Chapter 1

REAL NUMBERS

The foundation of Mathematical Analysis is the real numbers. While the set of real numbers is relatively simple, it provides nontrivial examples for most important ideas in analysis. A good understanding of real numbers is a necessary prerequisite for understanding the concepts of differential and integral calculus as well as more advanced topics in analysis.

In this chapter we introduce real numbers using the axiomatic approach. As primitive notions we take the set of real numbers, the operations of addition and multiplication, and the inequality. We then formulate ten axioms that completely describe the set of real numbers. Everything else in this book can be derived from these ten axioms.

Most facts in this chapter will look familiar. We prove these properties of real numbers not to verify their correctness, but to show that they follow from the axioms.

The set of all real numbers will be denoted by $\mathbb{R}$. In what follows, real numbers will be referred to simply as numbers.

1.1 Addition

These are the fundamental properties of addition of numbers:

$\mathbf{1}^+$ $a + b = b + a$;
$\mathbf{2}^+$ $(a + b) + c = a + (b + c)$;
$\mathbf{3}^+$ The equation $a + x = b$ is solvable.

Equalities $\mathbf{1}^+$ and $\mathbf{2}^+$ hold for all numbers a, b, and c. Property $\mathbf{3}^+$ says that for every pair of numbers a and b there exists a number x satisfying $a + x = b$. We do not prove properties $\mathbf{1}^+$, $\mathbf{2}^+$, and $\mathbf{3}^+$, so they can be considered as axioms.

Later we will assume, for the sake of logical completeness, that there are at least two distinct real numbers. Why that assumption is desirable will be dealt with when the need arises. Proposition 1.1.1 asserts the existence of a number with a very special property. But without an understanding tacitly assumed but not explicitly mentioned, the statement is not quite true and the proposed proof is not quite valid. See if you can find the chink in the logic and the remedy.

1.1.1. *There exists one and only one number x such that $b+x=b$ for all numbers b.*

Proof. The existence of a number x satisfying $b+x=b$ follows from $\mathbf{3}^+$. However we may only assert that for every b there exists some number x satisfying the required equation, but we do not know whether that number is the same for all b. This must be proved.

Let a denote an arbitrary number. There exists a number x satisfying

$$a+x=a. \tag{1.1}$$

We will prove that this same number x satisfies $b+x=b$ for every number b. In fact, from $\mathbf{3}^+$ it follows that there is a number y such that $a+y=b$, or, equivalently,

$$b=a+y. \tag{1.2}$$

By (1.2), $\mathbf{2}^+$, $\mathbf{1}^+$, $\mathbf{2}^+$, (1.1), and (1.2), we conclude that

$$b+x=(a+y)+x=a+(y+x)=a+(x+y)=(a+x)+y=a+y=b.$$

We thus have proved that the number x satisfying $a+x=a$ for some arbitrary a, satisfies the same equation for any a. We still have to prove that this is the only number with this property. Assume that there are two such numbers and denote them by x_1 and x_2. Then we have simultaneously

$$x_1+x_2=x_1 \quad \text{and} \quad x_2+x_1=x_2.$$

Consequently, by $\mathbf{1}^+$, we have

$$x_1=x_1+x_2=x_2+x_1=x_2.$$

This proves that there is only one number with the required property. □

Proposition 1.1.1 is interesting for the reason that it allows one to distinguish from the set of all real numbers exactly one real number with the following property: If we add that number to any number a, then as the result we obtain the same number a. The number with this particular property is called *zero* and is denoted by 0. In view of $\mathbf{1}^+$ we have

$$0+a=a+0=a. \tag{1.3}$$

1.1.2. *If $a+x=b$ and $a+y=b$, then $x=y$.*

In other words: The solution of $a+x=b$ is unique for each pair of numbers a and b.

Proof. If $a + x = b$ and $a + y = b$, then

$$a + x = a + y. \tag{1.4}$$

By $\mathbf{3}^+$ there is a number z such that

$$a + z = 0. \tag{1.5}$$

From (1.3), (1.5), $\mathbf{2}^+$, $\mathbf{1}^+$, (1.4), $\mathbf{1}^+$, $\mathbf{2}^+$, (1.5), and (1.3), we obtain

$$\begin{aligned} x &= x + 0 = x + (a + z) = (x + a) + z = (a + x) + z \\ &= (a + y) + z = (y + a) + z = y + (a + z) = y + 0 = y. \end{aligned}$$

□

Note that 1.1.2 implies the following useful property, which is often called the *cancellation law for addition*:

1.1.3. *If $a + x = a + y$, then $x = y$.*

The unique solution x of the equation $a + x = b$ is called the *difference* of a and b and is denoted by $b - a$. From this definition it follows that

1.1.4. $a + (b - a) = b$.

By introducing the difference we have defined a new operation which associates a number $b - a$ with a pair of numbers a and b. This operation is called *subtraction*. Proposition 1.1.2 asserts the uniqueness of subtraction and property $\mathbf{3}^+$ its feasibility.

1.1.5. $a - a = 0$.

Proof. By the definition of 0 we have $a + 0 = a$ and, by 1.1.4, $a + (a - a) = a$. Hence $a - a = 0$, by 1.1.2. □

1.1.6. $(b - a) + a = b$ *and* $(b + a) - a = b$.

Proof. The first of these identities follows at once from 1.1.4, by $\mathbf{1}^+$. In view of 1.1.4 we also may write $a + ((b + a) - a) = b + a$. Hence, by $\mathbf{1}^+$, we get $((b + a) - a) + a = b + a$, and finally $(b + a) - a = b$, by 1.1.3. □

The number $0 - a$ is denoted simply by $-a$ and is called the *opposite* of a. We thus have

$$0 - a = -a. \tag{1.6}$$

1.1.7. $a + (-a) = 0$.

Proof. Substitute $b = 0$ in 1.1.4 and use (1.6). □

1.1.8. $b + (-a) = b - a$.

Proof. From 1.1.7 we have $(a+(-a))+b = 0+b = b$ and consequently $a+(b+(-a)) = b$. Comparing this with 1.1.4 we see that $b+(-a) = b-a$, by 1.1.2. □

1.1.9. $-(-b) = b$.

Proof. Substituting b for a in 1.1.7 we get $b+(-b) = 0$ and therefore, by $\mathbf{1^+}$, $(-b)+b = 0$. On the other hand, substituting $-b$ for a into the same equation 1.1.7 we obtain $(-b)+(-(-b)) = 0$. Consequently $-(-b) = b$, by 1.1.2. □

EXERCISES 1.1

(1) Does the set $\{0\}$ with the usual definition of addition of numbers satisfy $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$?
(2) Does the empty set with the usual notion of addition of numbers satisfy $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$?
(3) In the proof of Proposition 1.1.1, find the chink in the logic and the remedy.
(4) Denote $\mathbb{Z}_3 = \{0, 1, 2\}$. Define addition $\oplus$ in $\mathbb{Z}_3$ by the table below. Does $(\mathbb{Z}_3, \oplus)$ satisfy $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$?

$\oplus$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

(5) Denote $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Define addition $\oplus$ in $\mathbb{Z}_4$ by the table below. Does $(\mathbb{Z}_4, \oplus)$ satisfy $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$?

$\oplus$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(6) Prove the following identities:
   (a) $a - 0 = a$.
   (b) $a + (b - c) = (a + b) - c$.
   (c) $a - (b - c) = (a + c) - b$.
   (d) $(a - b) + (c - d) = (a + c) - (b + d)$.
   (e) $-(a + b) = -a - b$.
   (f) $-(b - a) = a - b$.

1.2 Multiplication

Multiplication assigns to each pair of numbers a and b another number ab, called the *product* of a and b. Multiplication has properties similar to those of addition:

1* $ab = ba$;
2* $(ab)c = a(bc)$;
3* The equation $ax = b$ is solvable whenever $a \neq 0$.

Property **3*** differs from the analogous property of addition by the additional assumption that a is different from 0. The necessity of this restriction is discussed in Section 1.3.

1.2.1. *There exists one and only one number x such that, $bx = b$ for all numbers b.*

Proof. Let a denote an arbitrary number different from 0. In view of **3*** there exists a number x such that

$$ax = a. \tag{1.7}$$

We are going to show that the same number x also satisfies $bx = b$ for all b.

By **3*** there exists a number y satisfying $ay = b$, or

$$b = ay. \tag{1.8}$$

Hence

$$bx = (ay)x = a(yx) = a(xy) = (ax)y = ay = b.$$

We have proved existence of a number with the desired property. It remains to show its uniqueness. If there were two such numbers, x_1 and x_2, then we would have

$$x_1x_2 = x_1 \quad \text{and} \quad x_2x_1 = x_2.$$

By **1*** the second equation can be written as $x_1x_2 = x_2$ and thus it follows that $x_1 = x_2$. This proves that the number is unique. □

Proposition 1.2.1 distinguishes a number with the property that each number b multiplied by that number gives b as the result. This particular number is called the *unit* and denoted by 1. In view of **1*** and 1.2.1 we have

$$1 \cdot a = a \cdot 1 = a.$$

In expressions with specific numbers like the one above, it is customary to write $a \cdot b$ instead of ab.

1.2.2. *If $ax_1 = b$ and $ax_2 = b$, and $a \neq 0$, then $x_1 = x_2$.*

In other words: *The solution of the equation $ax = b$ with $a \neq 0$ is unique.*

Proof. If $ax_1 = b$ and $ax_2 = b$, then

$$ax_1 = ax_2. \tag{1.9}$$

By **3*** there is a number y such that

$$ay = 1. \tag{1.10}$$

From (1.9), (1.10), **1*** and **2***, we find successively

$$\begin{aligned}(ax_1)y &= (ax_2)y,\\ (x_1a)y &= (x_2a)y,\\ x_1(ay) &= x_2(ay),\\ x_1\cdot 1 &= x_2\cdot 1,\\ x_1 &= x_2.\end{aligned}$$

□

As in the case of addition, the above property implies the cancellation law for multiplication:

1.2.3. *If $ax = ay$ and $a \neq 0$, then $x = y$.*

In view of **3*** and 1.2.2, given a pair of numbers a and b such that $a \neq 0$, there exists exactly one number x such that $ax = b$. This number is called the *quotient* of the numbers b and a with *denominator* a and *numerator* b. This number is denoted by $\frac{b}{a}$. Since the number $\frac{b}{a}$ satisfies the equation $ax = b$, we have

$$a\frac{b}{a} = b \quad \text{for } a \neq 0. \tag{1.11}$$

Note that the above defines a new operation which assigns to every pair of numbers a and b such that $a \neq 0$, the number $\frac{b}{a}$. This operation is called *division*.

1.2.4. $\dfrac{a}{a} = 1$ *for $a \neq 0$.*

Proof. For $b = a$, (1.11) implies $a\,\frac{a}{a} = a$. On the other hand, $a \cdot 1 = a$. Hence, by 1.2.2, we obtain $\frac{a}{a} = 1$. □

1.2.5. $c\dfrac{b}{a} = \dfrac{b}{a}\,c = \dfrac{bc}{a}$.

Proof. The first equality is an immediate consequence of **1***. To establish the second equality, we multiply both sides of (1.11) by c to get $(a\frac{b}{a})c = bc$, and hence

$$a\left(\frac{b}{a}c\right) = bc \tag{1.12}$$

by **2***. Since formula (1.11) holds for each number b it thus remains true when b is replaced by bc:

$$a\frac{bc}{a} = bc. \tag{1.13}$$

Now (1.12) and (1.13) implies $\frac{b}{a}c = \frac{bc}{a}$, by 1.2.2. □

1.2.6. $\dfrac{b}{a}\,a = b$ *and* $\dfrac{ba}{a} = b$ *for $a \neq 0$.*

Proof. The first identity follows from (1.11) and $\mathbf{1^*}$. If in (1.11) we write ba instead of b, then we get $a\frac{ba}{a} = ba = ab$. Hence the identity $\frac{ba}{a} = b$ follows by 1.2.2. □

The number $\frac{1}{a}$, for $a \neq 0$, is called the *reciprocal* of a.

1.2.7. $c\dfrac{1}{a} = \dfrac{c}{a}$ *for* $a \neq 0$.

Proof. From 1.2.5 with $b = 1$ we get $c\frac{1}{a} = \frac{c\cdot 1}{a}$ and hence $c\frac{1}{a} = \frac{c}{a}$. □

EXERCISES 1.2

(1) Does the set $\{0\}$ satisfy $\mathbf{1^*}$, $\mathbf{2^*}$, $\mathbf{3^*}$?
(2) Is $0 = 1$ or is $0 \neq 1$? Explain.
(3) Denote $\mathbb{Z}_3 = \{0, 1, 2\}$. Define multiplication $\otimes$ in $\mathbb{Z}_3$ by the table below. Does $(\mathbb{Z}_3, \otimes)$ satisfy $\mathbf{1^*}$, $\mathbf{2^*}$, $\mathbf{3^*}$?

$\otimes$	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

(4) Show that $\frac{1}{2} = 2$ in $(\mathbb{Z}_3, \otimes)$.
(5) Denote $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Define multiplication $\otimes$ in $\mathbb{Z}_4$ by the table below. Does $(\mathbb{Z}_4, \otimes)$ satisfy $\mathbf{1^*}$, $\mathbf{2^*}$, $\mathbf{3^*}$?

$\otimes$	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(6) Denote $\mathbb{Y} = \{0,\ 1,\ 2\}$. Define addition and multiplication in $\mathbb{Y}$ by the following tables:

$\oplus$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	**0**	**1**	**2**
0	2	0	1
1	0	1	2
2	1	2	0

Does $\mathbb{Y}$ with addition $\oplus$ and multiplication $\otimes$ satisfy $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$, $\mathbf{1^*}$, $\mathbf{2^*}$, and $\mathbf{3^*}$? Which of the three elements in $\mathbb{Y}$ equals $\frac{1}{2}$?
(7) Does it follow from axioms $\mathbf{1^+}$, $\mathbf{2^+}$, $\mathbf{3^+}$, $\mathbf{1^*}$, $\mathbf{2^*}$, and $\mathbf{3^*}$ that $ab \neq 0$ whenever $a \neq 0$ and $b \neq 0$?
(8) Prove that $\frac{1}{a}\frac{1}{c} = \frac{1}{a\,c}$, provided $a \neq 0$, $c \neq 0$, and $ac \neq 0$.
(9) Prove that $\frac{1}{\left(\frac{1}{a}\right)} = a$, provided $a \neq 0$ and $\frac{1}{a} \neq 0$.

(10) In the proof of 1.2.5, both sides of (1.11) are multiplied by c to get $\left(a\frac{b}{c}\right)c = bc$. Why can we multiply both sides of an equality by the same number and then assert that the resulting quantities are equal?

1.3 Distributivity

We now complete the list of properties of addition and multiplication with a property that links the two operations.

$+*$ $a(b+c) = ab + ac$

This property is called the *distributivity of multiplication over addition.* In view of **1*** we may also write $(b+c)a = ba + ca$.

1.3.1. $a(b-c) = ab - ac$ *and* $(b-c)a = ba - ca$.

Proof. In view of 1.1.4 we have

$$ac + (ab - ac) = ab \tag{1.14}$$

and

$$c + (b - c) = b. \tag{1.15}$$

Multiplying both sides of (1.15) by a we get $a(c + (b-c)) = ab$ and then applying $+*$ we get

$$ac + a(b - c) = ab. \tag{1.16}$$

From (1.14) and (1.16) we get $a(b-c) = ab - ac$, by 1.1.2. This proves the first identity. The second identity follows by **1***. □

1.3.2. $0 \cdot a = a \cdot 0 = 0$.

Proof. From **1*** we have $0 \cdot a = a \cdot 0$. For $c = b$ we obtain, from the first identity in 1.3.1, $a(b-b) = ab - ab$ and hence $a \cdot 0 = 0$, by 1.1.5. □

From 1.3.2 it follows that the equation $ax = b$ has no solution if $a = 0$ and $b \neq 0$. This explains the necessity of the restriction $a \neq 0$ in **3***. On the other hand, if $a = 0$ and $b = 0$, then every number x satisfies $ax = b$. This explains the necessity of the restriction $a \neq 0$ in 1.2.2.

1.3.3. $(-a)b = -(ab)$ *and* $(-a)(-b) = ab$.

Proof. Since

$$(-a)b = (0-a)b = 0 \cdot b - ab = 0 - ab = -(ab),$$

we have $(-a)b = -(ab)$. Using this equality we may write

$$\begin{aligned}(-a)(-b) &= -(a(-b)) = -(a(0-b)) = -(a \cdot 0 - ab) \\ &= -(0 - ab) = -(-(ab)) = ab,\end{aligned}$$

by 1.3.1, 1.3.2, and 1.1.9. □

1.3.4. *If $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.*

Proof. It suffices to prove that if $a \neq 0$ and $ab = 0$, then $b = 0$. Indeed, since $a \cdot 0 = 0$ (by 1.3.2), $b = 0$ follows from 1.2.2. □

1.3.5. *If $a \neq 0$ and $b \neq 0$, then $\dfrac{b}{a} \neq 0$.*

Proof. It suffices to prove that, if $a \neq 0$ and

$$\frac{b}{a} = 0, \tag{1.17}$$

then $b = 0$. Multiplying (1.17) by a we get $\frac{b}{a}a = 0 \cdot a$. Hence $b = 0$, by 1.2.6 and 1.3.2. □

1.3.6. $\dfrac{b}{a}\dfrac{d}{c} = \dfrac{bd}{ac}$ *for $a \neq 0$ and $c \neq 0$.*

Proof. Since

$$\begin{aligned}(ac)\left(\frac{b}{a}\frac{d}{c}\right) &= \left((ac)\frac{b}{a}\right)\frac{d}{c} = \left(a\left(c\frac{b}{a}\right)\right)\frac{d}{c} \\ &= \left(a\left(\frac{b}{a}c\right)\right)\frac{d}{c} = \left(\left(a\frac{b}{a}\right)c\right)\frac{d}{c} = \left(a\frac{b}{a}\right)\left(c\frac{d}{c}\right),\end{aligned}$$

we have

$$(ac)\left(\frac{b}{a}\frac{d}{c}\right) = bd.$$

On the other hand, we may write

$$(ac)\frac{bd}{ac} = bd,$$

because ac is different from zero, by 1.3.4. Hence $\frac{b}{a}\frac{d}{c} = \frac{bd}{ac}$, by 1.2.2. □

1.3.7. $\dfrac{b}{a} = \dfrac{bc}{ac}$ *for $a \neq 0$ and $c \neq 0$.*

Proof. From 1.2.4 and 1.3.6 we obtain

$$\frac{b}{a} = \frac{b}{a} \cdot 1 = \frac{b}{a}\frac{c}{c} = \frac{bc}{ac}.$$

□

1.3.8. $\dfrac{b}{a} + \dfrac{c}{a} = \dfrac{b+c}{a}$ *and* $\dfrac{b}{a} - \dfrac{c}{a} = \dfrac{b-c}{a}$ *for $a \neq 0$.*

Proof. We have

$$\frac{b}{a} + \frac{c}{a} = b\frac{1}{a} + c\frac{1}{a} = (b+c)\frac{1}{a} = \frac{b+c}{a},$$

which proves the first identity. The proof of the second identity is similar. □

Identities in 1.3.7 and 1.3.8 allow us to add and subtract fractions with arbitrary denominators different from zero. Indeed,

$$\frac{b}{a} + \frac{d}{c} = \frac{bc}{ac} + \frac{ad}{ac} = \frac{bc+ad}{ac}$$

and

$$\frac{b}{a} - \frac{d}{c} = \frac{bc}{ac} - \frac{ad}{ac} = \frac{bc-ad}{ac}.$$

1.3.9. $\dfrac{c}{\left(\frac{b}{a}\right)} = c\dfrac{a}{b}$ *for* $a \neq 0$ *and* $b \neq 0$.

Proof. By 1.3.4, we have $ab \neq 0$ and thus

$$1 = \frac{ab}{ab} = \frac{ba}{ab} = \frac{b}{a} \cdot \frac{a}{b}$$

and hence

$$\left(\frac{b}{a} \cdot \frac{a}{b}\right) c = 1 \cdot c = c,$$

and

$$\frac{b}{a}\left(c\frac{a}{b}\right) = c. \tag{1.18}$$

Since $\frac{b}{a} \neq 0$, we may write

$$\frac{b}{a} \cdot \frac{c}{\left(\frac{b}{a}\right)} = c, \tag{1.19}$$

by (1.11). From (1.18) and (1.19), by using 1.2.2, we obtain the desired identity. $\square$

EXERCISES 1.3

(1) Prove that $\dfrac{\left(\frac{d}{c}\right)}{\left(\frac{b}{a}\right)} = \dfrac{ad}{bc}$ for $a \neq 0$, $b \neq 0$, $c \neq 0$.
(2) Does $(\mathbb{Y}, \oplus, \otimes)$ defined in Exercise 1.2.6 satisfy $+*$?
(3) Does $(\mathbb{Z}_3, \oplus, \otimes)$ satisfy $+*$? (see Exercises 1.1.4 and 1.2.4.)
(4) Does $(\mathbb{Z}_4, \oplus, \otimes)$ satisfy $+*$? (see Exercises 1.1.5 and 1.2.5.)

1.4 Inequalities

All properties of real numbers considered so far can be called algebraic. They concern the algebraic operations of addition and multiplication. We now include a non-algebraic property of being *positive*. To indicate that a is positive we write $0 < a$. We assume the following properties:

$\mathbf{1}^{<}$ For every number a, one and only one of the following relations holds:

$$a = 0 \quad \text{or} \quad 0 < a \quad \text{or} \quad 0 < -a.$$

$\mathbf{2}^{<}$ If $0 < a$ and $0 < b$, then $0 < a + b$ and $0 < ab$.

Any number a such that $0 < -a$ is called *negative*. Property $\mathbf{1}^<$ says that every number is either zero, positive, or negative. Property $\mathbf{2}^<$ tells us that the sum and the product of two positive numbers are positive.

1.4.1. *If* $0 < a$ *and* $0 < b$, *then* $0 < \dfrac{b}{a}$.

Proof. If we had $\frac{b}{a} = 0$, then we would get $b = \frac{b}{a}a = 0 \cdot a = 0$, which contradicts $\mathbf{1}^<$. If we had $0 < -\frac{b}{a}$, it would mean by 1.3.3 that $0 < \left(-\frac{b}{a}\right)a = -b$, which again contradicts $\mathbf{1}^<$. Consequently, we must have $0 < \frac{b}{a}$. □

1.4.2. *If* $a \neq 0$, *then* $0 < aa$.

Proof. If $a \neq 0$, then $0 < a$ or $0 < -a$, by $\mathbf{1}^<$. If $0 < a$, then $0 < aa$, by $\mathbf{2}^<$. If $0 < -a$, then $0 < (-a)(-a) = aa$, by $\mathbf{2}^<$ and 1.3.3. □

1.4.3. $0 < 1$.

Proof. By 1.4.2 we have $0 < 1 \cdot 1 = 1$. (See Exercise 1.4.1.) □

If $0 < b - a$, we say that a *is less than* b and write $a < b$. We can also say that b *is greater than* a and write $b > a$. By this convention the symbol $0 < b$ can be read in two ways: "the number b is positive" or "the number b is greater than zero", because $0 < b - 0$.

From the definition of inequality and from $\mathbf{1}^<$ we obtain the following important property:

1.4.4 (Trichotomy)**.** *For each pair of numbers a and b, one and only one of the following relations holds:*

$$a = b \quad \text{or} \quad a < b \quad \text{or} \quad b < a.$$

1.4.5 (Transitivity)**.** *If* $a < b$ *and* $b < c$, *then* $a < c$.

Proof. The inequalities $a < b$ and $b < c$ mean that $0 < b - a$ and $0 < c - b$. Therefore, in view of $\mathbf{2}^<$, we obtain $0 < (b - a) + (c - b) = c - a$. □

Instead of "$a < b$ and $b < c$" we often write "$a < b < c$."

1.4.6. *If* $a < b$, *then* $a + c < b + c$.

Proof. Since $b - a = (b + c) - (a + c)$, we have $0 < (b + c) - (a + c)$, which means that $a + c < b + c$. □

1.4.7. *If* $a < b$ *and* $c < d$, *then* $a + c < b + d$.

Proof. This is a direct consequence of $\mathbf{2}^<$ and the definition of inequality. □

1.4.8. *If* $a < b$ *and* $0 < c$, *then* $ac < bc$.

Proof. If $a < b$, then $0 < b - a$ and $0 < (b-a)c$ by $\mathbf{2}^<$. Hence $0 < bc - ac$, which means that $ac < bc$. □

1.4.9. *If $a < b$, $c < d$ and $0 < b$, $0 < c$, then $ac < bd$.*

Proof. From 1.4.8 it follows that $ac < bc$ and $bc < bd$. Hence, by transitivity, $ac < bd$. □

Note that in general, $a < b$ and $c < d$ does not imply $ac < bd$.

We write $a \leq b$ to indicate that either $a = b$ or $a < b$. As an immediate consequence of 1.4.4 and this notational convention we obtain the following property: *For each pair of real numbers a and b, one and only one of the following relations holds:*

$$a \leq b \quad \text{or} \quad b < a.$$

1.4.10. *If $a \leq b$ and $b \leq a$, then $a = b$.*

Proof. Since the inequalities $a < b$ and $b < a$ exclude each other, by 1.4.4, only one possibility remains, namely $a = b$. □

EXERCISES 1.4

(1) In the proof of 1.4.3, use was made of 1.4.2. But in order to legitimately use 1.4.2, an understanding, tacitly made but not explicitly mentioned, must have been employed. What was that understanding?
(2) Provide a complete proof for 1.4.4.
(3) Provide a complete proof for 1.4.7.
(4) Show that, if $0 < \varepsilon$, then $m - \varepsilon < m$ for any real number m.
(5) Show that, in general, $a < b$ and $c < d$ does not imply $ac < bd$.
(6) Let $a, b \in \mathbb{Z}_3$. We will write $a < b$ if the same inequality holds for the natural numbers a and b. Does $(\mathbb{Z}_3, \oplus, \otimes, <)$ satisfy $\mathbf{1}^<$, $\mathbf{2}^<$? (See Exercises 1.1.4 and 1.2.4.)
(7) Let $a, b \in \mathbb{Z}_4$. We will write $a < b$ if the same inequality holds for the natural numbers a and b. Does $(\mathbb{Z}_4, \oplus, \otimes, <)$ satisfy $\mathbf{1}^<$, $\mathbf{2}^<$? (See Exercises 1.1.5 and 1.2.5.)
(8) Is it possible to define in $\mathbb{Z}_3$ a relation "$<$" so that $\mathbf{1}^<$, $\mathbf{2}^<$ would be satisfied? How about $\mathbb{Z}_4$?
(9) Let X be a set with addition $+$, multiplication $\cdot$, and order $<$, such that all conditions $\mathbf{1}^+$, $\mathbf{2}^+$, $\mathbf{3}^+$, $\mathbf{1}^*$, $\mathbf{2}^*$, $\mathbf{3}^*$, $\mathbf{+*}$, $\mathbf{1}^<$, $\mathbf{2}^<$ are satisfied. Prove that, if X has at least two elements, then it has infinitely many elements.
(10) Does the set $\{0\}$ satisfy all conditions $\mathbf{1}^+$, $\mathbf{2}^+$, $\mathbf{3}^+$, $\mathbf{1}^*$, $\mathbf{2}^*$, $\mathbf{3}^*$, $\mathbf{+*}$, $\mathbf{1}^<$, $\mathbf{2}^<$?
(11) Does the set $\mathbb{N}$ of all natural numbers satisfy all conditions $\mathbf{1}^+$, $\mathbf{2}^+$, $\mathbf{3}^+$, $\mathbf{1}^*$, $\mathbf{2}^*$, $\mathbf{3}^*$, $\mathbf{+*}$, $\mathbf{1}^<$, $\mathbf{2}^<$?

(12) Does the set $\mathbb{Q}$ of all rational numbers satisfy all conditions $\mathbf{1}^+$, $\mathbf{2}^+$, $\mathbf{3}^+$, $\mathbf{1}^*$, $\mathbf{2}^*$, $\mathbf{3}^*$, $\mathbf{+*}$, $\mathbf{1}^<$, $\mathbf{2}^<$?

1.5 Bounded sets

A set of numbers is said to be *bounded from below* by a number m, if all its elements are greater than or equal to m. The number m is then called a *lower bound* of that set. If m is a lower bound of a set, then each number less than m is another lower bound of the same set. For instance the set of all positive numbers is bounded from below. All negative numbers as well as zero are its lower bounds. The number 0 is the greatest lower bound. It is also the greatest lower bound of the set of all non-negative numbers. In this case the greatest lower bound belongs to the set, whereas in the case of the set of all positive numbers it does not.

Definition 1.5.1. A number m is called the *greatest lower bound* of a given set P, if
(a) m is a lower bound for P, that is, $m \le x$ for each $x \in P$
and
(b) m is the greatest of the lower bounds for P, that is, if $n \le x$ for each $x \in P$, then $m \ge n$.

Notice that a set can have only one greatest lower bound. Indeed, assuming that m_1 and m_2 are the greatest lower bounds of P, we have $m_1 \le m_2$ and $m_2 \le m_1$, so $m_1 = m_2$, which proves the uniqueness.

A question arises, whether every set bounded from below possesses a greatest lower bound. This does not follow from the properties of real numbers considered so far (see Exercise 1.5.1). If we want to use this property, it must be adopted as an additional axiom.

D Every nonempty set bounded from below has a greatest lower bound.

This axiom is often called the Dedekind Axiom. Dedekind (Richard Dedekind, 1831–1916) was the first to construct a model of real numbers. All together we get the following Axioms of The Real Numbers:

$\mathbf{1}^+$ $a + b = b + a$;
$\mathbf{2}^+$ $(a + b) + c = a + (b + c)$;
$\mathbf{3}^+$ The equation $a + x = b$ is solvable;
$\mathbf{1}^*$ $ab = ba$;
$\mathbf{2}^*$ $(ab)c = a(bc)$;
$\mathbf{3}^*$ The equation $ax = b$ is solvable whenever $a \neq 0$;
$\mathbf{+*}$ $a(b + c) = ab + ac$;

1$^<$ For every number a, one and only one of the following relations holds:

$$a = 0 \quad \text{or} \quad 0 < a \quad \text{or} \quad 0 < -a;$$

2$^<$ If $0 < a$ and $0 < b$, then $0 < a + b$ and $0 < ab$;

D Every nonempty set bounded from below has a greatest lower bound.

We will refer to this collection of ten axioms as $\mathfrak{R}$.

S: Do these axioms completely characterize the set of real numbers?

T: People trained in formal logic would say no, because both the empty set and the set consisting of the single element 0 satisfy all ten of the axioms. And yet neither is the set of all real numbers.

S: What if we assume that the set contains at least two elements?

T: Then everything is fine. The existence of two numbers implies, by means of the adopted axioms, the existence of all real numbers. But we have to be very careful with the words "two elements" which have to be understood in the colloquial sense: "one element and another one." A careful reader could notice that we have used the existence of two different real numbers in the proofs of 1.1.1 and 1.4.3. In the first case we need an element b in order to have an equation which must then have 0 as its solution. In the second case we use the fact that $1 \neq 0$, which follows from the existence of two different elements.

S: So the existence of at least two elements is to be adopted as an additional axiom of real numbers.

T: This is one possibility. Or else we may say that the set of real numbers is the set containing at least two elements and satisfying the axioms in $\mathfrak{R}$.

S: I like this better, because then the number of axioms remains 10, and it is nice to have exactly as many axioms as fingers.

A set is said to be *bounded from above* if all its elements are less than or equal to a number n.

Definition 1.5.2. By the *least upper bound* of a given set P we mean a number m such that:
(a) m is an upper bound for P, that is, $x \leq m$ for each $x \in P$
and
(b) m is the least of the upper bounds for P, that is, if $x \leq n$ for each $x \in P$, then $m \leq n$.

Using axiom **D** one can easily prove property

D' Every nonempty set bounded from above has a least upper bound.

To see that **D** implies **D'** and, conversely, **D'** implies **D**, it suffices to consider the set P' of all elements opposite to those from P, that is, a number x belongs to P' if and only if $-x$ belongs to P. Consequently, axiom **D** can be replaced by **D'** and we will obtain an equivalent set of axioms. In view of this equivalence, we will use the same name, Dedekind Axiom, to mean either of the two versions.

In order to avoid possible misunderstanding it should be strongly emphasized that if we say "the set P has a greatest lower bound m" (or "a least upper bound m"), then m need not belong to P. This only means that a number with the required properties exists.

Here is a nice application of the Dedekind Axiom.

Theorem 1.5.3 (Archimedean Property)**.** *For any positive real number ε there is a natural number n such that $n\varepsilon > 1$.*

Proof. We argue by contradiction. If there is no n such that $n\varepsilon > 1$, then the set $S = \{n\varepsilon : n \in \mathbb{N}\}$ is bounded by 1. By the Dedekind Axiom, S has a least upper bound m. Then $n\varepsilon \leq m$ for all $n \in \mathbb{N}$. Hence, $(n-1)\varepsilon \leq m - \varepsilon$ for all $n \in \mathbb{N}$. But in this case we would have $n\varepsilon \leq m - \varepsilon$ for all $n \in \mathbb{N}$, contradicting the definition of m. □

From the Archimidean Property we easily obtain the following useful property of the real numbers.

Corollary 1.5.4. *There is a rational number between any two distinct numbers.*

Proof. Let a and b be arbitrary numbers such that $a < b$. Since $b - a > 0$, there exists a natural number n such that $n(b-a) > 1$. Then there must be an integer m such that $na < m < nb$. Otherwise, for some integer m we would have

$$m \leq na < nb \leq m + 1$$

and consequently

$$n(b-a) = nb - na \leq m + 1 - m = 1.$$

For any integer m such that $na < m < nb$ we have

$$a < \frac{m}{n} < b.$$

□

EXERCISES 1.5

(1) The set $\mathbb{Q}$ of all rational numbers with addition and multiplication defined as usual satisfy all conditions $\mathbf{1}^+$, $\mathbf{2}^+$, $\mathbf{3}^+$, $\mathbf{1}^*$, $\mathbf{2}^*$, $\mathbf{3}^*$, $\mathbf{+*}$, $\mathbf{1}^<$, $\mathbf{2}^<$ (see Exercise 2.4.12). Show that $\mathbb{Q}$ does not satisfy condition **D**. This will show that condition **D** cannot be deduced from the other nine in $\mathfrak{R}$.

(2) Provide details of the proof of equivalence of **D** and **D'**.

(3) Find greatest lower bounds and least upper bounds of the following sets:

(a) $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$,

(b) $\left\{0, -\frac{1}{2}, \frac{2}{3}, -\frac{3}{4}, \frac{4}{5}, -\frac{5}{6}, \dots\right\}$.

(4) Find the least upper bound of the set of all rational numbers whose square is less than 2.

(5) Consider the set $X = \{a_1, a_2, a_3, \dots\}$ where a_n's are defined inductively:

$$a_1 = 1, \; a_{n+1} = \frac{3a_n + 4}{2a_n + 3} \quad \text{for } n = 1, 2, 3, \dots$$

Show that X is bounded from above and from below. Can you find the least upper bound of X?

(6) Using Crolollary 1.5.4, show that there are infinitely many rational numbers between any two distinct numbers.

1.6 Countable and uncountable sets

Suppose we have two boxes of matches: one with white matches and the other one with red. Is there a way for a person who cannot count, to determine which box contains more matches?

Let's take one match from each box and put them aside. From the remaining matches, again take one match from each box and put them aside too. Continuing this process, either we will exhaust both boxes simultaneously or one of the boxes will become empty while the other box will still contain at least one match. The first case occurs if and only if the number of matches is the same in both boxes. In the second case, the box that became empty had fewer matches and the other more. Note that we do not have to count the matches.

Using the described idea, we can check whether two sets have the same quantity of elements without counting them. Two sets are called *equipotent* if, to every element from the first set we can assign exactly one element from the second set in such a way that each element of the second set is assigned to exactly one element of the first set. We then say that there is a bijection between those sets.

Obviously, every set is equipotent with itself. Moreover, if a set A is equipotent with a set B, then B is equipotent with A. Equipotency is also transitive, that is, if a set A is equipotent with a set B and B is equipotent with a set C, then A is equipotent with C. Thus equipotency is an equivalence relation.

In order to establish a correspondence between elements of equipotent sets, we do not necessarily need to join elements in pairs; it suffices to give a law which says how the elements should be joined. Here, however, facts may come to light which seem paradoxical at first glance. For instance the set of all natural numbers is equipotent with the set of all even natural numbers. To establish a bijection between these sets, we associate with every natural number the number that is exactly twice as large, thus even. This is an example of a set which is equipotent with one of its proper subsets. This property can be used as a definition of an infinite set: a nonempty set is called *infinite* if it is equipotent with a proper subset of itself. On the other hand, a nonempty set is called *finite* if it is not equipotent with any proper subset of itself. Finite sets can be also defined as follows: a set A is finite if it is empty or there exists a natural number n such that A is equipotent with the set $\{1, 2, \ldots, n\}$. In this case, we can write $A = \{a_1, a_2, \ldots, a_n\}$.

A set which is equipotent with the set of all natural numbers is called *countable.* Elements of such a set can be numbered so that to each element of the set there corresponds a natural number and each natural number corresponds to one and only one element from the set. All elements of a countable set can thus be arranged into an infinite sequence. In other words, if A is a countable set, we can write $A = \{a_1, a_2, a_3, \ldots\}$. Conversely, if all elements of a set can be arranged into an infinite sequence such that every element appears in the sequence exactly once, then the set is countable. Hence the union of a countable set and a finite set or another countable set is countable. It is also clear that a subset of a countable set is either countable or finite.

Theorem 1.6.1. *The union of a countable family of countable sets is countable.*

Proof. Let $Z_1, Z_2, Z_3, \ldots$ be a sequence of countable sets. The elements of each set Z_n can be arranged into an infinite sequence, so we can write

$$Z_n = \{a_{n,1}, a_{n,2}, a_{n,3}, \ldots\}.$$

Consequently, the elements of the union can be arranged into an infinite matrix

$$\begin{matrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots \\ \vdots & \vdots & \vdots & \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots \\ \vdots & \vdots & \vdots & \end{matrix}$$

Now we want to arrange all entries of this matrix into a single sequence. We can accomplish this by first splitting entries of the matrix into finite groups such that the n-th group consists of all entries $a_{i,j}$ such that $i + j = n + 1$. Thus, in the n-th group we will have

$$a_{n,1}, a_{n-1,2}, a_{n-2,3}, \ldots, a_{2,n-1}, a_{1,n}.$$

These entries form the n-th diagonal of the matrix.

By writing down the first diagonal, then the second diagonal, and so on, we will arrange all entries of the matrix into a single sequence:

$$a_{1,1}, a_{2,1}, a_{1,2}, a_{3,1}, a_{2,2}, a_{1,3}, \ldots$$

In this sequence, some elements of the union may appear several times if some Z_n's have elements in common. In such a case, we have to remove each element which is equal to one of the preceding elements. In this way we obtain an arrangement of the union in a sequence, which proves that the union is countable. □

The following diagram represents the idea of the above proof in a more intuitive and easier to remember way. To arrange all entries of the infinite matrix into a single sequence, we follow the indicated path.

$$\begin{tikzcd}
a_{1,1} \arrow[r] & a_{1,2} \arrow[dl] & a_{1,3} \arrow[r] & a_{1,4} \arrow[dl] & \cdots \\
a_{2,1} \arrow[d] & a_{2,2} \arrow[ur] & a_{2,3} \arrow[dl] & a_{2,4} & \cdots \\
a_{3,1} \arrow[ur] & a_{3,2} \arrow[dl] & a_{3,3} & a_{3,4} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & \cdots \\
\vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Theorem 1.6.2. *The set $\mathbb{Q}$ of all rational numbers is countable.*

Proof. Let, for $n = 1, 2, 3, \ldots$, Z_n denote the set of all rational numbers that can be written with n in the denominator, that is,

$$Z_n = \left\{ \frac{0}{n}, \frac{1}{n}, \frac{-1}{n}, \frac{2}{n}, \frac{-2}{n}, \ldots \right\}.$$

Clearly, each set Z_n is countable and we have

$$\mathbb{Q} = \bigcup_{n=1}^{\infty} Z_n.$$

Thus the set $\mathbb{Q}$ is countable by Theorem 1.6.1. □

Theorem 1.6.3. *The set $\mathbb{R}$ of all real numbers is not countable.*

In the proof of the above theorem we will use the fact that every real number between 0 and 1 can be uniquely represented in the form of an infinite sequence of digits

$$0.d_1 d_2 d_3 \ldots \tag{1.20}$$

such that $d_n \neq 0$ for some index n (to exclude 0) and there are arbitrarily large indices n for which $d_n \neq 9$ (to exclude sequences that have nothing but 9's from some point on.) The representation of a real number in the form (1.20) is called a *decimal expansion*. Any such sequence represents a real number between 0 and 1. (Decimal expansions of real numbers will be discussed in more detail in Section 5.7.)

Proof. We argue by contradiction. Suppose that the set $\mathbb{R}$ is countable. Then the set of all real numbers between 0 and 1 must be countable and thus its elements can be arranged into a sequence $a_1, a_2, a_3, \ldots$. Let

$$a_n = 0.d_{n,1}d_{n,2}d_{n,3}\ldots$$

be the unique decimal expansion of a_n. Now we consider a real number whose decimal expansion is

$$0.e_1e_2e_3\ldots, \tag{1.21}$$

where $e_n \neq d_{n,n}$ and $e_n \neq 9$. Note that (1.21) represents a real number between 0 and 1, though it is not among the numbers in the sequence $a_1, a_2, a_3, \ldots$. Thus the assumption that the set $\mathbb{R}$ is countable leads to a contradiction. □

A set that is neither finite nor countable is called *uncountable*. Real numbers which are not rational numbers are called *irrational numbers*. Note that Theorems 1.6.2 and 1.6.3 imply that the set of irrational numbers is uncountale. Moreover, we obtain the following useful theorem.

Theorem 1.6.4. *There are infinitely many irrational numbers between any two distinct numbers.*

Proof. If $a < b$, then

$$x \longleftrightarrow \frac{x-a}{b-a}$$

establishes a bijection between the set of all real numbers between a and b and the set of all real numbers between 0 and 1. Since there are uncountably many numbers between 0 and 1, there are uncountably many numbers between a and b. □

EXERCISES 1.6

(1) Prove that the union of a finite set and a countable set is countable.
(2) Prove that the union of a finite family of countable sets is countable.
(3) Let A and B be countable sets. Prove that the set $A \times B$ is countable. ($A \times B$ denotes the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.)
(4) Prove that every infinite subset A of a countable set B is countable.
(5) Is the set of all finite sequences of rational numbers countable?
(6) Is the set of all infinite sequences of rational numbers countable?
(7) Is the set of all infinite sequences of natural numbers countable?
(8) Is the set of all infinite binary sequences countable?
(9) A number $\alpha \in \mathbb{R}$ is called *algebraic* if it is a root of a polynomial with integer coefficients, that is, there are integers $\lambda_0, \lambda_1, \ldots, \lambda_n$, not all zero, such that $\lambda_0\alpha^n + \lambda_1\alpha^{n-1} + \cdots + \lambda_{n-1}\alpha + \lambda_n = 0$. Is the set of all algebraic numbers countable?