Chapter 2

Numbers

> God created the integers and the rest is the work of man. (Leopold Kronecker, in an after-dinner speech at a conference, Berlin, 1886)

> "God created the integers and the rest is the work of man." This maxim spoken by the algebraist Kronecker reveals more about his past as a banker who grew rich through monetary speculation than about his philosophical insight. There is hardly any doubt that, from a psychological and, for the writer, ontological point of view, the geometric continuum is the primordial entity. If one has any consciousness at all, it is consciousness of time and space; geometric continuity is in some way inseparably bound to conscious thought. (René Thom, 1986)

In this chapter, we describe the properties of the basic number systems. We briefly discuss the integers and rational numbers, and then consider the real numbers in more detail.

The real numbers form a complete number system which includes the rational numbers as a dense subset. We will summarize the properties of the real numbers in a list of intuitively reasonable axioms, which we assume in everything that follows. These axioms are of three types: (a) algebraic; (b) ordering; (c) completeness. The completeness of the real numbers is what distinguishes them from the rationals numbers and is the essential property for analysis.

The rational numbers may be constructed from the natural numbers as pairs of integers, and there are several ways to construct the real numbers from the rational numbers. For example, Dedekind used cuts of the rationals, while Cantor used equivalence classes of Cauchy sequences of rational numbers. The real numbers that are constructed in either way satisfy the axioms given in this chapter. These constructions show that the real numbers are as well-founded as the natural numbers (at least, if we take set theory for granted), but they don't lead to any new properties of the real numbers, and we won't describe them here.

2.1. Integers

> Why then is this view [the induction principle] imposed upon us with such an irresistible weight of evidence? It is because it is only the affirmation of the power of the mind which knows it can conceive of the indefinite repetition of the same act, when that act is once possible. (Poincaré, 1902)

The set of natural numbers, or positive integers, is

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

We add and multiply natural numbers in the usual way. (The formal algebraic properties of addition and multiplication on $\mathbb{N}$ follow from the ones stated below for $\mathbb{R}$.)

An essential property of the natural numbers is the following induction principle, which expresses the idea that we can reach every natural number by counting upwards from one.

Axiom 2.1. Suppose that $A \subset \mathbb{N}$ is a set of natural numbers such that: (a) $1 \in A$; (b) $n \in A$ implies $(n+1) \in A$. Then $A = \mathbb{N}$.

This principle, together with appropriate algebraic properties, is enough to completely characterize the natural numbers. For example, one standard set of axioms is the Peano axioms, first stated by Dedekind [**3**], but we won't describe them in detail here.

As an illustration of how induction can be used, we prove the following result for the sum of the first n squares, written in summation notation as

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2.$$

Proposition 2.2. For every $n \in \mathbb{N}$,

$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1).$$

Proof. Let A be the set of $n \in \mathbb{N}$ for which this identity holds. It holds for $n = 1$, so $1 \in A$. Suppose the identity holds for some $n \in \mathbb{N}$. Then

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 \\
&= \frac{1}{6} n(n+1)(2n+1) + (n+1)^2 \\
&= \frac{1}{6} (n+1)\left(2n^2 + 7n + 6\right) \\
&= \frac{1}{6} (n+1)(n+2)(2n+3).
\end{aligned}$$

It follows that the identity holds when n is replaced by $n+1$. Thus $n \in A$ implies that $(n+1) \in A$, so $A = \mathbb{N}$, and the proposition follows by induction. □

Note that the right hand side of the identity in Proposition 2.2 is always an integer, as it must be, since one of n, $n+1$ is divisible by 2 and one of n, $n+1$, $2n+1$ is divisible by 3.

Equations for the sum of the first n cubes,

$$\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2,$$

and other powers can be proved by induction in a similar way. Another example of a result that can be proved by induction is the Euler-Binet formula in Proposition 3.9 for the terms in the Fibonacci sequence.

One defect of such a proof by induction is that although it verifies the result, it does not explain where the original hypothesis comes from. A separate argument is often required to come up with a plausible hypothesis. For example, it is reasonable to guess that the sum of the first n squares might be a cubic polynomial in n. The possible values of the coefficients can then be found by evaluating the first few sums, after which the general result may be verified by induction.

The set of integers consists of the natural numbers, their negatives (or additive inverses), and zero (the additive identity):

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

We can add, subtract, and multiply integers in the usual way. In algebraic terminology, $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

Like the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$ are countably infinite.

Proposition 2.3. The set of integers $\mathbb{Z}$ is countably infinite.

Proof. The function $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(1) = 0$, and

$$f(2n) = n, \quad f(2n+1) = -n \qquad \text{for } n \geq 1,$$

is one-to-one and onto. □

The function in the previous proof corresponds to listing the integers as

$$0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 4,\ -4,\ 5,\ -5,\ \dots.$$

Alternatively, but less directly, we can prove Proposition 2.3 by writing

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$$

as a countable union of countable sets and applying Theorem 1.46.

2.2. Rational numbers

A rational number is a ratio of integers. We denote the set of rational numbers by

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$$

where we may cancel common factors from the numerator and denominator, meaning that

$$\frac{p_1}{q_1} = \frac{p_2}{q_2} \qquad \text{if and only if } p_1 q_2 = p_2 q_1.$$

We can add, subtract, multiply, and divide (except by 0) rational numbers in the usual way. In algebraic terminology, $(\mathbb{Q}, +, \cdot)$ a field. We state the field axioms explicitly for $\mathbb{R}$ in Axiom 2.6 below.

We can construct $\mathbb{Q}$ from $\mathbb{Z}$ as the collection of equivalence classes in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ with respect to the equivalence relation $(p_1, q_1) \sim (p_2, q_2)$ if $p_1 q_2 = p_2 q_1$. The usual sums and products of rational numbers are well-defined on these equivalence classes.

The rational numbers are linearly ordered by their standard order, and this order is compatible with the algebraic structure of $\mathbb{Q}$. Thus, $(\mathbb{Q}, +, \cdot, <)$ is an ordered field. Moreover, this order is dense, meaning that if $r_1, r_2 \in \mathbb{Q}$ and $r_1 < r_2$, then there exists a rational number $r \in \mathbb{Q}$ between them with $r_1 < r < r_2$. For example, we can take

$$r = \frac{1}{2}(r_1 + r_2).$$

The fact that the rational numbers are densely ordered might suggest that they contain all the numbers we need. But this is not the case: they have a lot of "gaps," which are filled by the irrational real numbers.

The following theorem shows that $\sqrt{2}$ is irrational. In particular, the length of the hypotenuse of a right-angled triangle with sides of length one is not rational. Thus, the rational numbers are inadequate even for Euclidean geometry; they are yet more inadequate for analysis.

The irrationality of $\sqrt{2}$ was discovered by the Pythagoreans of Ancient Greece in the 5th century BC, perhaps by Hippasus of Metapontum. According to one legend, the Pythagoreans celebrated the discovery by sacrificing one hundred oxen. According to another legend, Hippasus showed the proof to Pythagoras on a boat, while they were having a lesson. Pythagoras believed that, like the musical scales, everything in the universe could be reduced to ratios of integers and threw Hippasus overboard to drown.

Theorem 2.4. There is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof. Suppose for contradiction that $x^2 = 2$ and $x = p/q$ where $p, q \in \mathbb{N}$. By canceling common factors, we can assume p and q are relatively prime (that is, the only integers that divide both p and q are ± 1). Since $x^2 = 2$, we have

$$p^2 = 2q^2,$$

which implies that p^2 is even. Since the square of an odd number is odd, $p = 2r$ must be even. Therefore

$$2r^2 = q^2,$$

which implies that $q = 2s$ is even. Hence p and q have a common factor of 2, which contradicts the initial assumption. □

Theorem 2.4 may raise the question of whether there is a real number $x \in \mathbb{R}$ such that $x^2 = 2$. As we will see in Example 7.47 below, there is.

A similar proof, using the prime factorization of integers, shows that $\sqrt{n}$ is irrational for every $n \in \mathbb{N}$ that isn't a perfect square. Two other examples of irrational numbers are π and e. We will prove in Theorem 4.52 that e is irrational, but a proof of the irrationality of π is harder.

The following result may appear somewhat surprising at first, but it is another indication that there are not "enough" rationals.

Theorem 2.5. The rational numbers are countably infinite.

Proof. The rational numbers are not finite since, for example, they contain the countably infinite set of integers as a subset, so we just have to show that $\mathbb{Q}$ is countable.

Let $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$ denote the set of positive rational numbers, and define the onto (but not one-to-one) map

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}^+, \qquad g(p, q) = \frac{p}{q}.$$

Let $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be a one-to-one, onto map, as obtained in Proposition 1.45, and define $f : \mathbb{N} \to \mathbb{Q}^+$ by $f = g \circ h$. Then $f : \mathbb{N} \to \mathbb{Q}^+$ is onto, and Proposition 1.44 implies that $\mathbb{Q}^+$ is countable. It follows that $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$, where $\mathbb{Q}^- \approx \mathbb{Q}^+$ denotes the set of negative rational numbers, is countable. □

Alternatively, we can write

$$\mathbb{Q} = \bigcup_{q \in \mathbb{N}} \{p/q : p \in \mathbb{Z}\}$$

as a countable union of countable sets, and use Theorem 1.46. As we prove in Theorem 2.19, the real numbers are uncountable, so there are many "more" irrational numbers than rational numbers.

2.3. Real numbers: algebraic properties

The algebraic properties of $\mathbb{R}$ are summarized in the following axioms, which state that $(\mathbb{R}, +, \cdot)$ is a field.

Axiom 2.6. There exist binary operations

$$a, m : \mathbb{R} \times \mathbb{R} \to \mathbb{R},$$

written $a(x, y) = x + y$ and $m(x, y) = x \cdot y = xy$, and elements $0, 1 \in \mathbb{R}$ such that for all $x, y, z \in \mathbb{R}$:

(a) $x + 0 = x$ (existence of an additive identity 0);

(b) for every $x \in \mathbb{R}$ there exists $y \in \mathbb{R}$ such that $x + y = 0$ (existence of an additive inverse $y = -x$);

(c) $x + (y + z) = (x + y) + z$ (addition is associative);

(d) $x + y = y + x$ (addition is commutative);

(e) $x1 = x$ (existence of a multiplicative identity 1);

(f) for every $x \in \mathbb{R} \setminus \{0\}$, there exists $y \in \mathbb{R}$ such that $xy = 1$ (existence of a multiplicative inverse $y = x^{-1}$);

(g) $x(yz) = (xy)z$ (multiplication is associative);

(h) $xy = yx$ (multiplication is commutative);

(i) $(x + y)z = xz + yz$ (multiplication is distributive over addition).

Axioms (a)–(d) say that $\mathbb{R}$ is a commutative group with respect to addition; axioms (e)–(h) say that $\mathbb{R} \setminus \{0\}$ is a commutative group with respect to multiplication; and axiom (i) says that addition and multiplication are compatible, in the sense that they satisfy a distributive law.

All of the usual algebraic properties of addition, subtraction (subtracting x means adding $-x$), multiplication, and division (dividing by x means multiplying by x^{-1}) follow from these axioms, although we will not derive them in detail. The natural number $n \in \mathbb{N}$ is obtained by adding one to itself n times, the integer $-n$ is its additive inverse, and $p/q = pq^{-1}$, where p, q are integers with $q \neq 0$ is a rational number. Thus, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

2.4. Real numbers: ordering properties

The real numbers have a natural order relation that is compatible with their algebraic structure. We visualize the ordered real numbers as the real line, with smaller numbers to the left and larger numbers to the right.

Axiom 2.7. There is a strict linear order $<$ on $\mathbb{R}$ such that for all $x, y, z \in \mathbb{R}$:

(a) either $x < y$, $x = y$, or $x > y$;

(b) if $x < y$ then $x + z < y + z$;

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

For any $a, b \in \mathbb{R}$ with $a \leq b$, we define the open intervals

$$\begin{aligned}(-\infty, b) &= \{x \in \mathbb{R} : x < b\}, \\ (a, b) &= \{x \in \mathbb{R} : a < x < b\}, \\ (a, \infty) &= \{x \in \mathbb{R} : a < x\},\end{aligned}$$

the closed intervals

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

and the half-open intervals

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

All standard properties of inequalities follow from Axiom 2.6 and Axiom 2.7. For example: if $x < y$ and $z < 0$, then $xz > yz$, meaning that the direction of an inequality is reversed when it is multiplied by a negative number; and $x^2 > 0$ for every $x \neq 0$. In future, when we write an inequality such as $x < y$, we will implicitly require that $x, y \in \mathbb{R}$.

Real numbers satisfy many inequalities. A simple, but fundamental, example is the following.

Proposition 2.8. If $x, y \in \mathbb{R}$, then

$$xy \leq \frac{1}{2}\left(x^2 + y^2\right),$$

with equality if and only if $x = y$.

Proof. We have

$$0 \leq (x-y)^2 = x^2 - 2xy + y^2,$$

with equality if and only if $x = y$, so $2xy \leq x^2 + y^2$. □

On writing $x = \sqrt{a}$, $y = \sqrt{b}$, where $a, b \geq 0$, in the result of Proposition 2.8, we get that

$$\sqrt{ab} \leq \frac{a+b}{2},$$

which says that the geometric mean of two nonnegative numbers is less than or equal to their arithmetic mean, with equality if and only if the numbers are equal. A geometric interpretation of this inequality is that the square-root of the area of a rectangle is less than or equal to one-quarter of its perimeter, with equality if and only if the rectangle is a square. Thus, a square encloses the largest area among all rectangles of a given perimeter, which is a simple form of an isoperimetric inequality.

The arithmetic-geometric mean inequality generalizes to more than two numbers: If $n \in \mathbb{N}$ and $a_1, a_2, \ldots, a_n \geq 0$ are nonnegative real numbers, then

$$(a_1 a_2 \ldots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n},$$

with equality if and only if all of the a_k are equal. For a proof, see e.g., Steele [**13**].

2.5. The supremum and infimum

Next, we use the ordering properties of $\mathbb{R}$ to define the supremum and infimum of a set of real numbers. These concepts are of central importance in analysis. In particular, in the next section we use them to state the completeness property of $\mathbb{R}$.

First, we define upper and lower bounds.

Definition 2.9. A set $A \subset \mathbb{R}$ of real numbers is bounded from above if there exists a real number $M \in \mathbb{R}$, called an upper bound of A, such that $x \leq M$ for every $x \in A$. Similarly, A is bounded from below if there exists $m \in \mathbb{R}$, called a lower bound of A, such that $x \geq m$ for every $x \in A$. A set is bounded if it is bounded both from above and below.

Equivalently, a set A is bounded if $A \subset I$ for some bounded interval $I = [m, M]$.

Example 2.10. The interval $(0, 1)$ is bounded from above by every $M \geq 1$ and from below by every $m \leq 0$. The interval $(-\infty, 0)$ is bounded from above by every $M \geq 0$, but it not bounded from below. The set of integers $\mathbb{Z}$ is not bounded from above or below.

If $A \subset \mathbb{R}$, we define $-A \subset \mathbb{R}$ by

$$-A = \{y \in \mathbb{R} : y = -x \text{ for some } x \in A\}.$$

For example, if $A = (0, \infty)$ consists of the positive real numbers, then $-A = (-\infty, 0)$ consists of the negative real numbers. A number m is a lower bound of

A if and only if $M = -m$ is an upper bound of $-A$. Thus, every result for upper bounds has a corresponding result for lower bounds, and we will often consider only upper bounds.

Definition 2.11. Suppose that $A \subset \mathbb{R}$ is a set of real numbers. If $M \in \mathbb{R}$ is an upper bound of A such that $M \leq M'$ for every upper bound M' of A, then M is called the least upper bound or supremum of A, denoted

$$M = \sup A.$$

If $m \in \mathbb{R}$ is a lower bound of A such that $m \geq m'$ for every lower bound m' of A, then m is called the greatest lower bound or infimum of A, denoted

$$m = \inf A.$$

If $A = \{x_i : i \in I\}$ is an indexed subset of $\mathbb{R}$, we also write

$$\sup A = \sup_{i \in I} x_i, \qquad \inf A = \inf_{i \in I} x_i.$$

As an immediate consequence of the definition, we note that the supremum (or infimum) of a set is unique if one exists: If M, M' are suprema of A, then $M \leq M'$ since M' is an upper bound of A and M is a least upper bound; similarly, $M' \leq M$, so $M = M'$. Furthermore, the supremum of a nonempty set A is always greater than or equal to its infimum if both exist. To see this, choose any $x \in A$. Since $\inf A$ is a lower bound and $\sup A$ is an upper bound of A, we have $\inf A \leq x \leq \sup A$.

If $\sup A \in A$, then we also denote it by $\max A$ and refer to it as the maximum of A; and if $\inf A \in A$, then we also denote it by $\min A$ and refer to it as the minimum of A. As the following examples illustrate, $\sup A$ and $\inf A$ may or may not belong to A, so the concepts of supremum and infimum must be clearly distinguished from those of maximum and minimum.

Example 2.12. Every finite set of real numbers

$$A = \{x_1, x_2, \ldots, x_n\}$$

is bounded. Its supremum is the greatest element,

$$\sup A = \max\{x_1, x_2, \ldots, x_n\},$$

and its infimum is the smallest element,

$$\inf A = \min\{x_1, x_2, \ldots, x_n\}.$$

Both the supremum and infimum of a finite set belong to the set.

Example 2.13. If $A = (0, 1)$, then every $M \geq 1$ is an upper bound of A. The least upper bound is $M = 1$, so

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

Similarly, every $m \leq 0$ is a lower bound of A, so

$$\inf(0, 1) = 0.$$

In this case, neither $\sup A$ nor $\inf A$ belong to A. The set $R = (0, 1) \cap \mathbb{Q}$ of rational numbers in $(0, 1)$, the closed interval $B = [0, 1]$, and the half-open interval $C = (0, 1]$ all have the same supremum and infimum as A. Neither $\sup R$ nor $\inf R$ belong to R, while both $\sup B$ and $\inf B$ belong to B, and only $\sup C$ belongs to C.

Example 2.14. Let

$$A = \left\{ \frac{1}{n} : n \in \mathbb{N} \right\}$$

be the set of reciprocals of the natural numbers. Then $\sup A = 1$, which belongs to A, and $\inf A = 0$, which does not belong to A.

A set must be bounded from above to have a supremum (or bounded from below to have an infimum), but the following notation for unbounded sets is convenient. We introduce a system of extended real numbers

$$\overline{\mathbb{R}} = \{-\infty\} \cup \mathbb{R} \cup \{\infty\}$$

which includes two new elements denoted $-\infty$ and ∞, ordered so that $-\infty < x < \infty$ for every $x \in \mathbb{R}$.

Definition 2.15. If a set $A \subset \mathbb{R}$ is not bounded from above, then $\sup A = \infty$, and if A is not bounded from below, then $\inf A = -\infty$.

For example, $\sup \mathbb{N} = \infty$ and $\inf \mathbb{R} = -\infty$. We also define $\sup \varnothing = -\infty$ and $\inf \varnothing = \infty$, since — by a strict interpretation of logic — every real number is both an upper and a lower bound of the empty set. With these conventions, every set of real numbers has a supremum and an infimum in $\overline{\mathbb{R}}$. Moreover, we may define the supremum and infimum of sets of extended real numbers in an obvious way; for example, $\sup A = \infty$ if $\infty \in A$ and $\inf A = -\infty$ if $-\infty \in A$.

While $\overline{\mathbb{R}}$ is linearly ordered, we cannot make it into a field however we extend addition and multiplication from $\mathbb{R}$ to $\overline{\mathbb{R}}$. Expressions such as $\infty - \infty$ or $0 \cdot \infty$ are inherently ambiguous. To avoid any possible confusion, we will give explicit definitions in terms of $\mathbb{R}$ alone for every expression that involves $\pm\infty$. Moreover, when we say that $\sup A$ or $\inf A$ exists, we will always mean that it exists as a real number, not as an extended real number. To emphasize this meaning, we will sometimes say that the supremum or infimum "exists as a finite real number."

2.6. Real numbers: completeness

The rational numbers $\mathbb{Q}$ and real numbers $\mathbb{R}$ have similar algebraic and order properties (they are both densely ordered fields). The crucial property that distinguishes $\mathbb{R}$ from $\mathbb{Q}$ is its completeness. There are two main ways to define the completeness of $\mathbb{R}$. The first, which we describe here, is based on the order properties of $\mathbb{R}$ and the existence of suprema. The second, which we describe in Chapter 3, is based on the metric properties of $\mathbb{R}$ and the convergence of Cauchy sequences.

We begin with an example that illustrates the difference between $\mathbb{Q}$ and $\mathbb{R}$.

Example 2.16. Define $A \subset \mathbb{Q}$ by

$$A = \left\{ x \in \mathbb{Q} : x^2 < 2 \right\}.$$

Then A is bounded from above by every $M \in \mathbb{Q}^+$ such that $M^2 > 2$. Nevertheless, A has no supremum in $\mathbb{Q}$ because $\sqrt{2}$ is irrational: for every upper bound $M \in \mathbb{Q}$ there exists $M' \in \mathbb{Q}$ such that $\sqrt{2} < M' < M$, so M isn't a least upper bound of A in $\mathbb{Q}$. On the other hand, A has a supremum in $\mathbb{R}$, namely $\sup A = \sqrt{2}$.

The following axiomatic property of the real numbers is called Dedekind completeness. Dedekind (1872) showed that the real numbers are characterized by the condition that they are a complete ordered field (that is, by Axiom 2.6, Axiom 2.7, and Axiom 2.17).

Axiom 2.17. Every nonempty set of real numbers that is bounded from above has a supremum.

Since $\inf A = -\sup(-A)$ and A is bounded from below if and only if $-A$ is bounded from above, it follows that every nonempty set of real numbers that is bounded from below has an infimum. The restriction to nonempty sets in Axiom 2.17 is necessary, since the empty set is bounded from above, but its supremum does not exist.

As a first application of this axiom, we prove that $\mathbb{R}$ has the Archimedean property, meaning that no real number is greater than every natural number.

Theorem 2.18. If $x \in \mathbb{R}$, then there exists $n \in \mathbb{N}$ such that $x < n$.

Proof. Suppose, for contradiction, that there exists $x \in \mathbb{R}$ such that $x > n$ for every $n \in \mathbb{N}$. Then x is an upper bound of $\mathbb{N}$, so $\mathbb{N}$ has a supremum $M = \sup \mathbb{N} \in \mathbb{R}$. Since $n \leq M$ for every $n \in \mathbb{N}$, we have $n - 1 \leq M - 1$ for every $n \in \mathbb{N}$, which implies that $n \leq M - 1$ for every $n \in \mathbb{N}$. But then $M - 1$ is an upper bound of $\mathbb{N}$, which contradicts the assumption that M is a least upper bound. □

By taking reciprocals, we also get from this theorem that for every $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $0 < 1/n < \epsilon$.

These results say roughly that there are no infinite or infinitesimal real numbers. This property is consistent with our intuitive picture of a real line $\mathbb{R}$ that does not "extend past the natural numbers," where the natural numbers are obtained by counting upwards from 1. Robinson (1961) introduced extensions of the real numbers, called non-standard real numbers, which form non-Archimedean ordered fields with both infinite and infinitesimal elements, but they do not satisfy Axiom 2.17.

The following proof of the uncountability of $\mathbb{R}$ is based on its completeness and is Cantor's original proof (1874). The idea is to show that given any countable set of real numbers, there are additional real numbers in the "gaps" between them.

Theorem 2.19. The set of real numbers is uncountable.

Proof. Suppose that

$$S = \{x_1, x_2, x_3, \ldots, x_n, \ldots\}$$

is a countably infinite set of distinct real numbers. We will prove that there is a real number $x \in \mathbb{R}$ that does not belong to S.

If x_1 is the largest element of S, then no real number greater than x_1 belongs to S. Otherwise, we select recursively from S an increasing sequence of real numbers a_k and a decreasing sequence b_k as follows. Let $a_1 = x_1$ and choose $b_1 = x_{n_1}$ where n_1 is the smallest integer such that $x_{n_1} > a_1$. Then $x_n \notin (a_1, b_1)$ for all $1 \leq n \leq n_1$. If $x_n \notin (a_1, b_1)$ for all $n \in \mathbb{N}$, then no real number in (a_1, b_1) belongs to S, and we are done e.g., take $x = (a_1 + b_1)/2$. Otherwise, choose $a_2 = x_{m_2}$ where

$m_2 > n_1$ is the smallest integer such that $a_1 < x_{m_2} < b_1$. Then $x_n \notin (a_2, b_1)$ for all $1 \le n \le m_2$. If $x_n \notin (a_2, b_1)$ for all $n \in \mathbb{N}$, we are done. Otherwise, choose $b_2 = x_{n_2}$ where $n_2 > m_2$ is the smallest integer such that $a_2 < x_{n_2} < b_1$.

Continuing in this way, we either stop after finitely many steps and get an interval that is not included in S, or we get subsets $\{a_1, a_2, \dots\}$ and $\{b_1, b_2, \dots\}$ of $\{x_1, x_2, \dots\}$ such that

$$a_1 < a_2 < \cdots < a_k < \cdots < b_k < \cdots < b_2 < b_1.$$

It follows from the construction that for each $n \in \mathbb{N}$, we have $x_n \notin (a_k, b_k)$ when k is sufficiently large. Let

$$a = \sup_{k \in \mathbb{N}} a_k, \qquad \inf_{k \in \mathbb{N}} b_k = b,$$

which exist by the completeness of $\mathbb{R}$. Then $a \le b$ (see Proposition 2.22 below) and $x \notin S$ if $a \le x \le b$, which proves the result. □

This theorem shows that $\mathbb{R}$ is uncountable, but it doesn't show that $\mathbb{R}$ has the same cardinality as the power set $\mathcal{P}(\mathbb{N})$ of the natural numbers, whose uncountability was proved in Theorem 1.47. In Theorem 5.67, we show that $\mathbb{R}$ has the same cardinality as $\mathcal{P}(\mathbb{N})$; this provides a second proof that $\mathbb{R}$ is uncountable and shows that $\mathcal{P}(\mathbb{N})$ has the cardinality of the continuum.

2.7. Properties of the supremum and infimum

In this section, we collect some properties of the supremum and infimum for later use. This section can be referred back to as needed.

First, we state an equivalent way to characterize the supremum and infimum, which is an immediate consequence of Definition 2.11.

Proposition 2.20. If $A \subset \mathbb{R}$, then $M = \sup A$ if and only if: (a) M is an upper bound of A; (b) for every $M' < M$ there exists $x \in A$ such that $x > M'$. Similarly, $m = \inf A$ if and only if: (a) m is a lower bound of A; (b) for every $m' > m$ there exists $x \in A$ such that $x < m'$.

We frequently use this proposition as follows: (a) if M is an upper bound of A, then $\sup A \le M$; (b) if A is nonempty and bounded from above, then for every $\epsilon > 0$, there exists $x \in A$ such that $x > \sup A - \epsilon$. Similarly: (a) if m is a lower bound of A, then $m \le \inf A$; (b) if A is nonempty and bounded from below, then for every $\epsilon > 0$, there exists $x \in A$ such that $x < \inf A + \epsilon$.

Making a set smaller decreases its supremum and increases its infimum. In the following inequalities, we allow the sup and inf to be extended real numbers.

Proposition 2.21. Suppose that A, B are subsets of $\mathbb{R}$ such that $A \subset B$. Then $\sup A \le \sup B$, and $\inf A \ge \inf B$.

Proof. The result is immediate if $B = \varnothing$, when $A = \varnothing$, so we may assume that B is nonempty. If B is not bounded from above, then $\sup B = \infty$, so $\sup A \le \sup B$. If B bounded from above, then $\sup B$ is an upper bound of B. Since $A \subset B$, it follows that $\sup B$ is an upper bound of A, so $\sup A \le \sup B$. Similarly, either $\inf B = -\infty$ or $\inf B$ is a lower bound of A, so $\inf A \ge \inf B$. □

The next proposition states that if every element in one set is less than or equal to every element in another set, then the sup of the first set is less than or equal to the inf of the second set.

Proposition 2.22. Suppose that A, B are nonempty sets of real numbers such that $x \leq y$ for all $x \in A$ and $y \in B$. Then $\sup A \leq \inf B$.

Proof. Fix $y \in B$. Since $x \leq y$ for all $x \in A$, it follows that y is an upper bound of A, so $\sup A$ is finite and $\sup A \leq y$. Hence, $\sup A$ is a lower bound of B, so $\inf B$ is finite and $\sup A \leq \inf B$. □

If $A \subset \mathbb{R}$ and $c \in \mathbb{R}$, then we define

$$cA = \{y \in \mathbb{R} : y = cx \text{ for some } x \in A\}.$$

Multiplication of a set by a positive number multiplies its sup and inf; multiplication by a negative number also exchanges its sup and inf.

Proposition 2.23. If $c \geq 0$, then

$$\sup cA = c \sup A, \qquad \inf cA = c \inf A.$$

If $c < 0$, then

$$\sup cA = c \inf A, \qquad \inf cA = c \sup A.$$

Proof. The result is obvious if $c = 0$. If $c > 0$, then $cx \leq M$ if and only if $x \leq M/c$, which shows that M is an upper bound of cA if and only if M/c is an upper bound of A, so $\sup cA = c \sup A$. If $c < 0$, then then $cx \leq M$ if and only if $x \geq M/c$, so M is an upper bound of cA if and only if M/c is a lower bound of A, so $\sup cA = c \inf A$. The remaining results follow similarly. □

If $A, B \subset \mathbb{R}$, then we define

$$A + B = \{z \in \mathbb{R} : z = x + y \text{ for some } x \in A,\, y \in B\},$$
$$A - B = \{z \in \mathbb{R} : z = x - y \text{ for some } x \in A,\, y \in B\}.$$

Proposition 2.24. If A, B are nonempty sets, then

$$\sup(A + B) = \sup A + \sup B, \qquad \inf(A + B) = \inf A + \inf B,$$
$$\sup(A - B) = \sup A - \inf B, \qquad \inf(A - B) = \inf A - \sup B.$$

Proof. The set $A + B$ is bounded from above if and only if A and B are bounded from above, so $\sup(A + B)$ exists if and only if both $\sup A$ and $\sup B$ exist. In that case, if $x \in A$ and $y \in B$, then

$$x + y \leq \sup A + \sup B,$$

so $\sup A + \sup B$ is an upper bound of $A + B$, and therefore

$$\sup(A + B) \leq \sup A + \sup B.$$

To get the inequality in the opposite direction, suppose that $\epsilon > 0$. Then there exist $x \in A$ and $y \in B$ such that

$$x > \sup A - \frac{\epsilon}{2}, \qquad y > \sup B - \frac{\epsilon}{2}.$$

It follows that

$$x + y > \sup A + \sup B - \epsilon$$

for every $\epsilon > 0$, which implies that

$$\sup(A + B) \geq \sup A + \sup B.$$

Thus, $\sup(A+B) = \sup A + \sup B$. It follows from this result and Proposition 2.23 that

$$\sup(A - B) = \sup A + \sup(-B) = \sup A - \inf B.$$

The proof of the results for $\inf(A + B)$ and $\inf(A - B)$ is similar, or we can apply the results for the supremum to $-A$ and $-B$. □

Finally, we prove that taking the supremum over a pair of indices gives the same result as taking successive suprema over each index separately.

Proposition 2.25. Suppose that

$$\{x_{ij} : i \in I, j \in J\}$$

is a doubly-indexed set of real numbers. Then

$$\sup_{(i,j)\in I\times J} x_{ij} = \sup_{i\in I}\left(\sup_{j\in J} x_{ij}\right).$$

Proof. For each $a \in I$, we have $\{a\} \times J \subset I \times J$, so

$$\sup_{j\in J} x_{aj} \leq \sup_{(i,j)\in I\times J} x_{ij}.$$

Taking the supremum of this inequality over $a \in I$, and replacing 'a' by 'i', we get that

$$\sup_{i\in I}\left(\sup_{j\in J} x_{ij}\right) \leq \sup_{(i,j)\in I\times J} x_{ij}.$$

To prove the reverse inequality, first note that if

$$\sup_{(i,j)\in I\times J} x_{ij}$$

is finite, then given $\epsilon > 0$ there exists $a \in I$, $b \in J$ such that

$$x_{ab} > \sup_{(i,j)\in I\times J} x_{ij} - \epsilon.$$

It follows that

$$\sup_{j\in J} x_{aj} > \sup_{(i,j)\in I\times J} x_{ij} - \epsilon,$$

and therefore that

$$\sup_{i\in I}\left(\sup_{j\in J} x_{ij}\right) > \sup_{(i,j)\in I\times J} x_{ij} - \epsilon.$$

Since $\epsilon > 0$ is arbitrary, we have

$$\sup_{i\in I}\left(\sup_{j\in J} x_{ij}\right) \geq \sup_{(i,j)\in I\times J} x_{ij}.$$

Similarly, if

$$\sup_{(i,j)\in I\times J} x_{ij} = \infty,$$

then given $M \in \mathbb{R}$ there exists $a \in I$, $b \in J$ such that $x_{ab} > M$, and it follows that

$$\sup_{i \in I} \left(\sup_{j \in J} x_{ij} \right) > M.$$

Since M is arbitrary, we have

$$\sup_{i \in I} \left(\sup_{j \in J} x_{ij} \right) = \infty,$$

which completes the proof. □