NUMBERS

Michael E. Taylor

Contents

Introduction

These notes are intended as a companion to a text on introductory real analysis. Typically, books on the subject begin with an axiomatic development of the real number system. However, one can get the feeling that there is more emphasis on the axioms than on the development. For example, [BS] lists no fewer than 14 axioms for the real number system: the well ordering property of the natural numbers (basically, the principle of induction), 9 algebraic identities, 3 order axioms, and the supremum property (basically, the completeness property).

On the other hand, it has been known since the beginning of this century that one can make do with a tiny list of axioms for the natural numbers (i.e., the positive integers), and then build the rest of the edifice logically, obtaining the remaining "axioms" of the real number system, most particularly the crucial completeness property, as theorems.

The task of these notes is to give an account of that development.

1. Peano arithmetic

In Peano arithmetic, we assume we have a set $\mathbb{N}$ (the natural numbers). We assume given $0 \notin \mathbb{N}$, and form $\widetilde{\mathbb{N}} = \mathbb{N} \cup \{0\}$. We assume there is a map

$$s : \widetilde{\mathbb{N}} \longrightarrow \mathbb{N}, \tag{1.1}$$

which is *bijective.* That is to say, for each $k \in \mathbb{N}$, there is a $j \in \widetilde{\mathbb{N}}$ such that $s(j) = k$, so s is *surjective*; and furthermore, if $s(j) = s(j')$ then $j = j'$, so s is *injective.* The map s plays the role of "addition by 1," as we will see below. The only other axiom of Peano arithmetic is that the principle of mathematical induction holds. In other words, if $S \subset \widetilde{\mathbb{N}}$ is a set with the properties

$$0 \in S, \quad k \in S \Rightarrow s(k) \in S, \tag{1.2}$$

then $S = \widetilde{\mathbb{N}}$.

Actually, applying the induction principle to $S = \{0\} \cup s(\widetilde{\mathbb{N}})$, we see that it suffices to assume that s in (1.1) is injective; the induction principle ensures that it is surjective.

We define addition $x + y$, for $x, y \in \widetilde{\mathbb{N}}$, inductively on y, by

$$x + 0 = x, \quad x + s(y) = s(x + y). \tag{1.3}$$

Next, we define multiplication $x \cdot y$, inductively on y, by

$$x \cdot 0 = 0, \quad x \cdot s(y) = x \cdot y + x. \tag{1.4}$$

We also define

$$1 = s(0). \tag{1.5}$$

We now prove the basic laws of arithmetic.

Proposition 1.1. *$x + 1 = s(x)$.*

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

Proposition 1.2. *$0 + x = x$.*

Proof. Use induction on x. First, $0 + 0 = 0$. Now, assuming $0 + x = x$, we have

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

Proposition 1.3. $s(y+x) = s(y) + x$.

Proof. Use induction on x. First, $s(y+0) = s(y) = s(y) + 0$. Next, we have

$$s(y + s(x)) = ss(y+x),$$
$$s(y) + s(x) = s(s(y) + x).$$

Proposition 1.4. $x + y = y + x$.

Proof. Use induction on y. The case $y = 0$ follows from Proposition 1.2. Now, assuming $x + y = y + x$, for all $x \in \widetilde{\mathbb{N}}$, we must show $s(y)$ has the same property. In fact,

$$x + s(y) = s(x+y) = s(y+x),$$

and by Proposition 1.3 the last quantity is equal to $s(y) + x$.

Proposition 1.5. $(x+y)+z = x+(y+z)$.

Proof. Use induction on z. First, $(x+y)+0 = x+y = x+(y+0)$. Now, assuming $(x+y)+z = x+(y+z)$, for all $x, y \in \widetilde{\mathbb{N}}$, we must show $s(z)$ has the same property. In fact,

$$(x+y)+s(z) = s((x+y)+z),$$
$$x+(y+s(z)) = x+s(y+z) = s(x+(y+z)),$$

and we perceive the desired identity.

Proposition 1.6. $x \cdot 1 = x$.

Proof. We have

$$x \cdot s(0) = x \cdot 0 + x = 0 + x = x,$$

the last identity by Proposition 1.2.

Proposition 1.7. $0 \cdot y = 0$.

Proof. Use induction on y. First, $0 \cdot 0 = 0$. Next, assuming $0 \cdot y = 0$, we have $0 \cdot s(y) = 0 \cdot y + 0 = 0 + 0 = 0$.

Proposition 1.8. $s(x) \cdot y = x \cdot y + y$.

Proof. Use induction on y. First, $s(x) \cdot 0 = 0$, while $x \cdot 0 + 0 = 0 + 0 = 0$. Next, assuming $s(x) \cdot y = x \cdot y + y$, for all x, we must show that $s(y)$ has this property. In fact,

$$s(x) \cdot s(y) = s(x) \cdot y + s(x) = (x \cdot y + y) + (x + 1),$$
$$x \cdot s(y) + s(y) = (x \cdot y + x) + (y + 1),$$

and identity then follows via the commutative and associative laws of addition.

Proposition 1.9. $x \cdot y = y \cdot x$.

Proof. Use induction on y. First, $x \cdot 0 = 0 = 0 \cdot x$, the latter identity by Proposition 1.7. Next, assuming $x \cdot y = y \cdot x$ for all $x \in \widetilde{\mathbb{N}}$, we must show that $s(y)$ has the same property. In fact,

$$x \cdot s(y) = x \cdot y + x = y \cdot x + x,$$
$$s(y) \cdot x = y \cdot x + x,$$

the last identity by Proposition 1.8.

Proposition 1.10. $(x + y) \cdot z = x \cdot z + y \cdot z$.

Proof. Use induction on z. First, the identity clearly holds for $z = 0$. Next, assuming it holds for z (for all $x, y \in \widetilde{\mathbb{N}}$), we must show it holds for $s(z)$. In fact,

$$(x + y) \cdot s(z) = (x + y) \cdot z + (x + y) = (x \cdot z + y \cdot z) + (x + y),$$
$$x \cdot s(z) + y \cdot s(z) = (x \cdot z + x) + (y \cdot z + y),$$

and the desired identity follows from the commutative and associative laws of addition.

Proposition 1.11. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Proof. Use induction on z. First, the identity clearly holds for $z = 0$. Next, assuming it holds for z (for all $x, y \in \widetilde{\mathbb{N}}$), we have

$$(x \cdot y) \cdot s(z) = (x \cdot y) \cdot z + x \cdot y,$$

while

$$x \cdot (y \cdot s(z)) = x \cdot (y \cdot z + y) = x \cdot (y \cdot z) + x \cdot y,$$

the last identity by Proposition 1.10. These observations yield the desired identity.

We next demonstrate the cancellation law of addition:

Proposition 1.12. *Given* $x, y, z \in \widetilde{\mathbb{N}}$,

$$x + y = z + y \Longrightarrow x = z. \tag{1.6}$$

Proof. Use induction on y. If $y = 0$, (1.6) obviously holds. Assuming (1.6) holds for y, we must show that

$$x + s(y) = z + s(y) \tag{1.7}$$

implies $x = z$. In fact, (1.7) is equivalent to $s(x + y) = s(z + y)$. Since the map s is assumed to be one-to-one, this implies that $x + y = z + y$, so we are done.

We next define an order relation on $\widetilde{\mathbb{N}}$. Given $x, y \in \widetilde{\mathbb{N}}$, we say

$$x < y \Longleftrightarrow y = x + u, \quad \text{for some } u \in \mathbb{N}. \tag{1.8}$$

Similarly there is a definition of $x \leq y$. We have $x \leq y$ if and only if $y \in R_x$, where

$$R_x = \{x + u : u \in \widetilde{\mathbb{N}}\}. \tag{1.9}$$

Proposition 1.13. *If $x \le y$ and $y \le x$ then $x = y$.*

Proof. The hypotheses imply

$$y = x + u, \quad x = y + v, \quad u, v \in \widetilde{\mathbb{N}}. \tag{1.10}$$

Hence $x = x + u + v$, so, by Proposition 1.12, $u + v = 0$. Now, if $v \neq 0$, then $v = s(w)$, so $u + v = s(u + w) \in \mathbb{N}$. Thus $v = 0$, and $u = 0$.

Proposition 1.14. *Given $x, y \in \widetilde{\mathbb{N}}$, either*

$$x < y, \quad or \quad x = y, \quad or \quad y < x, \tag{1.11}$$

and no two can hold.

Proof. That no two of (1.11) can hold follows from Proposition 1.13. To show that one must hold, we want to show that

$$y \notin R_x \Longrightarrow y < x. \tag{1.12}$$

To do this, use induction on y. If $0 \notin R_x$, then $x \neq 0$, so $x \in \mathbb{N}$, and hence $x = 0 + x$ shows that $0 < x$. Now, assuming that y has the property (1.12), we must show that $s(y)$ has this property.

So assume $s(y) \notin R_z$. Since $R_0 = \widetilde{\mathbb{N}}$, we deduce that $z \neq 0$, hence $z \in \mathbb{N}$, hence $z = s(x)$ for some x. But

$$s(y) \notin R_{s(x)} \Longleftrightarrow y \notin R_x.$$

The inductive hypothesis gives $x = y + u,\ u \in \mathbb{N}$, hence $s(x) = s(y) + u$, and we are done.

We can now establish the cancellation law for multiplication.

Proposition 1.15. *Given $x, y, z \in \widetilde{\mathbb{N}}$,*

$$x \cdot y = x \cdot z,\ x \neq 0 \Longrightarrow y = z. \tag{1.13}$$

Proof. If $y \neq z$, then either $y < z$ or $z < y$. Suppose $y < z$, i.e., $z = y + u,\ u \in \mathbb{N}$. Then the hypotheses of (1.13) imply

$$x \cdot y = x \cdot y + x \cdot u, \quad x \neq 0,$$

hence, by Proposition 1.12,

$$x \cdot u = 0, \quad x \neq 0. \tag{1.14}$$

We thus need to show that (1.14) implies $u = 0$. In fact, if not, then we can write $u = s(w)$, and $x = s(a)$, with $w, a \in \widetilde{\mathbb{N}}$, and we have

$$x \cdot u = x \cdot w + s(a) = s(x \cdot w + a) \in \mathbb{N}.$$

This contradicts (1.14), so we are done.

We next establish the following variant of the principle of induction, called the well-ordering property of $\widetilde{\mathbb{N}}$.

Proposition 1.16. *If $S \subset \widetilde{\mathbb{N}}$ is nonempty, then S contains a smallest element.*

Proof. Suppose S contains no smallest element. Then $0 \notin S$. Let

$$T = \{x \in \widetilde{\mathbb{N}} : x < y,\ \forall\, y \in S\}. \tag{1.15}$$

Then $0 \in T$. We claim that

$$x \in T \Longrightarrow s(x) \in T. \tag{1.16}$$

Indeed, suppose $x \in T$, so $x < y$ for all $y \in S$. If $s(x) \notin T$, we have $s(x) \ge y_0$ for some $y_0 \in S$. Now, using Proposition 1.13, one can show that

$$x < y_0,\ s(x) \ge y_0 \Longrightarrow s(x) = y_0. \tag{1.17}$$

In turn, from this one can deduce that y_0 must be the smallest element of S. Thus, if S has no smallest element, (1.16) must hold. The induction principle then implies that $T = \widetilde{\mathbb{N}}$, which implies S is empty.

2. The integers

An integer is thought of as having the form $x - a$, with $x, a \in \widetilde{\mathbb{N}}$. To be more formal, we will define an element of $\mathbb{Z}$ as an equivalence class of ordered pairs $(x, a),\ x, a \in \widetilde{\mathbb{N}}$, where we define

$$(x, a) \sim (y, b) \Longleftrightarrow x + b = y + a. \tag{2.1}$$

Proposition 2.1. *This is an equivalence relation.*

Proof. We need to check that

$$(x, a) \sim (y, b),\ (y, b) \sim (z, c) \Longrightarrow (x, a) \sim (z, c), \tag{2.2}$$

i.e., that, for $x, y, z, a, b, c \in \widetilde{\mathbb{N}}$,

$$x + b = y + a,\ y + c = z + b \Longrightarrow x + c = z + a. \tag{2.3}$$

In fact, the hypotheses of (2.3) imply

$$(x + c) + (y + b) = (z + a) + (y + b),$$

and the conclusion of (2.3) then follows from the cancellation property, Proposition 1.12.

Let us denote the equivalence class containing (x, a) by $[(x, a)]$. We then define addition and multiplication in $\mathbb{Z}$ to satisfy

$$\begin{aligned} [(x, a)] + [(y, b)] &= [(x + y, a + b)], \\ [(x, a)] \cdot [(y, b)] &= [(xy + ab, ay + xb)]. \end{aligned} \tag{2.4}$$

To see that these operations are well defined, we need:

Proposition 2.2. *If* $(x, a) \sim (x', a')$ *and* $(y, b) \sim (y', b')$, *then*

$$(x + y, a + b) \sim (x' + y', a' + b'),$$

and

$$(xy + ab, ay + xb) \sim (x'y' + a'b', a'y' + x'b').$$

Proof. The hypotheses say

$$x + a' = x' + a, \quad y + b' = y' + b.$$

The conclusions follow from results of §1.

Similarly, it is routine to verify the basic commutative, associative, etc. laws incorporated in the next proposition. To formulate the results, set

$$m = [(x,a)],\ n = [(y,b)],\ k = [(z,c)] \in \mathbb{Z}.$$

Also, define

$$0 = [(0,0)], \quad 1 = [(1,0)],$$

and

$$-m = [(a,x)].$$

Proposition 2.3. *We have*

$$\begin{aligned} m+n &= n+m, \\ (m+n)+k &= m+(n+k), \\ m+0 &= m, \\ m+(-m) &= 0, \\ mn &= nm, \\ m(nk) &= (mn)k, \\ m\cdot 1 &= m, \\ m\cdot 0 &= 0, \\ m\cdot(-1) &= -m, \\ m\cdot(n+k) &= m\cdot n + m\cdot k. \end{aligned}$$

We next establish some cancellation laws.

Proposition 2.4. *Given $m,n,k \in \mathbb{Z}$,*

$$m+n = k+n \Longrightarrow m = k. \tag{2.5}$$

Proof. We give two proofs. For one, we can add $-n$ to both sides and use the results of Proposition 2.3. Alternatively, we can write the hypotheses of (2.5) as

$$x+y+c+b = z+y+a+b$$

and use Proposition 1.12 to deduce that $x+c = z+a$.

Note that it is reasonable to set

$$m-n = m+(-n).$$

Proposition 2.5. *Given $m, n, k \in \mathbb{Z}$,*

$$mk = nk,\ k \neq 0 \Longrightarrow m = n. \tag{2.7}$$

Proof. The hypothesis of (2.7) says

$$xz + ac + (bz + yc) = yz + bc + (az + xc).$$

Hence

$$(x + b)z + (a + y)c = (x + b)c + (a + y)z. \tag{2.8}$$

We want to deduce that

$$x + b = y + a, \tag{2.9}$$

given that $z \neq c$. By Proposition 1.14, if $z \neq c$, then either $z < c$ or $c < z$. Say $c < z$, i.e., $z = c + u,\ u \in \mathbb{N}$. Then (2.8) yields

$$(x + b + a + y)c + (x + b)u = (x + b + a + y)c + (a + y)u;$$

hence, by Proposition 1.12,

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

This implies (2.9), by Proposition 1.15.

There is a natural injection

$$\mathbb{N} \hookrightarrow \mathbb{Z}, \quad x \mapsto [(x, 0)], \tag{2.10}$$

whose image we identify with $\mathbb{N}$. Note that the map (2.10) preserves addition and multiplication. There is also an injection $x \mapsto [(0, x)]$, whose image we identify with $-\mathbb{N}$.

Proposition 2.6. *We have a disjoint union:*

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N}). \tag{2.11}$$

Proof. Suppose $m \in \mathbb{Z}$; write $m = [(x, a)]$. By Proposition 1.14, either

$$a < x, \quad \text{or} \quad x = a, \quad \text{or} \quad x < a.$$

In these three cases,

$$x = a + u,\ u \in \mathbb{N}, \quad \text{or} \quad x = a, \quad \text{or} \quad a = x + v,\ v \in \mathbb{N}.$$

Then, either

$$(x, a) \sim (u, 0), \quad \text{or} \quad (x, a) \sim (0, 0), \quad \text{or} \quad (x, a) \sim (0, v).$$

We define an order on $\mathbb{Z}$ by:

$$m < n \Longleftrightarrow n - m \in \mathbb{N}. \tag{2.12}$$

We then have:

Corollary 2.7. *Given $m, n \in \mathbb{Z}$, then either*

$$m < n, \quad \text{or} \quad m = n, \quad \text{or} \quad n < m, \tag{2.13}$$

and no two can hold.

The map (2.10) is seen to preserve order relations.

Another consequence of (2.11) and the argument around (1.14) is:

Proposition 2.8. *If $m, n \in \mathbb{Z}$ and $m \cdot n = 0$, then either $m = 0$ or $n = 0$.*

3. Prime factorization and the fundamental theorem of arithmetic

Let $x \in \mathbb{N}$. We say x is composite if one can write

$$x = ab, \quad a, b \in \mathbb{N}, \tag{3.1}$$

with neither a nor b equal to 1. If $x \neq 1$ is not composite, it is said to be prime. If (3.1) holds, we say $a|x$ (and that $b|x$), or that a is a divisor of x. Given $x \in \mathbb{N},\ x > 1$, set

$$D_x = \{a \in \mathbb{N} : a|x,\ a > 1\}. \tag{3.2}$$

Thus $x \in D_x$, so D_x is non-empty. By Proposition 1.16, D_x contains a smallest element, say p_1. Clearly p_1 is a prime. Set

$$x = p_1 x_1, \quad x_1 \in \mathbb{N}, \quad x_1 < x. \tag{3.3}$$

The same construction applies to x_1, which is > 1 unless $x = p_1$. Hence we have either $x = p_1$ or

$$x_1 = p_2 x_2, \quad p_2 \ \text{ prime },\ x_2 < x_1. \tag{3.4}$$

Continue this process, passing from x_j to x_{j+1} as long as x_j is not prime. The set S of such $x_j \in \mathbb{N}$ has a smallest element, say $x_{\mu-1} = p_\mu$, and we have

$$x = p_1 p_2 \cdots p_\mu, \quad p_j \ \text{ prime.} \tag{3.5}$$

This is part of the Fundamental Theorem of Arithmetic:

Theorem 3.1. *Given $x \in \mathbb{N}$, there is a unique product expansion*

$$x = p_1 \cdots p_\mu, \tag{3.6}$$

where $p_1 \le \cdots \le p_\mu$ are primes.

Only uniqueness remains to be established. This follows from:

Proposition 3.2. *Assume $a, b \in \mathbb{N} <$ and $p \in \mathbb{N}$ is prime. Then*

$$p|ab \Longrightarrow p|a \quad or \quad p|b. \tag{3.7}$$

We will deduce this from:

Proposition 3.3. *If $p \in \mathbb{N}$ is prime and $a \in \mathbb{N}$, is not a multiple of p, or more generally if $p, a \in \mathbb{N}$ have no common divisors > 1, then there exist $m, n \in \mathbb{Z}$ such that*

$$ma + np = 1. \tag{3.8}$$

Proof of Proposition 3.2. Assume p is a prime which does not divide a. Pick m, n such that (3.8) holds. Now, multiply (3.8) by b, to get

$$mab + npb = b.$$

Thus, if $p|ab$, i.e., $ab = pk$, we have

$$p(mk + nb) = b,$$

so $p|b$, as desired.

To prove Proposition 3.3, let us set

$$\Gamma = \{ma + np : m, n \in \mathbb{Z}\}. \tag{3.9}$$

Clearly Γ satisfies the following criterion:

Definition. *A nonempty subset $\Gamma \subset \mathbb{Z}$ is a subgroup of $\mathbb{Z}$ provided*

$$a, b \in \Gamma \Longrightarrow a + b, a - b \in \Gamma. \tag{3.10}$$

Proposition 3.4. *If $\Gamma \subset \mathbb{Z}$ is a subgroup, then either $\Gamma = \{0\}$, or there exists $x \in \mathbb{N}$ such that*

$$\Gamma = \{mx : m \in \mathbb{Z}\}. \tag{3.11}$$

Proof. Note that $n \in \Gamma \Leftrightarrow -n \in \Gamma$, so, with $\Sigma = \Gamma \cap \mathbb{N}$, we have a disjoint union

$$\Gamma = \Sigma \cup \{0\} \cup (-\Sigma).$$

If $\Sigma \neq \emptyset$, let x be its smallest element. Then we want to establish (3.11), so set $\Gamma_0 = \{mx : m \in \mathbb{Z}\}$. Clearly $\Gamma_0 \subset \Gamma$. Similarly, set $\Sigma_0 = \{mx : m \in \mathbb{N}\} = \Gamma_0 \cap \mathbb{N}$. We want to show that $\Sigma_0 = \Sigma$. If $y \in \Sigma \setminus \Sigma_0$, then we can pick $m_0 \in \mathbb{N}$ such that

$$m_0 x < y < (m_0 + 1)x,$$

and hence

$$y - m_0 x \in \Sigma$$

is smaller than x. This contradiction proves Proposition 3.4.

Proof of Proposition 3.3. Taking Γ as in (3.9), pick $x \in \mathbb{N}$ such that (3.11) holds. Since $a \in \Gamma$ and $p \in \Gamma$, we have

$$a = m_0 x, \quad p = m_1 x$$

for some $m_j \in \mathbb{Z}$. The assumption that a and p have no common divisor > 1 implies $x = 1$. We conclude that $1 \in \Gamma$, so (3.8) holds.

4. The rational numbers

A rational number is thought of as having the form m/n, with $m, n \in \mathbb{Z},\ n \neq 0$. Thus, we will define an element of $\mathbb{Q}$ as an equivalence class of ordered pairs $m/n,\ m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\}$, where we define

$$m/n \sim a/b \Longleftrightarrow mb = an. \tag{4.1}$$

Proposition 4.1. *This is an equivalence relation.*

Proof. We need to check that

$$m/n \sim a/b,\ a/b \sim c/d \Longrightarrow m/n \sim c/d, \tag{4.2}$$

i.e., that, for $m, a, c \in \mathbb{Z},\ n, b, d \in \mathbb{Z} \setminus \{0\}$,

$$mb = an,\ ad = cb \Longrightarrow md = cn. \tag{4.3}$$

Now the hypotheses of (4.3) imply $(mb)(ad) = (an)(cb)$, hence

$$(md)(ab) = (cn)(ab).$$

We are assuming $b \neq 0$. If also $a \neq 0$, then $ab \neq 0$, and the conclusion of (4.3) follows from the cancellation property, Proposition 2.5. On the other hand, if $a = 0$, then $m/n \sim a/b \Rightarrow mb = 0 \Rightarrow m = 0$ (since $b \neq 0$), and similarly $a/b \sim c/d \Rightarrow cb = 0 \Rightarrow c = 0$, so the desired implication also holds in that case.

We will (temporarily) denote the equivalence class containing m/n by $[m/n]$. We then define addition and multiplication in $\mathbb{Q}$ to satisfy

$$\begin{aligned} [m/n] + [a/b] &= [(mb + na)/(nb)], \\ [m/n] \cdot [a/b] &= [(ma)/(nb)]. \end{aligned} \tag{4.4}$$

To see that these operations are well defined, we need:

Proposition 4.2. *If $m/n \sim m'/n'$ and $a/b \sim a'/b'$, then*

$$(mb + na)/(nb) \sim (m'b' + n'a')/(n'b'),$$

and

$$(ma)/(nb) \sim (m'a')/(n'b').$$

Proof. The hypotheses say

$$mn' = m'n, \quad ab' = a'b.$$

The conclusions follow from the results of §2.

From now on, we drop the brackets, simply denoting the equivalence class of m/n by m/n, and writing (4.1) as $m/n = a/b$. We also may denote an element of $\mathbb{Q}$ by a single letter, e.g., $x = m/n$. There is an injection

$$\mathbb{Z} \hookrightarrow \mathbb{Q}, \quad m \mapsto m/1, \tag{4.5}$$

whose image we identify with $\mathbb{Z}$. This map preserves addition and multiplication. We define

$$-(m/n) = (-m)/n, \tag{4.6}$$

and, if $x = m/n \neq 0$, (i.e., $m \neq 0$ as well as $n \neq 0$), we define

$$x^{-1} = n/m. \tag{4.7}$$

The results stated in the following proposition are routine consequences of the results of §2.

Proposition 4.3. *Given $x, y, z \in \mathbb{Q}$, we have*

$$\begin{aligned} x + y &= y + x, \\ (x + y) + z &= x + (y + z), \\ x + 0 &= x, \\ x + (-x) &= 0, \\ x \cdot y &= y \cdot x, \\ (x \cdot y) \cdot z &= x \cdot (y \cdot z), \\ x \cdot 1 &= x, \\ x \cdot 0 &= 0, \\ x \cdot (-1) &= -x, \\ x \cdot (y + z) &= x \cdot y + x \cdot z. \end{aligned}$$

Furthermore,

$$x \neq 0 \Longrightarrow x \cdot x^{-1} = 1.$$

We also have cancellation laws:

Proposition 4.4. *Given $x, y, z \in \mathbb{Q}$,*

$$x + y = z + y \Longrightarrow x = z. \tag{4.8}$$

Also,

$$xy = zy, \ y \neq 0 \Longrightarrow x = z. \tag{4.9}$$

Proof. To get (4.8), add $-y$ to both sides of $x + y = z + y$ and use the results of Proposition 4.3. To get (4.9), multiply both sides of $x \cdot y = z \cdot y$ by y^{-1}.

It is natural to define

$$x - y = x + (-y), \tag{4.10}$$

and, if $y \neq 0$,

$$x/y = x \cdot y^{-1}. \tag{4.11}$$

We now define the order relation on $\mathbb{Q}$. Set

$$\mathbb{Q}^+ = \{m/n : mn > 0\}, \tag{4.12}$$

where, in (4.12), we use the order relation on $\mathbb{Z}$, discussed in §2. This is well defined (since $(-m)(-n) = mn$) and results of §2 imply that

$$\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup (-\mathbb{Q}^+) \tag{4.13}$$

is a disjoint uion, where $-\mathbb{Q}^+ = \{-x : x \in \mathbb{Q}^+\}$. Also, clearly

$$x, y \in \mathbb{Q}^+ \Longrightarrow x + y, xy, \frac{x}{y} \in \mathbb{Q}^+. \tag{4.14}$$

We define

$$x < y \Longleftrightarrow y - x \in \mathbb{Q}^+, \tag{4.15}$$

and we have, for any $x, y \in \mathbb{Q}$, either

$$x < y, \quad \text{or} \quad x = y, \quad \text{or} \quad y < x, \tag{4.16}$$

and no two can hold. The map (4.5) is seen to preserve the order relations. In light of (4.14), we see that

$$\text{given} \ \ x, y > 0, \quad x < y \Leftrightarrow \frac{x}{y} < 1 \Leftrightarrow \frac{1}{y} < \frac{1}{x}. \tag{4.17}$$

As usual, we say $x \leq y$ provided either $x < y$ or $x = y$. Similarly there are natural definitions of $x > y$ and of $x \geq y$.

The following result implies that $\mathbb{Q}$ has the Archimedean property.

Proposition 4.5. *Given $x \in \mathbb{Q}$, there exists $k \in \mathbb{Z}$ such that*

$$k - 1 < x \leq k. \tag{4.18}$$

Proof. It suffices to prove (4.18) assuming $x \in \mathbb{Q}^+$; otherwise, work with $-x$. Say $x = m/n,\ m, n \in \mathbb{N}$. Then

$$S = \{\ell \in \mathbb{N} : \ell \geq x\}$$

contains m, hence is nonempty. By Proposition 1.16, S has a smallest element; call it k. Then $k \geq x$. We cannot have $k - 1 \geq x$, for then $k - 1$ would belong to S. Hence (4.18) holds.

5. Sequences

In this section, we discuss infinite sequences. For now, we deal with sequences of rational numbers, but we will not explicitly state this restriction below. In fact, once the set of real numbers is constructed in §6, the results of this section will be seen to hold also for sequences of real numbers.

Definition. *A sequence (a_j) is said to converge to a limit a provided that, for any $n \in \mathbb{N}$, there exists $K(n)$ such that*

$$j \geq K(n) \Longrightarrow |a_j - a| < \frac{1}{n}. \tag{5.1}$$

We write $a_j \to a$, or $a = \lim\ a_j$, or perhaps $a = \lim_{j\to\infty}\ a_j$.

Here, we define the absolute value $|x|$ of x by

$$\begin{aligned} |x| = \ & x \ \text{ if } \ x \geq 0, \\ & -x \ \text{ if } \ x < 0. \end{aligned} \tag{5.2}$$

The absolute value function has various simple properties, such as $|xy| = |x| \cdot |y|$, which follow readily from the definition. One basic property is the triangle inequality:

$$|x + y| \leq |x| + |y|. \tag{5.3}$$

In fact, if either x and y are both positive or they are both negative, one has equality in (5.3). If x and y have opposite signs, then $|x + y| \leq \max(|x|, |y|)$, which in turn is dominated by the right side of (5.3).

Proposition 5.1. *If $a_j \to a$ and $b_j \to b$, then*

$$a_j + b_j \to a + b, \tag{5.4}$$

and

$$a_j b_j \to ab. \tag{5.5}$$

If furthermore, $b_j \neq 0$ for all j and $b \neq 0$, then

$$a_j / b_j \to a/b. \tag{5.6}$$

Proof. To see (5.4), we have, by (5.3),

$$|(a_j + b_j) - (a + b)| \leq |a_j - a| + |b_j - b|. \tag{5.7}$$

To get (5.5), we have

$$
\begin{aligned}
|a_jb_j - ab| &= |(a_jb_j - ab_j) + (ab_j - ab)| \\
&\le |b_j| \cdot |a_j - a| + |a| \cdot |b - b_j|.
\end{aligned} \tag{5.8}
$$

The hypotheses imply $|b_j| \le B$, for some B, and hence the criterion for convergence is readily verified. To get (5.6), we have

$$
\Bigl| \frac{a_j}{b_j} - \frac{a}{b} \Bigr| \le \frac{1}{|b| \cdot |b_j|} \bigl\{ |b| \cdot |a - a_j| + |a| \cdot |b - b_j| \bigr\}. \tag{5.9}
$$

The hypotheses imply $1/|b_j| \le M$ for some M, so we also verify the criterion for convergence in this case.

We next define the concept of a Cauchy sequence.

Definition. *A sequence (a_j) is a Cauchy sequence provided that, for any $n \in \mathbb{N}$, there exists $K(n)$ such that*

$$
j, k \ge K(n) \Longrightarrow |a_j - a_k| \le \frac{1}{n}. \tag{5.10}
$$

It is clear that any convergent sequence is Cauchy. On the other hand, we have:

Proposition 5.2. *Any Cauchy sequence is bounded.*

Proof. Take $n = 1$ in the definition above. Thus, if (a_j) is Cauchy, there is a K such that $j, k \ge K \Rightarrow |a_j - a_k| \le 1$. Hence, $j \ge K \Rightarrow |a_j| \le |a_K| + 1$, so, for all j,

$$
|a_j| \le M, \quad M = \max\bigl(|a_1|, \dots, |a_{K-1}|, |a_K| + 1\bigr).
$$

Now, the arguments proving Proposition 5.1 also establish:

Proposition 5.3. *If (a_j) and (b_j) are Cauchy sequences, so are $(a_j + b_j)$ and (a_jb_j). Furthermore, if, for all j, $|b_j| \ge c$ for some $c > 0$, then (a_j/b_j) is Cauchy.*

The following proposition is a bit deeper than the first three.

Proposition 5.4. *If (a_j) is bounded, i.e., $|a_j| \le M$ for all j, then it has a Cauchy subsequence.*

Proof. We may as well assume $M \in \mathbb{N}$. Now, either $a_j \in [0, M]$ for infinitely many j or $a_j \in [-M, 0]$ for infinitely many j. Let I_1 be any one of these two intervals containing a_j for infinitely many j, and pick $j(1)$ such that $a_{j(1)} \in I_1$. Write I_1 as the union of two closed intervals, of equal length, sharing only the midpoint of I_1. Let I_2 be any one of them with the property that $a_j \in I_2$ for infinitely many j, and pick $j(2) > j(1)$ such that $a_{j(2)} \in I_2$. Continue, picking $I_\nu \subset I_{\nu-1} \subset \cdots \subset I_1$, of length $M/2^{\nu-1}$, containing a_j for infinitely many j, and picking $j(\nu) > j(\nu-1) > \cdots > j(1)$ such that $a_{j(\nu)} \in I_\nu$. Setting $b_\nu = a_{j(\nu)}$, we see that (b_ν) is a Cauchy subsequence of (a_j), since, for all $k \in \mathbb{N}$,

$$
|b_{\nu+k} - b_\nu| \le M/2^{\nu-1}.
$$

Proposition 5.5. *Any bounded monotone sequence (a_j) is Cauchy.*

Proof. To say (a_j) is monotone is to say that either (a_j) is increasing, i.e., $a_j \le a_{j+1}$ for all j, or that (a_j) is decreasing, i.e., $a_j \ge a_{j+1}$ for all j. For the sake of argument, assume (a_j) is increasing.

By Proposition 5.4, there is a subsequence $(b_\nu) = (a_{j(\nu)})$ which is Cauchy. Thus, given $n \in \mathbb{N}$, there exists $K(n)$ such that

$$\mu, \nu \ge K(n) \Longrightarrow |a_{j(\nu)} - a_{j(\mu)}| < \frac{1}{n}. \tag{5.11}$$

Now, if $j(\nu_0) \ge K(n)$ and $k \ge j \ge j(\nu_0)$, pick ν_1 such that $j(\nu_1) \ge k$. Then

$$a_{j(\nu_0)} \le a_j \le a_k \le a_{j(\nu_1)},$$

so

$$k \ge j \ge j(\nu_0) \Longrightarrow |a_j - a_k| \le \frac{1}{n}. \tag{5.12}$$

We give a few simple but basic examples of convergent sequences.

Proposition 5.6. *If $|a| < 1$, then $a^j \to 0$.*

Proof. Set $b = |a|$; it suffices to show that $b_j \to 0$. Consider $c = 1/b > 1$, hence $c = 1 + y,\ y > 0$. We claim that

$$c^j = (1+y)^j \ge 1 + jy,$$

for all $j \ge 1$. In fact, this clearly holds for $j = 1$, and if it holds for $j = k$, then

$$c^{k+1} \ge (1+y)(1+ky) > 1 + (k+1)y.$$

Hence, by induction, the estimate is established. Consequently,

$$b^j < \frac{1}{jy},$$

so the appropriate analogue of (5.1) holds, with $K(n) = Kn$, for any integer $K > 1/y$.

Proposition 5.6 enables us to establish the following result on geometric series.

Proposition 5.7. *If $|x| < 1$ and*

$$a_j = 1 + x + \cdots + x^j,$$

then

$$a_j \to \frac{1}{1-x}.$$

Proof. Note that $xa_j = x + x^2 + \cdots + x^{j+1}$, so $(1-x)a_j = 1 - x^{j+1}$, i.e.,

$$a_j = \frac{1-x^{j+1}}{1-x}.$$

The conclusion follows from Proposition 5.6.

Note in particular that

$$0 < x < 1 \Longrightarrow 1 + x + \cdots + x^j < \frac{1}{1-x}. \tag{5.13}$$

It is an important mathematical fact that not every Cauchy sequence of rational numbers has a rational number as limit. We give one example here. Consider the sequence

$$a_j = \sum_{\ell=0}^{j} \frac{1}{\ell!}. \tag{5.14}$$

Then (a_j) is increasing, and

$$a_{n+j} - a_n = \sum_{\ell=n+1}^{n+j} \frac{1}{\ell!} \le \frac{1}{n!}\Bigl(\frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots + \frac{1}{(n+1)^j}\Bigr),$$

since $(n+1)(n+2)\cdots(n+j) \ge (n+1)^j$. Using (5.13), we have

$$a_{n+j} - a_n \le \frac{1}{(n+1)!}\,\frac{1}{1-\frac{1}{n+1}} = \frac{1}{n!}\cdot\frac{1}{n}. \tag{5.15}$$

Hence (a_j) is Cauchy. Taking $n = 2$, we see that

$$j > 2 \Longrightarrow 2\tfrac{1}{2} < a_j < 2\tfrac{3}{4}. \tag{5.16}$$

Proposition 5.8. *The sequence (5.14) cannot converge to a rational number.*

Proof. Assume $a_j \to m/n$ with $m, n \in \mathbb{N}$. By (5.16), we must have $n > 2$. Now, write

$$\frac{m}{n} = \sum_{\ell=0}^{n} \frac{1}{\ell!} + r, \quad r = \lim_{j\to\infty} (a_{n+j} - a_n). \tag{5.17}$$

Multiplying both sides of (5.17) by $n!$ gives

$$m(n-1)! = A + r \cdot n! \tag{5.18}$$

where

$$A = \sum_{\ell=0}^{n} \frac{n!}{\ell!} \in \mathbb{N}. \tag{5.19}$$

Thus the identity (5.17) forces $r \cdot n! \in \mathbb{N}$, while (5.15) implies

$$0 < r \cdot n! \le 1/n. \tag{5.20}$$

This contradiction proves the proposition.

6. The real numbers

We think of a real number as a quantity which can be specified by a process of approximation arbitrarily closely by rational numbers. Thus, we define an element of $\mathbb{R}$ as an equivalence class of Cauchy sequences of rational numbers, where we define

$$(a_j) \sim (b_j) \Longleftrightarrow a_j - b_j \to 0. \tag{6.1}$$

Proposition 6.1. *This is an equivalence relation.*

Proof. This is a straightforward consequence of Proposition 5.1. In particular, to see that

$$(a_j) \sim (b_j),\ (b_j) \sim (c_j) \Longrightarrow (a_j) \sim (c_j), \tag{6.2}$$

just use (5.4) of Proposition 5.1 to write

$$a_j - b_j \to 0,\ b_j - c_j \to 0 \Longrightarrow a_j - c_j \to 0.$$

We denote the equivalence class containing a Cauchy sequence (a_j) by $[(a_j)]$. We then define addition and multiplication on $\mathbb{R}$ to satisfy

$$\begin{aligned} [(a_j)] + [(b_j)] &= [(a_j + b_j)], \\ [(a_j)] \cdot [(b_j)] &= [(a_j b_j)]. \end{aligned} \tag{6.3}$$

To prove these operations are well defined, we need:

Proposition 6.2. *If Cauchy sequences of rational numbers are given which satisfy* $(a_j) \sim (a'_j)$ *and* $(b_j) \sim (b'_j)$, *then*

$$(a_j + b_j) \sim (a'_j + b'_j), \tag{6.4}$$

and

$$(a_j b_j) \sim (a'_j b'_j). \tag{6.5}$$

The proof is a straightforward variant of the proof of parts (5.4)-(5.5) in Proposition 5.1, with due account taken of Proposition 5.2.

There is a natural injection

$$\mathbb{Q} \hookrightarrow \mathbb{R}, \quad a \mapsto [(a, a, a, \dots)], \tag{6.6}$$

whose image we identify with $\mathbb{Q}$. This map preserves addition and multiplication.

If $x = [(a_j)]$, we define

$$-x = [(-a_j)]. \tag{6.7}$$

For $x \neq 0$, we define x^{-1} as follows. First, to say $x \neq 0$ is to say there exists $n \in \mathbb{N}$ such that $|a_j| \geq 1/n$ for infinitely many j. Since (a_j) is Cauchy, this implies that there exists K such that $|a_j| \geq 1/2n$ for all $j \geq K$. Now, if we set $\alpha_j = a_{k+j}$, we have $(\alpha_j) \sim (a_j)$; we propose to set

$$x^{-1} = [(\alpha_j^{-1})]. \tag{6.8}$$

We claim that this is well defined. First, by Proposition 5.3, (α_j^{-1}) is Cauchy. Furthermore, if for such x we also have $x = [(b_j)]$, and we pick K so large that also $|b_j| \geq 1/2n$ for all $j \geq K$, and set $\beta_j = b_{K+j}$, we claim that

$$(\alpha_j^{-1}) \sim (\beta_j^{-1}). \tag{6.9}$$

Indeed, we have

$$|\alpha_j^{-1} - \beta_j^{-1}| \leq \frac{|\beta_j - \alpha_j|}{|\alpha_j| \cdot |\beta_j|} \leq 4n^2 |\beta_j - \alpha_j|, \tag{6.10}$$

so (6.9) holds.

It is now a straightforward exercise to verify the basic algebraic properties of addition and multiplication in $\mathbb{R}$. We state the result.

Proposition 6.3. *Given $x, y, z \in \mathbb{R}$, all the algebraic properties stated in Proposition 4.3 hold.*

As in (4.10)-(4.11), we define $x - y = x + (-y)$ and, if $y \neq 0$, $x/y = x \cdot y^{-1}$.

We now define an order relation on $\mathbb{R}$. Take $x \in \mathbb{R}$, $x = [(a_j)]$. From the discussion above of x^{-1}, we see that, if $x \neq 0$, then one and only one of the following holds. Either, for some $n, K \in \mathbb{N}$,

$$j \geq K \Longrightarrow a_j \geq \frac{1}{2n}, \tag{6.11}$$

or, for some $n, K \in \mathbb{N}$,

$$j \geq K \Longrightarrow a_j \leq -\frac{1}{2n}. \tag{6.12}$$

If $(a_j) \sim (b_j)$ and (6.11) holds for a_j, it also holds for b_j, and ditto for (6.12). If (6.11) holds, we say $x \in \mathbb{R}^+$ (and we say $x > 0$), and if (6.12) holds we say $x \in \mathbb{R}^-$ (and we say $x < 0$). Clearly $x > 0$ if and only if $-x < 0$. It is also clear that the map $\mathbb{Q} \hookrightarrow \mathbb{R}$ in (6.6) preserves the order relation.

Thus we have the disjoint union

$$\mathbb{R} = \mathbb{R}^+ \cup \{0\} \cup \mathbb{R}^-, \quad \mathbb{R}^- = -\mathbb{R}^+. \tag{6.13}$$

Also, clearly

$$x, y \in \mathbb{R}^+ \Longrightarrow x + y, xy \in \mathbb{R}^+. \tag{6.14}$$

As in (4.15), we define

$$x < y \Longleftrightarrow y - x \in \mathbb{R}^+. \tag{6.15}$$

The following results are straightforward.

Proposition 6.4. *For elements of* $\mathbb{R}$, *we have*

$$x_1 < y_1, \ x_2 < y_2 \Longrightarrow x_1 + x_2 < y_1 + y_2, \tag{6.16}$$

$$x < y \Longleftrightarrow -y < -x, \tag{6.17}$$

$$0 < x < y, \ a > 0 \Longrightarrow 0 < ax < ay, \tag{6.18}$$

$$0 < x < y \Longrightarrow 0 < y^{-1} < x^{-1}. \tag{6.19}$$

Proof. The results (6.16) and (6.18) follow from (6.14); consider, for example, $a(y-x)$. The result (6.17) follows from (6.13). To prove (6.19), first we see that $x > 0$ implies $x^{-1} > 0$, as follows: if $-x^{-1} > 0$, the identity $x \cdot (-x^{-1}) = -1$ contradicts (6.14). As for the rest of (6.19), the hypotheses imply $xy > 0$, and multiplying both sides of $x < y$ by $a = (xy)^{-1}$ gives the result, by (6.18).

As in (5.2), define $|x|$ by

$$\begin{aligned} |x| = \ & x \quad \text{if} \quad x \geq 0, \\ & -x \quad \text{if} \quad x < 0. \end{aligned} \tag{6.20}$$

It is straightforward to verify

$$|xy| = |x| \cdot |y|, \quad |x + y| \leq |x| + |y|. \tag{6.21}$$

We now show that $\mathbb{R}$ has the Archimedean property.

Proposition 6.5. *Given $x \in \mathbb{R}$, there exists $k \in \mathbb{Z}$ such that*

$$k-1 < x \le k. \tag{6.22}$$

Proof. It suffices to prove (6.22) assuming $x \in \mathbb{R}^+$. Otherwise, work with $-x$. Say $x = [(a_j)]$ where (a_j) is a Cauchy sequence of rational numbers. By Proposition 5.2, there exists $M \in \mathbb{Q}$ such that $|a_j| \le M$ for all j. By Proposition 4.5, we have $M \le \ell$ for some $\ell \in \mathbb{N}$. Hence the set $S = \{\ell \in \mathbb{N} : \ell \ge x\}$ is nonempty. As in the proof of Proposition 4.5, taking k to be the smallest element of S gives (6.22).

Proposition 6.6. *Given any real $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $\varepsilon > 1/n$.*

Proof. Using Proposition 6.5, pick $n > 1/\varepsilon$ and apply (6.19). Alternatively, use the reasoning given above (6.8).

We are now ready to consider sequences of elements of $\mathbb{R}$.

Definition. *A sequence (x_j) converges to x if and only if, for any $n \in \mathbb{N}$, there exists $K(n)$ such that*

$$j \ge K(n) \Longrightarrow |x_j - x| < \frac{1}{n}. \tag{6.23}$$

In this case, we write $x_j \to x$, or $x = \lim\ x_j$.

The sequence (x_j) is Cauchy if and only if, for any $n \in \mathbb{N}$, there exists $K(n)$ such that

$$j,k \ge K(n) \Longrightarrow |x_j - x_k| < \frac{1}{n}. \tag{6.24}$$

We note that it is typical to phrase the definition above in terms of picking any $\varepsilon > 0$ and demanding that, e.g., $|x_j - x| < \varepsilon$, for large j. The equivalence of the two definitions follows from Proposition 6.6.

As in Proposition 5.2, we have that every Cauchy sequence is bounded.

It is clear that, if each $x_j \in \mathbb{Q}$, then the notion that (x_j) is Cauchy given above coincides with that in §5. If also $x \in \mathbb{Q}$, the notion that $x_j \to x$ also coincides with that given in §5. Furthermore, if each $a_j \in \mathbb{Q}$, and $x \in \mathbb{R}$, then

$$a_j \to x \Longleftrightarrow x = [(a_j)]. \tag{6.25}$$

In fact, given $x = [(a_j)]$,

$$\big(j,k \ge K \Rightarrow |a_j - a_k| \le 1/n\big) \Longrightarrow \big(j \ge K \Rightarrow |a_j - x| \le 1/n\big). \tag{6.26}$$

The proof of Proposition 5.1 extends to the present case, yielding:

Proposition 6.7. *If $x_j \to x$ and $y_j \to y$, then*

$$x_j + y_j \to x + y, \tag{6.27}$$

and

$$x_j y_j \to xy. \tag{6.28}$$

If furthermore $y_j \neq 0$ for all j and $y \neq 0$, then

$$x_j/y_j \to x/y. \tag{6.28}$$

So far, statements made about $\mathbb{R}$ have emphasized similarities of its properties with corresponding properties of $\mathbb{Q}$. The crucial difference between these two sets of numbers is given by the following result, known as the completeness property.

Theorem 6.8. *If (x_j) is a Cauchy sequence of real numbers, then there exists $x \in \mathbb{R}$ such that $x_j \to x$.*

Proof. Take $x_j = [(a_{j\ell} : \ell \in \mathbb{N})]$ with $a_{j\ell} \in \mathbb{Q}$. Using (6.26), take $a_{j,\ell(j)} = b_j \in \mathbb{Q}$ such that

$$|x_j - b_j| \le 2^{-j}. \tag{6.29}$$

Then (b_j) is Cauchy, since $|b_j - b_k| \le |x_j - x_k| + 2^{-j} + 2^{-k}$. Now, let

$$x = [(b_j)]. \tag{6.30}$$

It follows that

$$|x_j - x| \le |x_j - b_j| + |x - b_j| \le 2^{-j} + |x - b_j|, \tag{6.31}$$

and hence $x_j \to x$.

If we combine Theorem 6.8 with the argument behind Proposition 5.4, we obtain the following important result, known as the Bolzano-Weierstrass Theorem.

Theorem 6.9. *Any bounded sequence of real numbers has a convergent subsequence.*

Proof. If $|x_j| \le M$, the proof of Proposition 5.4 applies without change to show that (x_j) has a Cauchy subsequence. By Theorem 6.8, that Cauchy subsequence converges.

Similarly, adding Theorem 6.8 to the argument behind Proposition 5.5 yields:

Proposition 6.10. *Any bounded monotone sequence (x_j) of real numbers converges.*

A related property of $\mathbb{R}$ can be described in terms of the notion of the "supremum" of a set.

Definition. *If $S \subset \mathbb{R}$, one says that $x \in \mathbb{R}$ is an upper bound for S provided $x \geq s$ for all $s \in S$, and one says*

$$x = \sup\ S \tag{6.32}$$

provided x is an upper bound for S and further $x \leq x'$ whenever x' is an upper bound for S.

For some sets, such as $S = \mathbb{Z}$, there is no $x \in \mathbb{R}$ satisfying (6.32). However, there is the following result, known as the supremum property.

Proposition 6.11. *If S is a nonempty subset of $\mathbb{R}$ which has an upper bound, then there is a real $x = \sup\ S$.*

Proof. We use an argument similar to the one in the proof of Proposition 5.3. Let x_0 be an upper bound for S, pick s_0 in S, and consider

$$I_0 = [s_0, x_0] = \{y \in \mathbb{R} : s_0 \leq y \leq x_0\}.$$

If $x_0 = s_0$, then already $x_0 = \sup\ S$. Otherwise, I_0 is an interval of nonzero length, $L = x_0 - s_0$. In that case, divide I_0 into two equal intervals, having in common only the midpoint; say $I_0 = I_0^\ell \cup I_0^r$, where I_0^r lies to the right of I_0^ℓ.

Let $I_1 = I_0^r$ if $S \cap I_0^r \neq \emptyset$, and otherwise let $I_1 = I_0^\ell$. Let x_1 be the right endpoint of I_1, and pick $s_1 \in S \cap I_1$. Note that x_1 is also an upper bound for S.

Continue, constructing

$$I_\nu \subset I_{\nu-1} \subset \cdots \subset I_0,$$

where I_ν has length $2^{-\nu}L$, such that the right endpoint x_ν of I_ν satisfies

$$x_\nu \geq s, \quad \forall\ s \in S, \tag{6.33}$$

and such that $S \cap I_\nu \neq \emptyset$, so there exist $s_\nu \in S$ such that

$$x_\nu - s_\nu \leq 2^{-\nu}L. \tag{6.34}$$

The sequence (x_ν) is bounded and monotone (decreasing) so, by Proposition 6.10, it converges; $x_\nu \to x$. By (6.33), we have $x \geq s$ for all $s \in S$, and by (6.34) we have $x - s_\nu \leq 2^{-\nu}L$. Hence x satisfies (6.32).

We end this section with an exercise for the reader. Namely, given a real number $\xi \in (0,1)$, show it has an infinite decimal expansion, i.e., show there exist $b_k \in \{0,1,\dots,9\}$ such that

$$\xi = \sum_{k=1}^{\infty} b_k \cdot 10^{-k}. \tag{6.35}$$

As a hint, start by breaking $[0,1]$ into ten subintervals of equal length, and picking one to which ξ belongs.

7. Irrational numbers

There are real numbers which are not rational. One, called e, is given by the limit of the sequence (5.14); in standard notation,

$$e = \sum_{\ell=0}^{\infty} \frac{1}{\ell!} \tag{7.1}$$

Proposition 5.8 implies that e is not rational. One can approximate e to high accuracy. In fact, as a consequence of (5.15), one has

$$e - \sum_{\ell=0}^{n} \frac{1}{\ell!} \le \frac{1}{n!} \cdot \frac{1}{n}. \tag{7.2}$$

For example, one can verify that

$$120! > 6 \cdot 10^{198}, \tag{7.3}$$

and hence

$$e - \sum_{\ell=0}^{120} \frac{1}{\ell!} < 10^{-200}. \tag{7.4}$$

In less than a second, a personal computer with the right program can perform a highly accurate approximation to such a sum, yielding

$$\begin{aligned} 2.&7182818284\ 5904523536\ 0287471352\ 6624977572\ 4709369995 \\ &9574966967\ 6277240766\ 3035354759\ 4571382178\ 5251664274 \\ &2746639193\ 2003059921\ 8174135966\ 2904357290\ 0334295260 \\ &5956307381\ 3232862794\ 3490763233\ 8298807531\ \cdots \end{aligned}$$

accurate to 190 places after the decimal point.

A number in $\mathbb{R} \setminus \mathbb{Q}$ is said to be irrational. We present some more common examples of irrational numbers, such as $\sqrt{2}$. To begin, one needs to show that $\sqrt{2}$ is a well defined real number. The following general result includes this fact.

Proposition 7.1. *Given $a \in \mathbb{R}^+$, $k \in \mathbb{N}$, there is a unique $b \in \mathbb{R}^+$ such that $b^k = a$.*

Proof. Consider

$$S_{a,k} = \{x \ge 0 : x^k \le a\}. \tag{7.5}$$

Then $S_{a,k}$ is a nonempty bounded subset of $\mathbb{R}$. Take $b = \sup S_{a,k}$. One readily verifies that $b^k = a$.

We write

$$b = a^{1/k}. \tag{7.6}$$

Now for a list of irrational numbers:

Proposition 7.2. *Take $a \in \mathbb{N}$, $k \in \mathbb{N}$. If $a^{1/k}$ is not an integer, then $a^{1/k}$ is irrational.*

Proof. Assume $a^{1/k} = m/n$, with $m, n \in \mathbb{N}$. Then

$$m^k = an^k. \tag{7.7}$$

Using the Fundamental Theorem of Arithmetic, Theorem 3.1, write

$$m = p_1^{\mu_1} \cdots p_\ell^{\mu_\ell}, \quad n = p_1^{\nu_1} \cdots p_\ell^{\nu_\ell}, \quad a = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}, \tag{7.8}$$

with $p_1 < \cdots < p_\ell$ prime and $\mu_j, \nu_j, \alpha_j \in \widetilde{\mathbb{N}} = \mathbb{N} \cup \{0\}$. The identity (7.7) implies

$$p_1^{k\mu_1} \cdots p_\ell^{k\mu_\ell} = p_1^{\alpha_1 + k\nu_1} \cdots p_\ell^{\alpha_\ell + k\nu_\ell}, \tag{7.9}$$

and the uniqueness part of Theorem 3.1 then implies that $k\mu_j = \alpha_j + k\nu_j$, $1 \le j \le \ell$, hence

$$\alpha_j = k\beta_j, \quad \beta_j \in \widetilde{\mathbb{N}}, \tag{7.10}$$

and hence

$$a = b^k, \quad b = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell} \in \mathbb{N}. \tag{7.11}$$

Noting that $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, we have:

Corollary 7.3. *The following numbers are irrational:*

$$\sqrt{2}, \ \sqrt{3}, \ \sqrt{5}, \ \sqrt{6}, \ \sqrt{7}, \ \sqrt{8}.$$

The real line is thick with both rational numbers and irrational numbers. By construction, given any $x \in \mathbb{R}$, there exists $a_j \in \mathbb{Q}$ such that $a_j \to x$. Also, given any $x \in \mathbb{R}$, there exist *irrational* b_j such that $b_j \to x$. To see this, just take $a_j \in \mathbb{Q}$, $a_j \to x$, and set $b_j = a_j + 2^{-j}\sqrt{2}$.

In a sense that can be made precise, there are *more* irrational numbers than rational numbers. Namely, $\mathbb{Q}$ is *countable*, while $\mathbb{R}$ is *uncountable*. See §8 for a treatment of this.

Perhaps the most intriguing irrational number is π. See [Be] for material on this number.

8. Cardinal numbers

We return to the natural numbers considered in §1 and make contact with the fact that these numbers are used to count objects in collections. Namely, let S be some set. If S is empty, we say 0 is the number of its elements. If S is not empty, pick an element out of S and count "1." If there remain other elements of S, pick another element and count "2." Continue. If you pick a final element of S and count "n," then you say S has n elements. At least, that is a standard informal description of counting. We wish to restate this a little more formally, in the setting where we can apply the Peano axioms.

In order to do this, we consider the following subsets of $\mathbb{N}$. Given $n \in \mathbb{N}$, set

$$I_n = \{j \in \mathbb{N} : j \le n\}. \tag{8.1}$$

While the following is quite obvious, it is worthwhile recording that it is a consequence of the Peano axioms and the material developed in §1.

Lemma 8.1. *We have*

$$I_1 = \{1\}, \quad I_{n+1} = I_n \cup \{n+1\}. \tag{8.2}$$

Proof. Left to the reader.

Now we propose the following

Definition 8.1. *A nonempty set S has n elements if and only if there exists a bijective map $\varphi : S \to I_n$.*

A reasonable definition of counting should permit one to demonstrate that, if S has n elements and it also has m elements, then $m = n$. The key to showing this from the Peano postulates is the following.

Proposition 8.2. *Assume $m, n \in \mathbb{N}$. If there exists an injective map $\varphi : I_m \to I_n$, then $m \le n$.*

Proof. Use induction on n. The case $n = 1$ is clear (by Lemma 8.1). Assume now that $N \ge 2$ and that the result is true for $n < N$. Then let $\varphi : I_m \to I_N$ be injective. Two cases arise: either there is an element $j \in I_m$ such that $\varphi(j) = N$, or not. (Also, there is no loss of generality in assuming at this point that $m \ge 2$.)

If there is such a j, define $\psi : I_{m-1} \to I_{N-1}$ by

$$\begin{aligned} \psi(\ell) = \varphi(\ell) \qquad &\text{for } \ \ell < j, \\ \varphi(\ell+1) \quad &\text{for } \ j \le \ell < m. \end{aligned}$$

Then ψ is injective, so $m - 1 \le N - 1$, and hence $m \le N$.

On the other hand, if there is no such j, then we already have an injective map $\varphi : I_m \to I_{N-1}$. The induction hypothesis implies $m \le N-1$, which in turn implies $m \le N$.

Corollary 8.3. *If there exists a bijective map $\varphi : I_m \to I_n$, then $m = n$.*

Proof. We see that $m \le n$ and $n \le m$, so Proposition 1.13 applies.

Corollary 8.4. *If S is a set, $m, n \in \mathbb{N}$, and there exist bijective maps $\varphi : S \to I_m$, $\psi : S \to I_n$, then $m = n$.*

Proof. Consider $\psi \circ \varphi^{-1}$.

Definition 8.2. *If either $S = \emptyset$ or S has n elements for some $n \in \mathbb{N}$, as in Definiton 8.1, we say S is finite.*

The next result implies that any subset of a finite set is finite.

Proposition 8.5. *Assume $n \in \mathbb{N}$. If $S \subset I_n$ is nonempty, then there exists $m \le n$ and a bijective map $\varphi : S \to I_m$.*

Proof. Use induction on n. The case $n = 1$ is clear (by Lemma 8.1). Assume the result is true for $n < N$. Then let $S \subset I_N$. Two cases arise: either $N \in S$ or $N \notin S$.

If $N \in S$, consider $S' = S \setminus \{N\}$, so $S = S' \cup \{N\}$ and $S' \subset I_{N-1}$. The inductive hypothesis yields a bijective map $\psi : S' \to I_m$ (with $m \le N - 1$), and then we obtain $\varphi : S' \cup \{N\} \to I_{m+1}$, equal to ψ on S' and sending the element N to $m+1$.

If $N \notin S$, then $S \subset I_{N-1}$, and the inductive hypothesis directly yields the desired bijective map.

Proposition 8.6. *The set $\mathbb{N}$ is not finite.*

Proof. If there were an $n \in \mathbb{N}$ and a bijective map $\varphi : I_n \to \mathbb{N}$, then, by restriction, there would be a bijective map $\psi : S \to I_{n+1}$ for some subset S of I_n, hence by the results above a bijective map $\tilde{\psi} : I_m \to I_{n+1}$ for some $m \le n < n + 1$. This contradicts Corollary 8.3.

The next result says that, in a certain sense, $\mathbb{N}$ is a minimal set that is not finite.

Proposition 8.7. *If S is not finite, then there exists an injective map $\Phi : \mathbb{N} \to S$.*

Proof. We aim to show that there exists a family of injective maps $\varphi_n : I_n \to S$, with the property that $\varphi_n\big|_{I_m} = \varphi_m$ for all $m \le n$. We establish this by induction on n. For $n = 1$, just pick some element of S and call it $\varphi_1(1)$. Now assume this claim is true for all $n < N$. So we have $\varphi_{N-1} : I_{N-1} \to S$ injective, but not surjective (since we assume S is not finite). Pick $x \in S$ not in the range of φ_{N-1}. Then define $\varphi_N : I_N \to S$ so that

$$\begin{aligned} \varphi_N(j) &= \varphi_{N-1}(j), \quad j \le N-1, \\ \varphi_N(N) &= x. \end{aligned} \tag{8.3}$$

Having the family φ_n, we define $\Phi : \mathbb{N} \to S$ by $\Phi(j) = \varphi_n(j)$ for any $n \ge j$.

Two sets S and T are said to have the same cardinality if there exists a bijective map between them; we write $\mathrm{Card}(S) = \mathrm{Card}(T)$. If there exists an injective map $\varphi : S \to T$, we write $\mathrm{Card}(S) \le \mathrm{Card}(T)$. The following result, known as the Schroeder-Bernstein theorem, implies that $\mathrm{Card}(S) = \mathrm{Card}(T)$ whenever one has both $\mathrm{Card}(S) \le \mathrm{Card}(T)$ and $\mathrm{Card}(T) \le \mathrm{Card}(S)$.

Theorem 8.8. *Let S and T be sets. Suppose there exist injective maps $\varphi : S \to T$ and $\psi : T \to S$. Then there exists a bijective map $\Phi : S \to T$.*

Proof. Let us say an element $x \in T$ has a parent $y \in S$ if $\varphi(y) = x$. Similarly there is a notion of a parent of an element of S. Iterating this gives a sequence of "ancestors" of any element of S or T. For any element of S or T, there are three possibilities:

a) The set of ancestors never terminates.
b) The set of ancestors terminates at an element of S.
c) The set of ancestors terminates at an element of T.

We denote by S_a, T_a the elements of S, T, respectively for which case a) holds. Similarly we have S_b, T_b and S_c, T_c. We have disjoint unions

$$S = S_a \cup S_b \cup S_c, \quad T = T_a \cup T_b \cup T_c.$$

Now note that

$$\varphi : S_a \to T_a, \quad \varphi : S_b \to T_b, \quad \psi : T_c \to S_c$$

are all bijective. Thus we can set Φ equal to φ on $S_a \cup S_b$ and equal to ψ^{-1} on S_c, to get a desired bijection.

The terminology above suggests regarding $\text{Card}(S)$ as an object (some sort of number). Indeed, if S is finite we set $\text{Card}(S) = n$ if S has n elements (as in Definition 8.1). A set that is not finite is said to be infinite. We can also have a notion of cardinality of infinite sets. A standard notation for the cardinality of $\mathbb{N}$ is

$$\text{Card}(\mathbb{N}) = \aleph_0. \tag{8.4}$$

Here are some other sets with the same cardinality:

Proposition 8.9. *We have*

$$\textit{Card}(\mathbb{Z}) = \textit{Card}(\mathbb{N} \times \mathbb{N}) = \textit{Card}(\mathbb{Q}) = \aleph_0. \tag{8.5}$$

Proof. We can define a bijection of $\mathbb{N}$ onto $\mathbb{Z}$ by ordering elements of $\mathbb{Z}$ as follows:

$$0, 1, -1, 2, -2, 3, -3, \cdots .$$

We can define a bijection of $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ by ordering elements of $\mathbb{N} \times \mathbb{N}$ as follows:

$$(1,1),\ (1,2),\ (2,1),\ (1,3),\ (2,2),\ (3,1), \cdots .$$

We leave it to the reader to produce a similar ordering of $\mathbb{Q}$.

An infinite set that can be mapped bijectively onto $\mathbb{N}$ is called countably infinite. A set that is either finite or countably infinite is called countable. The following result is a natural extension of Proposition 8.5.

Proposition 8.10. *If X is a countable set and $S \subset X$, then S is countable.*

Proof. If X is finite, then Proposition 8.5 applies. Otherwise, we can assume $X = \mathbb{N}$, and we are looking at $S \subset \mathbb{N}$, so there is an injective map $\varphi : S \to \mathbb{N}$. If S is finite, there is no problem. Otherwise, by Proposition 8.7, there is an injective map $\psi : \mathbb{N} \to S$, and then Theorem 8.8 implies the existence of a bijection between S and $\mathbb{N}$.

There are sets that are not countable; they are said to be uncountable.

Proposition 8.11. *The set $\mathbb{R}$ of real numbers is uncountable.*

Proof. We may as well show that $(0,1) = \{x \in \mathbb{R} : 0 < x < 1\}$ is uncountable. If it were countable, there would be a bijective map $\varphi : \mathbb{N} \to (0,1)$. Expand the real number $\varphi(j)$ in its infinite decimal expansion:

$$\varphi(j) = \sum_{k=1}^{\infty} a_{jk} \cdot 10^{-k}, \quad a_{jk} \in \{0, 1, \dots 9\}. \tag{8.6}$$

Now set

$$\begin{aligned} b_k &= 2 \quad \text{if} \quad a_{kk} \neq 2, \\ &\ 3 \quad \text{if} \quad a_{kk} = 2, \end{aligned} \tag{8.7}$$

and consider

$$\xi = \sum_{k=1}^{\infty} b_k \cdot 10^{-k}, \quad \xi \in (0,1). \tag{8.8}$$

It is seen that ξ is not equal to $\varphi(j)$ for any $j \in \mathbb{N}$, contradicting the hypothesis that $\varphi : \mathbb{N} \to (0,1)$ is onto.

A common notation for the cardinality of $\mathbb{R}$ is

$$\text{Card}(\mathbb{R}) = c. \tag{8.9}$$

We leave it as an exercise to the reader to show that

$$\text{Card}(\mathbb{R} \times \mathbb{R}) = c. \tag{8.10}$$

Further development of the theory of cardinal numbers requires a formalization of the notions of set theory. In these notes we have used set theoretical notions rather informally. Our use of such notions has gotten somewhat heavier in this last section. In particular, in the proof of Proposition 8.7, the innocent looking use of the phrase "pick $x \in S \dots$" actually assumes the truth of a weak version of the Axiom of Choice. For an introduction to the axiomatic treatment of set theory we refer to [Dev], and at this point bring our own introduction to the study of numbers to an end.

References

[BS] R. Bartle and D. Sherbert, Introduction to Real Analysis, J. Wiley, New York, 1992.

[Be] P. Beckmann, A History of π, St. Martin's Press, New York, 1971.

[Dev] K. Devlin, The Joy of Sets: Fundamentals of Contemporary Set Theory, Springer-Verlag, New York, 1993.