Chapter 1

The Construction of Real and Complex Numbers

> Thus the System of Real Numbers—the definition of irrationals and the extension of the four species to the new numbers—is established. The method has the advantage of simplicity in detail. It is well for the student, after a first study of the method of Dedekind, to work it through in detail. He will then return to the former method with increased power and greater zest.
>
> The method of regular sequences is a middle-of-the-road method. It is an easy way to reach the mountain top. The traveler buys his ticket and takes the funicular. Many people prefer this mode of travel. But some like a stiff climb over rocks and across streams, and such an ascent has its advantages if the heart is good and the muscles are strong.
>
> – *William Fogg Osgood*
> *Functions of Real Variables*

Challenge Problems: I

Problem 1.1. How many congruent regular tetrahedra with edge length 1 can be packed inside a sphere of radius 1 if each tetrahedron has a vertex at the center of the sphere?

A lattice point in n-dimensional Euclidean space is a point all of whose coordinates are integers. A lattice polygon in $\mathbb{R}^2$ is a polygon all of whose vertices are lattice points. Similarly, a lattice polyhedron in $\mathbb{R}^n$ is a polyhedron all of whose vertices are lattice points.

Problem 1.2. Find all possible areas of lattice squares in $\mathbb{R}^2$. (Hint: The first answer you get is probably not the final answer we are looking for.)

Problem 1.3. Find all possible volumes of lattice cubes in $\mathbb{R}^3$.

Problem 1.4. Find all possible volumes of lattice hypercubes in $\mathbb{R}^n$ for $n > 3$.

PROBLEM 1.5. If $f : \mathbb{R} \to \mathbb{R}$ is a polynomial function such that $f(\mathbb{Q}) \subseteq \mathbb{Q}$ and $f(\mathbb{R} \setminus \mathbb{Q}) \subseteq \mathbb{R} \setminus \mathbb{Q}$, show that $f(x) = ax + b$ for some $a, b \in \mathbb{Q}$.

To begin this chapter, we assume that the reader is familiar with the integers $\mathbb{Z}$ as an ordered integral domain and the rational numbers $\mathbb{Q}$ as an ordered field that is the field of fractions of the integers $\mathbb{Z}$ (see Appendix A).

EXERCISE 1.0.1. Prove that any ordered integral domain contains the integers.

EXERCISE 1.0.2. Prove that any field that contains the integers contains the rationals as a subfield.

In this chapter, we do several things. First, we introduce the real numbers by adding the least upper bound property to the axioms for an ordered field. Second, despite Osgood, we construct the real numbers from the rational numbers by the method of Cauchy sequences. Third, we construct the complex numbers from the real numbers and prove a few useful theorems about them. Intermingled in all of this is a discussion of the fields of algebraic numbers and real algebraic numbers. As a project at the end of the chapter, we lead the reader through a discussion of the construction of the real numbers via Dedekind cuts. In other projects, we study the convergence properties of infinite series and decimal expansions of real numbers.

1.1. The Least Upper Bound Property and the Real Numbers

DEFINITION 1.1.1. Let F be an ordered field. Let A be a nonempty subset of F. We say that A is *bounded above* if there is an element $M \in F$ with the property that if $x \in A$, then $x \leq M$. We call M an *upper bound* for A. Similarly, we say that A is *bounded below* if there is an element $m \in F$ such that if $x \in A$, then $m \leq x$. We call m a *lower bound* for A. We say that A is *bounded* if A is bounded above and A is bounded below.

EXAMPLES 1.1.2.

(i) Consider the subset A of $\mathbb{Q}$:
$$A = \left\{ 1 + \frac{(-1)^n}{n} \;\middle|\; n \in \mathbb{N} \right\}.$$
Then A is bounded above by $3/2$ and bounded below by 0.

(ii) Let $A = \{x \in \mathbb{Q} \mid 0 < x^3 < 27\}$. Then A is bounded below by 0 and bounded above by 3.

EXERCISE 1.1.3. Let a be a positive rational number and let $A = \{x \in \mathbb{Q} \mid x^2 < a\}$. Show that A is bounded in $\mathbb{Q}$.

DEFINITION 1.1.4. Let F be an ordered field, and let A be a nonempty subset of F which is bounded above. We say that $L \in F$ is a *least upper bound* for A if the following two conditions hold:

(a) L is an upper bound for A;
(b) if M is any upper bound for A, then $L \leq M$.

EXERCISE 1.1.5. Show the least upper bound of a set is unique.

We now give a formal definition of the real numbers which provides a working basis for proving theorems. Later in this chapter, starting with the rational numbers as an ordered field we will give a precise construction of the real numbers as an ordered field in which the least upper bound property holds.

DEFINITION 1.1.6. The *real numbers* are an ordered field in which every nonempty subset that is bounded above has a least upper bound and are denoted by the symbol $\mathbb{R}$.

We say that the real numbers are an ordered field with the least upper bound property. In many texts, the real numbers are defined as a *complete ordered field*. This is actually a misuse of the word "complete" which is defined in terms of the convergence of Cauchy sequences. This will be discussed later in this chapter.

EXERCISE 1.1.7. Find the least upper bound in $\mathbb{R}$ of the set A in Exercise 1.1.3.

DEFINITION 1.1.8. Suppose that F and F' are ordered integral domains. We say that F and F' are *order isomorphic* if there is a bijection $\phi : F \longrightarrow F'$ such that

(a) $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in F$;
(b) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in F$;
(c) if $x, y \in F$ and $x < y$, then $\phi(x) < \phi(y)$ in F'.

EXERCISE 1.1.9. Show that any two ordered fields with the least upper bound property are order isomorphic.

This exercise proves that if the real numbers exist, they are unique up to order isomorphism.

DEFINITION 1.1.10. An ordered field F has the *greatest lower bound property* if every nonempty subset A of F that is bounded below has a greatest lower bound. That is, there exists an element ℓ of F such that:

(a) ℓ is a lower bound for A;
(b) if m is any lower bound for A, then $m \leq \ell$.

EXERCISE 1.1.11. Prove that an ordered field has the least upper bound property iff it has the greatest lower bound property.

If L is the least upper bound of a set A, we write $L = \text{lub } A$ or $L = \sup A$ (sup stands for *supremum*). If ℓ is the greatest lower bound of a set A, we write $\ell = \text{glb } A$ or $\ell = \inf A$ (inf stands for *infimum*).

Exercise 1.1.12. Let n be a positive integer that is not a perfect square. Let $A = \{x \in \mathbb{Q} \mid x^2 < n\}$. Show that A is bounded in $\mathbb{Q}$ but has neither a greatest lower bound nor a least upper bound in $\mathbb{Q}$. Conclude that $\sqrt{n}$ exists in $\mathbb{R}$, that is, there exists a real number a such that $a^2 = n$.

We have observed that the rational numbers are contained in $\mathbb{R}$. A real number is *irrational* if it is not in $\mathbb{Q}$.

Fact 1.1.13. We can conclude from Exercise 1.1.12 that if n is a positive integer that is not a perfect square, then $\sqrt{n}$ exists in $\mathbb{R}$ and is irrational.

Exercise 1.1.14. Suppose that A and B are bounded sets in $\mathbb{R}$. Prove or disprove the following:

(i) $\operatorname{lub}(A \cup B) = \max\{\operatorname{lub} A, \operatorname{lub} B\}$.
(ii) If $A + B = \{a + b \mid a \in A, b \in B\}$, then $\operatorname{lub}(A + B) = \operatorname{lub} A + \operatorname{lub} B$.
(iii) If the elements of A and B are positive and $A \cdot B = \{ab \mid a \in A, b \in B\}$, then $\operatorname{lub}(A \cdot B) = (\operatorname{lub} A)(\operatorname{lub} B)$.
(iv) Formulate the analogous problems for the greatest lower bound.

1.2. Consequences of the Least Upper Bound Property

We now present some facts which follow from the least upper bound property and the properties of the integers. The first is the *Archimedean Property* of the real numbers.

Theorem 1.2.1 **(Archimedean property of $\mathbb{R}$)**. *If a and b are positive real numbers, then there exists a natural number n such that $na > b$.*

Proof. If $a > b$, take $n = 1$. If $a = b$, take $n = 2$. If $a < b$, consider the set $S = \{na \mid n \in \mathbb{N}\}$. The set $S \neq \varnothing$ since $a \in S$. Suppose S is bounded above by b. Let $L = \operatorname{lub} S$. Then, since $a > 0$, there exists an element $n_0 a \in S$ such that $L - a < n_0 a$. But then $L < (n_0 + 1)a$, which is a contradiction.

Corollary 1.2.2. *If ε is a positive real number, then there exists a natural number n such that $1/n < \varepsilon$.*

Definition 1.2.3. Let F be an ordered field. From Exercise 1.0.1, we know that $\mathbb{Z} \subseteq F$ and by Exercise 1.0.2 we know $\mathbb{Q} \subseteq F$. We say that F is an *Archimedean ordered field* if for every $x \in F$ there exists $N \in \mathbb{Z}$ such that $x < N$.

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

Exercise 1.2.4. Let F be an Archimedean ordered field. Show that F is order isomorphic to a subfield of $\mathbb{R}$.

Next, we show that every real number lies between two successive integers.

Theorem 1.2.5. *If a is a real number, then there exists an integer N such that $N - 1 \leq a < N$.*

Proof. Let $S = \{n \in \mathbb{Z} \mid n > a\}$. Then by the Archimedean property, $S \neq \varnothing$. The set S is bounded below by a, so by the well-ordering principle, S has a least element N. Then $N - 1 \notin S$, so $N - 1 \leq a < N$.

We now show that there is a rational number between any two real numbers.

Theorem 1.2.6. *If a and b are real numbers with $a < b$, then there exists a rational number $r = p/q$ such that $a < r < b$.*

Proof. From the Archimedean property of $\mathbb{R}$ (Corollary 1.2.2) there exists $q \in \mathbb{N}$ such that $1/q < b - a$. Now consider the real number qa. By Theorem 1.2.5, there exists an integer p such that $p - 1 \leq qa < p$. It follows that $\frac{p-1}{q} \leq a < \frac{p}{q}$. This implies that $\frac{p}{q} - \frac{1}{q} \leq a$, that is, $a < \frac{p}{q} \leq a + \frac{1}{q} < b$.

Definition 1.2.7. A subset A of $\mathbb{R}$ is said to be *dense* in $\mathbb{R}$ if for any pair of real numbers a and b with $a < b$, there is an $r \in A$ such that $a < r < b$.

Corollary 1.2.8. *The rational numbers are dense in the real numbers.*

How do the irrational numbers behave?

Exercise 1.2.9.

(i) Show that any irrational number multiplied by any nonzero rational number is irrational.
(ii) Show that the product of two irrational numbers may be rational or irrational.

Next we show that there is an irrational number between any two real numbers.

Corollary 1.2.10. *The irrational numbers are dense in $\mathbb{R}$.*

Proof. Take $a, b \in \mathbb{R}$ such that $a < b$. We know that $\sqrt{2}$ is irrational and greater than 0. But then $\frac{a}{\sqrt{2}} < \frac{b}{\sqrt{2}}$. By Corollary 1.2.8, there exists a rational number p/q with $p \neq 0$ such that $\frac{a}{\sqrt{2}} < \frac{p}{q} < \frac{b}{\sqrt{2}}$. Thus $a < \sqrt{2}p/q < b$, and $\sqrt{2}p/q$ is irrational.

The real numbers are the union of two disjoint sets, the rational numbers and the irrational numbers, and each of these sets is dense in $\mathbb{R}$. Density implies nothing about cardinality since the rationals are countable and the irrationals are not, as shown in Appendix A.

1.3. Rational Approximation

We have just shown that both the rational numbers and the irrational numbers are dense in the real numbers. But, really, how dense are they? It is reasonable to think that proximity for rational numbers can be measured in terms of the size of the denominator. To illustrate this, we ask the question, "How close do two rational numbers have to be in order to be the same rational number?" This is not a trick question—it is designed to illustrate the principle mentioned above. In particular, if $a/b, c/d \in \mathbb{Q}$ and $|a/b - c/d| < 1/bd$, then $a/b = c/d$.

This idea can be encapsulated in the following theorem. Throughout this section, we shall assume that the denominator of a rational number is a positive integer and that the numerator and denominator are relatively prime.

THEOREM 1.3.1. *If a/b is a fixed rational number and p/q is a rational number such that $0 < |p/q - a/b| < 1/mb$ for some positive integer m, then $q > m$.*

Proof. Easy.

We now present several facts on rational approximation. For α in various subsets of the real numbers, we prove results which give an idea of the degree of accuracy with which α may be approximated. The results take the following form: Given a real number α,

(1) positive real numbers $c(\alpha)$ and t exist so that there are infinitely many rational numbers p/q with $|\alpha - p/q| < c(\alpha)/q^t$;
(2) positive real numbers $c(\alpha)$ and t exist so that there are only finitely many rational numbers p/q with $|\alpha - p/q| < c(\alpha)/q^t$;
(3) for $\delta > 0$, there exist real numbers $c(\alpha, \delta)$ and t so that $|\alpha - p/q| \geq c(\alpha, \delta)/q^{t+\delta}$ for all rational numbers p/q.

To begin, we present an exercise which follows easily from elementary number theory.

EXERCISE 1.3.2. Let a and b be relatively prime integers. Show that the equation $ax + by = 1$ has infinitely many solutions (x, y) with x and y relatively prime.

THEOREM 1.3.3. *Let $\alpha = a/b$ with a and b relatively prime and $b \neq 1$. Then there exist infinitely many $p/q \in \mathbb{Q}$ such that $|a/b - p/q| < 1/q$.*

Proof. Let $(x, y) = (q, -p)$ be a solution to the equation $ax + by = 1$. Then $q \neq 0$ since $b \neq 1$. We may assume $q > 0$. We then have $|a/b - p/q| = 1/bq < 1/q$.

REMARK 1.3.4. If $b = 1$, then the same result holds with $<$ replaced by $\leq$.

The next theorem characterizes rational numbers in terms of rational approximation. We first need the following exercise.

EXERCISE 1.3.5. Let α be a real number, and let η and t be positive real numbers. Show that there exists only a finite number of rational numbers p/q with $q < \eta$ which satisfy $|\alpha - p/q| < 1/q^t$.

THEOREM 1.3.6. *Let $\alpha = a/b \in \mathbb{Q}$. Then there are only finitely many p/q so that $|a/b - p/q| \leq 1/q^2$.*

Proof. Suppose there are infinitely many p/q satisfying the inequality. Then by the exercise above, q gets arbitrarily large. Thus there exists a p/q with $q > b$ such that $|a/b - p/q| < 1/q^2$. This implies that $|aq - bp| < b/q < 1$, which is a contradiction.

We next consider rational approximation of irrational numbers. The question is, "If α is irrational, are there any rational numbers p/q satisfying the inequality $|\alpha - p/q| < 1/q^2$?" The affirmative answer follows from a theorem of Dirichlet on rational approximation of any real number.

THEOREM 1.3.7 **(Dirichlet)**. *Let α be a real number and n a positive integer. Then there is a rational number p/q with $0 < q \leq n$ satisfying the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(n+1)q}.$$

Proof. If $n = 1$, then $p/q = [\alpha]$ or $p/q = [\alpha + 1]$ satisfies $|\alpha - p/q| \leq 1/2$. Suppose that $n \geq 2$. Consider the $n + 2$ numbers

$$0, \alpha - [\alpha], 2\alpha - [2\alpha], \ldots, n\alpha - [n\alpha], 1$$

in the interval $[0, 1]$. Assume that the numbers in our list are distinct, which is the case if α is irrational. By the pigeonhole principle, two of the numbers differ in absolute value by at most $1/(n+1)$. If one of the numbers is 0 and the other is $i\alpha - [i\alpha]$, then $i \leq n$, $|i\alpha - [i\alpha]| \leq 1/(n+1)$, and

$$\left|\alpha - \frac{[i\alpha]}{i}\right| \leq \frac{1}{(n+1)i}.$$

After $[i\alpha]/i$ is reduced to lowest terms p/q, the rational number p/q satisfies the required inequality. Similarly, if the two numbers are $j\alpha - [j\alpha]$ and 1, then $j \leq n$, and reducing $([j\alpha] + 1)/j$ to lowest terms p/q, we have p/q satisfies the required inequality. Finally, if the two numbers are $i\alpha - [i\alpha]$ and $j\alpha - [j\alpha]$, where $i < j$, then

$$|j\alpha - [j\alpha] - (i\alpha - [i\alpha])| = |(j - i)\alpha + ([j\alpha] - [i\alpha])| \leq \frac{1}{n+1}.$$

Then, $j - i < n$, and

$$\left|\alpha - \frac{[j\alpha] - [i\alpha]}{j - i}\right| \leq \frac{1}{(n+1)(j-i)}.$$

Thus, after $([j\alpha] - [i\alpha])/(j - i)$ is reduced to lowest terms p/q, the rational number p/q satisfies the inequality. In the event that the $n+2$ numbers are not distinct, then α itself is a rational number with denominator at most n. For this case, either there exists $1 \leq i \leq n$ so that

$$\alpha = \frac{[i\alpha]}{i}$$

or there exist $1 \leq i < j \leq n$ so that

$$\alpha = \frac{[j\alpha] - [i\alpha]}{j - i}.$$

Thus, if the numbers are not distinct, the required inequality is trivially satisfied by α itself.

COROLLARY 1.3.8. *Given any real number α, there is a rational number p/q such that $|\alpha - p/q| < 1/q^2$.*

Proof. This follows immediately from the theorem.

Now comes the good news (or bad news depending on how you look at it).

THEOREM 1.3.9. *If α is irrational, then there are infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^2$.*

Proof. Suppose there are only a finite number of rational numbers p_1/q_1, $p_2/q_2, \ldots, p_k/q_k$ satisfying the inequality. Then, there is a positive integer n such that $|\alpha - p_i/q_i| > 1/(n+1)q_i$ for $i = 1, 2, \ldots, k$. This contradicts Theorem 1.3.7, which asserts the existence of a rational number p/q satisfying $q \leq n$ and $|\alpha - p/q| < 1/(n+1)q < 1/q^2$.

So, there you have it, a real number α is rational if and only if there exists only a finite number of rational numbers p/q such that $|\alpha - p/q| \leq 1/q^2$. Moreover, a real number α is irrational if and only if there exists an infinite number of rational numbers p/q such that $|\alpha - p/q| \leq 1/q^2$.

1.4. Intervals

At this stage we single out certain subsets of $\mathbb{R}$ which are called intervals.

DEFINITION 1.4.1. A subset of $\mathbb{R}$ is an *interval* if it falls into one of the following categories.

(a) For $a, b \in \mathbb{R}$ with $a < b$, the *open interval* (a, b) is defined by $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.
(b) For $a, b \in \mathbb{R}$ with $a \leq b$, the *closed interval* $[a, b]$ is defined by $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.
(c) For $a, b \in \mathbb{R}$ with $a < b$, the *half-open interval* $[a, b)$ is defined by $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$.
(d) For $a, b \in \mathbb{R}$ with $a < b$, the *half-open interval* $(a, b]$ is defined by $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$.
(e) For $a \in \mathbb{R}$, the *infinite open interval* (a, ∞) is defined by $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$.
(f) For $b \in \mathbb{R}$, the *infinite open interval* $(-\infty, b)$ is defined by $(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$.
(g) For $a \in \mathbb{R}$, the *infinite closed interval* $[a, \infty)$ is defined by $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$.

(h) For $b \in \mathbb{R}$, the *infinite closed interval* $(-\infty, b]$ is defined by $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$.
(i) $\mathbb{R} = (-\infty, \infty)$.

DEFINITION 1.4.2. If $x \in \mathbb{R}$, a *neighborhood* of x is an open interval containing x. In many instances, it is helpful to use symmetric neighborhoods. That is, if $x \in \mathbb{R}$, a *symmetric neighborhood* of x is an interval of the form $(x - \varepsilon, x + \varepsilon)$, where $\varepsilon > 0$.

These intervals, and their counterparts in other spaces, are used extensively throughout analysis.

EXERCISE 1.4.3. Suppose that I is a subset of $\mathbb{R}$. Show that I is an interval if and only if for all $a, b \in I$, with $a \leq b$, the closed interval $[a, b] \subseteq I$.

The notion of interval is valid in any ordered field, and we will occasionally find this useful. We end this section with a theorem about intervals in $\mathbb{R}$, which is called the Nested Intervals Theorem.

THEOREM 1.4.4 **(Nested Intervals Theorem)**. *Let $([a_n, b_n])_{n \in \mathbb{N}}$ be a nested sequence of closed bounded intervals in $\mathbb{R}$. That is, for any n we have $[a_{n+1}, b_{n+1}] \subseteq [a_n, b_n]$, or equivalently, $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ for all n. Then $\bigcap_{n \in \mathbb{N}} [a_n, b_n] \neq \varnothing$.*

Proof. Let $A = \{a_n \mid n \in \mathbb{N}\}$. Then A is bounded above by b_1. If $a = \text{lub}A$, then $a \in \bigcap_{n \in \mathbb{N}} [a_n, b_n]$.

The nested intervals property is actually not exclusive to the real numbers. In fact, it is really a theorem about a sequence of nested compact sets in a metric space. This result will be proved in the next chapter. There is often some confusion about the relationship between the Nested Interval Theorem in $\mathbb{R}$ and the least upper bound property. Although our proof in $\mathbb{R}$ involves the least upper bound property, it can be done in alternate ways which involve sequential compactness.

1.5. The Construction of the Real Numbers

We are now ready to proceed with the construction of the real numbers from the rational numbers using the fact that the rational numbers are the field of fractions of $\mathbb{Z}$. We have already defined $\mathbb{R}$ as an ordered field in which the least upper bound property holds. We now proceed to build such a field starting from $\mathbb{Q}$.

Recall that the *absolute value* on $\mathbb{Q}$ is defined as

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

Also recall that the absolute value on $\mathbb{Q}$ satisfies the following three properties.

(1) For any $a \in \mathbb{Q}$, $|a| \geq 0$, and $|a| = 0$ if and only if $a = 0$.
(2) For any $a, b \in \mathbb{Q}$, $|ab| = |a||b|$.
(3) For any $a, b \in \mathbb{Q}$, $|a + b| \leq |a| + |b|$ (triangle inequality).

EXERCISE 1.5.1. Show that, for any $a, b \in \mathbb{Q}$, we have $||a| - |b|| \leq |a - b|$.

DEFINITION 1.5.2. A sequence $(a_k)_{k\in\mathbb{N}}$ of rational numbers is a *Cauchy sequence* in $\mathbb{Q}$ if, given any rational number $r > 0$, there exists an integer N such that if $n, m \geq N$, then $|a_n - a_m| < r$.

DEFINITION 1.5.3. A sequence $(a_k)_{k\in\mathbb{N}}$ *converges in* $\mathbb{Q}$ to $a \in \mathbb{Q}$ if, given any rational number $r > 0$, there exists an integer N such that if $n \geq N$, then $|a_n - a| < r$. Sometimes, we just say that the sequence $(a_k)_{k\in\mathbb{N}}$ converges in $\mathbb{Q}$ without mentioning the *limit* a.

EXERCISE 1.5.4. If a sequence $(a_k)_{k\in\mathbb{N}}$ converges in $\mathbb{Q}$, show that $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}$. In addition, show also that the limit a of a convergent sequence is unique.

DEFINITION 1.5.5. Let $(a_k)_{k\in\mathbb{N}}$ be a sequence of rational numbers. We say that $(a_k)_{k\in\mathbb{N}}$ is a *bounded sequence* if the set $\{a_k \mid k \in \mathbb{N}\}$ is a bounded set in $\mathbb{Q}$.

LEMMA 1.5.6. *Let $(a_k)_{k\in\mathbb{N}}$ be a Cauchy sequence of rational numbers. Then $(a_k)_{k\in\mathbb{N}}$ is a bounded sequence.*

Proof. Let $(a_k)_{k\in\mathbb{N}}$ be a Cauchy sequence of rational numbers. Pick $N \in \mathbb{N}$ such that $|a_n - a_m| < 1$ for $n, m \geq N$. Then $|a_n - a_N| < 1$ for all $n \geq N$, so that $|a_n| < 1 + |a_N|$ for all $n \geq N$. Let M be the max of $|a_1|, |a_2|, \ldots, |a_{N-1}|, 1 + |a_N|$. Then $(|a_k|)_{k\in\mathbb{N}}$ is bounded by M.

Let $\mathcal{C}$ denote the set of all Cauchy sequences of rational numbers. We define addition and multiplication of Cauchy sequences termwise; that is, $(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} = (a_k + b_k)_{k\in\mathbb{N}}$ and $(a_k)_{k\in\mathbb{N}}(b_k)_{k\in\mathbb{N}} = (a_k b_k)_{k\in\mathbb{N}}$.

EXERCISE 1.5.7. Show that the sum of two Cauchy sequences in $\mathbb{Q}$ is a Cauchy sequence in $\mathbb{Q}$.

THEOREM 1.5.8. *The product of two Cauchy sequences in $\mathbb{Q}$ is a Cauchy sequence in $\mathbb{Q}$.*

Proof. Let $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$ be Cauchy sequences in $\mathbb{Q}$. Then

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_n b_m + a_n b_m - a_m b_m| \\ &\leq |a_n||b_n - b_m| + |b_m||a_n - a_m| \\ &\leq A|b_n - b_m| + B|a_n - a_m|, \end{aligned}$$

where A and B are upper bounds for the sequences $(|a_k|)_{k\in\mathbb{N}}$ and $(|b_k|)_{k\in\mathbb{N}}$. Since $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$ are Cauchy sequences, the theorem now follows.

Exercise 1.5.9. Show that, with addition and multiplication defined as above, $\mathcal{C}$ is a commutative ring with 1 (see Appendix A).

Now let $\mathcal{I}$ be the subset of $\mathcal{C}$ consisting of sequences $(a_k)_{k\in\mathbb{N}}$ with the property that, given any rational $r > 0$, there exists an integer N such that if $n \geq N$, then $|a_n| < r$. The set $\mathcal{I}$ consists of Cauchy sequences which converge to 0.

Suppose $(a_k)_{k\in\mathbb{N}} \notin \mathcal{I}$. Then there exists an $r > 0$ such that $|a_k| \geq r$ infinitely often. Pick $N \in \mathbb{N}$ such that $|a_n - a_m| < r/2$ for $n, m \geq N$. This implies that

$$|a_n| > |a_m| - \frac{1}{2}r \quad \text{for } n, m \geq N.$$

Fix an $m \geq N$ for which $|a_m| \geq r$. Then for all $n \geq N$, we have

$$|a_n| > \frac{1}{2}r.$$

Thus, Cauchy sequences which do not converge to 0 are eventually bounded below (in absolute value) by some positive constant.

Exercise 1.5.10. Show that if a Cauchy sequence does not converge to 0, all the terms of the sequence eventually have the same sign.

Definition 1.5.11. Let $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$ be Cauchy sequences in $\mathbb{Q}$. We say that $(a_k)_{k\in\mathbb{N}}$ is *equivalent to* $(b_k)_{k\in\mathbb{N}}$, denoted by $(a_k)_{k\in\mathbb{N}} \sim (b_k)_{k\in\mathbb{N}}$, if $(c_k)_{k\in\mathbb{N}} = (a_k - b_k)_{k\in\mathbb{N}}$ is in $\mathcal{I}$.

Exercise 1.5.12. Show that $\sim$ defines an equivalence relation on $\mathcal{C}$.

Exercise 1.5.13. Given $a \in \mathbb{Q}$, show that the collection of Cauchy sequences in $\mathcal{C}$ converging to a is an equivalence class. In particular, $\mathcal{I}$ is an equivalence class.

Denote by $\mathbf{R}$ the set of equivalence classes in $\mathcal{C}$. We claim that, with appropriate definitions of addition and multiplication (already indicated above) and order (to be defined below), $\mathbf{R}$ is an ordered field satisfying the least upper bound property.

If $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence, denote its equivalence class by $[a_k]$. As one might expect, the sum and product of equivalence classes are defined as follows: $[a_k] + [b_k] = [a_k + b_k]$ and $[a_k][b_k] = [a_k b_k]$.

Exercise 1.5.14. Show that addition and multiplication are well-defined on $\mathbf{R}$.

Exercise 1.5.15. Show that $\mathbf{R}$ is a commutative ring with 1, with $\mathcal{I}$ as the additive identity and $[a_k]$ such that $a_k = 1$ for all k as the multiplicative identity. This follows easily from Exercise 1.5.9.

THEOREM 1.5.16. **R** *is a field.*

Proof. We need only show that multiplicative inverses exist for nonzero elements. So assume that $[a_k] \neq \mathcal{I}$. Then, as we saw above, a_k is eventually bounded below in absolute value. Hence, we can pick $M \in \mathbb{N}$ and $c > 0$ such that $|a_k| > c$ for all $k \geq M$. Define a sequence $(b_k)_{k \in \mathbb{N}}$ as follows: $b_k = 1$ for $k \leq M$, and $b_k = 1/a_k$ for $k > M$. Observe that for n, m large enough

$$\left| \frac{1}{a_n} - \frac{1}{a_m} \right| = \frac{|a_n - a_m|}{|a_n a_m|} \leq \frac{|a_n - a_m|}{c^2}.$$

So $(b_k)_{k \in \mathbb{N}}$ is a Cauchy sequence and $[b_k]$ is the multiplicative inverse of $[a_k]$.

The next step is to define order on **R**. Let $[a_k]$ and $[b_k]$ represent distinct elements of **R**. Then $[c_k] = [a_k - b_k]$ is not equal to $\mathcal{I}$. Hence there exists $N \in \mathbb{N}$ such that all the terms of c_k have the same sign for $k > N$. Thus, either $a_k < b_k$ for all $k \geq N$ or $b_k < a_k$ for $k \geq N$. We use this fact to define an order on **R**.

DEFINITION 1.5.17. Let $a = [a_k], b = [b_k]$ be distinct elements of **R**. We define $a < b$ if $a_k < b_k$ eventually and $b < a$ if $b_k < a_k$ eventually.

EXERCISE 1.5.18. Show that the order relation on **R** defined above is well-defined and makes **R** an ordered field.

To finish this, we must show that **R** is an Archimedean ordered field that satisfies the least upper bound property. We will then have reached the mountain top so we can dismount the funicular and ski happily down the slope.

Define a map $i : \mathbb{Q} \longrightarrow \mathbf{R}$ by sending $r \in \mathbb{Q}$ to the equivalence class of $(r, r, \dots)$. It is evident that this map is injective and order-preserving, so we may consider $\mathbb{Q} \subseteq \mathbf{R}$ as ordered fields.

THEOREM 1.5.19. *The field* **R** *is an Archimedean ordered field.*

Proof. Suppose $a \in \mathbf{R}$ and $a > 0$. Let $(a_k)_{k \in \mathbb{N}}$ represent a. As noted above, the Cauchy sequence $(a_k)_{k \in \mathbb{N}}$ is bounded above by some integer N; that is, $a_k < N$ for all sufficiently large k. It follows that a is less than the integer $(N, N, \dots)$ in **R** (under the inclusion $\mathbb{Q} \subseteq \mathbf{R}$).

THEOREM 1.5.20. *The least upper bound property holds in* **R**.

Proof. Let A be a nonempty subset of **R** that is bounded above by, say, m. Then, by the Archimedean property, we can find $M \in \mathbb{Z}$ with $m \leq M$. Let a be in A and let n be an integer with $n < a$. For $p \in \mathbb{N}$ set $S_p = \{k2^{-p} \mid k \in \mathbb{Z} \text{ and } n \leq k2^{-p} \leq M\} \cup \{m\}$. Note that $S_p \neq \varnothing$ and is finite. Now let $a_p = \min\{x \mid x \in S_p \text{ and } x \text{ is an upper bound for } A\}$.

Note that if $p < q$, then

$$a_p - 2^{-p} < a_q \leq a_p,$$

since, for example, $a_p - 2^{-p}$ is not an upper bound for A, while a_q is an upper bound. But this implies that

$$|a_p - a_q| \leq 2^{-p} \quad \text{for all } p < q,$$

from which it follows that $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence. Let $L = [a_k]$.

We claim that L is a least upper bound for A. Suppose $x \in A$ and $x > L$. Choose p such that $2^{-p} < (x - L)$ (using the Archimedean property). Since $a_p - 2^{-p} < a_q$ for $p < q$ and $(a_p)_{p\in\mathbb{N}}$ is a decreasing Cauchy sequence, it follows that $a_p - 2^{-p} \leq L \leq a_p$. In particular, if we add $2^{-p} < x - L$ and $a_p - 2^{-p} \leq L$, we obtain $a_p < x$, which is a contradiction. Therefore L is an upper bound for A.

Suppose that H is an upper bound for A and that $H < L$. Choose p such that $2^{-p} < L - H$. Take $x \in A$ such that $a_p - 2^{-p} < x$. Then $a_p - 2^{-p} < H$. Adding, we get $a_p < L$. But, as noted above, $L \leq a_p$ for all $p \in \mathbb{N}$, so this is a contradiction.

EXERCISE 1.5.21. Prove that $\mathbf{R}$ is order-isomorphic to $\mathbb{R}$. (Hint: You have already done this.)

1.6. Convergence in $\mathbb{R}$

We define the absolute value on $\mathbb{R}$ in exactly the same manner as on $\mathbb{Q}$.

DEFINITION 1.6.1. Suppose $x \in \mathbb{R}$. The *absolute value* of x is defined by

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

The following are the essential properties of the absolute value.

THEOREM 1.6.2 **(Properties of the absolute value on $\mathbb{R}$).**

(1) *For any $x \in \mathbb{R}$, $|x| \geq 0$, and $|x| = 0$ iff $x = 0$.*
(2) *For any $x, y \in \mathbb{R}$, $|xy| = |x||y|$.*
(3) *For any $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$ (triangle inequality).*

EXERCISE 1.6.3. Prove these properties of the absolute value.

With absolute value defined, we can talk about Cauchy and convergent sequences in $\mathbb{R}$.

DEFINITION 1.6.4. A sequence $(a_k)_{k\in\mathbb{N}}$ of real numbers is *convergent* if there exists an element $a \in \mathbb{R}$ such that the sequence satisfies the following property: given any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $k \geq N$ implies that $|a_k - a| < \varepsilon$. We say that $(a_k)_{k\in\mathbb{N}}$ *converges to* a, and a is called the *limit* of the sequence $(a_k)_{k\in\mathbb{N}}$. Symbolically, we write

$$\lim_{k\to\infty} a_k = a.$$

We will often say that a sequence of real numbers is convergent without specific reference to the limit a. Note that N depends on ε.

EXERCISE 1.6.5. Show that the limit a of a convergent sequence is unique.

DEFINITION 1.6.6. A sequence $(a_k)_{k\in\mathbb{N}}$ of real numbers is *monotonic increasing* if $a_k \leq a_{k+1}$ for all $k \in \mathbb{N}$. A sequence $(a_k)_{k\in\mathbb{N}}$ of real numbers is *strictly monotonic increasing* if $a_k < a_{k+1}$ for all $k \in \mathbb{N}$. Monotonic decreasing and strictly monotonic decreasing sequences are defined similarly.

EXERCISE 1.6.7. Define the notion of a bounded sequence in $\mathbb{R}$.

The following lemma is one of the more useful lemmas in discussing convergence in $\mathbb{R}$ (and $\mathbb{R}^n$).

LEMMA 1.6.8. *Let $(a_k)_{k\in\mathbb{N}}$ be a sequence in $\mathbb{R}$. Then $(a_k)_{k\in\mathbb{N}}$ has a monotonic subsequence.*

Proof. Suppose $(a_k)_{k\in\mathbb{N}}$ does not have a monotonic increasing subsequence. Then, there exists $n_1 \in \mathbb{N}$ such that $a_{n_1} > a_k$ for all $k > n_1$. Again, since $(a_k)_{k>n_1}$ does not have a monotonic increasing subsequence, there exists $n_2 > n_1$ such that $a_{n_2} > a_k$ for all $k > n_2$. Moreover $a_{n_1} > a_{n_2}$. Continuing in this way, we obtain a strictly monotonic decreasing subsequence.

LEMMA 1.6.9. *Every bounded monotonic sequence converges in $\mathbb{R}$.*

Proof. Suppose $(a_k)_{k\in\mathbb{N}}$ is monotonic increasing and bounded. Let a be the least upper bound of the set $\{a_1, a_2, \ldots\}$. For all $\varepsilon > 0$, there exists an N such that $a - \varepsilon < a_N \leq a$. Since $(a_k)_{k\in\mathbb{N}}$ is increasing, if $k > N$, we have $a \geq a_k \geq a_N > a - \varepsilon$. So $\lim_{k\to\infty} a_k = a$.

The next lemma is basic for analysis on $\mathbb{R}$.

LEMMA 1.6.10. *Every bounded sequence in $\mathbb{R}$ has a convergent subsequence.*

EXERCISE 1.6.11. Prove Lemma 1.6.10. This should not take long.

The next definition should be compared with Definition 1.5.2.

DEFINITION 1.6.12. A sequence $(a_k)_{k\in\mathbb{N}}$ in $\mathbb{R}$ is a *Cauchy sequence* if, given any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $n, m \geq N$ implies $|a_m - a_n| < \varepsilon$.

EXERCISE 1.6.13.

(i) Prove that every Cauchy sequence in $\mathbb{R}$ is bounded.
(ii) If $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}$, show that for any $\varepsilon > 0$ there exists a subsequence $(a_j)_{j\in\mathbb{N}}$ so that $|a_j - a_{j+1}| < \varepsilon/2^{j+1}$.

THEOREM 1.6.14 **(Cauchy criterion)**. *A sequence $(a_k)_{k\in\mathbb{N}}$ of real numbers is convergent if and only if it is a Cauchy sequence.*

Proof. We already did half of this in $\mathbb{Q}$, but we will do it again. First, we prove that if $(a_k)_{k\in\mathbb{N}}$ is convergent, then it is Cauchy. Suppose $\lim_{k\to\infty} a_k =$

a. Then, since the sequence converges, given $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $|a_n - a| < \frac{\varepsilon}{2}$ for all $n \geq N$. Thus, if $n, m \geq N$, we have

$$|a_n - a_m| \leq |a_n - a| + |a_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

and so $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence.

Suppose now that $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}$. Then, by Exercise 1.6.13, $(a_k)_{k\in\mathbb{N}}$ is a bounded sequence and hence by Lemma 1.6.10 has a convergent subsequence. Call the limit of this subsequence a. Then, since $(a_k)_{k\in\mathbb{N}}$ is Cauchy, it is clear that $\lim_{k\to\infty} a_k = a$.

Exercise 1.6.15. Show that if $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are Cauchy sequences in $\mathbb{R}$, then $(a_n + b_n)_{n\in\mathbb{N}}$ and $(a_n \cdot b_n)_{n\in\mathbb{N}}$ are Cauchy sequences in $\mathbb{R}$.

Definition 1.6.16. Let S be a subset of $\mathbb{R}$. Then $x \in \mathbb{R}$ is an *accumulation point* of S if, for all $\varepsilon > 0$, we have $((x-\varepsilon, x+\varepsilon) \setminus \{x\}) \cap S \neq \varnothing$.

Remark 1.6.17. Thus, x is an accumulation point of S if every interval around x contains points of S other than x. Of course, x does not have to be an element of S in order to be an accumulation point of S.

Exercise 1.6.18. Find the accumulation points of the following sets:

(i) $S = (0, 1)$;
(ii) $S = \{(-1)^n + \frac{1}{n} \mid n \in \mathbb{N}\}$;
(iii) $S = \mathbb{Q}$;
(iv) $S = \mathbb{Z}$;
(v) S is the set of rational numbers whose denominators are prime.

Lemma 1.6.19. *Let S be a subset of $\mathbb{R}$. Then every neighborhood of an accumulation point of S contains infinitely many points of S.*

Proof. Let x be an accumulation point of S. Given $\varepsilon > 0$, there is a point $x_1 \in (x-\varepsilon, x+\varepsilon) \cap S$ such that $x_1 \neq x$. Let $\varepsilon_1 = |x - x_1|$. Then, there is a point $x_2 \in (x-\varepsilon_1, x+\varepsilon_1) \cap S$ such that $x_2 \neq x$. Iterating this procedure, we get an infinite set of elements in S which is contained in $(x-\varepsilon, x+\varepsilon)$.

Now here is a big-time theorem!

Theorem 1.6.20 **(Bolzano-Weierstrass)**. *Let S be a bounded, infinite subset of $\mathbb{R}$. Then S has an accumulation point.*

Proof. Pick an infinite sequence $(a_k)_{k\in\mathbb{N}}$ of distinct elements of S. Then, by Lemma 1.6.10, $(a_k)_{k\in\mathbb{N}}$ has a convergent subsequence, $(b_j)_{j\in\mathbb{N}}$. If $\lim_{j\to\infty} b_j = b$, then b is an accumulation point of S.

Exercise 1.6.21.

(i) Find an infinite subset of $\mathbb{R}$ which does not have an accumulation point.
(ii) Find a bounded subset of $\mathbb{R}$ which does not have an accumulation point.

DEFINITION 1.6.22. Let S be a subset of $\mathbb{R}$. We say that S is an *open set* in $\mathbb{R}$ if, for each point $x \in S$, there is an $\varepsilon > 0$ (depending on x) such that $(x - \varepsilon, x + \varepsilon) \subseteq S$.

DEFINITION 1.6.23. Let $S \subseteq \mathbb{R}$. We say S is a *closed set* in $\mathbb{R}$ if the complement of S is an open set in $\mathbb{R}$.

Note that the empty set and $\mathbb{R}$ are both open and closed subsets of $\mathbb{R}$.

EXERCISE 1.6.24. (i) Show that $\varnothing$ and $\mathbb{R}$ are the only subsets of $\mathbb{R}$ which are both open and closed in $\mathbb{R}$.

(ii) Show that every nonempty open set in $\mathbb{R}$ can be written as a countable union of pairwise disjoint open intervals.
(iii) Show that an arbitrary union of open sets in $\mathbb{R}$ is open in $\mathbb{R}$.
(iv) Show that a finite intersection of open sets in $\mathbb{R}$ is open in $\mathbb{R}$.
(v) Show, by example, that an infinite intersection of open sets is not necessarily open.
(vi) Show that an arbitrary intersection of closed sets in $\mathbb{R}$ is a closed set in $\mathbb{R}$.
(vii) Show that a finite union of closed sets in $\mathbb{R}$ is a closed set in $\mathbb{R}$.
(viii) Show, by example, that an infinite union of closed sets in $\mathbb{R}$ is not necessarily a closed set in $\mathbb{R}$.

EXERCISE 1.6.25. Show that a subset of $\mathbb{R}$ is closed iff it contains all its accumulation points.

EXERCISE 1.6.26. In this exercise, we define the *Cantor set*. This is a subset of the closed interval $[0, 1]$ constructed as follows. First, remove the open interval $(1/3, 2/3)$ from $[0, 1]$. Next, remove the open intervals $(1/9, 2/9)$ and $(7/9, 8/9)$. At each step, remove the middle third of the remaining closed intervals. Repeating this process a countable number of times, we are left with a subset of the closed interval $[0, 1]$ called the *Cantor set*. Show that:

(i) the Cantor set is closed;
(ii) the Cantor set is uncountable;
(iii) the Cantor set consists of all numbers in the closed interval $[0, 1]$ whose ternary expansion consists of only 0's and 2's and may end in infinitely many 2's;
(iv) every point of the Cantor set is an accumulation point of the Cantor set;
(v) the set $[0, 1] \setminus \{\text{Cantor set}\}$ is a dense subset of $[0, 1]$.

The next theorem, the Heine-Borel theorem for $\mathbb{R}$, is the second of the two basic topological theorems for the real numbers; the other is the Bolzano-Weierstrass theorem. We shall see more details about these two theorems in Chapter 2.

Theorem 1.6.27 **(Heine-Borel)**. *Let S be a closed and bounded subset of $\mathbb{R}$. Given a collection $\{U_i\}_{i\in I}$ of open sets such that $S \subseteq \bigcup_{i\in I} U_i$, there exists a finite subcollection $U_1, \ldots, U_n$ of $\{U_i\}_{i\in I}$ such that $S \subseteq U_1 \cup \cdots \cup U_n$.*

Proof. Suppose that S is a nonempty, closed, bounded subset of $\mathbb{R}$. If $a = \text{glb } S$ and $b = \text{lub } S$, then, since S is closed, a and b are in S, and $S \subseteq [a, b]$. Let $\{U_i\}$ be a collection of open sets such that $S \subseteq \bigcup U_i$. By adjoining the complement of S (if necessary), we obtain a collection $\mathcal{U}$ of open sets whose union contains $[a, b]$.

Now let $B = \{x \in [a, b] \mid [a, x]$ is covered by a finite number of open sets in $\mathcal{U}\}$. Then B is nonempty since $a \in B$, and B is bounded above by b. Let $c = \text{lub } B$. If $c = b$, we are done. If $c < b$, then there exists y such that $c < y < b$ and $[c, y]$ is in the same open set that contains c. Thus $[a, y]$ is covered by the same collection of open sets from $\mathcal{U}$ that covers $[a, c]$. This is a contradiction, and hence b must equal c. Thus $[a, b]$ is covered by a finite number of open sets from $\mathcal{U}$, and by throwing away the complement of S (if necessary), S is covered by a finite number of open sets from the original collection.

Definition 1.6.28. Let A be a subset of $\mathbb{R}$. An *open cover of* A is a collection of open sets $\{U_i\}_{i\in I}$ such that $A \subseteq \bigcup_{i\in I} U_i$.

Definition 1.6.29. Let A be a subset of $\mathbb{R}$. We say that A is a *compact set* if every open covering of A has a finite subcovering. That is, if $\{U_i\}_{i\in I}$ is an open covering of A, then there is a finite subcollection $U_1, U_2, \ldots, U_n$ of the collection $\{U_i\}_{i\in I}$ so that $A \subseteq U_1 \cup U_2 \cup \cdots \cup U_n$.

Definition 1.6.30. A subset A of $\mathbb{R}$ is *sequentially compact* if every infinite sequence in A has a subsequence that converges to an element of A.

Exercise 1.6.31. Show that a subset of $\mathbb{R}$ is compact if and only if it is closed and bounded.

The result in the following exercise can be proved easily using the Bolzano-Weierstrass and Heine-Borel theorems in $\mathbb{R}$. We will see in Chapter 2 that the same theorem is true in metric spaces. In the next section, we give an indication of how this works in $\mathbb{C}$.

Exercise 1.6.32. A subset of $\mathbb{R}$ is compact if and only if it is sequentially compact.

1.7. Automorphisms of Fields

For any field F, we can consider the following problem: given $f : F \longrightarrow F$ such that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in F$, what can you say about f? Well, if $f(x) = 0$ for all $x \in F$, then it clearly has these properties, but it is not of much use. So, let us assume that there exists an $a \in F$ such that $f(a) \neq 0$.

EXERCISE 1.7.1. Under this assumption,

(i) show that $f(1) = 1$, and
(ii) show that f is an injection.
(iii) Must such an f be a surjection?

Consider f satisfying only the additive property above in the case when $F = \mathbb{Q}$. We have

$$f(x) = f(x + 0) = f(x) + f(0),$$

so $f(0) = 0$. Next we have, for $n \in \mathbb{N}$, $f(n) = nf(1)$ and $f(m/n) = (m/n)f(1)$ for any positive rational number m/n. While we are not assuming the multiplicative property here, to avoid the trivial, we assume that there exists an $x \in \mathbb{Q}$, so that $f(x) \neq 0$. From this, it follows that $f(1) \neq 0$. Also, for any positive rational number r, we have $f(-r) = -f(r)$. Thus, $f(r) = rf(1)$ for all $r \in \mathbb{Q}$.

Let us see what happens for $\mathbb{R}$. We assume that $f(1) \neq 0$. We have $f(r) = rf(1)$ for all $r \in \mathbb{Q}$. However, as we point out after the definition of Hamel basis in Appendix B, things go completely awry unless we impose further properties. So, assume that f preserves multiplication, that is $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{R}$. Then, it follows from the above exercise that $f(1) = 1$, and $f(a^{-1}) = f(a)^{-1}$ if $a \neq 0$. The next thing to note here is that if $a \in \mathbb{R}$ and $a \neq 0$, then $a^2 > 0$ and $f(a^2) = (f(a))^2$, so $f(a^2) > 0$. Since all positive real numbers have unique positive square roots, we can conclude that if $c > 0$, then $f(c) > 0$. Thus, if $a < b$, then $f(a) < f(b)$ since $b - a > 0$. Now take any real number c. If $c \in \mathbb{Q}$, then $f(c) = c$. If $c \notin \mathbb{Q}$ and $f(c) \neq c$, then there are two possibilities. If $c < f(c)$, choose a rational number r so that $c < r < f(c)$. Then $f(c) < f(r) = r$, which is a contradiction. If $f(c) < c$, we run into the same problem. So we conclude that f is the identity.

DEFINITION 1.7.2. Let F be a field. An *automorphism of* F is a bijection, $f : F \longrightarrow F$, such that

(a) $f(x + y) = f(x) + f(y)$ for all $x, y \in F$,
(b) $f(xy) = f(x)f(y)$ for all $x, y \in F$.

EXERCISE 1.7.3. If F is a field, show that the automorphisms of F form a group under composition of functions. This group is called *the automorphism group of the field* F and is denoted by $\mathrm{Aut}\,(F)$.

THEOREM 1.7.4. *The groups* $\mathrm{Aut}\,(\mathbb{Q})$ *and* $\mathrm{Aut}\,(\mathbb{R})$ *consist only of the identity map.*

EXERCISE 1.7.5. Find a field F such that $\mathrm{Aut}\,(F) \neq \{1\}$.

EXERCISE 1.7.6.

(i) Let F be a field and let f be an element of $\mathrm{Aut}\,(F)$. Define $H_f = \{x \in F \mid f(x) = x\}$. Show that H_f is a subfield of F.
(ii) Suppose that F is a field and that $\mathbb{Q}$ is a subfield of F. If $f \in \mathrm{Aut}\,(F)$, show that $\mathbb{Q}$ is a subfield of H_f.

EXERCISE 1.7.7.

(i) Find Aut $(\mathbb{F}_p)$ where p is a prime and $\mathbb{Z}_p$ is the finite field with p elements.

(ii) Let $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Show that F is a field and find Aut (F). This is the beginning of the subject called Galois theory, in which one of the goals is to determine Aut (F) when F is a so-called "algebraic extension" of $\mathbb{Q}$.

1.8. Complex Numbers

To start this section, we give a somewhat inexact definition of complex numbers. This is often used as a definition of the complex numbers, but it does contain some ambiguity, which we will rectify immediately.

DEFINITION 1.8.1 **(Rural definition)**. The set of *complex numbers*, $\mathbb{C}$, is the collection of expressions of the form $z = a + bi$ where $a, b \in \mathbb{R}$ and i is a symbol which satisfies $i^2 = -1$. If $z = a + bi$ and $w = c + di$ are in $\mathbb{C}$, then we define $z + w = (a + c) + (b + d)i$ and $zw = (ac - bd) + (bc + ad)i$.

Actually, one can go a long way with this definition if the symbol i with the property that $i^2 = -1$ does not cause insomnia. To be more precise, we consider the Cartesian product $\mathbb{R}\times\mathbb{R}$ with addition defined by $(a, b)+(c, d) = (a + c, b + d)$ and multiplication defined by $(a, b)(c, d) = (ac - bd, bc + ad)$.

EXERCISE 1.8.2. Show that $\mathbb{R} \times \mathbb{R}$ with addition and multiplication as defined above is a field with $(0, 0)$ as the additive identity, $(1, 0)$ as the multiplicative identity, $-(a, b) = (-a, -b)$, and $(a, b)^{-1} = (a/(a^2+b^2), -b/(a^2+b^2))$ if $(a, b) \neq (0, 0)$.

So $\mathbb{R} \times \mathbb{R}$ with these operations forms a field which we denote by $\mathbb{C}$ and call *the field of complex numbers*. Note that $\mathbb{R}$ is isomorphic to the subfield of $\mathbb{C}$ given by $\{(a, 0) \mid a \in \mathbb{R}\}$. If we set $i = (0, 1)$, then $i^2 = (-1, 0)$. Finally, to fix things up really nice, we write $(a, b) = (a, 0)+(b, 0)(0, 1)$, or, returning to our original rural definition, $(a, b) = a + bi$.

The first observation to make is that $\mathbb{C}$ cannot be made into an ordered field. That is, it cannot satisfy the order axioms given in Appendix A. This is immediate because in any ordered field, if $a \neq 0$, then $a^2 > 0$. This would imply that $i^2 = -1 > 0$, but $1^2 = 1 > 0$, and this is a contradiction.

DEFINITION 1.8.3. If $z = a + bi$, we call a the *real part* of z and b the *imaginary part* of z. We write $a = \text{Re } z$ and $b = \text{Im } z$. The complex number z is called *pure imaginary* if $a = \text{Re } z = 0$.

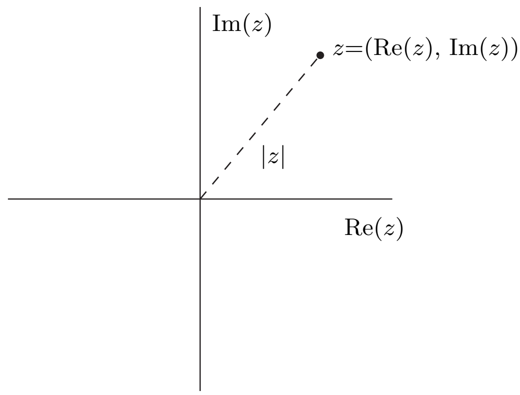
DEFINITION 1.8.4. If $z = a + bi$, the *complex conjugate* of z, denoted $\bar{z}$, is $\bar{z} = a - bi$. The *absolute value* of z is

$$|z| = (z\bar{z})^{\frac{1}{2}} = (a^2 + b^2)^{\frac{1}{2}},$$

where, of course, we mean the nonnegative square root in $\mathbb{R}$.

If z and w are complex numbers, then $|z|, |w| \in \mathbb{R}$ and hence it makes sense to say that $|z| < |w|$. However, it makes no sense to say that $z < w$.

EXERCISE 1.8.5. Show that if we identify $z = a + bi$ with the point $(a, b) \in \mathbb{R}^2$, then the absolute value of z is equal to the distance of the point (a, b) from $(0, 0)$.



EXERCISE 1.8.6. Show that the absolute value on $\mathbb{C}$ satisfies all the properties of the absolute value on $\mathbb{R}$.

(i) For any $z \in \mathbb{C}$, we have $|z| \geq 0$, and $|z| = 0$ iff $z = 0$.
(ii) For any $z, w \in \mathbb{C}$, we have $|zw| = |z||w|$.
(iii) For any $z, w \in \mathbb{C}$, we have $|z + w| \leq |z| + |w|$ (triangle inequality).

EXERCISE 1.8.7. Show that the field of complex numbers is not isomorphic to the field of real numbers.

1.9. Convergence in $\mathbb{C}$

Now that we have an absolute value on $\mathbb{C}$, we can define the notions of Cauchy sequence and convergent sequence in $\mathbb{C}$.

DEFINITION 1.9.1. A sequence $(z_k)_{k\in\mathbb{N}}$ of complex numbers is *convergent* if there exists an element $z \in \mathbb{C}$ such that the sequence satisfies the following property: given any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $k \geq N$ implies that $|z_k - z| < \varepsilon$. We say that $(z_k)_{k\in\mathbb{N}}$ *converges to* z, and z is called the *limit* of the sequence $(z_k)_{k\in\mathbb{N}}$. Symbolically, we write

$$\lim_{k\to\infty} z_k = z.$$

We will often say that a sequence of complex numbers is convergent without specific reference to the limit z. Note that N depends on ε. As usual, the limit of a convergent sequence is unique.

DEFINITION 1.9.2. Let r be a positive real number, and let $z_0 \in \mathbb{C}$. The *open ball* of radius r with center at z_0 is

$$B_r(z_0) = \{z \in \mathbb{C} \mid |z - z_0| < r\}. \tag{1.1}$$

The *closed ball* of radius r with center z_0 is

$$\bar{B}_r(z_0) = \{z \in \mathbb{C} \mid |z - z_0| \leq r\}. \tag{1.2}$$

The open balls and closed balls in $\mathbb{C}$ are the analogs of open and closed intervals in $\mathbb{R}$. We can define open and closed sets in $\mathbb{C}$ in a fashion similar to the definitions in $\mathbb{R}$.

Definition 1.9.3. Let S be a subset of $\mathbb{C}$. We say that S is an *open set* in $\mathbb{C}$ if, for each point $z \in S$, there is an $\varepsilon > 0$ (depending on z) such that $B_\varepsilon(z) \subseteq S$.

Definition 1.9.4. Let S be a subset of $\mathbb{C}$. We say that S is a *closed set* in $\mathbb{C}$ if the complement of S is an open set in $\mathbb{C}$.

Note that the empty set and $\mathbb{C}$ are both open and closed subsets of $\mathbb{C}$.

Exercise 1.9.5. (i) Show that $\varnothing$ and $\mathbb{C}$ are the only subsets of $\mathbb{C}$ which are both open and closed in $\mathbb{C}$.

(ii) Show that every open set in $\mathbb{C}$ can be written as a countable union of open balls.

(iii) Show, by example, that there are open sets in $\mathbb{C}$ for which the open balls in (ii) cannot be made pairwise disjoint.

(iv) Show that an arbitrary union of open sets in $\mathbb{C}$ is an open set in $\mathbb{C}$.

(v) Show that a finite intersection of open sets in $\mathbb{C}$ is an open set in $\mathbb{C}$.

(vi) Show, by example, that an infinite intersection of open sets in $\mathbb{C}$ need not be an open set in $\mathbb{C}$.

(vii) Show that an arbitrary intersection of closed sets in $\mathbb{C}$ is a closed set in $\mathbb{C}$.

(viii) Show that a finite union of closed sets in $\mathbb{C}$ is a closed set in $\mathbb{C}$.

(ix) Show, by example, that an infinite union of closed sets in $\mathbb{C}$ is not necessarily a closed set in $\mathbb{C}$.

Exercise 1.9.6. Consider the collection of open balls $\{B_r(z)\}$ in $\mathbb{C}$ where $r \in \mathbb{Q}$ and where $\operatorname{Re} z$ and $\operatorname{Im} z \in \mathbb{Q}$. Show that any open set in $\mathbb{C}$ can be written as a finite or countable union from this collection of sets.

Definition 1.9.7. Let $A \subseteq \mathbb{C}$. The set A is *bounded* if there exists $r > 0$ such that $A \subseteq B_r(0)$.

Exercise 1.9.8. Define the notion of a bounded sequence in $\mathbb{C}$.

Definition 1.9.9 (See Definition 1.6.12). A sequence $(z_k)_{k\in\mathbb{N}}$ in $\mathbb{C}$ is a *Cauchy sequence* if, given any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $n, m \geq N$ implies $|z_n - z_m| < \varepsilon$.

Exercise 1.9.10. Prove that every Cauchy sequence in $\mathbb{C}$ is bounded.

Theorem 1.9.11 **(Cauchy criterion)**. *A sequence $(z_k)_{k\in\mathbb{N}}$ of complex numbers is convergent if and only if it is a Cauchy sequence.*

Proof. The first half of the proof is identical to the proof of Theorem 1.6.14.

Suppose now that $(z_k)_{k\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{C}$. Let $z_k = a_k + b_k i$, where $a_k, b_k \in \mathbb{R}$. Then $|z_m - z_n|^2 = (a_m - a_n)^2 + (b_m - b_n)^2$. It follows immediately that $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$ are Cauchy sequences in $\mathbb{R}$. If $\lim_{k\to\infty} a_k = a$ and $\lim_{k\to\infty} b_k = b$, then $\lim_{k\to\infty} z_k = z$ where $z = a + bi$.

Exercise 1.9.12. Show that every bounded sequence in $\mathbb{C}$ has a convergent subsequence.

Definition 1.9.13. Let S be a subset of $\mathbb{C}$. Then z is an *accumulation point* of S if, for all $\varepsilon > 0$, we have $(B_\varepsilon(z) \setminus \{z\}) \cap S \neq \varnothing$.

Remark 1.9.14. Thus, z is an accumulation point of S if every open ball around z contains points of S other than z. Of course, z does not have to be an element of S in order to be an accumulation point of S.

Exercise 1.9.15. Find the accumulation points of the following sets:

(i) $S = \{z \in \mathbb{C} \mid |z| = 1\}$ (this is the *unit circle in* $\mathbb{C}$);
(ii) $S = \{z \in \mathbb{C} \mid \operatorname{Re} z > \operatorname{Im} z\}$;
(iii) $S = \{a + bi \mid a, b \in \mathbb{Q}\}$;
(iv) $S = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Exercise 1.9.16.

(i) Let S be a subset of $\mathbb{C}$. Show that every neighborhood of an accumulation point of S contains infinitely many points of S.
(ii) (Bolzano-Weierstrass theorem for $\mathbb{C}$) Prove that any bounded infinite set in $\mathbb{C}$ has an accumulation point in $\mathbb{C}$.

Theorem 1.9.17 **(Heine-Borel)**. *Let S be a closed and bounded subset of $\mathbb{C}$. Given a collection $\{U_i\}_{i\in I}$ of open sets such that $S \subseteq \bigcup_{i\in I} U_i$, there exists a finite subcollection $U_1, \dots, U_n$ of $\{U_i\}_{i\in I}$ such that $S \subseteq U_1 \cup \cdots \cup U_n$.*

Proof. For the purposes of this proof, we treat $\mathbb{C}$ as $\mathbb{R}^2$. We prove it for $S = [a, b] \times [c, d]$ where $a, b, c, d \in \mathbb{R}$ and $a < b$ and $c < d$ and leave the general case as an exercise. Take a point $x_0 \in [a, b]$ and consider the set $\{x_0\} \times [c, d]$. We take an open set $N \subseteq \mathbb{C}$ containing $\{x_0\} \times [c, d]$. We claim that there exists an open interval I around x_0 such that $I \times [c, d] \subseteq N$. For each point in $(x_0, y) \in \{x_0\} \times [c, d]$, choose $r_y > 0$ such that the open square $(x_0 - r_y, x_0 + r_y) \times (y - r_y, y + r_y) \subseteq N$. By intersecting these squares with $\{x_0\} \times \mathbb{R}$ and projecting on the second coordinate, we get a collection of open intervals of the form $\{x_0\} \times (y - r_y, y + r_y)$ that cover $\{x_0\} \times [c, d]$. By the Heine-Borel theorem in $\mathbb{R}$, there exists a finite subcollection of these open intervals that covers the interval $\{x_0\} \times [c, d]$. Hence the corresponding collection of open squares also covers $\{x_0\} \times [c, d]$. Let r be the minimum of the r_y from this finite collection. Then $I = (x_0 - r, x_0 + r)$ is the interval we sought.

Now let $\{U_j\}_{j\in J}$ be an open covering of S. For each $x \in [a, b]$, the collection $\{U_j\}_{j\in J}$ covers $\{x\} \times [c, d]$. As we did above, we choose a finite subcollection $U_1, \ldots, U_n$ that covers $\{x\} \times [c, d]$. The open set $N_x = U_1 \cup \cdots \cup U_n$ contains a set of the form $I_x \times [c, d]$ by the preceding discussion, where I_x is an open interval containing x. The collection $\{I_x\}_{x \in [a,b]}$ covers $[a, b]$, and hence by the Heine-Borel theorem for $\mathbb{R}$, there exists a finite subcollection $I_{x_1}, \ldots, I_{x_m}$ that covers $[a, b]$. We take our finite subcollection of the original open cover $\{U_j\}_{j \in J}$ to be $\{U \mid \text{for some } x_i \text{ the set } U \text{ is one of the elements in the union that defines } N_{x_i}\}$.

EXERCISE 1.9.18. Show that a subset of $\mathbb{C}$ is closed iff it contains all its accumulation points.

EXERCISE 1.9.19. Define the notion of sequentially compact for a subset of $\mathbb{C}$, and show that a subset of $\mathbb{C}$ is sequentially compact if and only if it is closed and bounded.

DEFINITION 1.9.20. If $z = x + iy \in \mathbb{C}$, $z \neq 0$, and $r = |z|$, then the *polar form* of z is $z = r(\cos\theta + i \sin\theta)$ where θ is the unique solution to the equations

$$\begin{aligned} x &= r\cos\theta, \\ y &= r\sin\theta \end{aligned}$$

in the interval $[0, 2\pi)$. The angle θ is called *the principal branch of the argument of* z and is denoted $\mathrm{Arg}(z)$. For z as above, we often write $z = re^{i\theta}$ where $e^{i\theta}$ is defined to be $\cos\theta + i\sin\theta$. In fact, this is the value of the complex exponential function $f(z) = e^z$ when $z = i\theta$.

EXERCISE 1.9.21. Suppose that $n \in \mathbb{N}$. Prove that if $z = e^{\frac{2\pi i k}{n}}$, for $k \in \mathbb{Z}$ and $0 \leq k \leq n-1$, then $z^n = 1$. Such a z is called an *n-th root of unity.* Note that these are all distinct.

The n-th roots of unity form a cyclic group of order n under multiplication. An n-th root of unity is *primitive* if it is a generator of this group.

EXERCISE 1.9.22. Show that the primitive n-th roots of unity are of the form $e^{2\pi i k/n}$ where k and n are relatively prime.

PROPOSITION 1.9.23. *If $n > 1$, the sum of the n distinct n-th roots of unity is* 0.

Proof. For any $z \in \mathbb{C}$,

$$1 - z^n = (1 - z)(1 + z + z^2 + \cdots + z^{n-1}).$$

Now let z be a primitive n-th root of unity.

EXERCISE 1.9.24. Suppose z is a nonzero complex number, and write $z = re^{i\theta}$. Show that z has exactly n distinct complex n-th roots given by $r^{1/n} e^{i(2\pi k + \theta)/n}$ for $0 \leq k \leq n-1$.

We now consider the ring of polynomials $\mathbb{C}[z]$ over $\mathbb{C}$.

Exercise 1.9.25. Show that $\mathbb{C}[z]$ is an integral domain. Determine the elements in this domain which have multiplicative inverses.

Definition 1.9.26. Let F be a field. We say that F is *algebraically closed* if every nonconstant polynomial in $F[x]$ has a root in F. That is, F is algebraically closed if, for every nonconstant $p(x) \in F[x]$, there is an element $r \in F$ such that $p(r) = 0$.

The most important example of an algebraically closed field is the complex numbers. There are a semi-infinite number of proofs of this theorem. We will present one of these as a project in Section 2.7.2 using the properties of continuous functions developed in Chapter 2.

Exercise 1.9.27. Let F be a field and suppose that $p(x) \in F[x]$. Show that r is a root of $p(x)$ if and only if $(x - r)$ is a factor of $p(x)$. That is, we can write $p(x) = (x - r)q(x)$ for some $q(x) \in F[x]$.

Definition 1.9.28. Let $\mathbb{A}$ be the collection of all complex roots of polynomials in $\mathbb{Z}[x]$. The set $\mathbb{A}$ is called *the set of algebraic numbers* in $\mathbb{C}$. The set $\mathbb{A}_{\mathbb{R}} = \mathbb{A} \cap \mathbb{R}$ is called *the set of real algebraic numbers.* A real number which is not a real algebraic number is called *transcendental.*

Example 1.9.29. Among the more famous algebraic numbers are i and $-i$. For real algebraic numbers, the most famous one is probably $\sqrt{2}$. The most famous transcendental numbers are π and e.

Exercise 1.9.30. Show that $\mathbb{A}$ and $\mathbb{A}_{\mathbb{R}}$ are fields.

Exercise 1.9.31. Show that the field $\mathbb{A}$ of algebraic numbers is countable.

Remark 1.9.32. It follows from the exercise above that the field $\mathbb{A}_{\mathbb{R}}$ of real algebraic numbers is countable and hence the set of transcendental numbers is uncountable.

1.10. Independent Projects

1.10.1. Another Construction of $\mathbb{R}$.

Definition 1.10.1. A subset α of $\mathbb{Q}$ is said to be a *cut* (or a *Dedekind cut*) if it satisfies the following:

(a) the set $\alpha \neq \varnothing$ and $\alpha \neq \mathbb{Q}$;
(b) if $r \in \alpha$ and if $s \in \mathbb{Q}$ satisfies $s < r$, then $s \in \alpha$;
(c) if $r \in \alpha$, then there exists $s \in \mathbb{Q}$ with $s > r$ and $s \in \alpha$.

Let R denote the collection of all cuts.

Definition 1.10.2. For $\alpha, \beta \in R$, we define $\alpha + \beta = \{r + s \mid r \in \alpha \text{ and } s \in \beta\}$. Let $\mathbf{0} = \{r \in \mathbb{Q} \mid r < 0\}$.

EXERCISE 1.10.3. If α and β are cuts, show that $\alpha+\beta$ is a cut, and also show that $\mathbf{0}$ is a cut.

EXERCISE 1.10.4. Show that with this addition $(R,+)$ is an abelian group with $\mathbf{0}$ as the identity element.

We now define an order on R.

DEFINITION 1.10.5. If $\alpha, \beta \in R$, we say that $\alpha < \beta$ if α is a proper subset of β.

EXERCISE 1.10.6. Show that the relation $<$ satisfies the following properties:

(i) (trichotomy) if $\alpha, \beta \in R$, then one and only one of the following holds: $\alpha < \beta$, $\alpha = \beta$, or $\beta < \alpha$;
(ii) (transitivity) if $\alpha, \beta, \gamma \in R$ with $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$;
(iii) (additivity) if $\alpha, \beta, \gamma \in R$ with $\alpha < \beta$, then $\alpha + \gamma < \beta + \gamma$.

It is now possible to define the notions of bounded above, bounded below, bounded, upper bound, least upper bound, lower bound, and greatest lower bound in R just as we did earlier in this chapter.

EXERCISE 1.10.7. Show that the least upper bound property holds in R, that is, if A is a nonempty subset of R which is bounded above, then A has a least upper bound in R.

Next, we must define multiplication in R.

DEFINITION 1.10.8. If $\alpha, \beta \in R$ with $\alpha, \beta > 0$, then

$$\alpha\beta = \{p \in \mathbb{Q} \mid \text{there are positive elements } r \in \alpha \text{ and } s \in \beta \text{ so that } p \leq rs\}.$$

The next step is multiplication by $\mathbf{0}$, which is exactly as it should be, namely for any $\alpha \in R$, we define $\alpha\mathbf{0} = \mathbf{0}$.

EXERCISE 1.10.9. If $\alpha < 0$ or $\beta < 0$ or both, replace any negative element by its additive inverse and use the multiplication of positive elements to define multiplication accordingly. For example, if $\alpha < 0$ and $\beta > 0$, $\alpha\beta = -[(-\alpha)(\beta)]$. Show that R with addition, multiplication, and order as defined above is an ordered field.

EXERCISE 1.10.10. Put it all together and show that R is an Archimedean ordered field in which the least upper bound property holds.

1.10.2. Infinite Series.

An important topic in analysis is the study of infinite series. This theory will be used in the remaining chapters of this book.

We assume that the reader has had at least an elementary introduction to infinite series and their convergence properties. In fact, the theory of infinite series actually reduces to the convergence of sequences, which we have covered thoroughly in this chapter. An infinite series is expressed as a sum of an infinite number of elements from some place or other. These elements could be numbers, functions, or what have you, so we begin with one-sided series of numbers.

An infinite series is an expression of the form $\sum_{n=1}^{\infty} a_n$, where the elements a_n come from a number system in which addition makes sense. So that we don't wander around aimlessly, let's fix our number system to be the complex numbers, that is, $a_n \in \mathbb{C}$, with the possibility of restricting ourselves to the real numbers or even the rational numbers. In the definition we have chosen to use the natural numbers as the index set, but in considering infinite series, we could start the summation with any integer and write $\sum_{n=n_0}^{\infty} a_n$. Later, we will also consider two-sided series where the index set is the integers and we write $\sum_{-\infty}^{\infty} a_n$. If these expressions are going to have any meaning at all, we must look at the partial sums.

Definition 1.10.11. If $\sum_{n=1}^{\infty} a_n$ is an infinite series of complex numbers, the *N-th partial sum* of the series is $S_N = \sum_{n=1}^{N} a_n$.

Examples 1.10.12.

(i) Let $a_n = 1$ for all n. Then $S_N = N$.
(ii) Let $a_n = 1/n$. Then $S_N = 1 + 1/2 + \cdots + 1/N$.
(iii) Let $a_n = 1/2^n$. Then $S_N = 1 - 1/2^N$.
(iv) Let $a_n = (-1)^{n+1}$. In this case, $S_N = 1$ if N is odd and 0 if N is even.
(v) Fix θ, with $0 < \theta < 2\pi$, and let $a_n = e^{in\theta}/n$. Then $S_N = \sum_{n=1}^{N} e^{in\theta}/n$, which is the best we can do without more information about θ.
(vi) Let $a_n = \sin n\pi/n^2$. In this case, $S_N = \sum_{n=1}^{N} \sin(n\pi)/n^2$.

Definition 1.10.13. Let $\sum_{n=1}^{\infty} a_n$ be an infinite series of complex numbers. The sequence $(S_N)_{N\in\mathbb{N}}$ is called *the sequence of partial sums.* We say that the series $\sum_{n=1}^{\infty} a_n$ *converges* if the sequence of partial sums $(S_N)_{N\in\mathbb{N}}$ converges. If the sequence $(S_N)_{N\in\mathbb{N}}$ does not converge, we say that $\sum_{n=1}^{\infty} a_n$ *diverges.*

Of course, since we are working in $\mathbb{C}$, the series converges if and only if the sequence $(S_N)_{N\in\mathbb{N}}$ is a Cauchy sequence. That is, given $\varepsilon > 0$, there is an $N \in \mathbb{N}$ so that for $n, m > N$ (assuming $n > m$), $|\sum_{k=m+1}^{n} a_n| < \varepsilon$.

Exercise 1.10.14. Determine which of the series in Example 1.10.12 converge.

We are faced with two problems. The first is, "How do we tell if a series converges?" The second is, "If a series does converge, how do we find the explicit sum?" There is extensive literature about these two questions, but the fact is that the second question presents many more difficulties than the first. In Chapter 7, the theory of Fourier series will provide some assistance.

The most helpful series in all of this discussion is the geometric series.

Definition 1.10.15. Let z be a complex number. The geometric series defined by z is $\sum_{n=0}^{\infty} z^n$.

Exercise 1.10.16.

(i) If $N \in \mathbb{N}$ and $z \neq 1$, show that $S_N = \sum_{n=0}^{N} z^n = \frac{1-z^{N+1}}{1-z}$.
(ii) If $|z| < 1$, show that $\lim_{n\to\infty} z^n = 0$.
(iii) If $|z| > 1$, show that $\lim_{n\to\infty} z^n$ does not exist.

Theorem 1.10.17. *Consider the geometric series defined by a complex number z. If $|z| < 1$, then the series converges. If $|z| > 1$, then the series diverges.*

Proof. This follows from the exercise above.

Exercise 1.10.18.

(i) What can you say if $|z| = 1$?
(ii) Suppose that a series $\sum_{n=1}^{\infty} a_n$ converges. Show that $\lim_{n\to\infty} a_n = 0$.

The property $\lim_{n\to\infty} a_n = 0$ does not ensure that the series $\sum_{n=1}^{\infty} a_n$ converges. The most useful example is given above where $a_n = 1/n$. In this case, $S_1 = 1$, $S_4 > 2$, and it is easy to check that $S_{2^n} > n$ for $n \in \mathbb{N}$. It follows that the series $\sum_{n=1}^{\infty} 1/n$ diverges. The series $S = \sum_{n=1}^{\infty} 1/n$ is often called the *harmonic series*. We have just proved that this series diverges.

Exercise 1.10.19.

(i) Let $S_N = \sum_{n=1}^{N} 1/n$. Show that, for $N \geq 2$, S_N is never an integer.
(ii) Show that, by suitably eliminating an infinite number of terms, the remaining subseries can be made to converge to any positive real number.

Exercise 1.10.20.

(i) If $s \in \mathbb{R}$ and $s > 1$, show that $\sum_{n=1}^{\infty} 1/n^s$ converges.
(ii) If $s \in \mathbb{R}$ and $s < 1$, show that $\sum_{n=1}^{\infty} 1/n^s$ diverges.
(iii) For which $s \in \mathbb{R}$ does the series $\sum_{p \text{ prime}} 1/p^s$ converge?

Definition 1.10.21. A series $\sum_{n=1}^{\infty} a_n$ of complex numbers *converges absolutely* if the series $\sum_{n=1}^{\infty} |a_n|$ converges.

Proposition 1.10.22. *If $\sum_{n=1}^{\infty} a_n$ converges absolutely, then $\sum_{n=1}^{\infty} a_n$ converges*

Proof. This follows from the fact that $|\sum_{k=m+1}^{n} a_k| \leq \sum_{k=m+1}^{n} |a_k|$.

The converse to Proposition 1.10.22 is false and is shown by the example $\sum_{n=1}^{\infty}(-1)^{n+1}/n$. This series converges since $|\sum_{k=m+1}^{n}(-1)^{k+1}/k| < 1/m$. However, as we have seen above, the series does not converge absolutely.

There are various tests to determine if a series converges. These include the comparison test, the ratio test, and the root test. The comparison test is often very useful, but its use depends on knowing ahead of time a series which converges.

Theorem 1.10.23 **(Comparison test)**. *Suppose $a_n > 0$ for $n \in \mathbb{N}$ and suppose $\sum_{n=1}^{\infty} a_n$ converges. If $b_n \in \mathbb{C}$ satisfies $|b_n| \leq a_n$ for all n, then the series $\sum_{n=1}^{\infty} b_n$ converges absolutely and hence converges.*

Exercise 1.10.24.

(i) Prove the comparison test.

(ii) If the series $\sum_{n=1}^{\infty} a_n$ converges to s and c is any constant, show that the series $\sum_{n=1}^{\infty} ca_n$ converges to cs.

(iii) Suppose that $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ are infinite series. Suppose that $a_n > 0$ and $b_n > 0$ for $n \in \mathbb{N}$ and $\lim_{n\to\infty} a_n/b_n = c > 0$. Show that $\sum_{n=1}^{\infty} a_n$ converges if and only if $\sum_{n=1}^{\infty} b_n$ converges.

The most useful series for comparison is the geometric series defined by a real number r, with $0 < r < 1$.

Theorem 1.10.25 **(Ratio test)**. *Suppose that $\sum_{n=1}^{\infty} a_n$ is a series of nonzero complex numbers. If $r = \lim_{n\to\infty} |a_{n+1}/a_n|$ exists, then the series converges absolutely if $r < 1$ and the series diverges if $r > 1$.*

Proof. Suppose $\lim_{n\to\infty} |a_{n+1}/a_n| = r < 1$. If ρ satisfies $r < \rho < 1$, then there exists $N \in \mathbb{N}$ such that $|a_{n+1}|/|a_n| < \rho$ for all $n \geq N$. Consequently, $|a_n| \leq |a_N|\rho^{n-N}$ for all $n \geq N$. The result follows from the comparison test.

Exercise 1.10.26. Show that if $r > 1$, then the series above diverges, while, if $r = 1$, anything can happen.

Our final test for convergence is called the root test. This can be quite effective when the comparison test and ratio test fail.

Theorem 1.10.27 **(Root test)**. *Suppose that $\sum_{n=1}^{\infty} a_n$ is a series of complex numbers. Let*

$$r = \limsup_{n\to\infty} |a_n|^{1/n}$$

(consult Chapter 2 for a discussion of $\limsup$*). If $r < 1$, then the series converges absolutely. If $r > 1$, then the series diverges.*

Proof. Suppose that $\limsup_{n\to\infty} |a_n|^{1/n} = r < 1$. Pick ρ so that $r < \rho < 1$. Then, there exists $N \in \mathbb{N}$ such that $|a_n| \leq \rho^n$ for all $n \geq N$. The convergence of the series now follows from the comparison test.

Exercise 1.10.28. Show that if $r > 1$, then the above series diverges, while, if $r = 1$, anything can happen.

Exercise 1.10.29. Suppose that the ratio test applies to a series. That is, $\lim_{n\to\infty} |a_{n+1}|/|a_n| = r$. Show that the $\limsup_{n\to\infty} |a_n|^{1/n} = r$.

Definition 1.10.30. Let z_0 be a fixed complex number. A *complex power series* around z_0 is a series of the form $\sum_{n=0}^{\infty} a_n(z - z_0)^n$, where the coefficients $a_n \in \mathbb{C}$. When this series converges, it converges to a function of the complex variable z.

Exercise 1.10.31. Show that if the series converges absolutely for a complex number z, then it also converges for any complex number w such that $|w - z_0| \leq |z - z_0|$. That is, the series converges on the disk

$$\{w \in \mathbb{C} \mid |w - z_0| \leq |z - z_0|\}.$$

From this exercise, it follows that a complex power series around z_0 that converges absolutely at any point other then z_0 will have a disk of convergence of the form $\{z \in \mathbb{C} \mid |z - z_0| < r\}$. The supremum of all such r is called the *radius of convergence* of the power series. If the power series converges only at the point $z = z_0$, we say that the series has radius of convergence equal to 0.

To determine the radius of convergence for a complex power series, we use the convergence tests developed above, in particular the root test.

THEOREM 1.10.32. *Suppose that* $\limsup_{n\to\infty} |a_n|^{1/n} = r$. *If* $0 < r < \infty$, *then the power series* $\sum_{n=0}^{\infty} a_n(z - z_0)^n$ *has radius of convergence* $1/r$. *If* $r = 0$, *then the radius of convergence is infinity. If* $r = \infty$, *then the radius of convergence is* 0.

EXAMPLES 1.10.33.

(i) Consider the series $\sum_{n=0}^{\infty} n(z - z_0)^n$. Then $\lim_{n\to\infty} n^{1/n} = 1$, and the power series converges absolutely for $|z - z_0| < 1$, that is, the radius of convergence is 1.
(ii) Consider the series $\sum_{n=1}^{\infty} n^n(z - z_0)^n$. Then $\lim_{n\to\infty}(n^n)^{1/n} = \infty$, so the radius of convergence is 0 and the series converges only for $z = z_0$.

EXERCISE 1.10.34. Determine the radius of convergence of the following power series:

(i) $\sum_{n=1}^{\infty} \frac{z^n}{n!}$;
(ii) $\sum_{n=2}^{\infty} \frac{z^n}{\ln(n)}$;
(iii) $\sum_{n=1}^{\infty} \frac{n^n}{n!} z^n$.

1.10.3. Decimal Expansions of Real Numbers.

In Appendix A, we used a decimal representation of the real numbers to show that the real numbers between 0 and 1 form an uncountable set. In this project, we actually prove that every real number between 0 and 1 has a decimal expansion which is unique with the condition that no expansion can terminate in all 9's. In addition, we discuss the fact that rational numbers have decimal expansions of three different types. The first is terminating decimals, the second is rational numbers whose denominators are relatively prime to 10, and the third is a combination of the first two.

Since we know that every real number lies between two consecutive integers, we start with a real number x so that $0 < x < 1$. Let $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Assume first that x is irrational. The construction proceeds as follows. Let a_1 be the largest element of S which is less than $10x$. Then $0 < x - a_1/10 < 1/10$. Let a_2 be the largest integer in S less than $100x - 10a_1$. Proceeding as before, we get $0 < x - a_1/10 - a_2/10^2 < 1/10^2$. Continuing this process, we obtain a monotonic increasing sequence

$$S_n = a_1/10 + a_2/10^2 + \cdots + a_n/10^n,$$

where $a_j \in S$ and $0 < x - S_n < 1/10^n$. We conclude that S_n converges to x and we get

$$x = a_1/10 + a_2/10^2 + \cdots + a_n/10^n + \cdots . \tag{1.3}$$

EXERCISE 1.10.35. Let x be a irrational number between 0 and 1. Show that there is only one way to express x in the form (1.3).

We now turn to rational numbers between 0 and 1. We can apply the above procedure to rational numbers with the possibility of equality in any of the inequalities above. Suppose that x has a *terminating decimal expansion.* That is, suppose there exists N so that $a_n = 0$ for all $n > N$ and $a_N \neq 0$. Then we can write $x = a_1/10 + a_2/10^2 + \cdots + a_N/10^N$.

EXERCISE 1.10.36.

(i) Show that if r is a rational number in $(0,1)$, then the decimal expansion of r terminates if and only if the denominator of r has the form $2^a 5^b$ where a and b are nonnegative integers and are not both zero.
(ii) With r as above, show that the last nonzero digit of r is in the m-th place where $m = \max(a, b)$.

Note that rational numbers with terminating decimal expansions are the only real numbers between 0 and 1 for which equality can occur in the procedure above.

Next consider a rational number $r = p/q$ in $(0,1)$ for which q is relatively prime to 10. From Euler's theorem (see the project in Section A.10.1), q divides $10^{\phi(q)} - 1$. Let n be the smallest natural number so that q divides $10^n - 1$. Then $(p/q)(10^n - 1)$ is an integer which we denote by m. That is,

$$m = \frac{p}{q}(10^n - 1) \quad \text{or} \quad \frac{p}{q} = \frac{m}{10^n - 1}.$$

We can now write

$$\begin{aligned} \frac{p}{q} &= \frac{m}{10^n - 1} = \frac{m}{10^n}(1 - 10^{-n})^{-1} = \frac{m}{10^n}(1 + 10^{-n} + 10^{-2n} + \cdots) \\ &= m/10^n + m/10^{2n} + \cdots . \end{aligned}$$

As $0 < p/q < 1$, we have $m < 10^n$. Thus the right-hand side of the equation above gives us a periodic decimal expansion of p/q whose period has length n.

EXERCISE 1.10.37. Let p/q be a rational number between 0 and 1. If q and 10 are relatively prime, show that p/q has a unique periodic decimal expansion with the length of the period equal to the order of 10 mod q.

We now present the remaining case as an exercise.

EXERCISE 1.10.38. Let p/q be a rational number in $(0,1)$ with $q = 2^a 5^b r$ where r is relatively prime to 10. Let $k = \max(a, b)$ and let n be the smallest positive integer such that r divides $10^n - 1$. Show that, after k digits, the decimal expansion of p/q is periodic of length n.

EXERCISE 1.10.39. Can any of the above decimal expansions terminate in all 9's?