a \cdot 1 = a.$$
Moreover, $0 \neq 1$.
6. **(Additive Inverses)** For each $a \in \mathbb{R}$, there exists $-a \in \mathbb{R}$ such that
$$a + (-a) = 0.$$
We write $b - a$ to mean $b + (-a)$.
7. **(Multiplicative Inverses)** For each $a \in \mathbb{R}$ such that $a \neq 0$, there exists $a^{-1} \in \mathbb{R}$ such that
$$a \cdot a^{-1} = 1.$$
We write $\frac{b}{a}$ to mean $b \cdot a^{-1}$.
8. **(Positive Integers)** There is a subset $\mathbb{R}_{>0}$ of $\mathbb{R}$ which we call the **positive real numbers**. We write $a < b$ when $b - a \in \mathbb{R}_{>0}$.
9. **(Positive Closure)** For all $a, b \in \mathbb{R}_{>0}$,
$$a + b \in \mathbb{R}_{>0} \qquad \text{and} \qquad a \cdot b \in \mathbb{R}_{>0}.$$
10. **(Trichotomy)** For every $a \in \mathbb{R}$, exactly one of the the following is true:
    (i) $a \in \mathbb{R}_{>0}$, or
    (ii) $a = 0$, or
    (iii) $-a \in \mathbb{R}_{>0}$.
11. **(Least Upper Bound Property)** Every non-empty subset of $\mathbb{R}$ which has an upper bound has a *least upper bound* in $\mathbb{R}$.

These properties are **axioms**, meaning that we declare them to be true without proof.

2. Basic consequences of the axioms

Notice that many of the axioms for $\mathbb{R}$ also appeared in the list of axioms for the integers $\mathbb{Z}$. As a result, many of the basic facts we proved about $\mathbb{Z}$ are also true for $\mathbb{R}$. We collect these below.

Lemma 1. *For all $a, b, c \in \mathbb{R}$, we have the following:*

- *(a)* (Additive Cancellation Property) *If $a + b = a + c$, then $b = c$.*
- *(b)* (Uniqueness of Additive Inverses) *If $a + b = 0$, then $b = -a$.*
- *(c)* $a \cdot 0 = 0$.
- *(d) If $a \cdot b = 0$, then $a = 0$ or $b = 0$.*
- *(e)* $-(-a) = a$.
- *(f)* $-a = (-1) \cdot a$.
- *(g)* (Multiplicative Cancellation Property) *If $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$.*
- *(h) The multiplicative identity 1 is an element of $\mathbb{R}_{>0}$.*
- *(i) Exactly one of the following is true:*
  - *(i) $a < b$, or*
  - *(ii) $a = b$, or*
  - *(iii) $b < a$.*
- *(j) If $a < b$, then $a + c < b + c$.*
- *(k) If $a < b$ and $0 < c$, then $a \cdot c < b \cdot c$.*

Proof. The proofs of these statements are identical to the proofs of the analogous statements for $\mathbb{Z}$. See the Integers handout for details. □

The Multiplicative Inverses axiom guarantees that each non-zero real number has a multiplicative inverse. This is significantly different from the integers, where only 1 and -1 have multiplicative inverses. In the next lemma, we record some basic properties of multiplicative inverses.

Lemma 2. *For all $a, b \in \mathbb{R}$ such that $a \neq 0$ and $b \neq 0$, we have the following:*

- *(a)* (Uniqueness of Multiplicative Inverses) *If $a \cdot b = 1$, then $b = a^{-1}$.*
- *(b)* $(a^{-1})^{-1} = a$
- *(c)* $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$
- *(d)* $(-a)^{-1} = -a^{-1}$
- *(e) $a > 0$ if and only if $a^{-1} > 0$.*

Proof. Let $a, b \in \mathbb{R}$ with $a \neq 0$ and $b \neq 0$.

- (a) Suppose $a \cdot b = 1$. We also know that $a \cdot a^{-1} = 1$, so $a \cdot b = a \cdot a^{-1}$. By the Multiplicative Cancellation Property (Lemma 1(g)), we conclude that $b = a^{-1}$.
- (b) By the Multiplicative Inverses axiom (and Commutativity), $a^{-1} \cdot a = 1$. Thus, by Uniqueness of Mutliplicative Inverses, we have $a = (a^{-1})^{-1}$.
- (c) By the Multiplicative Inverses, Commutativity, and Associativity axioms, we have

$$(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1 \cdot 1 = 1.$$

Therefore, by Uniqueness of Multiplicative Inverses, $a^{-1} \cdot b^{-1} = (a \cdot b)^{-1}$.

(d) Observe that $(-1)\cdot(-1) = -(-1) = 1$ by Lemma 1 parts (e) and (f). Therefore, $(-1)^{-1} = -1$ by Uniqueness of Multiplicative Inverses. Thus,

$$(-a)^{-1} = \big((-1)\cdot a)\big)^{-1} = (-1)^{-1}\cdot a^{-1} = -a^{-1}$$

by part (c).

(e) Suppose $a > 0$. By the Trichotomy axiom, exactly one of the following possibilities holds true: $a^{-1} > 0$ or $a^{-1} = 0$ or $-a^{-1} > 0$.

We cannot have $a^{-1} = 0$, because this would imply $1 = a \cdot a^{-1} = a \cdot 0 = 0$ by Lemma 1(c), which contradicts the fact that $1 \neq 0$ by the Identity axiom.

Assume, for the sake of contradiction, that $-a^{-1} > 0$. Then the Positive Closure axiom implies that

$$a\cdot(-a^{-1}) = a\cdot(-1)\cdot a^{-1} = (-1)\cdot(a\cdot a^{-1}) = -1\cdot 1 = -1$$

is an element of $\mathbb{R}_{>0}$; that is, $-1 > 0$. But this contradicts the Trichotomy axiom, because $1 > 0$ by Lemma 1(h).

Thus, we have shown that $a^{-1} > 0$ if $a > 0$.

Conversely, if $a^{-1} > 0$, then we apply the same argument to get that $(a^{-1})^{-1} > 0$. But $(a^{-1})^{-1} = a$ by part (b), and so $a > 0$.

□

3. Division and Rational Numbers

Unsurprisingly, the real numbers contain the integers.

Theorem 3. *Every integer is in* $\mathbb{R}$.

Proof. By the Trichotomy axiom for $\mathbb{Z}$, the integers consist of the natural numbers, 0, and the additive inverses of the natural numbers.

First, we know that $0 \in \mathbb{R}$ by the Identity axiom.

Next, we show that the natural numbers $\mathbb{N}$ are contained in $\mathbb{R}$. We proceed by induction. As the base case, $1 \in \mathbb{R}$ by the Identity axiom. Now, let $n \in \mathbb{N}$ be a natural number and suppose that $n \in \mathbb{R}$. Then $n + 1 \in \mathbb{R}$ because the sum of two real numbers is a real number. This completes the inductive proof, showing that every natural number is in $\mathbb{R}$.

Finally, for each natural number $n \in \mathbb{N}$, since n is in $\mathbb{R}$, the additive inverse $-n$ is a real number by the Additive Inverses axiom for $\mathbb{R}$. □

By thinking of the integers as living inside the real numbers, we may now divide integers to get "fractions," or rational numbers.

Definition. A real number $x \in \mathbb{R}$ is a **rational number** if there exist integers $a, b \in \mathbb{Z}$ such that $b \neq 0$ and $x = a \cdot b^{-1}$. We write $x = \frac{a}{b}$, and say that $\frac{a}{b}$ is a **fraction** representing the rational number x. The **numerator** of $\frac{a}{b}$ is a and the **denominator** of $\frac{a}{b}$ is b. The set of all rational numbers is denoted $\mathbb{Q}$.

Remark. Every integer n is a rational number, because $n = \frac{n}{1} \in \mathbb{Q}$.

Remark. A rational number may be represented by (infinitely) many fractions. Specifically, we have $\frac{a}{b} = \frac{c}{d}$ if and only if $a \cdot b^{-1} = c \cdot d^{-1}$ if and only if $ad = bc$.

Lemma 4. *For all $x, y \in \mathbb{Q}$, we have the following:*

(a) $x + y \in \mathbb{Q}$
(b) $x - y \in \mathbb{Q}$
(c) $x \cdot y \in \mathbb{Q}$
(d) If $y \neq 0$, then $x \cdot y^{-1} \in \mathbb{Q}$.

Proof. We prove (a) and leave (b)–(d) as exercises.

Since x and y are rational numbers, there exist $a, b, c, d \in \mathbb{Z}$ such that $b \neq 0$, $d \neq 0$, and $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Then

$$x + y = \frac{a}{b} + \frac{c}{d} = a \cdot b^{-1} + c \cdot d^{-1}.$$

Now, clearing denominators, we see that

$$bd(x + y) = bd(a \cdot b^{-1} + c \cdot d^{-1}) = ad + bc.$$

Multiplying by $(bd)^{-1}$ on both sides yields

$$x + y = (ad + bc) \cdot (bd)^{-1}.$$

Notice that $ad + bc$ and bd are integers, and $bd \neq 0$ because $b \neq 0$ and $d \neq 0$. Thus, we have shown that $x + y = \frac{ad+bc}{bd}$ is a rational number. □

The next lemma shows that we may always write a rational number as a fraction with a positive denominator.

Lemma 5. *Let $x \in \mathbb{Q}$. Then there exists $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $x = \frac{m}{n}$.*

Proof. By definition of rational numbers, there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $x = \frac{a}{b}$. If $b > 0$, then we may set $m = a$ and $n = b$ and we are done.

Otherwise, $b < 0$. Then $-b > 0$. Since $x = \frac{a}{b} = \frac{-a}{-b}$, we set $m = -a$ and $n = -b$. □

We now set out to show that each rational number can be written in lowest terms.

Definition. A fraction $\frac{a}{b}$ is in **lowest terms** if for every $d \in \mathbb{N}$, if $d|a$ and $d|b$, then $d = 1$.

Example. The fractions $\frac{2}{3}$ and $\frac{10}{15}$ are representations of the same rational number (because cross-multiplying gives $2 \cdot 15 = 3 \cdot 10$. The representation $\frac{2}{3}$ is in lowest terms, while $\frac{10}{15}$ is not.

In order to prove that any rational number x can be represented in lowest terms, we will focus on the denominators that show up in the representations of x as fractions. The representation in lowest terms will be the fraction with the smallest denominator. The following definition is useful in making this precise.

Definition. Let $x \in \mathbb{Q}$. A **possible positive denominator** for x is a positive integer $n \in \mathbb{N}$ such that there exists $m \in \mathbb{Z}$ with $x = \frac{m}{n}$.

Example. The rational number $\frac{2}{3}$ may be represented as $\frac{4}{6}$, $\frac{6}{9}$, and $\frac{10}{15}$ (among infinitely many other fractions). So 3, 6, 9, and 15 are some of the possible positive denominators for this rational number.

Theorem 6. *Let $x \in \mathbb{Q}$. There exist $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $x = \frac{m}{n}$ and $\frac{m}{n}$ is in lowest terms.*

Proof. Let S be the set of all possible positive denominators of x. By Lemma 5, x has at least one possible positive denominator, and so S is a non-empty subset of $\mathbb{N}$. By the Well-Ordering Principle, the set S has a least element n. Then there exists $m \in \mathbb{Z}$ such that $x = \frac{m}{n}$.

We claim that $\frac{m}{n}$ is in lowest terms. For the sake of contradiction, assume it is not. Then there is some $d \in \mathbb{N}$ such that $d|m$, $d|n$, and $d \neq 1$. Thus, there exist integers k and ℓ such that

$$m = dk \qquad \text{and} \qquad n = d\ell.$$

Therefore,

$$x = \frac{m}{n} = \frac{dk}{d\ell} = \frac{k}{\ell}.$$

Because $n, d \in \mathbb{N}$, we have $\ell \in \mathbb{N}$ as well. Moreover, since $d \neq 1$, we have $d > 1$. Hence, $\ell < n$. This shows that ℓ is a possible positive denominator for x which is smaller than n, a contradiction.

It follows that $\frac{m}{n}$ is in lowest terms. □

4. Least Upper Bounds

The Least Upper Bound Property is perhaps the most subtle of the axioms for $\mathbb{R}$, but it captures the fundamental nature of the real numbers. Indeed, the standard picture of the real numbers as a "continuum" along a number line rests on this axiom. You will learn more about this axiom in a real analysis course. Here, we will only try to give an idea of what it is and how it is used.

Let S be a subset of the real numbers. A real number a is called an **upper bound** of S if $x \leq a$ for all $x \in S$. A real number a is called a **least upper bound** of S if a is an upper bound of S and for all upper bounds b of S, $a \leq b$.

Lemma 7. *Let S be a subset of $\mathbb{R}$. The least upper bound of S, if it exists, is unique.*

Proof. Suppose a and b are both least upper bounds of S. Then, in particular, b is an upper bound of S, so by the fact that a is a least upper bound we get $a \leq b$. Similarly, a is an upper bound of S, and so the fact that b is a least upper bound implies that $b \leq a$. Therefore, $a = b$. □

The Least Upper Bound Property guarantees that any (non-empty) set of real numbers which has an upper bound has a least upper bound in $\mathbb{R}$. As the following example illustrates, the least upper bound of a set may or may not be an element of the set.

Example. Let $S = [0, 1]$ be the set of all real numbers x satisfying $0 \leq x \leq 1$, and let $T = (0, 1)$ be the set of all real numbers x satisfying $0 < x < 1$. Then $a \in \mathbb{R}$ is an upper bound for S if and only if a is an upper bound for T if and only if $a \geq 1$. The number 1 is the least upper bound of both sets. Notice that $1 \in S$ but $1 \notin T$.

Example. Let S be the set of all *rational* numbers x such that $x^2 \leq 2$. Notice that $1 \in S$, and so S is non-empty. We can see also that 2 is an upper bound for S. Indeed, if $x > 2$, then $x^2 > 4 > 2$, so $x \notin S$. By contrapositive, if $x \in S$ then $x \leq 2$.

Therefore, the Least Upper Bound Property implies that S has a least upper bound $a \in \mathbb{R}$. One can show that $a^2 = 2$; that is, $a = \sqrt{2}$. (You do this by contradiction: If $a^2 < 2$, then a cannot be an upper bound; if $a^2 > 2$, then a will be an upper bound which is not the least upper bound.)

This shows that $\sqrt{2} \in \mathbb{R}$. It turns out (as we will soon prove) that there is no rational number a such that $a^2 = 2$. Thus, this example also shows that $\mathbb{Q}$ *does not* satisfy the Least Upper Bound Property.