Chapter 1

The Real Numbers and the Completeness Property

This chapter defines the real numbers and studies their basic properties. The real numbers are characterized by three types of properties. The first type is algebraic properties (having to do with addition and multiplication). These properties are called the field axioms and are shared by other sets of numbers such as the rational numbers and the complex numbers, but not, for example, by the integers. The second consists of the order properties, which introduce an order structure (an inequality), and are also shared by the rational numbers, but not, for example, by the complex numbers. The third type is completeness, also called order completeness, which is probably new to the reader as it is not satisfied by the rational numbers and is the more difficult to state. There are several formulations of the completeness property; we defined completeness in terms of the supremum and discuss equivalent formulations in later chapters.

We define the real numbers by the properties they possess. The **real numbers** are defined to be an ordered field that is complete under that order. Ordered fields are defined in Section 1.1 and completeness is defined in Section 1.2.

There are two natural questions that arise from this definition. The first one is of the existence of a set that is a complete ordered field; i.e., is there a set satisfying the properties of the real numbers? The second question is whether there is only one such set; i.e., in what sense is the set satisfying these properties unique? There are now several constructions of the real numbers, and we outline the construction due to Dedekind in Section 1.4; this establishes the existence of a complete ordered field. The construction of the real numbers is optional as all the properties that we need of the real numbers can be deduced from the axioms of field, order, and completeness that we cover in this chapter. Regarding the question of uniqueness,

we note that it can be shown that in some reasonable sense a set satisfying these properties is unique; this is outlined in one of the exercises.

1.1. Field and Order Properties of $\mathbb{R}$

1.1.1. Field Properties. The field properties consist of the axioms of addition, multiplication, and the distributive axiom. We state them in the setting of a field F (defined after the statement of the distributive axiom), but the case we are most interested in is when F is the set of real numbers.

Definition 1.1.1. Axioms for Addition. A set F is said to satisfy the axioms of addition if it has a function from $F \times F$ to F, called an operation and denoted by $+$, so that for any pair of elements x and y in F there is an element denoted $x + y$ in F satisfying the following properties.

(A1) *Commutativity of addition:* $x + y = y + x$ for all x and y in F.

(A2) *Associativity of addition:* $(x + y) + z = x + (y + z)$ for all x, y and z in F.

(A3) *Existence of a zero:* There is an element of F denoted by 0 that satisfies $x + 0 = x$ for all $x \in F$.

(A4) *Existence of additive inverse:* For every $x \in F$ there exists an element of F denoted $-x$, called its **additive inverse**, such that $x + (-x) = 0$. ◊

We note that the zero element, 0, is unique. What we mean is that there is no other element of the set F that satisfies the characteristic or defining property of 0, i.e., property (A3). To show this, we start by supposing that z is an arbitrary element of F satisfying the same property as 0, i.e., that $x + z = x$ for all $x \in F$. It suffices to show that z must be 0. In fact, by letting $x = 0$ in the property of z and then using the commutativity of addition, we have

$$0 = 0 + z = z + 0 = z.$$

Also, the additive inverse (defined by property (A4)) is unique. If for a given x in F there is a w in F such that $x + w = 0$, then

$$w = 0 + w = (x + (-x)) + w = (-x) + (x + w) = -x.$$

We write $x - y$ instead of $x + (-y)$. It follows from here that $-(-x) = x$.

Definition 1.1.2. Axioms for Multiplication. A set F, which already satisfies the axioms for addition, is said to satisfy the axioms of multiplication if it has an operation denoted $\cdot$ so that for any pair of elements x and y in F there is an element in F denoted $x \cdot y$ satisfying the following properties.

(M1) *Commutativity of multiplication:* $x \cdot y = y \cdot x$ for all x and y in F.

(M2) *Associativity of multiplication:* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all x, y and z in F.

(M3) *Existence of a unit:* There is an element of F denoted by 1 and different from 0 that satisfies $1 \cdot x = x$ for all $x \in F$.

(M4) *Existence of multiplicative inverse:* For every $x \neq 0$ in F there exists an element of F denoted $\frac{1}{x}$ (or $1/x$), called its **multiplicative inverse**, such that $x \cdot \frac{1}{x} = 1$. ◊

The element 1 is also unique. If z satisfies $z \cdot x = x$ for all $x \in F$, then

$$z = 1 \cdot z = z \cdot 1 = 1.$$

Similarly, if for $x \neq 0$ there exists w such that $x \cdot w = 1$, then

$$w = 1 \cdot w = \left(\frac{1}{x} \cdot x\right) \cdot w = \frac{1}{x} \cdot (x \cdot w) = \frac{1}{x} \cdot 1 = \frac{1}{x}.$$

We often write x^{-1} instead of $\frac{1}{x}$ and write xy instead of $x \cdot y$.

Definition 1.1.3. Distributive Axiom. A set F with operations $+$ and $\cdot$ satisfies the distributive axiom if

(D) $$x(y+z) = xy + xz \text{ for all } x, y \text{ and} z \text{ in } F.$$ ◊

Definition 1.1.4. A **field** consists of a set F with two operations $+$ and $\cdot$ that satisfies the addition, multiplication, and distributive axioms. ◊

For example, the set of rational numbers $\mathbb{Q}$ with $+$ and $\cdot$ is a field. The set of integers $\mathbb{Z}$ with $+$ and $\cdot$ is not a field since elements of $\mathbb{Z}$, other than 1 and -1, do not have multiplicative inverses.

It is possible to derive all the algebraic properties we use for the real numbers from the axioms of a field. The following proposition is included as an example of some of the many algebraic properties of the real numbers that can be deduced from the field axioms; additional properties are in the Exercises. We will use algebraic properties of the reals even if they are not listed here, though the reader should know how to derive them from the axioms.

Proposition 1.1.5. *The elements of a field F satisfy the following properties.*

(1) *If $x + w = y$, then $w = y - x$.*
(2) $0 \cdot x = 0$.
(3) *If $xw = y$ and $x \neq 0$, then $w = x^{-1}y$.*
(4) $-1 \cdot x = -x$.
(5) $(-x)y = x(-y) = -xy$.

Proof. We show (1) one step at a time. We start with $x + w = y$. Then

$$\begin{aligned}
(x+w) - x &= y - x, \text{ by (A4) and the property of equality,} \\
(w+x) - x &= y - x, \text{ by (A1),} \\
w + (x - x) &= y - x, \text{ by (A2),} \\
w + 0 &= y - x, \text{ by (A4),} \\
w &= y - x, \text{ by (A3).}
\end{aligned}$$

For the remaining properties we give an outline of the proof, but the reader should know how to justify each step. To show (2) note that

$$0x = (0+0)x = 0x + 0x.$$

Hence $0x = 0x - 0x = 0$. For (3), use that x^{-1} exists and multiply both sides of $xw = y$ by x^{-1}. For part (4) note that

$$x + (-1 \cdot x) = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0x = 0.$$

By the uniqueness of the additive inverse, $-1 \cdot x = -x$. For part (5) we use (4) and associativity to write

$$(-x)y = ((-1)x)y = (-1)(xy) = -(xy).$$

A similar argument shows that $x(-y) = -xy$. □

As a final example we mention that division by 0 is not consistent with our properties. Suppose w was the multiplicative inverse of 0; then it would satisfy $0w = 1$, but this contradicts Proposition 1.1.5(2).

Definition 1.1.6. For x in F and each positive integer n, we can define x^n by induction. Let $x^1 = x$ and $x^{n+1} = x \cdot x^n$. We extend this to all integers by setting $x^0 = 1$ and $x^{-n} = 1/x^n$ when $x \neq 0$. Also, for $y \neq 0$, write

$$\frac{x}{y} = x\ \frac{1}{y}.$$ ◊

Example 1.1.7. We show that if F is a field, then for all $x \in F$ such that $x \neq 0$ we have that $-(\frac{1}{x}) = \frac{-1}{x}$. The defining property of $1/x$ is that it is the multiplicative inverse of x, so $x \cdot (1/x) = 1$. Multiplying both sides by -1 and using Proposition 1.1.5, $x \cdot [-(1/x)] = -1$. Next we multiply both sides by $1/x$ and use Proposition 1.1.5 to obtain $-(1/x) = (-1)(1/x) = \frac{-1}{x}$.

1.1.2. Order Axioms

Definition 1.1.8. A field F with operations $+$ and $\cdot$ is said to be an **ordered field** if there is a subset of F denoted by F^+ and called the **positive set** satisfying the following properties.

(O1) *Closure of F^+ under $+$ and $\cdot$*: $x + y$ and xy are in F^+ for all x, y in F^+.

(O2) *Trichotomy property*: For every x in F, exactly one of the following is true: $x = 0$, or $x \in F^+$, or $-x \in F^+$. ◊

The idea is to think of F^+ as the set of positive elements of the field. Then the closure property is simply saying that the "sum and product of positive elements are positive". The trichotomy property then states that a nonzero element is either positive or its negative is positive.

We typically do not use the set F^+ but instead use the $>$ notation. Write

- $a > 0$ if and only if $a \in F^+$;
- $b > a$ if and only if $b - a > 0$ (i.e., $b - a \in F^+$).

Also, write $a < b$ when $b > a$. Hence $a < 0$ if and only if $-a > 0$, and $a < b$ is equivalent to $a - b < 0$. Further, write $x \geq y$ if $x > y$ or $x = y$, and similarly for $x \leq y$. This establishes an "order" in F, i.e., any two elements x and y in F can be compared: if $x \neq y$, then either $x > y$ or $y > x$.

We claim that $1 \in F^+$ (equivalently, $1 > 0$). From the trichotomy property we know that, as $1 \neq 0$, either $1 \in F^+$ or $-1 \in F^+$. If we had that $-1 \in F^+$, by the closure property $1 = (-1) \cdot (-1) \in F^+$, contradicting the trichotomy property. Thus $-1 \notin F^+$ and $1 \in F^+$. In particular, F^+ is nonempty.

Question 1.1.9. Let F be an ordered field. Prove that $-3 < -2$.

We note that $\mathbb{Q}$ is an ordered field (Exercise 1.1.13). We now mention the important fact that one can regard the natural numbers $\mathbb{N}$ as a subset of any ordered field F. The identification of elements of $\mathbb{N}$ with elements of F is the natural one. We identify 1 in $\mathbb{N}$ with the 1 in F, 2 in $\mathbb{N}$ with $1+1$ in F, completing the process by induction. (There is something that needs to be clarified. Since $1 > 0$, using induction one shows that $1+\cdots+1 (n+1 \text{ times}) > 1+\cdots+1 (n \text{ times})$.) Technically, we would say that F contains a copy of $\mathbb{N}$, but in practice we consider $\mathbb{N}$ a subset of F. Since F is a field, if it contains n it must contain $-n$. It follows that an ordered field includes the set of integers $\mathbb{Z}$, and thus it includes the rational numbers $\mathbb{Q}$ (again, technically a copy of $\mathbb{Q}$). A consequence of this is that an ordered field must be infinite.

The following proposition shows some properties of the order we have introduced.

Proposition 1.1.10. *The following properties hold in an ordered field.*

(1) *For each x one and only one of the following hold: $x = 0$, $x < 0$, or $0 < x$.*

(2) *If $x < y$ and $y < z$, then $x < z$.*

(3) *If $x < y$, then $x + z < y + z$ for all z.*

(4) *If $x < y$ and $z > 0$, then $xz < yz$.*

Proof. Part (1) follows from the definition and the trichotomy property. For (2), assume $x < y$ and $y < z$, which means that $y - x \in F^+$ and $z - y \in F^+$. Then $y-x+z-y \in F^+$, so $x < z$. For (3), $y-x > 0$, so for every z, $(y+z)-(x+z) > 0$. For (4), $y - x > 0$, so for every $z > 0$, $(y - x)z > 0$. Thus $yz - xz > 0$, or $yz > xz$. □

Corollary 1.1.11. *The following properties hold in an ordered field.*

(1) *If $x < y$, then $-x > -y$.*

(2) *If $x < y$ and $z < 0$, then $xz > yz$.*

(3) *If $x > 0$, then $-x < 0$ and $1/x > 0$.*

Proof. If $x < y$, then $x - y < 0$, so $-(x - y) > 0$ or $(-x) - (-y) > 0$, which means $-x > -y$. For part (2) first note that we have $y - x > 0$ and $-z > 0$, so $(y - x)(-z) > 0$. Thus, $-yz + xz > 0$ or $xz > yz$. For the last part, let $x > 0$. By (2), $-0 > -x$, so $-x < 0$. Now, if $1/x < 0$, then $-(1/x) > 0$, so $-(1/x)x > 0$, which would imply $-1 > 0$, a contradiction. □

Question 1.1.12. Let F be an ordered field. Prove that if $xy > 0$, then either $x > 0$ and $y > 0$ or $x < 0$ and $y < 0$, and that if $xy < 0$, then either $x > 0$ and $y < 0$ or $x < 0$ and $y > 0$.

Remark 1.1.13. We have seen that from a positive set F^+ in a field F we can define an order on F; namely, we can define $a < b$ if and only if $b - a \in F^+$. There is a parallel theory which starts with the idea of an abstract order. While we do not need this, we discuss it now as it is interesting to see how one can define an abstract order. From this, one can define a positive set F^+.

We can define an **order** on a set S as a relation on S (i.e., a subset of $S \times S$) that we denote by $<$, satisfying two properties. First, regarding notation, rather than writing $(x, y) \in <$ (i.e., that (x, y) belongs to the order $<$), we write $x < y$. Then we require the following properties.

(1) For each $x, y \in S$, one and only one of the following hold: $x = y$, $x < y$, or $y < x$.

(2) If $x < y$ and $y < z$, then $x < z$.

If now F is an ordered field, we can define a relation $<$ on F so that $a < b$ if and only if $b - a \in F^+$. Then by Proposition 1.1.10, $<$ is an order on the set F. In addition, this order satisfies the following:

(3) $x < y$, then $x + z < y + z$ for all z;

(4) if $x < y$ and $z > 0$, then $xz < yz$.

Exercise 1.1.18 shows that one could alternatively define an ordered field using the notion of order.

Exercises: Field and Order Properties of $\mathbb{R}$

1.1.1 Give complete details in the proof of Proposition 1.1.5(5).

1.1.2 Let F be a field, and let $x, y \in F$. Prove that $(-x)(-y) = xy$.

1.1.3 Let F be a field, and let $x, y \in F$. Prove that

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2).$$

1.1.4 Let F be an ordered field. Prove that for every $x \in F$, $x^2 \geq 0$.

1.1.5 Prove that for all x in a field F, $x \neq 0$, $-(1/x) = 1/(-x)$.

1.1.6 Let F be an ordered field. Let $x \geq 0$ be in F. Prove that if $x < \varepsilon$ for all $\varepsilon > 0$, $\varepsilon \in F$, then $x = 0$.

1.1.7 Let F be an ordered field. Suppose that x and y are in F and satisfy $x < y + \varepsilon$ for all $\varepsilon > 0$, $\varepsilon \in F$. Prove that then $x \leq y$.

1.1.8 Let F be an ordered field, and let $\varepsilon \in F$. Show that if $0 < \varepsilon < 1$, then $\varepsilon^2 < \varepsilon$.

1.1.9 Let F be an ordered field, and let $a, b \in F$. Prove that if $0 < a < b$, then $1/b < 1/a$.

1.1.10 *Binomial formula*: Let F be a field. Prove that for all a and b in F, and for all $n \in \mathbb{N}$,

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

where

$$\binom{n}{i} = \frac{n!}{i!(n - i)!}$$

is the **binomial coefficient**.

1.1.11 *Bernoulli's inequality*: Let F be an ordered field, and let $x \in F$. Prove that

$$(1+x)^n \geq 1 + nx$$

for all $n \in \mathbb{N}$ and $x > -1$.

1.1.12 *Geometric sum*: Let F be a field. Use induction to prove that for all $r \in F$ with $r \neq 1$ and all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} r^{i-1} = \frac{1-r^n}{1-r}.$$

Write and prove a formula for $\sum_{i=k}^{n} r^{i-1}$ for $k \in \mathbb{N}$.

1.1.13 Verify that the rational numbers $\mathbb{Q}$ satisfy the properties of an ordered field.

1.1.14 Let $\mathbb{Z}_2$ denote the set $\{0,1\}$ with addition defined by $0+0=0$, $0+1=+0=1$, $1+1=0$ (this is called addition mod 2) and multiplication defined by $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. Prove that this is a field. Is it ordered?

1.1.15 Construct a set with three elements and two operations so that it satisfies the axioms of a field.

1.1.16 Let F be an ordered field, and let $x \in F$. Prove that if $x > 1$, then $x^n \geq x$ for all $n \in N$.

1.1.17 Let F be a field, and let $a, b \in F^+$. Prove that if $a^2 > b^2$, then $a > b$.

1.1.18 Let F be a field. Let $<$ be an order on F (see Remark 1.1.13), which in addition satisfies (a) if $x < y$, then $x + z < y + z$ for all z; and (b) if $x < y$ and $z > 0$, then $xz < yz$. Define a set F^+ by $F^+ = \{x \in F : x > 0\}$. Prove that F^+ is a positive set for F.

1.1.19 Let F be a field, and let $F[x]$ consist of the set of polynomials with coefficients in F, i.e., the set of functions of the form $f(x) = a_n x^n + \cdots + a_1 x + a_0$ where $a_i \in F$ (call a_n the leading coefficient). Let $F(x)$ denote the set of rational functions with coefficients in F, i.e., functions of the form $f(x)/g(x)$ where $f(x), g(x) \in F[x]$, $g(x)$ is not identically zero, and $f(x)$ and $g(x)$ do not have any common factors ($f(x)/g(x)$ is defined at the points where g does not vanish). Prove that $F[x]$ is not a field but $F(x)$ is a field with the usual addition and multiplication, i.e.,

$$\frac{f(x)}{g(x)} + \frac{h(x)}{k(x)} = \frac{k(x)f(x) + g(x)h(x)}{g(x)k(x)} \quad \text{and} \quad \frac{f(x)}{g(x)} \cdot \frac{h(x)}{k(x)} = \frac{f(x)h(x)}{g(x)k(x)}.$$

1.1.20 Let $F(x)$ be the field defined in Exercise 1.1.19. Define the set $F(x)^+$ to consist of all elements $f(x)/g(x)$ where the leading coefficient of f and g have the same sign. Prove that with this definition $F(x)$ is an ordered field.

1.2. Completeness Property of $\mathbb{R}$

The completeness property, also called order completeness, is one of the most important properties of the real numbers. Together with the field and order axioms, the completeness property finishes the definition of the real numbers.

1.2.1. Numbers that Are Not in the Field $\mathbb{Q}$. There are some important numbers that are missing from the set of rational numbers $\mathbb{Q}$ and that will be added by the completeness property (namely the *irrational numbers*). It turns out that numbers such as $\sqrt{2}$ are not rational. What we mean by $\sqrt{2}$ is a positive number α such that $\alpha^2 = 2$. It follows from Pythagoras' theorem that if α is the hypotenuse of a right-angle isosceles triangle with sides of length 1, then α must satisfy $\alpha^2 = 2$. Thus the number α is needed to measure simple geometric figures. To their amazement, the ancient Greeks discovered that α is not a rational number. Before studying the completeness property, we prove that α is missing from $\mathbb{Q}$. As we shall see, a consequence of this fact is that the ordered field $\mathbb{Q}$ is not complete.

The following is a classic theorem; a proof of this theorem can already be found in Euclid's *Elements*, written around 300 BCE.

Theorem 1.2.1. *There is no rational number α such that $\alpha^2 = 2$ (i.e., $\sqrt{2} \notin \mathbb{Q}$).*

Proof. We show by contradiction that there is no positive rational number α satisfying $\alpha^2 = 2$ (this also implies there is no such negative rational number α). Consider the set A defined by

$$A = \{q \in \mathbb{N} : \alpha = \frac{p}{q} \text{ for some } p \in \mathbb{N}\}.$$

If α is a rational number, then the set A is a nonempty subset of $\mathbb{N}$. By the well-ordering principle, it has a least element, which we denote by b. Then

$$\alpha = \frac{a}{b} \text{ for some } a \in \mathbb{N}.$$

Therefore

$$2b^2 = a^2. \tag{1.1}$$

This implies that 2 is a factor of a^2, and as 2 is prime, 2 is a factor of a. Then we can write a as $a = 2c$, for some positive integer c. From (1.1) we obtain

$$2b^2 = 4c^2, \tag{1.2}$$

$$b^2 = 2c^2. \tag{1.3}$$

By the same argument as before, this implies that 2 divides b, so $b = 2d$ for some $d \in \mathbb{N}$. Again, replacing b in (1.3), we obtain

$$2d^2 = c^2 \text{ or} \tag{1.4}$$

$$\alpha = \frac{c}{d} \text{ for } c, d \in \mathbb{N}. \tag{1.5}$$

Thus $d \in A$, but $d < b$, contradicting that b is the least element of A. Therefore α is not a rational number. □

There are now many different proofs of this theorem, and our proof can be extended to show that many other numbers are not rational. We mention one modification of the argument. We could start the proof by contradiction by supposing that α can be written in the form $\alpha = \frac{a}{b}$, where a and b have been simplified so that they do not both have 2 as a factor. Then, following as in the proof of Theorem 1.2.1, one can obtain a contradiction by showing that 2 must divide both a and b.

There are numbers, however, that are still not known to be rational. For example, while it is believed that these numbers are not rational, it is not known whether either of 2^e or $\pi + e$ is rational (though it is known that either $\pi + e$ or $e\pi$ is not rational).

1.2.2. Infimum and Supremum. As we shall see, there are many equivalent formulations of the completeness property. We start our development in terms of the notions of infimum and supremum. We state these definitions in the context of ordered fields to emphasize that the main property of the real numbers used here is that of being an ordered field.

Definition 1.2.2. Let S be a nonempty subset of an ordered field F. An element $b \in F$ is said to be an **upper bound** for S if

$$x \leq b \text{ for all } x \in S.$$

Similarly, $c \in F$ is said to be a **lower bound** for S if

$$c \leq x \text{ for all } x \in S. \qquad \lozenge$$

In the case of the empty set, every element of F is both an upper bound and a lower bound for $\varnothing$.

Definition 1.2.3. A set S in F is said to be **bounded below** if it has a lower bound and it is **bounded above** if it has an upper bound. A set $S \subseteq F$ is said to be **bounded** if it is bounded above and bounded below. $\lozenge$

For example, $\mathbb{N}$ is not bounded above and is bounded below by 0 (and also by $1/2$, for example). The empty set is a bounded set.

Question 1.2.4. Let F be an ordered field, and let $S \subseteq F$. Prove that $b \in F$ is an upper bound of S if and only if $-b$ is a lower bound of $-S$, where $-S = \{-x : x \in S\}$.

Definition 1.2.5. The **supremum** or **least upper bound** of S, denoted $\sup S$, is defined to be an element β of F such that

- β is an upper bound for S;
- if c is any other upper bound for S, then $c \geq \beta$ (i.e., β is less than any other upper bound). $\lozenge$

The second property in the definition readily implies that the supremum, when it exists, is unique.

Question 1.2.6. Let F be an ordered field, and let A and B be subsets of F such that $\sup A$ and $\sup B$ exist (and so are elements of F). Prove that $\sup A \cup B$ exists and $\sup A \cup B = \max\{\sup A, \sup B\}$. Conclude that if $A \subseteq B$, then $\sup A \leq \sup B$.

Definition 1.2.7. We extend the definition of supremum to a nonempty set S that does not have an upper bound by writing $\sup S = \infty$. Also, for the empty set we write $\sup \varnothing = -\infty$. $\lozenge$

We justify the definition above by noting that every element x of an ordered field F is an upper bound for $\varnothing$ (otherwise, there would be an element of $\varnothing$ greater than x); thus every such element x should be greater than or equal to the supremum

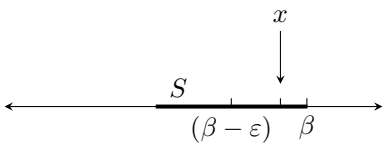

Figure 1.1. For each $\epsilon > 0$ there exists $x \in S$ with $\beta - \epsilon < x$.

of $\varnothing$. Thus it makes sense to set $\sup \varnothing = -\infty$. A consequence of this is that for all sets B, one has $\sup \varnothing \leq B$. So, in particular, when $A \subseteq B$, then $\sup A \leq \sup B$ even when A is empty. We note, however, that when we say $\sup S$ exists, we mean that it exists as an element of F.

For example, if $S = \{x \in F : 0 < x < 1\}$, then $\sup S = 1$. Clearly, 1 is an upper bound for S and, in addition, if c is any upper bound for S, then $c \geq 1$.

Question 1.2.8. Let F be an ordered field, and let S be a subset of F. Prove that if β is an upper bound of S and $\beta \in S$, then $\sup S = \beta$.

Definition 1.2.9. The **infimum** or **greatest lower bound** of a set $S \subseteq F$, denoted $\inf S$, is defined to be the element α of F such that

- α is a lower bound for S;
- if b is any lower bound for S, then $b \leq \alpha$ (i.e., α is greater than any other lower bound). ♢

The infimum of the empty set is ∞, and we write $\inf \varnothing = \infty$. If S is nonempty and does not have a lower bound, we write $\inf S = -\infty$.

The following lemma gives a useful characterization of the supremum of a set; a similar statement holds for the infimum.

Lemma 1.2.10. *Let S be a nonempty subset of an ordered field F. An element $\beta \in F$ satisfies $\beta = \sup S$ if and only if β is an upper bound for S and for every $\varepsilon > 0$, there exists $x \in S$ such that $x > \beta - \varepsilon$.*

Proof. Suppose that $\beta = \sup S$. Clearly, β is an upper bound for S. Let $\varepsilon > 0$. Suppose to the contrary that every $x \in S$ satisfies $x \leq \beta - \varepsilon$. Then $\beta - \varepsilon$ is also an upper bound for S, but this contradicts that β is the least upper bound. Therefore, there exists $x \in S$ with

$$x > \beta - \varepsilon.$$

To show the converse assume that β is an upper bound and that for every $\varepsilon > 0$ there is $x \in S$ with $x > \beta - \varepsilon$; see Figure 1.1.

Let c be an upper bound for S. Assume to the contrary that $c < \beta$. Then we can take $\varepsilon = \beta - c > 0$. Therefore, there exists $x \in S$ with

$$x > \beta - \varepsilon = \beta - (\beta - c) = c,$$

contradicting that c is an upper bound for S. It follows that $c \geq \beta$, and as β is an upper bound, $\beta = \sup S$. □

1.2.3. Completeness Property of the Reals. Now we state the completeness property, which together with the field and order properties, completes the characterization of the real numbers.

Definition 1.2.11. An ordered field F satisfies the **completeness property**, or is **order complete**, if every nonempty subset of F that has an upper bound has a supremum in F. ◊

We have already seen that the supremum of the empty set is $-\infty$. Also, when a set is not bounded above, its supremum is ∞. So if we allow $\pm\infty$ as a possible value, we can say that for any set S, its supremum $\sup S$ is defined. We know that when the set is nonempty and bounded above, this supremum is in the ordered field, but it will be convenient to know that we can write $\sup S$ for any set $S \subseteq F$. The completeness property has an equivalent formulation in terms of the infimum (see Exercise 1.2.3).

The following theorem will be proved in Section 1.4.

Theorem 1.2.12. *There exists a field that is an ordered field and satisfies the completeness property.*

There is a natural way in which one can claim there is a unique complete ordered field: it can be shown (see Exercise 1.4.5) that given any two complete ordered fields F_1 and F_2 there is a bijection between them that preserves the field and order operations.

Definition 1.2.13. We choose a complete ordered field (for example, the one constructed in Section 1.4), call it the field of **real numbers**, and denote it by $\mathbb{R}$. Whenever we use the real numbers, we will only use the properties of a complete ordered field. ◊

We have already seen that any ordered field, hence $\mathbb{R}$, includes the set of rational numbers $\mathbb{Q}$.

Definition 1.2.14. Define an **irrational** number to be an element of $\mathbb{R} \setminus \mathbb{Q}$. ◊

We can think of the completeness property as "completing" the rational numbers by adding the irrational numbers. For example, we will see in Proposition 1.2.19 that $\sqrt{2}$ is the supremum of a certain set of rational numbers; therefore, it is an element of $\mathbb{R}$. (It will also follow from this that $\mathbb{Q}$ is not complete.)

The completeness property has many applications, and we start with an important property that is named after Archimedes of Syracuse (an equivalent property appears as an axiom in his *On the Sphere and Cylinder* treatise). While we obtain the Archimedean property of the real numbers as a consequence of the completeness property, one can verify that the rational numbers also satisfy this property.

Theorem 1.2.15 (Archimedean property)**.** *If x is a real number, then there exists a natural number n such that $n > x$.*

Proof. If this were not the case, there would exist $x \in \mathbb{R}$ such that $n \leq x$ for all $n \in \mathbb{N}$. This would mean that the set $\mathbb{N}$ is bounded above. Let $\beta = \sup \mathbb{N} \in \mathbb{R}$. By Lemma 1.2.10, for $\varepsilon = 1$ there exists $n \in \mathbb{N}$ such that

$$\beta - 1 < n.$$

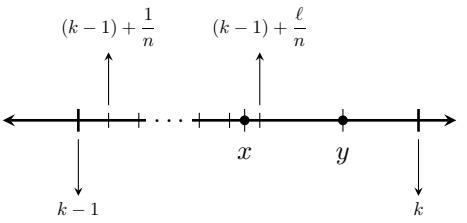

Figure 1.2. Construction of q such that $x < q < y$ (when $y - x < 1$).

Then $\beta < n+1 \in \mathbb{N}$, a contradiction to the fact that β is an upper bound for $\mathbb{N}$. □

This property can also be stated in the following equivalent way (see Exercise 1.2.6).

Corollary 1.2.16. *For each $x \in \mathbb{R}$, $x > 0$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < x$.*

The following is an important consequence, which shows that given any real number there is a rational number that is arbitrarily close to it.

Corollary 1.2.17. *Let x and y be real numbers. If $x < y$, then there exists a rational number q such that*

$$x < q < y.$$

Proof. We may assume that $0 \leq x < y$ (if $x < 0 < y$, let $q = 0$; if $x < y \leq 0$, consider $0 \leq -y < -x$). Let k be the smallest natural number greater than x, i.e.,

$$k = \min\{i \in \mathbb{N} : x < i\}.$$

Then $k-1 \leq x < k$. If $k < y$, then we are done by letting $q = k$, so we may assume that $y \leq k$, the case illustrated by Figure 1.2.

Since $y - x > 0$, by the Archimedean property (Corollary 1.2.16) there exists $n \in \mathbb{N}$ such that

$$\frac{1}{n} < y - x.$$

Starting at $k - 1$, we want to move forward by multiples of $1/n$ until we have a rational number that lands inside the interval (x, y). This is possible since $1/n$ is less than the distance from x to y.

Hence, let

$$\ell = \min\{i \in \mathbb{N} : x < k - 1 + \frac{i}{n}\},$$

and set

$$q = k - 1 + \frac{\ell}{n}.$$

Figure 1.2 shows the construction of q (it shows the case when $y - x < 1$).

We claim that $x < q < y$. First, from the definition of q we have that $x < q$. Now, if it were the case that $q \geq y$, then

$$k - 1 + \frac{\ell - 1}{n} = q - \frac{1}{n} > q + x - y \geq x,$$

contradicting the definition of ℓ. Therefore $q < y$, completing the proof. □

Definition 1.2.18. A set D in $\mathbb{R}$ is said to be **dense** (in $\mathbb{R}$) if for any $x \in \mathbb{R}$ and every $\varepsilon > 0$ there exists $q \in D$ such that $q \in (x - \varepsilon, x + \varepsilon)$. $\Diamond$

Corollary 1.2.17 states that the set of rational numbers is dense in the set of real numbers. The set of integers $\mathbb{Z}$ is not dense in $\mathbb{R}$ as there are no integers that are arbitrarily close to $1/2$, for example. But the set $\mathbb{R} \setminus \mathbb{Z}$ is dense in $\mathbb{R}$.

Now we are in a position to prove that there is a positive number β in $\mathbb{R}$, and only one such element of $\mathbb{R}$, such that $\beta^2 = 2$. We denote this β by $\sqrt{2}$ and recall that we have already shown it is not in $\mathbb{Q}$.

Proposition 1.2.19. *There is a unique positive number $\beta \in \mathbb{R}$ such that $\beta^2 = 2$.*

Proof. Let $S = \{x \in \mathbb{R} : x^2 < 2\}$. Then $S \neq \varnothing$ (as $0 \in S$) and is bounded above by 2 (if $x \in S$, then $x^2 < 2 < 4$, so $x < 2$). Hence by the completeness property, S has a supremum in $\mathbb{R}$, which we denote by β. It is clear that $\beta > 0$ as $1 \in S$. We will show that assuming $\beta^2 < 2$ and assuming $\beta^2 > 2$ each lead to a contradiction. Therefore, it must be that $\beta^2 = 2$.

Now, if $\beta^2 < 2$, we will show there exists $\varepsilon > 0$ such that $(\beta + \varepsilon)^2 < 2$. This will imply $\beta + \varepsilon \in S$, contradicting that β is an upper bound of S as $\beta + \varepsilon > \beta$. For this we need ε to satisfy

$$\beta^2 + 2\beta\varepsilon + \varepsilon^2 < 2 \text{ or} \tag{1.6}$$

$$2\beta\varepsilon + \varepsilon^2 < 2 - \beta^2. \tag{1.7}$$

If we choose $\varepsilon < 1$, then $\varepsilon^2 < \varepsilon$, so if ε satisfies

$$2\beta\varepsilon + \varepsilon < 2 - \beta^2 \text{ or} \tag{1.8}$$

$$\varepsilon(2\beta + 1) < 2 - \beta^2, \tag{1.9}$$

we would have the desired inequality (1.6). This suggests that we choose

$$\varepsilon = \frac{1}{2} \cdot \frac{2 - \beta^2}{2\beta + 1}.$$

Then clearly ε satisfies (1.9). Also, as $\beta > 1$, $0 < \varepsilon < 1$, so ε satisfies (1.6). This shows that assuming $\beta^2 < 2$ leads to a contradiction.

Finally, we assume $\beta^2 > 2$. Now we show that there exists $\varepsilon > 0$ with $\varepsilon < \beta$ such that $(\beta - \varepsilon)^2 > 2$. This would contradict that β is the smallest upper bound of S. Hence we need ε to satisfy

$$\beta^2 - 2\beta\varepsilon + \varepsilon^2 > 2 \text{ or} \tag{1.10}$$

$$2\beta\varepsilon < \beta^2 - 2 + \varepsilon^2. \tag{1.11}$$

It suffices to have

$$2\beta\varepsilon < \beta^2 - 2.$$

Thus choose ε such that $0 < \varepsilon < \beta$ and

$$\varepsilon < \frac{\beta^2 - 2}{2\beta}.$$

This shows that assuming $\beta^2 > 2$ leads to a contradiction. We conclude that $\beta^2 = 2$. It is clear that $\beta \in \mathbb{R}$.

To see uniqueness, let y be any positive element of $\mathbb{R}$ such that $y \neq \beta$. If $y < \beta$, then $y^2 < \beta^2 = 2$, so $y^2 \neq 2$; similarly, if $y > \beta$, then $y^2 \neq 2$. □

Remark 1.2.20. The proof of Proposition 1.2.19 only uses the properties of a complete ordered field. Hence it also follows from the proof that the ordered field $\mathbb{Q}$ is not complete, since if it were complete it would have to have a number whose square is 2, but we have shown no such number exists in $\mathbb{Q}$.

1.2.4. Absolute Value and Intervals

Definition 1.2.21. We define the **absolute value** of a real number x denoted $|x|$. For $x \in \mathbb{R}$ set

$$|x| = \begin{cases} x, & \text{if } x \geq 0; \\ -x, & \text{if } x < 0. \end{cases} \tag{1.12}$$

◊

Proposition 1.2.22. *The absolute value satisfies the following properties.*

(1) $|x| \geq 0$, *with equality holding if and only if* $x = 0$;

(2) $|xy| = |x||y|$;

(3) Triangle inequality: $|x + y| \leq |x| + |y|$.

Proof. We show the triangle inequality. The other properties are immediate from the definition. First note that $x \leq |x|$ and $-x \leq |x|$ for every $x \in \mathbb{R}$. Let $x, y \in \mathbb{R}$. If $x + y \geq 0$, then

$$|x + y| = x + y \leq |x| + |y|.$$

If $x + y < 0$, then

$$|x + y| = -x - y \leq |x| + |y|.$$

Hence, $|x + y| \leq |x| + |y|$. □

We conclude with the notation and definition for **intervals** in $\mathbb{R}$.

Definition 1.2.23. For $a \leq b$, write

$$\begin{aligned} (a, b) &= \{x \in \mathbb{R} : a < x < b\}, \text{ this is called an } \textbf{open interval}, \\ [a, b] &= \{x \in \mathbb{R} : a \leq x \leq b\}, \text{ this is called a } \textbf{closed interval}, \\ (a, b] &= \{x \in \mathbb{R} : a < x \leq b\}, \\ [a, b) &= \{x \in \mathbb{R} : a \leq x < b\}. \end{aligned}$$

◊

Note that when $b = a$, the interval (a, a) is the empty set. (Some authors require intervals to be nonempty.)

Definition 1.2.24. We define the **infinite intervals**:

$$\begin{aligned} (a, \infty) &= \{x \in \mathbb{R} : x > a\}, \\ [a, \infty) &= \{x \in \mathbb{R} : x \geq a\}, \\ (-\infty, b) &= \{x \in \mathbb{R} : x < b\}, \\ (-\infty, b] &= \{x \in \mathbb{R} : x \leq b\}, \\ (-\infty, \infty) &= \mathbb{R}. \end{aligned}$$

◊

Exercises: Completeness Property of $\mathbb{R}$

1.2.1 Prove that $\sqrt{p} \notin \mathbb{Q}$ when p is prime.

1.2.2 Prove that $\sqrt{a} \notin \mathbb{Q}$ when a is not a perfect square (i.e., a is an integer not of the form b^2 for some integer b).

1.2.3 State the analogue of the completeness property using the infimum instead of the supremum. Prove that the completeness property for the infimum is equivalent to the completeness property for the supremum. (*Hint*: Note that for any set $S \subseteq \mathbb{R}$, $\sup S = -\inf(-S)$, where $-S = \{-x : x \in S\}$.)

1.2.4 Let S be a nonempty set of real numbers. Show that a real number α satisfies $\alpha = \inf S$ if and only if α is a lower bound for S and for every $\varepsilon > 0$ there exists $x \in S$ such that $x < \alpha + \varepsilon$.

1.2.5 Prove that the rational numbers satisfy the Archimedean property: for each $r \in \mathbb{Q}$ there exists $n \in \mathbb{N}$ such that $n > r$. Prove this without using the completeness property of the real numbers.

1.2.6 Prove that the following property is equivalent to the Archimedean property: for each $x \in \mathbb{R}$, $x > 0$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < x$.

1.2.7 (Gauss) Let $p(x)$ be a polynomial with integer coefficients of the form $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where all $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$. Show that if $a \in \mathbb{R}$ is a **root** of $p(x)$, i.e., $p(a) = 0$, and a is not an integer, then a is irrational.

1.2.8 Prove that for each $n \in \mathbb{N}$, if $\sqrt{n}$ is not an integer, then it is irrational.

1.2.9 Extend the proof of Proposition 1.2.19 to show that for every real number $x > 0$, the square root of x is a real number.

∗ 1.2.10 Prove that for each $a \in \mathbb{R}^+$ and each $q \in \mathbb{N}$ there exists a unique $s \in \mathbb{R}^+$ such that $s^q = a$; this number s defines $a^{1/q}$.

1.2.11 Let $a \in \mathbb{R}^+$. Use Exercise 1.2.10 to define a^r for each rational number r.
(a) Prove that $(a^{1/q})^p = (a^p)^{1/q}$ for $p, q \in \mathbb{N}$.
(b) Prove that if $r, s \in \mathbb{Q}$, then $a^r a^s = a^{r+s}$ and $a^{-r} = 1/a^r$.

1.2.12 Let $a \in \mathbb{R}^+$. For $x \in \mathbb{R}$ define

$$a^x = \sup\{a^r : r \in \mathbb{Q}, r < x\}.$$

(a) Prove that when $x \in \mathbb{Q}$ this gives the same definition as Exercise 1.2.11.
(b) Prove that $a^{x+y} = a^x a^y$ for $x, y \in \mathbb{R}$.

1.2.13 Prove that for all positive real numbers x and y there exists $n \in \mathbb{N}$ such that $y < nx$.

1.2.14 Find:
(a) $\sup(0, 1)$;
(b) $\inf(0, 1)$.
Prove your answer in each case.

1.2.15 Find:
(a) $\sup[(1,2) \cap \mathbb{Q}]$;
(b) $\inf[(1,2) \cap \mathbb{Q}]$ in the ordered field $\mathbb{Q}$.
Prove your answer in each case.

1.2.16 Complete the details in the proof of Corollary 1.2.17.

1.2.17 Let F be an ordered field and let $A \subseteq B \subseteq F$.
(a) Prove that $\inf A \geq \inf B$.
(b) Prove that if A is nonempty, $\inf A \leq \sup A$.

1.2.18 Give another proof of the triangle inequality by expanding the expression $(x+y)^2$.

1.2.19 Let $x, y \in \mathbb{R}$, $y > 0$. Prove that $|x| < y$ if and only if $-y < x < y$.

1.2.20 Prove that $|x-a| < \varepsilon$ if and only if $a - \varepsilon < x < a + \varepsilon$ for every $x, a, \varepsilon \in \mathbb{R}, \varepsilon > 0$.

1.2.21 Prove that for all real numbers x and all $n \in \mathbb{N}$, $|x^n| = |x|^n$.

1.2.22 Prove that for all real numbers x and y, $||x| - |y|| \leq |x - y|$.

1.2.23 Let F be an ordered field. Prove that F satisfies the Archimedean property if and only if the natural numbers in F are not bounded above.

1.2.24 Prove that the ordered field $F(x)$ of Exercise 1.1.20 does not satisfy the Archimedean property (i.e., the set $\mathbb{N}$ is bounded in $F(x)$).

1.3. Countable and Uncountable Sets

While the definition of finite (and hence infinite) sets does not hold any surprises, we shall see that there are different "sizes" of infinite sets. This is a fundamental and nontrivial observation that we owe to Cantor. The simplest (i.e., smallest in some reasonable sense) kind of infinite sets are the countably infinite sets. To distinguish the subtle differences between different kinds of infinity, we use the notion of a function. The reader who has not seen finite sets should read Subsection 0.5.4.

1.3.1. Countable Sets

Definition 1.3.1. A set A is **countable** if it is finite or if there is a bijection $f : \mathbb{N} \to A$ (in this case we can see A as the set $\{f(1), f(2), \ldots\}$). A set is **countably infinite** if it is countable and not finite. ♢

In particular, the set of natural numbers $\mathbb{N}$ is a countable set. We observe now that $\mathbb{N}$ is not finite. In fact, if for some $n \in \mathbb{N}$ we have a function $f_n : J_n \to \mathbb{N}$, we can define

$$a = f_n(1) + \cdots + f_n(n) + 1.$$

Then a is in $\mathbb{N}$ and, from its definition, it is greater than $f_n(i)$ for all $i = 1, \ldots, n$. It follows that f_n cannot be a surjective function. Thus $\mathbb{N}$ is not finite, and so it is countably infinite. From this argument it also follows that if a set is bijective with $\mathbb{N}$, then it is not finite, so is countably infinite.

We make a remark regarding notation. There is no universal agreement in the literature on the use of the term "countable"; sometimes countable is used to mean what we call "countably infinite". A countably infinite set is also called "denumerable".

Definition 1.3.2. A set is **uncountable** if it is not countable. ◊

Clearly, an uncountable set has to be infinite, but it must be an infinity "greater" than the infinity of sets like $\mathbb{N}$. The existence of uncountable sets is a surprising result which is due to Cantor. Before proving this, we show that many familiar sets are countable. We start with a lemma that will be used later.

Lemma 1.3.3. *If $K \subseteq \mathbb{N}$, then K is countable.*

Proof. If K is finite, we are done, so suppose K is infinite. We wish to define a function $h : \mathbb{N} \to K$ that is a bijection. We define $h(i)$ recursively. Define first

$$h(1) = \min K,$$

which exists as K is nonempty. Assuming that $h(1), \ldots, h(n-1)$ have been defined, set

$$h(n) = \min(K \setminus \{h(1), \ldots, h(n-1)\}).$$

The induction principle is what justifies that h is well-defined. By definition $h(n) \neq h(i)$ for all $i < n, i \in \mathbb{N}$, so h is injective. If h were not surjective, there would exist $k \in K$ such that $h(i) \neq k$ for all $i \in \mathbb{N}$. If $k < h(\ell)$ for some $\ell \in \mathbb{N}$, then k should have been chosen as a value of h before the ℓth step. Thus $k > h(i)$ for all $i \in \mathbb{N}$, a contradiction since h takes infinitely many values (see Exercise 1.3.4). Therefore, h is a bijection. □

Proposition 1.3.4. *Let A be a nonempty set. The following statements are equivalent.*

(1) *A is countable.*

(2) *There exists a function $f : \mathbb{N} \to A$ that is surjective.*

(3) *There exists a function $g : A \to \mathbb{N}$ that is injective.*

Proof. We start by showing that if A is countable, then (2) holds. If A is finite, there exists a bijection $h : J_n \to A$ for some integer n. Define $f : \mathbb{N} \to A$ by

$$f(i) = \begin{cases} h(i) & \text{for } 1 \leq i \leq n, \\ h(1) & \text{for } i > n. \end{cases} \tag{1.13}$$

(There is a lot of freedom in defining f.) It is clear that f is surjective. Next, when A is infinite, it is countably infinite, so there is already a bijection $\mathbb{N} \to A$, which is, of course, surjective.

Now we show that (2) implies (3). Using f, we define g for $a \in A$ by

$$g(a) = \min f^{-1}(\{a\}).$$

Recall that $f^{-1}(\{a\})$ is the set of all points n in $\mathbb{N}$ whose image under f is a, i.e., $f(n) = a$. Since f is surjective, this set is nonempty for each $a \in A$. As it is a subset of $\mathbb{N}$, it has a least element, or minimum, so g is defined for all $a \in A$. Note

also that by its definition, g satisfies the property that $f(g(a)) = a$ for all $a \in A$. Then, by Exercise 0.4.15, g is injective.

Finally, assume that (3) holds. We first note that the function g defines a bijection from A to $g(A)$. Therefore, it follows that if $g(A)$ is countable, then A is countable. Next we observe that $g(A)$ is a subset of $\mathbb{N}$, and so by Lemma 1.3.3, $g(A)$ is countable, completing the proof. □

Question 1.3.5. Let A and B be two sets. Prove that if A is countable and $B \subseteq A$, then B is countable.

It follows that the set of even integers $2\mathbb{N}$, for example, is countably infinite. Something unexpected occurs with infinite sets that does not happen with finite sets: a proper subset of an infinite set, such as $2\mathbb{N}$, may be bijective with the bigger set. We can express this in terms of the notion of "cardinality" of sets.

Definition 1.3.6. We extend the notion of having the same cardinality to arbitrary sets by saying that two sets A and B have the **same cardinality** if they are in one-to-one correspondence, i.e., there is bijection between them. We may write $\text{card}(A) = \text{card}(B)$. The set $\mathbb{N}$ is said to have **cardinality** $\aleph_0$ (pronounced "aleph naught"), where $\aleph$ is the first letter of the Hebrew alphabet. ◊

Thus a countably infinite set is said to have cardinality $\aleph_0$.

We can express the remark above by saying that both $2\mathbb{N}$ and $\mathbb{N}$ have cardinality $\aleph_0$, while $2\mathbb{N}$ is a proper subset of $\mathbb{N}$. (In contrast to this, no proper subset of a finite set A can have the same cardinality as A; see Exercise 1.3.4.)

In the proofs that follow it will be useful to have the notion of a sequence. The reader may be familiar with the basic notion of a sequence from a calculus course, and we will study sequences in greater depth in Chapter 2, but here we introduce some useful notation.

Definition 1.3.7. A **sequence** in a (nonempty) set A is a function from $\mathbb{N}$ to A. We denote this function with $a : \mathbb{N} \to A$. Rather than writing the values of the function as $a(1), a(2), \ldots$, we write $a_1, a_2, \ldots$. We call a_n a **term** of the sequence. In particular a_n is the nth term; we write the sequence as (a_n) or $(a_n)_{n\in\mathbb{N}}$. (Some authors may also denote the sequence (a_n) by $\{a_n\}$ or $\{a_n\}_{n\in\mathbb{N}}$.) ◊

For example, we can define a sequence by setting $a_n = 2n$, for $n \in \mathbb{N}$; this is the sequence of even integers $2, 4, 6, \ldots$.

Proposition 1.3.8. *Let A and B be two sets. If A and B are countable sets, then $A \times B$ is a countable set.*

Proof. We give two proofs as they illustrate different ideas.

Let $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ be injective functions. Let p and q be two distinct primes in $\mathbb{N}$. Define a function $h : A \times B \to \mathbb{N}$ by

$$h(a, b) = p^{f(a)}q^{g(b)}.$$

As integers have a unique decomposition as a product of primes p and q and f, g are injective, it follows that h is injective. Proposition 1.3.4 implies that $A \times B$ is countable.

For the second proof assume that there are surjective functions $a : \mathbb{N} \to A$ and $b : \mathbb{N} \to B$. It suffices to define a surjective function from $\mathbb{N}$ to $A \times B$. We order the elements of $A \times B$ in an array in the following way. First think of a row of the form

$$(a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots, (a_1, b_j), \ldots.$$

(The row is finite if B is finite.) For the second row use a_2 wherever a_1 was used in the first row to obtain

$$(a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots, (a_2, b_j), \ldots.$$

Continue in this way so that the ith row is

$$(a_i, b_1), (a_i, b_2), (a_i, b_3), \ldots, (a_i, b_j), \ldots.$$

If A is finite, there are finitely many rows. Now we define $f : \mathbb{N} \to A \times B$, which is surjective. First set $f(1) = (a_1, b_1)$. Then move down in the array so that each diagonal is covered completely one at a time from top to bottom; this is illustrated in Figure 1.3. (Another equally valid construction could go from bottom to top). The reader should make the appropriate changes in case either A or B is finite. Hence, to cover the second diagonal, we set $f(2) = (a_1, b_2)$ and $f(3) = (a_2, b_1)$. Then start with the third diagonal by setting $f(4) = (a_1, b_3)$, etc. In this way we have a surjective function f. □

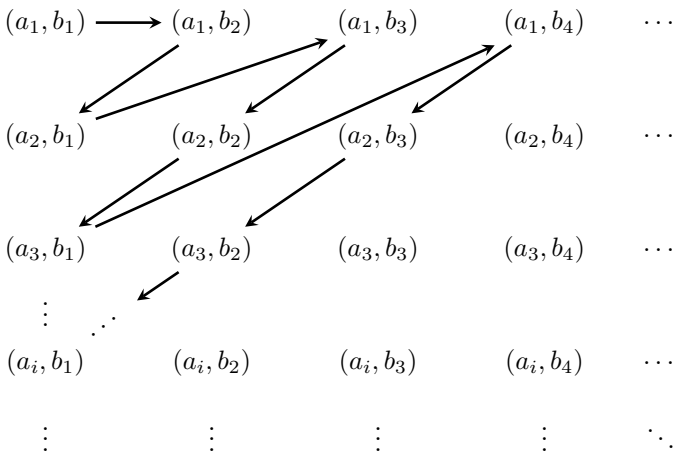

Figure 1.3. Construction of the function f in Proposition 2.3.2.

Corollary 1.3.9. *The set of rational numbers $\mathbb{Q}$ is countable.*

Proof. Let $\mathbb{Q}^+$ stand for the set of positive rational numbers. Define a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}^+$ by

$$f(m, n) = \frac{m}{n}.$$

Then by definition f is surjective. As $\mathbb{N} \times \mathbb{N}$ is countable (by Proposition 1.3.8), it follows that $\mathbb{Q}^+$ is countable. So there is a surjective function $g : \mathbb{N} \to \mathbb{Q}^+$. Now, using g, define a function $h : \mathbb{N} \to \mathbb{Q}$ by

$$h(1) = 0,$$
$$h(2i) = g(i) \text{ for } i \in \mathbb{N},$$
$$h(2i+1) = -g(i) \text{ for } i \in \mathbb{N}.$$

The reader can verify that h is surjective, and therefore $\mathbb{Q}$ is countable. □

The reader is asked to give another proof that $\mathbb{Q}$ is countable along the lines of the second proof in Proposition 1.3.8 (Exercise 1.3.10).

1.3.2. Unions and Intersections of Families of Sets. The definition of union and intersection of two sets can be extended to an arbitrary collection of sets. We use "collection of sets" or "family of sets" instead of "set of sets".

Definition 1.3.10. Let Γ be an arbitrary nonempty set. If for each $\alpha \in \Gamma$ there is a set denoted A_α, we say that $\{A_\alpha : \alpha \in \Gamma\}$ is a **family of sets indexed by** Γ. When Γ is a countable set, we say it is a **countable family**. ◊

For example, if $\Gamma = \mathbb{N}$, then we have a family denoted by $\{A_n : n \in \mathbb{N}\}$. It is possible to have a countable family of sets $\{A_n : n \in \mathbb{N}\}$ where each set A_n is uncountable, as well as an infinite family of sets $\{A_\alpha : \alpha \in \Gamma\}$ (Γ is infinite) where each set A_α is finite.

Definition 1.3.11. Given a family of sets $\{A_\alpha : \alpha \in \Gamma\}$, we define their **union** or **intersection** as follows:

$$\bigcup_{\alpha\in\Gamma} A_\alpha = \{x : x \in A_\alpha \text{ for some } \alpha \in \Gamma\},$$
$$\bigcap_{\alpha\in\Gamma} A_\alpha = \{x : x \in A_\alpha \text{ for all } \alpha \in \Gamma\}.$$

◊

In the case of a countable collection we usually write $\bigcup_{n=1}^{\infty} A_n$ and $\bigcap_{n=1}^{\infty} A_n$ for $\bigcup_{n\in\mathbb{N}} A_n$ and $\bigcap_{n\in\mathbb{N}} A_n$, respectively.

Question 1.3.12. Show that $\bigcap_{n\in\mathbb{N}} \{i \in \mathbb{N} : i > n\} = \varnothing$.

Definition 1.3.13. A family of sets $\{A_\alpha\}_{\alpha\in\Gamma}$ is said to be **disjoint**, sometimes also called *pairwise disjoint*, if $A_\alpha \cap A_\beta = \varnothing$ for all $\alpha, \beta \in \Gamma$ with $\alpha \neq \beta$. ◊

When $\{A_\alpha : \alpha \in \Gamma\}$ is a family of disjoint sets, we may write

$$\bigsqcup_{\alpha\in\Gamma} A_\alpha$$

for the union $\bigcup_{\alpha\in\Gamma} A_\alpha$ to make explicit in the notation that the union is over a pairwise disjoint family. If two sets A and B are disjoint, we may write $A \sqcup B$ for the union $A \cup B$.

Theorem 1.3.14. *A countable union of countable sets is countable: if $\{A_n : n \in \mathbb{N}\}$ is a family such that each set A_n is countable, then their union $\bigcup_{n=1}^{\infty} A_n$ is a countable set.*

Proof. First assume that the sets A_n are disjoint. For each $n \in \mathbb{N}$, let $f_n : A_n \to \mathbb{N}$ be injective, and let p_n be the nth prime (we use that there exist infinitely many primes). Define a function $f : \bigsqcup_{n=1}^{\infty} A_n \to \mathbb{N}$ by

$$f(x) = p_n^{f_n(x)} \text{ if } x \in A_n,$$

where f is a function since the sets are disjoint. We claim that f is injective. Indeed, if $f(x) = f(y)$, then

$$p_n^{f_n(x)} = p_m^{f_m(y)},$$

which implies that $p_n = p_m$ and $f_n(x) = f_m(y)$. Then $n = m$ and $x = y$. Then by Proposition 1.3.4, $\bigsqcup_{n=1}^{\infty} A_n$ is countable.

If the sets A_n are not disjoint, we define a new sequence of sets by

$$B_n = A_n \times \{n\}.$$

The sets B_n are disjoint since if B_n and B_m have a common element (x, y), then $y = n$ and $y = m$, so $n = m$ and they are the same set. Also, $\operatorname{card}(A_n) = \operatorname{card}(B_n)$ for all $n \in \mathbb{N}$, since there is a natural bijection that sends $x \in A_n$ to (x, n) in B_n. By the first part, the union $\bigsqcup_{n=1}^{\infty} B_n$ is countable. The function

$$g : \bigsqcup_{n=1}^{\infty} B_n \to \bigcup_{n=1}^{\infty} A_n,$$

defined by $g(x, n) = x$, is surjective. Proposition 1.3.4 implies that $\bigcup_{n=1}^{\infty} A_n$ is countable. □

Question 1.3.15. Show that if Γ is a countable set and for each $\alpha \in \Gamma$ the set A_α is countable, then $\bigcup_{\alpha \in \Gamma} A_\alpha$ is countable.

1.3.3. An Uncountable Set: $\mathcal{P}(\mathbb{N})$. Let $\{0, 1\}^{\mathbb{N}}$ denote the set of all functions from $\mathbb{N}$ to $\{0, 1\}$. According to our notation, this is the same as the set of all sequences with values in $\{0, 1\}$. For example, $b : \mathbb{N} \to \{0, 1\}$ defined by

$$b_i = \begin{cases} 0 & \text{if } i \text{ is even,} \\ 1 & \text{if } i \text{ is odd,} \end{cases} \tag{1.14}$$

is an element of $\{0, 1\}^{\mathbb{N}}$. This is the sequence whose terms are $0, 1, 0, 1, \ldots$.

The set $\{0, 1\}^{\mathbb{N}}$ can be identified with the set of all subsets of $\mathbb{N}$, namely $\mathcal{P}(\mathbb{N})$. To see this, we will define a one-to-one correspondence that will associate to each subset of $\mathbb{N}$ a unique sequence with values in $\{0, 1\}$. Given a set $A \subseteq \mathbb{N}$, we can define a sequence (a_n) by setting

$$a_n = \begin{cases} 0 & \text{if } n \notin A, \\ 1 & \text{if } n \in A. \end{cases} \tag{1.15}$$

The idea is that we could think of tagging each natural number with 1 if that number is in A and with 0 if the number is not in A. This gives a sequence of 0's and 1's, so in this way each subset of $\mathbb{N}$ is associated with an element of $\{0, 1\}^{\mathbb{N}}$. Conversely, given a sequence $a \in \{0, 1\}^{\mathbb{N}}$, one can define a set $A \subseteq \mathbb{N}$ by setting $A = \{n \in \mathbb{N} : a_n = 1\}$. For example, the sequence $0, 1, 0, 1, \ldots$ corresponds to the even integers. This identification defines a one-to-one correspondence between

sequences with values in $\{0,1\}$ ($\{0,1\}^{\mathbb{N}}$) and $\mathcal{P}(N)$. Therefore $\mathcal{P}(\mathbb{N})$ and $\{0,1\}^{\mathbb{N}}$ have the same cardinality.

Theorem 1.3.16 (Cantor)**.** *The set of subsets of* $\mathbb{N}$*,* $\mathcal{P}(N)$*, is uncountable.*

Proof. We give two proofs, both due to Cantor. The first one proves that $\mathcal{P}(N)$ is uncountable. The second one uses the identification of $\mathcal{P}(\mathbb{N})$ with $\{0,1\}^{\mathbb{N}}$ and shows that $\{0,1\}^{\mathbb{N}}$ is uncountable.

We proceed by contradiction and suppose that the set $\mathcal{P}(\mathbb{N})$ is countable. By Theorem 1.3.4 there exists a surjection $g : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Note that $g(i)$ is a subset of $\mathbb{N}$ for each $i \in \mathbb{N}$. Define the set S by

$$S = \{i \in \mathbb{N} : i \notin g(i)\}.$$

By definition S is a subset of $\mathbb{N}$, and since g is surjective there must exist $n \in \mathbb{N}$ such that $g(n) = S$. Now, either n is an element of S or not. But if $n \in S$, by the definition of n and S we obtain that $n \notin S$. And if $n \notin S$, again by the definition of S we have that $n \in S$. In both cases we have a contradiction; therefore, the function g cannot be surjective. It follows that $\mathcal{P}(\mathbb{N})$ is not countable.

The second proof is a well-known proof that introduces what is known as Cantor's *diagonalization argument*. We show that the set $\{0,1\}^{\mathbb{N}}$ is uncountable.

We again proceed by contradiction and suppose that the set $\{0,1\}^{\mathbb{N}}$ is countable. Then there exists a surjection $f : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Each $f(n)$ is a sequence whose ith element we denote by $f(n)_i$ (where $n, i \in \mathbb{N}$). Now we construct a sequence that is not in the image of f, showing that f could not be surjective, a contradiction. Define a new sequence $\alpha \in \{0,1\}^{\mathbb{N}}$ by

$$\alpha_n = 1 - f(n)_n = \begin{cases} 1 & \text{if } f(n)_n = 0, \\ 0 & \text{if } f(n)_n = 1. \end{cases} \tag{1.16}$$

(The sequence α has been constructed so that at the nth place it differs from the value of the sequence $f(n)$ at the nth place.) As $\alpha \in \{0,1\}^{\mathbb{N}}$ and f is surjective, there must exist $k \in \mathbb{N}$ so that $f(k) = \alpha$. But, from the construction of α, $\alpha_k \neq f(k)_k$, a contradiction. Therefore, f is not surjective and $\{0,1\}^{\mathbb{N}}$ is uncountable. □

It is interesting to note that the argument in the first proof of Theorem 1.3.16 is similar to the argument in Russell's paradox, which appeared a couple of decades after Cantor's theorem. Theorem 1.3.16 will be used to show that the set of real numbers $\mathbb{R}$ is uncountable. This will follow from the representation of the real numbers in binary. The details (addressing the fact that some real numbers may have two representations) will be discussed in Section 2.2 after we cover additional properties of the real numbers that are a consequence of the completeness property.

Exercises: Countable and Uncountable Sets

1.3.1 Write $\mathbb{N}$ as a union of infinitely many disjoint sets each of which is infinite.

1.3.2 Let A and B be sets. Prove that if A is countable and there exists a function $f : A \to B$ that is surjective, then B is countable.

1.3.3 Let A and B be sets. Prove that if B is countable and there exists a function $f : A \to B$ that is injective, then A is countable.

1.3.4 Let A be a finite set. Prove that if $B \subseteq A$, then B is finite. Furthermore, prove that if in addition $B \neq A$, then $\text{card}(B) < \text{card}(A)$.

1.3.5 Let K be an infinite subset of $\mathbb{N}$. Prove that there does not exist $n \in \mathbb{N}$ such that $n > k$ for all $k \in K$.

1.3.6 Let A be a finite nonempty set. A *word* in A is a finite sequence of symbols from A. For example, if $A = \{a, b, c\}$, then an example of a word in A is *abca*. We consider *ab* and *ba* to be different words. Prove that the set of all words in A is countable.

1.3.7 Give a definition of the Cartesian product of k sets $A_1 \times A_2 \times \cdots \times A_k$, and show that if the sets $A_1, \ldots, A_k$ are countable, then their Cartesian product is countable.

1.3.8 Let A be a finite nonempty set. Prove that the set of all functions from A to $\mathbb{N}$ is countable.

1.3.9 Give another proof of the part that (2) implies (3) in Proposition 1.3.4 by using the following construction. Assume that A is infinite. Using f, define a new function $\tilde{f} : \mathbb{N} \to A$ by

$$\tilde{f}(1) = f(1),$$
$$\tilde{f}(n) = f(\tilde{k}) \text{ where } \tilde{k} = \min\{k : f(k) \notin \{\tilde{f}(1), \ldots, \tilde{f}(n-1)\}\}, \text{ for } n > 1.$$

We use induction to justify in detail that $\tilde{f}$ is defined for every element of $\mathbb{N}$. Prove that $\tilde{f}$ is a bijection, and use this to complete the proof.

1.3.10 Give a second proof that $\mathbb{Q}$ is countable using the diagonal construction of the second proof in Proposition 1.3.8.

1.3.11 Give another proof of Theorem 1.3.14 using part (2) in Proposition 1.3.4.

1.3.12 Let A be a countably infinite set. Is the set of all functions from A to $\mathbb{N}$ a countably infinite set? Prove your answer.

1.3.13 Prove that every collection of disjoint intervals (of positive length) is countable.

1.3.14 A number a is said to be an **algebraic number** if it is a root of a polynomial with integer coefficients; i.e., there exists a polynomial p of the form $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_n, \ldots, a_0$ are integers, and $p(a) = 0$. (For example, $\sqrt{2}$ is a root of the polynomial $x^2 - 2 = 0$, so it is algebraic.) Prove that the set of algebraic numbers is countable. (You may use that a polynomial of degree n has at most n roots.)

1.3.15 Let A be a set, and let $\{B_\alpha\}$ be a collection of sets indexed by some set Γ. Show the following distributive properties.
(a) $A \cap (\bigcup_{\alpha\in\Gamma} B_\alpha) = \bigcup_{\alpha\in\Gamma}(A \cap B_\alpha)$
(b) $A \cup (\bigcap_{\alpha\in\Gamma} B_\alpha) = \bigcap_{\alpha\in\Gamma}(A \cup B_\alpha)$

1.3.16 Let A be a set, and let $\{B_\alpha\}$ be a collection of sets indexed by some set Γ. Determine whether the following equality holds. If it does not hold, determine whether one is a subset of the other.

$$A \triangle (\bigcup_{\alpha\in\Gamma} B_\alpha) = \bigcup_{\alpha\in\Gamma} A \triangle B_\alpha.$$

1.3.17 (Inclusion-Exclusion) Let A, B be finite sets. Prove that

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B).$$

Formulate a formula for the cardinality of the union of n finite sets.

1.3.18 (De Morgan's laws) Let Γ be a set, and let $\{G_\alpha\}$ be a collection of sets in some set X indexed by Γ. Show that

$$(\bigcup_{\alpha\in\Gamma} G_\alpha)^c = \bigcap_{\alpha\in\Gamma} G_\alpha^c$$

and

$$(\bigcap_{\alpha\in\Gamma} G_\alpha)^c = \bigcup_{\alpha\in\Gamma} G_\alpha^c.$$

1.3.19 Define the **limit supremum** and **limit infimum** of the sequence of sets $(A_n), n \geq 1$ in a set X by

$$\liminf_{n\to\infty} A_n = \bigcup_{m=1}^{\infty} \bigcap_{n=m}^{\infty} A_n,$$

$$\limsup_{n\to\infty} A_n = \bigcap_{m=1}^{\infty} \bigcup_{n=m}^{\infty} A_n.$$

(a) Show that $\liminf_{n\to\infty} A_n$ is precisely the set of points $x \in X$ such that there exists $k \geq 1$ with $x \in A_n$ for all $n \geq k$. (In this case we say that this is the set of points that are eventually in A_n, i.e., in A_n for all large n.)
(b) Show that $\limsup_{n\to\infty} A_n$ consists of the sets of points $x \in X$ that are in infinitely many A_n.
(c) When does $\liminf_{n\to\infty} A_n = \limsup_{n\to\infty} A_n$? Give a condition that guarantees equality and an example when equality does not hold.

1.3.20 Show that $\{0,1\}^{\mathbb{N}}$ and $\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ have the same cardinality.

∗ 1.3.21 Prove that a set A is finite if and only if whenever $f : A \to A$ is injective, then f is bijective.

1.3.22 Let A be a finite nonempty set. Prove that $A^{\mathbb{N}}$, the set of sequences in A (i.e., functions from $\mathbb{N}$ to A), is uncountable if and only if A has more than one element.

1.3.23 Let A be a set. Prove that there is no surjective function from A to $\mathcal{P}(A)$.

1.4. Construction of the Real Numbers

In this section we outline a construction of the real numbers. It is not necessary for later chapters, and the reader may omit this section. At the same time, many details are left for the interested reader and completing all the details of this section could be viewed as a project.

We follow Dedekind's construction which is based on Dedekind cuts. We will construct an ordered field and prove it has all the properties that we expect: it is a field, it is ordered, and it is order complete. This construction was published by Richard Dedekind in 1872; another construction due to Cantor was published at about the same time (it uses Cauchy sequences to construct what is now called a *metric completion*; see Subsection 4.5.1).

The idea of the construction is to start with the field of rational numbers (which we have already seen is not order complete) and then construct a new set which is an order-complete ordered field. Each element of this new field will be a particular collection of rational numbers, so each real number will be a set of rational numbers with some special properties.

We want this new set (which we will call the set of real numbers) to contain numbers such as $\sqrt{2}$, for example (where as before, by $\sqrt{2}$ we understand a positive number whose square is 2). The idea is to represent $\sqrt{2}$ by the set ρ of all rational numbers that approximate $\sqrt{2}$ from below; we wish to think of ρ as an infinite "ray" to the left of the real number we want to represent. Then we can define ρ as consisting of all negative rational numbers plus the nonnegative rational numbers whose square is less than 2. (If we just say that ρ consists of rational numbers x such that $x^2 < 2$, then this set would not include numbers such as -4, for example, so we had to be more careful with the definition.) Note that we only need properties of $\mathbb{Q}$ to define this set. Now we note two properties of this set ρ. The first is that if x is in ρ and $y < x$, then y is also in ρ. (The idea is that ρ is an infinite ray to the left.) The second property is that if x is in ρ, there is also another rational z in ρ such that $x < z$. This is crucial to the idea that ρ "approximates" $\sqrt{2}$ from below; it says we can get closer and closer to $\sqrt{2}$. These two properties characterize what we call a Dedekind cut, which we define next.

Definition 1.4.1. A subset α of $\mathbb{Q}$ is said to be a **Dedekind cut** (sometimes simply called a **cut**) if it satisfies the following three properties.

(1) Both α and its complement α^c in $\mathbb{Q}$ are nonempty.

(2) If $x \in \alpha$ and $y < x$, then $y \in \alpha$.

(3) If $x \in \alpha$, then there is some $z \in \alpha$ such that $x < z$. ◊

It follows from these properties that if α is a cut, then there must be a rational number r in its complement, and every element of α must be less than r. For an example of a cut, the reader should verify that the set $\rho = \{r \in \mathbb{Q} : r < 0, \text{ or } r \geq 0 \text{ and } r^2 < 2\}$ is a Dedekind cut.

Definition 1.4.2. We define the set of **real numbers** $\mathbb{R}$ to be the set of all Dedekind cuts. Hence, $\mathbb{R}$ is a certain subset of the power set of $\mathbb{Q}$. ◊

There is a natural way in which we can think of $\mathbb{R}$ as containing $\mathbb{Q}$, which will be a consequence of the following definition.

Definition 1.4.3. For each rational number r, define the **cut corresponding to** r by

$$[r] = \{x \in \mathbb{Q} : x < r\}. \qquad \Diamond$$

It follows that each set $[r]$ is a cut. By identifying each rational number r with the cut $[r]$, we can think of $\mathbb{R}$ as containing a copy of $\mathbb{Q}$.

Our next task is to define operations of addition "+" and multiplication "$\cdot$" on $\mathbb{R}$ with respect to which $\mathbb{R}$ becomes a field, and then to define an order on $\mathbb{R}$ so that $\mathbb{R}$ is order complete with respect to this order.

We first define addition.

Definition 1.4.4. Given two cuts α and β in $\mathbb{R}$, let

$$\alpha + \beta = \{x + y : x \in \alpha \text{ and } y \in \beta\}. \qquad \Diamond$$

One needs verify that $\alpha+\beta$ is indeed a cut (Exercise 1.4.1). From the definitions one can see that $\alpha + \beta = \beta + \alpha$ and $\alpha + [0] = \alpha$. The verification of associativity is also straightforward. The definition of multiplication needs some care, and we first define the additive inverse.

Definition 1.4.5. For each α in $\mathbb{R}$ define

$$-\alpha = \{y \in \mathbb{Q} : -y - r \notin \alpha \text{ for some } r \in \mathbb{Q}, r > 0\}. \qquad \Diamond$$

For example,

$$\begin{aligned} -[2] = \{y : -y - r \notin [2]\} &= \{y : -y - r \geq 2\} = \{y : y \leq -2 - r\} \\ &= \{y : y < -2\} = [-2], \end{aligned}$$

as expected. Now we show that this indeed defines the additive inverse. A similar argument shows that for all $r \in \mathbb{Q}$,

$$-[r] = [-r].$$

Lemma 1.4.6. *For each α in $\mathbb{R}$, $\alpha + (-\alpha) = [0]$.*

Proof. Let $s \in \alpha + (-\alpha)$. Then $s = p + q$ where $p \in \alpha$ and $q \in -\alpha$. Since $-q - r \notin \alpha$ for some $r > 0$, then $-q \notin \alpha$. This means that $p < -q$, or $p + q < 0$, so $s \in [0]$. The converse is left to the reader. $\square$

We are not quite ready to define the product, as this is defined in parts, and needs the notion of a positive cut. Thus we first need to define an order.

Definition 1.4.7. Define the **positive reals** $\mathbb{R}^+$ to consist of all cuts α in $\mathbb{R}$ so that some element of α is a positive rational number. Write $\alpha > [0]$ if $\alpha \in \mathbb{R}^+$, and $\alpha > \beta$ if $\alpha - \beta > 0$. Also, we write $\alpha \geq \beta$ if $\alpha > \beta$ or $\alpha = \beta$, and $\alpha < \beta$ if $\beta > \alpha$. $\Diamond$

We need to show that $\mathbb{R}^+$ is a positive set in the field $\mathbb{R}$. We start with the trichotomy property. For the other property of a positive set we need the product of two elements in $\mathbb{R}$ in Definition 1.4.10.

Lemma 1.4.8. *Let α be a cut. Then exactly one of the following holds: $\alpha = [0]$, or $\alpha > [0]$, or $-\alpha > [0]$.*

Proof. Let α be a cut. If $\alpha = [0]$, then $\alpha \notin R^+$ since it does not contain any positive elements, and $-\alpha = -[0] = \alpha$ is similarly not in $\mathbb{R}^+$. Suppose now that $\alpha \neq [0]$. If α contains a positive rational number, then $\alpha \in \mathbb{R}^+$. If not, every element of α is negative, and as α is not $[0]$, there exists $q < 0$ such that $q \notin \alpha$. We claim that $-q \in -\alpha$. In fact $r = -q > 0$, and $q - r = 2q \notin \alpha$ since $q < 2q$ and q is not in α. Thus $-q$ is in $-\alpha$. Finally, suppose $\alpha \in \mathbb{R}^+$. If $-\alpha$ is also in $\mathbb{R}^+$, then there exists $p \in -\alpha$ such that $p > 0$. But for all $r > 0$, we have that $-p - r < 0$, so $-p - r \in \alpha$, a contradiction to the choice of p. □

Question 1.4.9. Let α be a cut. Show that if $\alpha > [0]$, then $-\alpha < [0]$.

We now define the product of two cuts.

Definition 1.4.10. Let α and β be two cuts. First assume that α and β are in $\mathbb{R}^+$. Then define

$$\alpha \cdot \beta = \{r \in \mathbb{Q} : r \leq pq \text{ for some } p \in \alpha, p > 0, \text{ and } q \in \beta, q > 0\}.$$

When $-\alpha$ and $-\beta$ are both in $\mathbb{R}^+$, we define $\alpha \cdot \beta = (-\alpha) \cdot (-\beta)$. Other cases are defined similarly: when α is positive and $-\beta$ is positive, we define $\alpha \cdot \beta = -(\alpha \cdot (-\beta))$, and when $-\alpha$ is positive and β is positive, we define $\alpha \cdot \beta = -((-\alpha) \cdot \beta)$. Finally, for any α and β, $\alpha \cdot [0]$ and $[0] \cdot \beta$ are defined to be $[0]$. ◊

One has to check of course that this product is a cut.

Lemma 1.4.11. *For each α in $\mathbb{R}$, $\alpha \cdot [1] = \alpha$.*

Proof. Let $p \in \alpha \cdot [1]$. Then $p \leq rq$ for $r \in \alpha$ and $0 < q < 1$. Hence $p \leq r$. As r is in α, then $p \in \alpha$. Conversely, let $p \in \alpha$. Then there is $p' \in \alpha$ with $p < p'$, and we may assume $p' \neq 0$. Hence $p = p' \cdot \frac{p}{p'}$. As $p/p' \in [1]$, then $p \in \alpha \cdot [1]$. □

Now the reader is invited to complete the proof of the following proposition.

Proposition 1.4.12. *The set of Dedekind cuts $\mathbb{R}$ with the operations $+$ and $\cdot$ that have been defined form a field.*

Lemma 1.4.13. *The set $\mathbb{R}^+$ is a positive set and makes $\mathbb{R}$ into an ordered field.*

Proof. We show that $\mathbb{R}^+$ satisfies the properties of Definition 1.1.8. Let α and β be in $\mathbb{R}^+$. Then there exists $q_1 \in \alpha, q_2 \in \beta$ such that $q_1 > 0$ and $q_2 > 0$. Thus $q_1 + q_2 > 0$, and since $q_1 + q_2 \in \alpha + \beta$, it follows that $\alpha + \beta$ is in $\mathbb{R}^+$. For the product, we similarly have that $pq > 0$ and $pq \in \alpha \cdot \beta$, so $\alpha \cdot \beta \in \mathbb{R}^+$.

The trichotomy property is in Lemma 1.4.8. □

The following properties give a useful alternative characterization of order.

Question 1.4.14. Let α and β be two cuts in $\mathbb{R}$.

(a) Show that for all $r \in \mathbb{Q}$, $r \in \alpha$ if and only if $[r] \leq \alpha$.

(b) Show that $\beta \leq \alpha$ if and only if $\beta \subseteq \alpha$.

We now prove that $\mathbb{R}$ is order complete.

Proposition 1.4.15. *The set $\mathbb{R}$ with the order $<$ satisfies the supremum property.*

Proof. Let A be a nonempty subset of $\mathbb{R}$ that is bounded above with respect to the order $<$. Hence A is a set of cuts. To construct its supremum in $\mathbb{R}$, let α^* be union of all the cuts in A, i.e., $x \in \alpha^*$ if and only if $x \in \alpha$ for some $\alpha \in A$. We first verify α^* is a cut. It is nonempty as A must contain some cut. Let γ be an upper bound for A. As every cut in A is a subset of γ, it follows that $\alpha^* \subseteq \gamma$, so $(\alpha^*)^c$ is nonempty since it contains γ^c.

Now let $x \in \alpha^*$ and suppose $y < x$. As x must be in some cut $\alpha \in A$, then y is in α, so it is in α^*. For the last cut property let $x \in \alpha^*$. Then again x must be in some cut $\alpha \in A$. Hence, there is $z \in \alpha$ such that $x < z$, but this z must be in α^*. This completes the proof that α^* is a cut, so it is an element of $\mathbb{R}$.

It remains to show that α^* is the supremum of A. It is clearly an upper bound since if α is in A, then it must be a subset of α^*, so $\alpha < \alpha^*$. Now suppose γ is any other upper bound for A. Then every cut in A must be a subset of γ, so α^* is a subset of γ, or $\alpha^* \leq \gamma$. □

Exercises: Construction of the Real Numbers

1.4.1 Prove that for all $\alpha, \beta \in \mathbb{R}$, $\alpha + \beta$ as defined is a cut and that $\alpha + \beta = \beta + \alpha$ and $\alpha + [0] = \alpha$.

1.4.2 Prove that for all $\alpha, \beta \in \mathbb{R}$, $\alpha \cdot \beta$ as defined is a cut and that $\alpha \cdot \beta = \beta \cdot \alpha$.

1.4.3 Complete the proof of Lemma 1.4.6.

1.4.4 Complete the proof of Proposition 1.4.12 that $\mathbb{R}$ is a field.

* 1.4.5 Let $\mathbb{R}$ denote the set of real numbers defined in this section. Let F be any complete ordered field. Prove that there exists a bijection $\phi : F \to \mathbb{R}$ such that for all $x, y \in F$, $\phi(x + y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$ and if $x <_F y$, then $\phi(x) < \phi(y)$ (where $<_F$ is the order in F).

1.4.6 (Dedekind cut property) Let F be an ordered field. Prove that F is order complete if and only if whenever A and B are two nonempty subsets of F such that $A \cup B = F$, and for all $a \in A$ and $b \in B$ one has $a < b$, then there exists an element $c \in F$ such that $a \in A$ is equivalent to $a \leq c$.

1.5. The Complex Numbers

The complex numbers form an important and interesting field that is not ordered.

Definition 1.5.1. The set of **complex numbers** $\mathbb{C}$ consists of all ordered pairs of real numbers (a, b), where $a, b \in \mathbb{R}$. A real number a is identified with $(a, 0) \in \mathbb{C}$. ◊

In this way the real numbers can be seen as a subset of the complex numbers. As a set $\mathbb{C}$ is the same as $\mathbb{R} \times \mathbb{R}$ (or $\mathbb{R}^2$) but the notation we now introduce emphasizes

the fact that we endow $\mathbb{C}$ with two operations that make it a field. Rather than writing a complex number $z \in \mathbb{C}$ as $z = (a, b)$, we write

$$z = a + bi.$$

Definition 1.5.2. We call $i = 0 + 1 \cdot i$ the **imaginary unit** and it corresponds to $(0, 1)$. The **real part** of a complex number $z = a + bi$ is $\mathfrak{Re}(z) = a$, and its **imaginary part** is $\mathfrak{Im}(z) = b$. ◊

Both the real and imaginary parts of a complex number are real numbers. Hence, a complex number z is real if and only if $\mathfrak{Im}(z) = 0$.

Definition 1.5.3. We define two operations on $\mathbb{C}$ called **complex addition** and **complex multiplication**. They are defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$ ◊

For example, $i \cdot i = -1$, or $i^2 = -1$.

Theorem 1.5.4. *The set of complex numbers $\mathbb{C}$, with complex addition, additive inverse 0, and complex multiplication, with unit 1, forms a field.*

Proof. The fact that the complex addition is commutative follows immediately from the commutativity of addition of real numbers. Associativity of addition is similar and is left to the reader to verify. It is also clear that $(a + bi) + 0 = a + bi$.

We show that every nonzero element $z = a+bi$ of $\mathbb{C}$ has a multiplicative inverse. Let

$$w = \frac{a - bi}{a^2 + b^2}.$$

As $z \neq 0$, $a^2 + b^2 \neq 0$, so w is defined. We calculate

$$z \cdot w = (a + bi) \cdot \frac{a - bi}{a^2 + b^2} = \frac{a^2 - abi + abi - bi^2}{a^2 + b^2} = 1.$$

The remaining properties are left as an exercise. □

Definition 1.5.5. Given a number $z = a+bi \in \mathbb{C}$, define its **complex conjugate** by

$$\bar{z} = a - bi$$

and its **modulus** by

$$|z| = \sqrt{a^2 + b^2}.$$

It follows that

$$z \cdot \bar{z} = a^2 + b^2 = |z|^2.$$ ◊

We have the following properties.

Lemma 1.5.6. *For complex numbers z and w, the following hold.*

(1) $\overline{z + w} = \bar{z} + \bar{w}$
(2) $\overline{zw} = \bar{z}\bar{w}$
(3) $\bar{\bar{z}} = z$
(4) $|z + w| \leq |z| + |w|$
(5) $|zw| = |z||w|$

Proof. Let $z = a + bi$ and $w = c + di$. For part (1), we compute

$$\begin{aligned}\overline{z+w} &= \overline{a+bi+c+di} = \overline{a+c+(b+d)i} \\ &= a + c - (b+d)i \\ &= a - bi + c - di = \overline{z} + \overline{w}.\end{aligned}$$

For part (4), we first calculate

$$\begin{aligned}|z+w|^2 &= (z+w)\overline{(z+w)} \\ &= (z+w)(\bar{z}+\bar{w}) \\ &= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\ &= |z|^2 + z\bar{w} + w\bar{z} + |w|^2.\end{aligned}$$

Now note that $\overline{(z\bar{w})} = w\bar{z}$, so by Exercise 1.5.8, $z\bar{w} + w\bar{z} = 2\,\mathfrak{Re}(z\bar{w})$ (one could just do this by direct computation). We will also need that $\mathfrak{Re}(z\bar{w}) \leq |z\bar{w}|$. Hence,

$$\begin{aligned}|z+w|^2 &\leq |z|^2 + 2\,\mathfrak{Re}(z\bar{w}) + |w|^2 \\ &\leq |z|^2 + 2|z||w| + |w|^2 \\ &= (|z| + |w|)^2.\end{aligned}$$

The remaining parts are left as exercises. □

Exercises: The Complex Numbers

1.5.1 Prove that there is a bijection from $\mathbb{R}$ to $\mathbb{C}$.

1.5.2 Prove that the set $R = \{(a, 0) : a \in \mathbb{R}\}$, with the operations it inherits from $\mathbb{C}$, is a field. Prove that the map $\phi : R \to \mathbb{R}$ defined by $\phi((a, 0)) = a$ is a bijection that satisfies $\phi(z + w) = \phi(z) + \phi(w)$ and $\phi(z \cdot w) = \phi(z) \cdot \phi(w)$ for all $z, w \in R$.

1.5.3 Is the set $B = \{(0, b) : b \in \mathbb{R}\}$, with the operations it inherits from $\mathbb{C}$, a field?

1.5.4 Complete the proof of Theorem 1.5.4.

1.5.5 Prove that there is no order that can be defined on the field of complex numbers $\mathbb{C}$.

1.5.6 Complete the proof of Lemma 1.5.6.

1.5.7 Prove that for all complex numbers z and w,

$$\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}.$$

1.5.8 Prove that for all complex numbers z and w,

$$\mathfrak{Re}(z) = \frac{z+\bar{z}}{2} \quad \text{and} \quad \mathfrak{Im}(z) = \frac{z-\bar{z}}{2}.$$

1.5.9 Prove that for all complex numbers z, $z = \bar{z}$ if and only if z is real.

1.5.10 Let $p(z) = a_n z^n + \cdots + a_0$ be a polynomial with real coefficients (i.e., $a_i \in \mathbb{R}$). Prove that if w is a root of p (i.e., $p(w) = 0$), then $\bar{w}$ is also a root of p. What if the coefficients are complex but not real?