Our goal is to create an axiomatic basis for the real numbers $\mathbb{R}$. We need to establish axioms for $\mathbb{R}$ and then derive all further properties from the axioms. We would like these axioms to be as minimal and agreeable as possible; however, finding axioms that characterize $\mathbb{R}$ is not easy. Instead, we'll start from the natural numbers $\mathbb{N}$ and expand from there.

0.1 Natural Numbers $\mathbb{N}$ and Induction

How do we define the natural numbers? Listing every natural number is definitely not an option. We could try to define the natural numbers as $\mathbb{N} := \{1, 2, \ldots\}$. However, the "…" is ambiguous. Instead, we can define $\mathbb{N}$ in terms of its properties.

Definition 0.1.1 ▸ Peano Axioms for $\mathbb{N}$

The ***Peano axioms*** are five axioms that can be used to define the natural numbers $\mathbb{N}$.

1. $1 \in \mathbb{N}$
2. Every $n \in \mathbb{N}$ has a successor called $n + 1$.
3. 1 is **not** the successor of any $n \in \mathbb{N}$.
4. If $n, m \in \mathbb{N}$ have the same successor, then $n = m$.
5. If $1 \in S$ and every $n \in S$ has a successor, then $\mathbb{N} \subseteq S$.

Note that there is not one "prescribed" way to do define the natural numbers. This is just the most popular approach.

From the fifth axiom, we can derive a new proof technique for proving an arbitrary statement for all natural numbers.

Theorem 0.1.1 ▸ Principle of Induction

Let $P(n)$ be a statement for each $n \in \mathbb{N}$. Suppose that:

1. $P(1)$ is true, and
2. if $P(n)$ is true, then $P(n+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $S := \{n \in \mathbb{N} : P(n)\}$. Then $1 \in S$ because $P(1)$ is true. Note that if $n \in S$, then $P(n)$ is true. Hence, $P(n+1)$ is true by assumption, so $n+1 \in S$. By the fifth Peano axiom, we have $\mathbb{N} \subseteq S$. Since S was defined as a subset of $\mathbb{N}$, we have $\mathbb{N} = S$. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

A proof by induction kind of has a "domino effect". We set up the dominoes by proving $P(n) \implies P(n+1)$ and knock over the first domino by proving $P(1)$. The result is that all the dominoes will topple each other, leaving no domino standing.

$$\underbrace{P(1)}_{\text{by 1.}} \implies \underbrace{P(2)}_{\text{by 2.}} \implies \underbrace{P(3)}_{\text{by 2.}} \implies \cdots$$

Technique 0.1.1 ▸ Proof by Induction

To prove a statement $P(n)$ for all $n \in \mathbb{N}$, we need two things:

1. ***Base Case***: Prove $P(1)$.
2. ***Induction Step***: Assume $P(n)$ is true from some $n \in \mathbb{N}$, then prove $P(n) \implies P(n+1)$.

It is crucial that we actually use our assumption that $P(n)$ is true in the induction step. Otherwise, our proof is most likely wrong.

Example 0.1.1 ▸ Simple Proof by Induction

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Proof. Let $P(n)$ be the statement $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base Case: When $n = 1$, LHS $= 1$ and RHS $= \frac{1(1+1)}{2} = 1$, so $P(1)$ is true.

Induction Step: Assume that $P(n)$ is true for some $n \in \mathbb{N}$. Then:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

That is, $P(n+1)$ is true. By the Principle of Induction, $P(n)$ is true for all $n \in \mathbb{N}$. ▢

0.2 Integers $\mathbb{Z}$

From the natural numbers, we can easily construct the integers. First, we assume the existence an operation, addition $(+)$ and multiplication $(\cdot)$. On $\mathbb{N}$, we assume addition and multiplication satisfy the following properties for all $a, b, c \in \mathbb{N}$:

- ***Commutativity*** $a + b = b + a$ $a \cdot b = b \cdot a$
- ***Associativity*** $(a + b) + c = a + (b + c)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- ***Distributivity*** $a \cdot (b + c) = a \cdot b + a \cdot c$
- ***Identity*** $1 \cdot n = n$

We can expand this number system by including:

1. an ***additive identity*** ($n + 0 = n$ for all $n \in \mathbb{N}$)
2. ***additive inverses*** (for all $n \in \mathbb{N}$, add $-n$ so $-n + n = 0$)

From this, we can construct the set of integers.

Definition 0.2.1 ▸ Integers $\mathbb{Z}$

The set of ***integers*** is defined as:

$$Z := \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$$

Definition 0.2.2 ▸ Even, Odd, Parity

Let $a \in \mathbb{Z}$.

- a is ***even*** if there exists $k \in \mathbb{Z}$ where $a = 2k$.
- a is ***odd*** if there exists $k \in \mathbb{Z}$ where $a = 2k + 1$.
- ***Parity*** describes whether an integer is even or odd.

Theorem 0.2.1 ▸ Parity Exclusivity

Every integer is either even or odd, never both.

TODO: prove this

Example 0.2.1 ▸ Parity of Square

For $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof. We proceed by contraposition. Suppose n is not even. Then n is odd, and thus can be expressed as $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then:

$$\begin{aligned} n^2 &= (2k+1)(2k+1) \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Since the integers are closed under addition and multiplication, then $4k^2 + 4k \in \mathbb{Z}$. Thus, n^2 is odd. $\square$

0.3 Rational Numbers $\mathbb{Q}$

We can further expand this number system by the following:

1. Include ***multiplicative inverses*** (for all $n \in \mathbb{Z} \setminus \{0\}$, define $1/n$ such that $n \cdot 1/n = 1$)
2. Define $m \cdot 1/n := m/n$ when $n \neq 0$.

From this, we can construct the set of rational numbers.

Definition 0.3.1 ▸ Rational Numbers $\mathbb{Q}$

The set of ***rational numbers*** is defined as:

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in Z \land n \neq 0 \right\}$$

To ensure multiplication works as intended, we also define $\frac{m}{n} \cdot \frac{k}{l} := \frac{m \cdot k}{n \cdot l}$.

We say $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ if and only if $m_1 n_1 = m_2 n_2$ where $n_1, n_2 \neq 0$. In other words, $\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \iff m_1 n_2 = m_2 n_1$. Thus, $\mathbb{Q}$ is the set of equivalence classes for this relation.

If $n = kp$ and $m = kq$, where $k, p, q \in \mathbb{Z}$, $k \neq 0$, $q \neq 0$, then:

$$\frac{n}{m} = \frac{kp}{kq} = \frac{k}{p}, \quad \text{because } kpq = kqp$$

If n and m have no common factor (except ± 1), then we say that $n/m \in \mathbb{Q}$ is in the "lowest terms" or "reduced terms". The set $(Q, +, \cdot)$ forms a field. However, we cannot write $x = n/m$

where $x^2 = 2$.

Theorem 0.3.1 ▶ $\sqrt{2}$ is not a Rational Number

$\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose for contradiction $\sqrt{2}$ is a rationa number. Then, there exist $n, m \in \mathbb{Z}$ such that $(n/m)^2 = 2$. If $n = kp$ and $m = kq$, then we can "cancel" the common factor k to write $n/m = p/q$. That is, we can assume that n and m have no (non-trivial) common factors. Now, $n^2/m^2 = 2$, so by multiplying both sides by m^2, we get $n^2 = 2m^2$. Thus, n^2 is an even number, so n is also even (Example 0.2.1). Then, we can write $n = 2k$ where $k \in \mathbb{Z}$. Then:

$$\begin{aligned} \implies \quad (2k)^2 &= 2m^2 \\ \implies \quad 4k^2 &= 2m^2 \\ \implies \quad 2k^2 &= m^2 \end{aligned}$$

Then m^2 is even, so m is even. Thus, m and n are both even, so they are multiples of 2. This contradicts the fact that we defined n/m in the lowest terms. $\square$

Does there exist $r \in \mathbb{Q}$ such that $r^2 = 3$?

Definition 0.3.2 ▶ Divides

For $a, b, \in \mathbb{Z}$, we say a ***divides*** b if b is a multiple of a.

$$a \mid b \iff \exists(c \in \mathbb{Z})(b = ac)$$

Theorem 0.3.2 ▶ Division Algorithm

Suppose $a, b \in \mathbb{Z}$. Then $a = kb + r$ where $k \in \mathbb{Z}$ and $r \in \mathbb{Z}$ where $0 \leq r < a$.

Example 0.3.1

If $p \in \mathbb{N}$ and $3 \mid p^2$, then $3 \mid p$.

Proof. By the division algorithm, $p = 3k + j$ where $k \in \mathbb{Z}$ and $j \in \mathbb{Z}$ where $0 \leq j < 3$. Then, $p^2 = (3k+j)^2 = 9k^2+6kj+j^2$. Suppose that $3 \mid p^2$. Then, $p^2 = 3l = 9k^2+6kj+j^2$. Thus:

$$j^2 = 3l - 9k^2 - 6kj = 3(l - 3k^2 - 2kj)$$

We have $3 \mid j^2$. Hence, $j \neq 1, j \neq 2$, leaving only $j = 0$. Therefore, $p = 3k + 0$, so $3 \mid p$. ▢

Example 0.3.2 ▶ $\sqrt{3}$ is not a Rational Number

Proof. Suppose for contradiction $\sqrt{3}$ is a rational number. Then, there exist $n, m \in \mathbb{Z}$ such that $({}^n/_m)^2$. If n and m share a common factor, then we can "cancel" the common factor to where ${}^n/_m = {}^{kp}/_{kq} = {}^p/_q$. Thus, we may assume that n and m have no nontrivial common factor.

$$\begin{aligned} &\left(\frac{n}{m}\right)^2 = 3 \\ \implies \quad &\frac{n^2}{m^2} = 3 \\ \implies \quad &n^2 = 3m^2 \end{aligned}$$

Thus, $3 \mid n^2$, so $3 \mid n$ by the previous lemma. Writing $n = 3k$ for some $k \in \mathbb{Z}$, we have:

$$\begin{aligned} &(3k)^2 = 3m^2 \\ \implies \quad &9k^2 = 3m^2 \\ \implies \quad &3k^2 = m^2 \end{aligned}$$

That is, $3 \mid m^2$ so $3 \mid m$. Thus, 3 divides both n and m. This contradicts the fact that we defined ${}^n/_m$ in the lowest terms. ▢

0.4 Fields

Definition 0.4.1 ▶ Field

A ***field*** is a set F with two defined operations, addition and multiplication, satisfying the following for all $a, b, c \in F$:

Axiom	Addition	Multiplication
Associativity	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
Commutativity	$a+b = b+a$	$ab = ba$
Distributivity	$a(b+c) = ab+ac$	$(a+b)c = ac+bc$
Identities	$\exists(0 \in \mathbb{F})(a+0=a)$	$\exists(1 \in \mathbb{F})(1 \neq 0 \wedge 1a = a)$
Inverses	$\exists(-a \in \mathbb{F})(a+(-a)=0)$	$(a \neq 0) \iff \exists(a^{-1} \in \mathbb{F})(aa^{-1} = 1)$

All the “standard facts” of arithmetic and algebra in $\mathbb{R}$ follows from these axioms.

$\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are infinite fields, but $\mathbb{Z}_p$ (arithmetic modulo p) is a finite field if p is prime.

More generally, F_q where $q = p^k$ is a finite field.

Theorem 0.4.1 ▸ Facts about Fields

Let F be a field. For all $a, b, c \in F$:

(a) if $a + c = b + c$, then $a = b$
(b) $a \cdot 0 = 0$
(c) $(-a) \cdot b = -(a \cdot b)$
(d) $(-a) \cdot (-b) = a \cdot b$
(e) if $a \cdot c = b \cdot c$ and $c \neq 0$, then $a = b$
(f) if $a \cdot b = 0$, then $a = 0$ or $b = 0$
(g) $-(-a) = a$
(h) $-0 = 0$

Proof of (g).

$$\begin{aligned}
-(-a) &= -(-a) + 0 \\
&= -(-a) + (a + (-a)) \\
&= -(-a) + (-a + a) \\
&= (-(-a) + (-a)) + a \\
&= ((-a) + -(-a)) + a \\
&= 0 + a \\
&= a + 0 \\
&= a
\end{aligned}$$

□

0.5 Ordered Fields

Definition 0.5.1 ▶ Ordered Field

An ***ordered field*** is a field with a relation $<$ such that for all $a, b, c \in F$:

Axiom	Description
Trichotomy	Only one is true: $a < b$, $a = b$, or $b < a$
Transitivity	if $a < b$ and $b < c$ then $a < c$
Additive Property	if $b < c$, then $a + b < a + c$
Multiplicative Property	if $b < c$ and $0 < a$, then $a \cdot b < a \cdot c$

We then define $>$ as the inverse relation of $<$.

Theorem 0.5.1 ▶ Facts about Ordered Fields

- if $a < b$ then $-b < -a$
- if $a < b$ and $c < 0$, then $cb < ca$
- if $a \neq 0$, then $a^2 = a \cdot a > 0$
- $0 < 1$
- if $0 < a < b$ then $0 < 1/b < 1/a$

Although $\mathbb{C}$ is a field, it is not an ordered field. We can certainly define some kind of "order" on $\mathbb{C}$, but there is no way to make it satisfy the four axioms of an ordered field. For example, $i^2 = -1 < 0$, contradicting the fact that any nonzero number's square is greater than 0 in an ordered field.

$\mathbb{R}$ and $\mathbb{Q}$ are ordered fields.

Definition 0.5.2 ▶ Absolute Value

Let F be an ordered field. For $a \in F$, we define the ***absolute value*** of a as:

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

We can think of $|a-b|$ as the distance between a and b. More egnerally, $|a-b| = d(a,b)$ is the metric we are using.

Theorem 0.5.2 ▶ Properties of Absolute Value

- $|a| \geq 0$, $a \leq |a|$, and $-a \leq |a|$
- $|ab| = |a||b|$

Theorem 0.5.3 ▶ Triangle Inequality

Let F be an ordered field. For any $a, b \in F$, $|a+b| \leq |a| + |b|$.

Proof. There are two cases to consider. If $a + b \geq 0$, then:

$$\begin{aligned} |a+b| &= a+b \\ &\leq |a| + b \\ &\leq |a| + |b| \end{aligned}$$

If $a + b < 0$, then:

$$\begin{aligned} |a+b| &= -(a+b) \\ &= -a-b \\ &\leq |a| - b \\ &\leq |a| + |b| \end{aligned}$$

$\square$

0.6 Completeness

Definition 0.6.1 ▶ Bounded Above, Bounded Below, Bounded

Let F be an ordered field, and let $A \subseteq F$.

- A is ***bounded above*** if there exists $b \in F$ such that $a \leq b$ for all $a \in A$. In this context, b is an ***upper bound*** for A.
- A is ***bounded below*** if there exists $c \in F$ such that $c \leq a$ for all $a \in A$. In this context, c is a ***lower bound*** for A.
- A is ***bounded*** if A is bounded above and bounded below.

Example 0.6.1 ▶ Upper and Lower Bounds

Consider the set $(0, 1) \coloneqq \{x \in \mathbb{R} : 0 < x < 1\}$.

- $(0, 1)$ is bounded above by 1 and any number greater than 1.
- $(0, 1)$ is bounded below by 0 and any negative number.

Consider the set $[3, \infty) \coloneqq \{x \in \mathbb{R} : 3 \leq x\}$.

- $[3, \infty)$ is not bounded above.
- $[3, \infty)$ is bounded below by 3 and any number less than 3.

Definition 0.6.2 ▶ Maximum, Minimum

Let F be an ordered field, and let $A \subseteq F$.

- If there exists $M \in A$ such that M is an upper bound for A, then M is the ***maximum*** of A, denoted $M = \max A$
- If there exists $m \in A$ such that m is a lower bound for A, then m is the ***minimum*** of A, denoted $m = \min A$.

Note that from the above example, $(0, 1)$ has neither a maximum nor a minimum. However, 3 is the minimum of $[3, \infty)$.

Definition 0.6.3 ▶ Supremum, Infimum

Let F be an ordered field, and let $A \subseteq F$. If there exists $s \in F$ such that:

1. s is an upper bound for A, and
2. $s < t$ for any upper bound t for A,

then s is the ***supremum*** of A, denoted $s = \sup A$.

If A has a supremum, then that supremum is unique. ()

Theorem 0.6.1 ▶ Maximum is the Supremum

Let F be an ordered field, and let $A \subseteq F$. If A has a maximum M, then $M = \sup A$.

Proof. Since $M = \max A$, we know M is an upper bound for A. Let t be an upper bound for A. Since $M \in A$, then $t \geq M$. Thus, M is less than or equal to any upper bound t, so $M = \sup A$. ▢

Example 0.6.2 ▸ Supremum of $(0, 1)$

Prove that $\sup(0,1) = 1$.

Proof. First, note that 1 is an upper bound for $(0,1)$. Next, suppose that $t \in \mathbb{Q}$ is an upper bound for $(0,1)$. Since $0 < 1/2 < 1$, then $0 < 1/2 \leq t$. By transitivity, $t > 0$. Suppose for contradiction $t < 1$. Because $0 < t < 1$, we have $1 < 1 + t < 2$. Dividing across by 2, we have $1/2 < {}^{1+t}/2 < 1$. That is, ${}^{1+t}/2 \in (0,1)$. But $t < 1$, so $2t < 1 + t$. Thus, $t < {}^{1+t}/2$. This contradicts our assumption that t is an upper bound for $(0,1)$. Therefore, $t \geq 1$, so $\sup(0,1) = 1$. ▢

Definition 0.6.4 ▸ Completeness

An ordered field F is ***complete*** if every nonempty subset of F that is bounded above has a supremum in F.

Theorem 0.6.2 ▸ $\mathbb{Q}$ is not complete