CHAPTER 5

CONSTRUCTION OF THE REAL NUMBERS[1]

In Chapter 4 we gave a set-theoretic construction of the set ω of natural numbers. In the present chapter we will continue to show how mathematics can be embedded in set theory, by giving a set-theoretic construction of the real numbers. (The operative phrase is "can be," not "is" or "must be." We will return to this point in the section on "Two.")

INTEGERS

First we want to extend our set ω of natural numbers to a set $\mathbb{Z}$ of integers (both positive and negative). Here "extend" is to be loosely interpreted, since ω will not actually be a subset of $\mathbb{Z}$. But $\mathbb{Z}$ will include an "isomorphic copy" of ω (Fig. 19).

A negative integer can be named by using two natural numbers and a subtraction symbol: $2 - 3$, $5 - 10$, etc. We need some sets to stand behind these names.

As a first guess, we could try taking the integer -1 to be the pair $\langle 2, 3 \rangle$ of natural numbers used to name -1 in the preceding paragraph. And

[1] Other chapters do not depend on Chapter 5.

similarly we could try letting the integer -5 be the pair $\langle 5, 10\rangle$ of natural numbers. But this first guess fails, because -1 has a multiplicity of names: $2 - 3 = 0 - 1$ but $\langle 2, 3\rangle \neq \langle 0, 1\rangle$.

As a second guess, we can define an equivalence relation $\sim$ such that $\langle 2, 3\rangle \sim \langle 0, 1\rangle$. (Imposing such an equivalence relation is sometimes described as "identifying" $\langle 2, 3\rangle$ and $\langle 0, 1\rangle$.) Then we will have the one equivalence class

$$[\langle 2, 3\rangle] = [\langle 0, 1\rangle],$$

and we can take -1 to be this equivalence class. Then for the set $\mathbb{Z}$ of all integers, we can take the set of all equivalence classes:

$$\mathbb{Z} = (\omega \times \omega)/\sim.$$

This is in fact what we do. Call a pair of natural numbers a *difference*; then an integer will be an equivalence class of differences. Consider two differences $\langle m, n\rangle$ and $\langle p, q\rangle$. When should we call them equivalent?

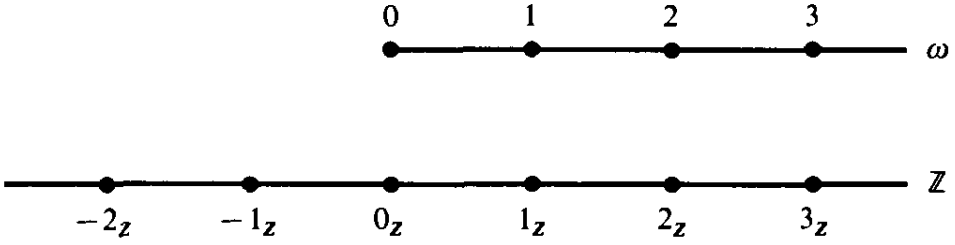

Fig. 19. There is a subset of $\mathbb{Z}$ that looks like ω.

Informally, they are equivalent iff $m - n = p - q$, but this equation has no official meaning for us yet. But the equation is equivalent to $m + q = p + n$, and the latter equation is meaningful. Consequently we formulate the following definition.

Definition Define $\sim$ to be the relation on $\omega \times \omega$ for which

$$\langle m, n\rangle \sim \langle p, q\rangle \quad \text{iff} \quad m + q = p + n.$$

Thus $\sim$ is a set of ordered pairs whose domain and range are also sets of ordered pairs. In more explicit (but less readable) form, the above definition can be stated:

$$\sim = \{\langle\langle m, n\rangle, \langle p, q\rangle\rangle \mid m + q = p + n \text{ and all are in } \omega\}.$$

Theorem 5ZA The relation $\sim$ is an equivalence relation on $\omega \times \omega$.

Proof We leave it to you to check that $\sim$ is reflexive on $\omega \times \omega$ and is symmetric. To show transitivity, suppose that $\langle m, n\rangle \sim \langle p, q\rangle$ and $\langle p, q\rangle \sim \langle r, s\rangle$. Then (by the definition of $\sim$)

$$m + q + p + s = p + n + r + q.$$

By use of the cancellation law (Corollary 4P), we obtain $m + s = r + n$, and thus $\langle m, n\rangle \sim \langle r, s\rangle$. ⊣

Definition The set $\mathbb{Z}$ of *integers* is the set $(\omega \times \omega)/\sim$ of all equivalence classes of differences.

For example, the integer 2_Z is the equivalence class

$$[\langle 2, 0\rangle] = \{\langle 2, 0\rangle, \langle 3, 1\rangle, \langle 4, 2\rangle, \ldots\},$$

and the integer -3_Z is the equivalence class

$$[\langle 0, 3\rangle] = \{\langle 0, 3\rangle, \langle 1, 4\rangle, \langle 2, 5\rangle, \ldots\}.$$

These equivalence classes can be pictured as 45° lines in the Cartesian product $\omega \times \omega$ (Fig. 20).

Next we want to endow $\mathbb{Z}$ with a suitable addition operation. Informally, we can add differences:

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

This indicates that the correct addition function $+_Z$ for integers will satisfy the equation

$$[\langle m, n\rangle] +_Z [\langle p, q\rangle] = [\langle m + p, n + q\rangle].$$

This equation will serve to define $+_Z$, once we have verified that it makes sense. The situation here is of the sort discussed in Theorem 3Q. We want to specify the value of the operation $+_Z$ at a pair of equivalence classes by (1) selecting representatives $\langle m, n\rangle$ and $\langle p, q\rangle$ from the classes, (2)

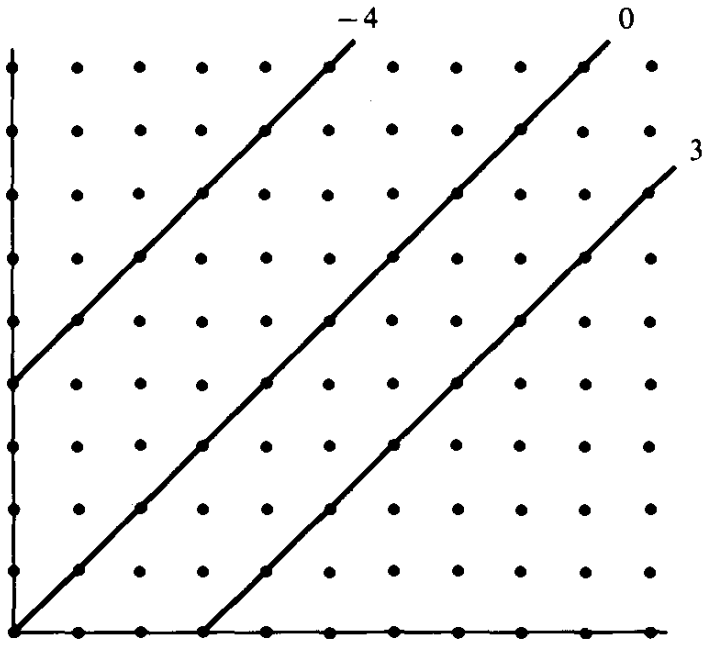

Fig. 20. An integer is a line in $\omega \times \omega$.

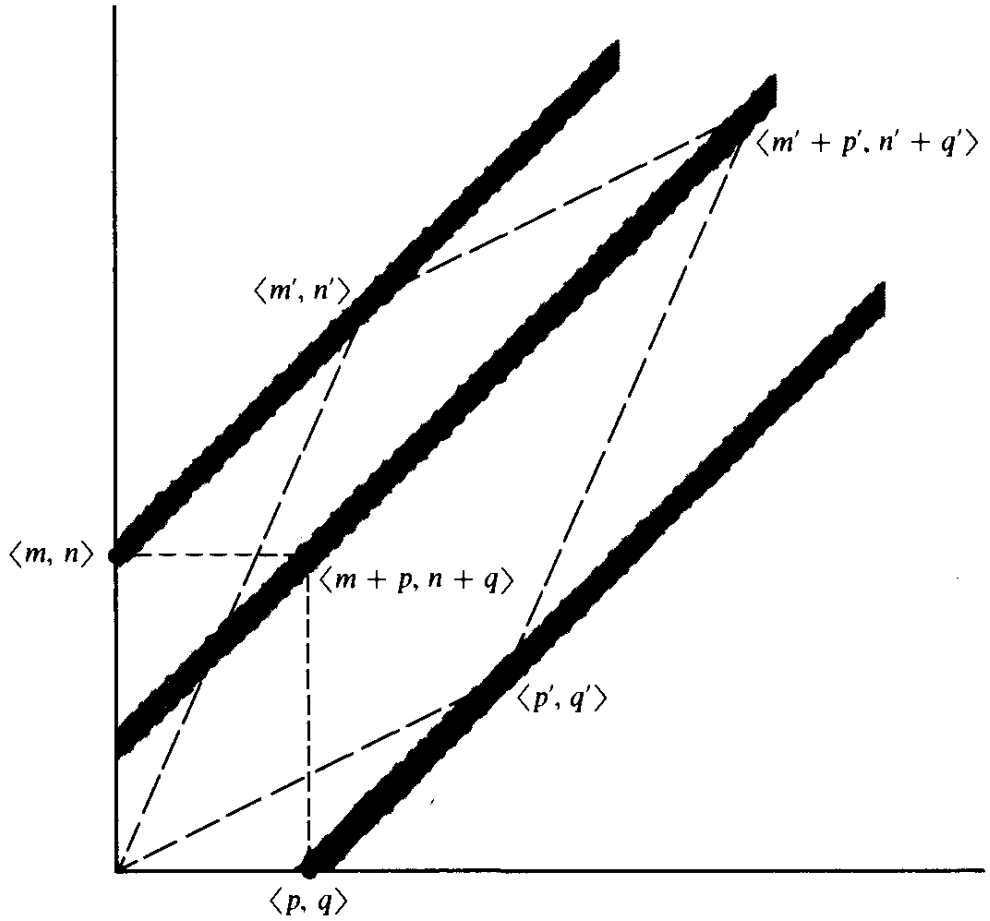

Fig. 21. Addition of lines is well defined.

operating on the representatives (by vector addition in this case), and then (3) forming the equivalence class of the result of the vector addition. For $+_Z$ to be well defined, we must verify that choice of other representatives $\langle m', n' \rangle$ and $\langle p', q' \rangle$ from the given classes would yield the same equivalence class for the sum (Fig. 21).

Lemma 5ZB If $\langle m, n \rangle \sim \langle m', n' \rangle$ and $\langle p, q \rangle \sim \langle p', q' \rangle$, then

$$\langle m + p, n + q \rangle \sim \langle m' + p', n' + q' \rangle.$$

Proof We are given, by hypothesis, the two equations

$$m + n' = m' + n \qquad \text{and} \qquad p + q' = p' + q.$$

We want to obtain the equation

$$m + p + n' + q' = m' + p' + n + q.$$

But this results from just adding together the two given equations. ⊣

This lemma justifies the definition of $+_Z$. In the terminology of Theorem 3Q, it says that the function F of vector addition

$$F(\langle m, n \rangle, \langle p, q \rangle) = \langle m + p, n + q \rangle$$

is compatible with $\sim$. Hence there is a well-defined function $\hat{F}$ on the quotient set; $\hat{F}$ is just our operation $+_Z$. It satisfies the equation

$$[\langle m, n\rangle] +_Z [\langle p, q\rangle] = [\langle m + p, n + q\rangle].$$

In other words, for integers a and b our addition formula is

$$a +_Z b = [\langle m + p, n + q\rangle],$$

where $\langle m, n\rangle$ is chosen from a and $\langle p, q\rangle$ is chosen from b. Theorem 3Q assures us that the equivalence class on the right is independent of how these choices are made.

Example We can calculate $2_Z +_Z (-3_Z)$. Since $2_Z = [\langle 2, 0\rangle]$ and $-3_Z = [\langle 0, 3\rangle]$, we have

$$\begin{aligned} 2_Z +_Z (-3_Z) &= [\langle 2, 0\rangle] +_Z [\langle 0, 3\rangle] \\ &= [\langle 2 + 0, 0 + 3\rangle] \\ &= [\langle 2, 3\rangle] \\ &= -1_Z. \end{aligned}$$

The familiar properties of addition, such as commutativity and associativity, now follow easily from the corresponding properties of addition of natural numbers.

Theorem 5ZC The operation $+_Z$ is commutative and associative:

$$a +_Z b = b +_Z a,$$

$$(a +_Z b) +_Z c = a +_Z (b +_Z c).$$

Proof The integer a must be of the form $[\langle m, n\rangle]$ for some natural numbers m and n; similarly b is $[\langle p, q\rangle]$. Then:

$$\begin{aligned} a +_Z b &= [\langle m, n\rangle] +_Z [\langle p, q\rangle] \\ &= [\langle m + p, n + q\rangle] && \text{by definition of } +_Z \\ &= [\langle p + m, q + n\rangle] && \text{by commutativity of } + \text{ on } \omega \\ &= [\langle p, q\rangle] +_Z [\langle m, n\rangle] \\ &= b +_Z a. \end{aligned}$$

The calculation for associativity is similar (Exercise 4). ⊣

Let $0_Z = [\langle 0, 0\rangle]$. Then it is straightforward to verify that $a +_Z 0_Z = a$ for any integer a, i.e., 0_Z is an identity element for addition. And the new feature that $\mathbb{Z}$ has (and the feature for which the extension from ω to $\mathbb{Z}$ was made), is the existence of additive inverses.

Theorem 5ZD (a) 0_Z is an identity element for $+_Z$:

$$a +_Z 0_Z = a$$

for any a in $\mathbb{Z}$.

(b) Additive inverses exist: For any integer a, there is an integer b such that

$$a +_Z b = 0_Z.$$

Proof (b) Given an integer a, it must be of the form $[\langle m, n\rangle]$. Take b to be $[\langle n, m\rangle]$. Then $a +_Z b = [\langle m + n, n + m\rangle] = [\langle 0, 0\rangle] = 0_Z$. ⊣

Theorems 5ZC and 5ZD together say that $\mathbb{Z}$ with the operation $+_Z$ and the identity element 0_Z is an *Abelian group*. The concept of an Abelian group is central to abstract algebra, but in this book the concept will receive only passing attention.

Inverses are unique. That is, if $a +_Z b = 0_Z$ and $a +_Z b' = 0_Z$, then $b = b'$. To prove this, observe that

$$b = b +_Z (a +_Z b') = (b +_Z a) +_Z b' = b'.$$

(This proof works in any Abelian group.) The inverse of a is denoted as $-a$. Then as the proof to Theorem 5ZD shows,

$$-[\langle m, n\rangle] = [\langle n, m\rangle].$$

Inverses provide us with a subtraction operation, which we define by the equation

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

We can also endow the set $\mathbb{Z}$ with a multiplication operation, which we obtain in much the same way as we obtained the addition operation. First we look at the informal calculation with differences

$$(m - n) \cdot (p - q) = (mp + nq) - (mq + np),$$

which tells us that the desired operation $\cdot_Z$ will satisfy the equation

$$[\langle m, n\rangle] \cdot_Z [\langle p, q\rangle] = [\langle mp + nq, mq + np\rangle].$$

(Here we write, as usual, mp in place of $m \cdot p$.) Again we must verify that the above equation characterizes a well-defined operation on equivalence classes. That is, we must verify that the operation on differences

$$G(\langle m, n\rangle, \langle p, q\rangle) = \langle mp + nq, mq + np\rangle$$

is compatible with $\sim$. This verification is accomplished by the following lemma.

Lemma 5ZE If $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then

$$\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q', m'q' + n'p'\rangle.$$

Proof We are given the two equations

$$m + n' = m' + n, \tag{1}$$

$$p + q' = p' + q, \tag{2}$$

and we want to obtain the equation

$$mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np.$$

The idea is take multiples of (1) and (2) that contain the terms we need. First multiply Eq. (1) by p; this gives us an mp on the left and an np on the right. Second, multiply the reverse of Eq. (1) by q; this gives us an nq on the left and an mq on the right. Third, multiply Eq. (2) by m'. Fourth, multiply the reverse of Eq. (2) by n'. Now add the four equations we have obtained from (1) and (2). All the unwanted terms cancel, and we are left with the desired equation. It works. ⊣

As for addition, we can prove the basic properties of multiplication from the corresponding properties of multiplication of natural numbers.

Theorem 5ZF The multiplication operation $\cdot_Z$ is commutative, associative, and distributive over $+_Z$:

$$a \cdot_Z b = b \cdot_Z a$$

$$(a \cdot_Z b) \cdot_Z c = a \cdot_Z (b \cdot_Z c)$$

$$a \cdot_Z (b +_Z c) = (a \cdot_Z b) +_Z (a \cdot_Z c)$$

Proof Say that $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. For the commutative law, we have

$$a \cdot_Z b = [\langle mp + nq, mq + np\rangle],$$

whereas

$$b \cdot_Z a = [\langle pm + qn, pn + qm\rangle].$$

The equality of these two follows at once from the commutativity of addition and multiplication in ω.

The other parts of the theorem are proved by the same method. Say that $c = [\langle r, s\rangle]$. Then $(a \cdot_Z b) \cdot_Z c$ is

$$[\langle mp + nq)r + (mq + np)s, (mp + nq)s + (mq + np)r\rangle],$$

where $a \cdot_Z (b \cdot_Z c)$ is

$$[\langle m(pr + qs) + n(ps + qr), m(ps + qr) + n(pr + qs)\rangle].$$

The equality of these follows from laws of arithmetic in ω (Theorem 4K).

As for the distributive law, when we expand $a \cdot_Z (b +_Z c)$, we obtain

$$[\langle m(p + r) + n(q + s), m(q + s) + n(p + r)\rangle],$$

whereas when we expand $a \cdot_Z b +_Z a \cdot_Z c$ we obtain

$$[\langle mp + nq + mr + ns, mq + np + ms + nr\rangle].$$

Again equality is clear from laws of arithmetic in ω. ⊣

The remaining properties of multiplication that we will need constitute the next theorem. Let 1_Z be the integer $[\langle 1, 0\rangle]$.

Theorem 5ZG (a) The integer 1_Z is a multiplicative identity element:

$$a \cdot_Z 1_Z = a$$

for any integer a.

(b) $0_Z \neq 1_Z$.

(c) Whenever $a \cdot_Z b = 0_Z$, then either $a = 0_Z$ or $b = 0_Z$.

Part (c) is sometimes stated: There are no "zero divisors" in $\mathbb{Z}$.

Proof Part (a) is a trivial calculation.

For part (b) it is necessary to check that $\langle 0, 0\rangle \not\sim \langle 1, 0\rangle$. This reduces to checking that $0 \neq 1$ in ω, which is true.

For part (c), assume that $a \neq 0_Z$ and $b \neq 0_Z$; it will suffice to prove that $a \cdot_Z b \neq 0_Z$. We know that for some m, n, p, and q:

$$a = [\langle m, n\rangle], \qquad b = [\langle p, q\rangle],$$

$$a \cdot_Z b = [\langle mp + nq, mq + np\rangle].$$

Since $a \neq [\langle 0, 0\rangle]$, we have $m \neq n$. So either $m \in n$ or $n \in m$. Similarly, either $p \in q$ or $q \in p$. This leads to a total of four cases, but in each case we have

$$mp + nq \neq mq + np$$

by Exercise 25 of Chapter 4. Hence $a \cdot_Z b \neq [\langle 0, 0\rangle]$. ⊣

In algebraic terminology, we can say that $\mathbb{Z}$ together with $+_Z$, $\cdot_Z$, 0_Z, and 1_Z forms an *integral domain*. This means that:

(i) $\mathbb{Z}$ with $+_Z$ and 0_Z forms as Abelian group (Theorems 5ZC and 5ZD).

(ii) Multiplication is commutative and associative, and is distributive over addition (Theorem 5ZF).

(iii) 1_Z is a multiplicative identity (different from 0_Z), and no zero divisors exist (Theorem 5ZG).

There is a summary of these algebraic concepts near the end of this chapter. The value of the concepts stems from the large array of structures that satisfy the various conditions. In this book, however, we are concerned with only the most standard cases.

Example The calculation

$$[\langle 0, 1\rangle] \cdot_Z [\langle m, n\rangle] = [\langle n, m\rangle]$$

shows that $-1_Z \cdot_Z a = -a$.

Next we develop an ordering relation $<_Z$ on the integers. The informal calculation

$$m - n < p - q \quad \text{iff} \quad m + q < p + n$$

indicates that ordering $<_Z$ on $\mathbb{Z}$ should be defined by

$$[\langle m, n\rangle] <_Z [\langle p, q\rangle] \quad \text{iff} \quad m + q \in p + n.$$

As usual, it is necessary to check that this condition yields a well-defined relation on the integers. That is, we want to define

$$a <_Z b \quad \text{iff} \quad m + q \in p + n,$$

where m, n, p, and q are chosen so that $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. But that choice can be made in infinitely many ways; we must verify that we have the same outcome each time. The following lemma does just this.

Lemma 5ZH If $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then

$$m + q \in p + n \quad \text{iff} \quad m' + q' \in p' + n'.$$

Proof The hypotheses give us the equations

$$m + n' = m' + n \qquad \text{and} \qquad p + q' = p' + q.$$

In order to utilize these equations in the inequality $m + q \in p + n$, we add n' and q' to each side of this inequality:

$$\begin{aligned} m + q \in p + n &\Leftrightarrow m + q + n' + q' \in p + n + n' + q' \\ &\Leftrightarrow m' + n + q + q' \in p' + q + n + n' \\ &\Leftrightarrow m' + q' \in p' + n'. \end{aligned}$$

Here the first and third steps use Theorem 4N, while the middle step uses the given equations. ⊣

Theorem 5ZI The relation $<_Z$ is a linear ordering relation on the set of integers.

Proof We must show that $<_Z$ is a transitive relation that satisfies trichotomy on $\mathbb{Z}$.

To prove transitivity, consider integers $a = [\langle m, n\rangle]$, $b = [\langle p, q\rangle]$, and $c = [\langle r, s\rangle]$. Then

$$\begin{aligned} a <_Z b \,\&\, b <_Z c &\Rightarrow m + q \in p + n \,\&\, p + s \in r + q \\ &\Rightarrow m + q + s \in p + n + s \,\&\, p + s + n \in r + q + n \\ &\Rightarrow m + q + s \in r + q + n \\ &\Rightarrow m + s \in r + n \qquad \text{by Theorem 4N} \\ &\Rightarrow a <_Z c. \end{aligned}$$

Proving trichotomy is easy. To say that exactly one of

$$a <_Z b, \qquad a = b, \qquad b <_Z a$$

holds is to say that exactly one of

$$m + q \in p + n, \qquad m + q = p + n, \qquad p + n \in m + q$$

holds. Thus the result follows from trichotomy in ω. ⊣

An integer b is called *positive* iff $0_Z <_Z b$. It is easy to check that

$$b <_Z 0_Z \quad \text{iff} \quad 0_Z <_Z -b.$$

Thus a consequence of trichotomy is the fact that for an integer b, exactly one of the three alternatives

$$b \text{ is positive}, \qquad b \text{ is zero}, \qquad -b \text{ is positive}$$

holds.

The next theorem shows that addition preserves order, as does multiplication by a positive integer. (The corresponding theorem for ω was Theorem 4N.)

Theorem 5ZJ The following are valid for any integers a, b, and c:

(a) $a <_Z b \Leftrightarrow a +_Z c <_Z b +_Z c$.

(b) If $0_Z <_Z c$, then

$$a <_Z b \;\Leftrightarrow\; a \cdot_Z c <_Z b \cdot_Z c.$$

Proof Assume that a, b, and c are $[\langle m, n\rangle]$, $[\langle p, q\rangle]$, and $[\langle r, s\rangle]$, respectively. The result to be proved in part (a) then translates to the following statement about natural numbers:

$$m + q \in p + n \;\Leftrightarrow\; m + r + q + s \in p + r + n + s.$$

This is an immediate consequence of the fact that addition in ω preserves order (Theorem 4N).

Part (b) is similar in spirit. As in Theorem 4N, it suffices to prove one direction:

$$0_Z <_Z c \;\&\; a <_Z b \;\Rightarrow\; a \cdot_Z c <_Z b \cdot_Z c.$$

This translates to:

$$s \in r \;\&\; m + q \in p + n \;\Rightarrow\; mr + ns + ps + qr \in pr + qs + ms + nr.$$

This is not as bad as it looks. If we let $k = m + q$ and $l = p + n$, then it becomes

$$s \in r \;\&\; k \in l \;\Rightarrow\; kr + ls \in ks + lr.$$

This is just Exercise 25 of Chapter 4. ⊣

Corollary 5ZK For any integers a, b, and c the cancellation laws hold:

$$a +_Z c = b +_Z c \;\Rightarrow\; a = b,$$

$$a \cdot_Z c = b \cdot_Z c \;\&\; c \neq 0_Z \;\Rightarrow\; a = b.$$

Proof This follows from the preceding theorem in the same way that the cancellation laws in ω (Corollary 4P) followed from the order-preserving properties (Theorem 4N). ⊣

Although ω is not actually a subset of $\mathbb{Z}$, nonetheless $\mathbb{Z}$ has a subset that is "just like" ω. To make this precise, define the function $E\colon \omega \to \mathbb{Z}$ by

$$E(n) = [\langle n, 0\rangle].$$

For example, $E(0) = 0_Z$ and $E(1) = 1_Z$.

The following theorem, in algebraic terminology, says that E is an "isomorphic embedding" of the system $\langle \omega, +, \cdot, \in_\omega \rangle$ into the system $\langle \mathbb{Z}, +_Z, \cdot_Z, <_Z \rangle$. That is, E is a one-to-one function that preserves addition, multiplication, and order.

Theorem 5ZL E maps ω one-to-one into $\mathbb{Z}$, and satisfies the following properties for any natural numbers m and n:

(a) $E(m + n) = E(m) +_Z E(n)$.
(b) $E(mn) = E(m) \cdot_Z E(n)$.
(c) $m \in n$ iff $E(m) <_Z E(n)$.

Proof To show that E is one-to-one we calculate

$$\begin{aligned} E(m) = E(n) &\Rightarrow [\langle m, 0\rangle] = [\langle n, 0\rangle] \\ &\Rightarrow \langle m, 0\rangle \sim \langle n, 0\rangle \\ &\Rightarrow m = n. \end{aligned}$$

Parts (a), (b), and (c) are proved by routine calculations (Exercise 8). ⊣

Finally we can give a precise counterpart to our motivating guideline that the difference $\langle m, n\rangle$ should name $m - n$. For any m and n,

$$[\langle m, n\rangle] = E(m) - E(m)$$

as is verified by evaluating the right side of this equation (Exercise 9).

Henceforth we will streamline our notation by omitting the subscript "Z" on $+_Z$, $\cdot_Z$, $<_Z$, 0_Z, 1_Z, etc. Furthermore $a \cdot b$ will usually be written as just ab.

Exercises

1. Is there a function $F: \mathbb{Z} \to \mathbb{Z}$ satisfying the equation

$$F([\langle m, n\rangle]) = [\langle m + n, n\rangle]?$$

2. Is there a function $G: \mathbb{Z} \to \mathbb{Z}$ satisfying the equation

$$G([\langle m, n\rangle]) = [\langle m, m\rangle]?$$

3. Is there a function $H: \mathbb{Z} \to \mathbb{Z}$ satisfying the equation

$$H([\langle m, n\rangle]) = [\langle n, m\rangle]?$$

4. Prove that $+_Z$ is associative. (This is part of Theorem 5ZC.)
5. Give a formula for subtraction of integers:

$$[\langle m, n\rangle] - [\langle p, q\rangle] = \ ?$$

6. Show that $a \cdot_Z 0_Z = 0_Z$ for every integer a.
7. Show that

$$a \cdot_Z (-b) = (-a) \cdot_Z b = -(a \cdot_Z b)$$

for all integers a and b.

8. Prove parts (a), (b), and (c) of Theorem 5ZL.
9. Show that

$$[\langle m, n\rangle] = E(m) - E(n)$$

for all natural numbers m and n.

RATIONAL NUMBERS

We can extend our set $\mathbb{Z}$ of integers to the set $\mathbb{Q}$ of rational numbers in much the same way as we extended ω to $\mathbb{Z}$. In fact, the extension from $\mathbb{Z}$ to $\mathbb{Q}$ is to multiplication what the extension from ω to $\mathbb{Z}$ is to addition. In the integers we get additive inverses, i.e., solutions to the equation $a + x = 0$.

In the rationals we will get multiplicative inverses, i.e., solutions to the equation $r \cdot_Q x = 1_Q$ (for nonzero r).

We can name a rational number by using two integers and a symbol for division:

$$1/2, \quad -3/4, \quad 6/12.$$

But as before, each number has a multiplicity of names, e.g., $1/2 = 6/12$. So the name "1/2" must be identified with the name "6/12."

By a *fraction* we mean an ordered pair of integers, the second component of which (called the *denominator*) is nonzero. For example, $\langle 1, 2\rangle$ and $\langle 6, 12\rangle$ are fractions; we want a suitable equivalence relation $\sim$ for which $\langle 1, 2\rangle \sim \langle 6, 12\rangle$. Since $a/b = c/d$ iff $a \cdot d = c \cdot b$, we choose to define $\sim$ as follows. Let $\mathbb{Z}'$ be the set $\mathbb{Z} - \{0\}$ of nonzero integers. Then $\mathbb{Z} \times \mathbb{Z}'$ is the set of all fractions.

Definition Define $\sim$ to be the binary relation on $\mathbb{Z} \times \mathbb{Z}'$ for which

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \text{iff} \quad a \cdot d = c \cdot b.$$

The set $\mathbb{Q}$ of *rational numbers* is the set $(\mathbb{Z} \times \mathbb{Z}')/\sim$ of all equivalence classes of fractions.

We use the same symbol "$\sim$" that has been used previously for other equivalence relations, but as we discuss only one equivalence relation at a time, no confusion should result.

For example, $\langle 1, 2\rangle \sim \langle 6, 12\rangle$ since $1 \cdot 12 = 6 \cdot 2$. The equivalence class $[\langle 1, 2\rangle]$ is the rational number "one-half." The rationals zero and one are

$$0_Q = [\langle 0, 1\rangle] \qquad \text{and} \qquad 1_Q = [\langle 1, 1\rangle].$$

These are distinct, because $\langle 0, 1\rangle \not\sim \langle 1, 1\rangle$. Of course we must check that $\sim$ is indeed an equivalence relation.

Theorem 5QA The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$.

Proof You should verify that the relation is reflexive on $\mathbb{Z} \times \mathbb{Z}'$ and is symmetric. As for transitivity, suppose that

$$\langle a, b\rangle \sim \langle c, d\rangle \qquad \text{and} \qquad \langle c, d\rangle \sim \langle e, f\rangle.$$

Then

$$ad = cb \qquad \text{and} \qquad cf = ed.$$

Multiply the first equation by f and the second by b to get

$$adf = cbf \qquad \text{and} \qquad cfb = edb.$$

From this we conclude that $adf = edb$ and hence (by canceling the nonzero d) $af = eb$. This tells us that $\langle a, b\rangle \sim \langle e, f\rangle$. ⊣

We can picture the equivalence classes as nonhorizontal lines (in the "plane" $\mathbb{Z} \times \mathbb{Z}'$) through the origin (Fig. 22). The fraction $\langle 1, 2\rangle$ lies on the line with slope 2; in general, $[\langle a, b\rangle]$ is the line with slope b/a.

We arrive at addition and multiplication operations for $\mathbb{Q}$ by the same methods used for $\mathbb{Z}$. For addition, the informal calculation

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

indicates that $+_Q$ should be defined by the equation

$$[\langle a, b\rangle] +_Q [\langle c, d\rangle] = [\langle ad + cb, bd\rangle].$$

Note that $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Hence $\langle ad + cb, bd\rangle$ *is* a fraction. As usual, we must check that there is a well-defined function $+_Q$ on equivalence classes that satisfies the above equation. The following lemma, together with Theorem 3Q, does just that.

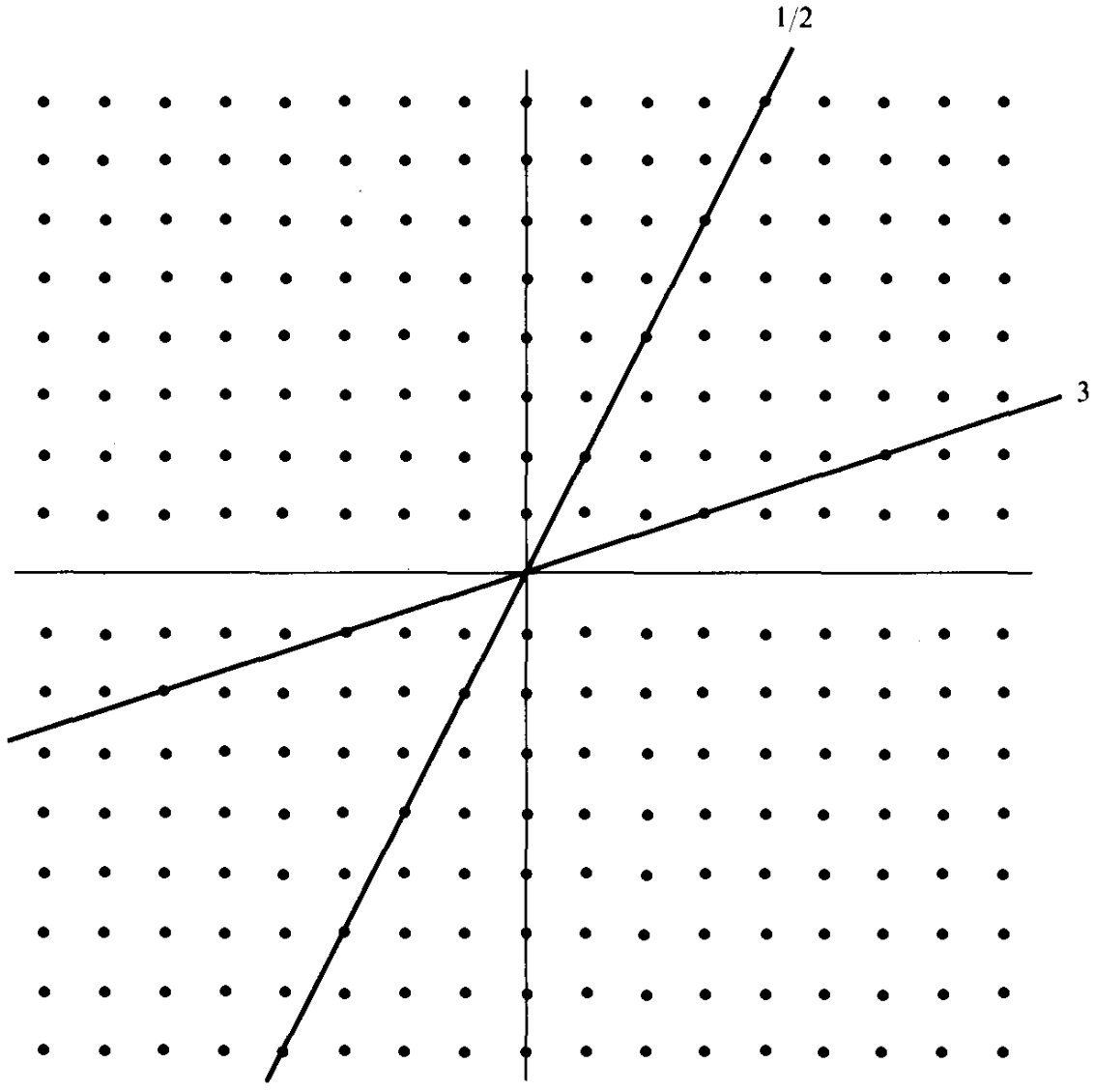

Fig. 22. Rational numbers are nonhorizontal lines.

Lemma 5QB If $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$, then

$$\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle.$$

Proof We are given the equations

$$ab' = a'b \qquad \text{and} \qquad cd' = c'd.$$

We want the equation

$$(ad + cb)b'd' = (a'd' + c'b')bd,$$

which, when expanded (with the factors in alphabetic order), becomes

$$ab'dd' + bb'cd' = a'bdd' + bb'c'd.$$

This clearly is obtainable from the given equations. ⊣

Example Just to be on the safe side, we will check that $2 + 2 = 4$ in $\mathbb{Q}$. Let $2_Q = [\langle 2, 1\rangle]$ and $4_Q = [\langle 4, 1\rangle]$. Then

$$\begin{aligned} 2_Q +_Q 2_Q &= [\langle 2, 1\rangle] +_Q [\langle 2, 1\rangle] \\ &= [\langle 2 + 2, 1\rangle] \\ &= [\langle 4, 1\rangle] = 4_Q, \end{aligned}$$

where we use the fact that $2 + 2 = 4$ in $\mathbb{Z}$.

The rationals with $+_Q$ and 0_Q also form an Abelian group:

Theorem 5QC (a) Addition $+_Q$ is associative and commutative:

$$(q +_Q r) +_Q s = q +_Q (r +_Q s),$$

$$r +_Q s = s +_Q r.$$

(b) 0_Q is an identity element for $+_Q$:

$$r +_Q 0_Q = r$$

for any r in $\mathbb{Q}$.

(c) Additive inverses exist: For any r in $\mathbb{Q}$ there is an s in $\mathbb{Q}$ such that $r +_Q s = 0_Q$.

Proof First we verify commutativity. On the one hand,

$$[\langle a, b\rangle] +_Q [\langle c, d\rangle] = [\langle ad + cb, bd\rangle],$$

and on the other

$$[\langle c, d\rangle] +_Q [\langle a, b\rangle] = [\langle cb + ad, db\rangle].$$

But the right sides of these two equations are equal, by known commutative laws for arithmetic in $\mathbb{Z}$.

The verification of associativity is similar. Consider three rational numbers $[\langle a, b\rangle]$, $[\langle c, d\rangle]$, and $[\langle e, f\rangle]$. Then one grouping for the sum is

$$\begin{aligned}([\langle a, b\rangle] +_Q [\langle c, d\rangle]) +_Q [\langle e, f\rangle] &= [\langle ad + cb, bd\rangle] +_Q [\langle e, f\rangle] \\ &= [\langle (ad + cb)f + e(bd), (bd)f\rangle] \\ &= [\langle adf + cbf + ebd, bdf\rangle].\end{aligned}$$

The same expansion for the other grouping is

$$\begin{aligned}[\langle a, b\rangle] +_Q ([\langle c, d\rangle] +_Q [\langle e, f\rangle]) &= [\langle a, b\rangle] +_Q [\langle cf + ed, df\rangle] \\ &= [\langle a(df) + (cf + ed)b, b(df)\rangle] \\ &= [\langle adf + cfb + edb, bdf\rangle],\end{aligned}$$

which agrees with the first calculation.

Part (b) is a routine calculation. We know that $r = [\langle a, b\rangle]$ for some integers a and b. Then

$$\begin{aligned}r +_Q 0_Q &= [\langle a, b\rangle] +_Q [\langle 0, 1\rangle] \\ &= [\langle a \cdot 1 + 0 \cdot b, b \cdot 1\rangle] \\ &= [\langle a, b\rangle] = r.\end{aligned}$$

Finally for part (c) we select (with r as above) $s = [\langle -a, b\rangle]$. Then it is easy to calculate that

$$\begin{aligned}r +_Q s &= [\langle a, b\rangle] +_Q [\langle -a, b\rangle] \\ &= [\langle ab + (-a)b, bb\rangle] \\ &= [\langle 0, bb\rangle] = 0_Q,\end{aligned}$$

since $\langle 0, bb\rangle \sim \langle 0, 1\rangle$. ⊣

As in any Abelian group, the inverse of r is unique; we denote it as $-r$. The above proof shows that $-[\langle a, b\rangle] = [\langle -a, b\rangle]$.

For rational numbers, multiplication is simpler than addition. The informal calculation

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

indicates that $\cdot_Q$ should be defined by the equation

$$[\langle a, b\rangle] \cdot_Q [\langle c, d\rangle] = [\langle ac, bd\rangle].$$

(Notice the close analogy with $+_Z$.) This multiplication function is well defined, as the following lemma verifies.

Lemma 5QD If $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$, then

$$\langle ac, bd\rangle \sim \langle a'c', b'd'\rangle.$$

Proof The proof is exactly as in Lemma 5ZB, but with addition replaced by multiplication. ⊣

Example Recall that $1_Q = [\langle 1, 1\rangle]$. We can now check that 1_Q is a multiplicative identity element, i.e., that $r \cdot_Q 1_Q = r$. We know that $r = [\langle a, b\rangle]$ for some a and b. Thus

$$\begin{aligned} r \cdot_Q 1_Q &= [\langle a, b\rangle] \cdot_Q [\langle 1, 1\rangle] \\ &= [\langle a \cdot 1, b \cdot 1\rangle] \\ &= [\langle a, b\rangle] \\ &= r. \end{aligned}$$

You should also verify that $r \cdot_Q 0_Q = 0_Q$.

Theorem 5QE Multiplication of rationals is associative, commutative, and distributive over addition:

$$(p \cdot_Q q) \cdot_Q r = p \cdot_Q (q \cdot_Q r),$$

$$q \cdot_Q r = r \cdot_Q q,$$

$$p \cdot_Q (q +_Q r) = (p \cdot_Q q) +_Q (p \cdot_Q r).$$

Proof The verification of associativity and commutativity is directly analogous to verification of the same properties for $+_Z$.

We will proceed to prove the distributive law. We know that we can write $p = [\langle a, b\rangle]$, $q = [\langle c, d\rangle]$, and $r = [\langle e, f\rangle]$ for some integers a, b, c, d, e, and f. Then

$$\begin{aligned} p \cdot_Q (r +_Q s) &= [\langle a, b\rangle] \cdot_Q ([\langle c, d\rangle] +_Q [\langle e, f\rangle]) \\ &= [\langle a, b\rangle] \cdot_Q [\langle cf + ed, df\rangle] \\ &= [\langle acf + aed, bdf\rangle]. \end{aligned}$$

On the other side of the expected equation we have

$$\begin{aligned} (p \cdot_Q r) +_Q (p \cdot_Q s) &= ([\langle a, b\rangle] \cdot_Q [\langle c, d\rangle]) +_Q ([\langle a, b\rangle] \cdot_Q [\langle e, f\rangle]) \\ &= [\langle ac, bd\rangle] +_Q [\langle ae, bf\rangle] \\ &= [\langle acbf + aebd, bdbf\rangle]. \end{aligned}$$

This agrees with the first calculation because $\langle i, j\rangle \sim \langle bi, bj\rangle$. ⊣

The new property the rationals have (and that integers lack) is the existence of multiplicative inverses.

Theorem 5QF For every nonzero r in $\mathbb{Q}$ there is a nonzero q in $\mathbb{Q}$ such that $r \cdot_Q q = 1_Q$.

Proof The given r must be of the form $[\langle a, b\rangle]$, where $a \neq 0$, lest $r = 0_Q$. Let $q = [\langle b, a\rangle]$. Then $q \neq 0_Q$ and $r \cdot_Q q = [\langle ab, ab\rangle] = 1_Q$. ⊣

We can use the existence of multiplicative inverses to show that there are no zero divisors in $\mathbb{Q}$:

Corollary 5QG If r and s are nonzero rational numbers, then $r \cdot_Q s$ is also nonzero.

Proof The preceding theorem provides us with rationals r' and s' for which $r \cdot_Q r' = s \cdot_Q s' = 1_Q$. Hence

$$(r \cdot_Q s) \cdot_Q (r' \cdot_Q s') = 1_Q$$

by using commutative and associative laws. But this implies that $r \cdot_Q s \neq 0_Q$, because $0_Q \cdot_Q (r' \cdot_Q s') = 0_Q \neq 1_Q$. ⊣

We can restate this corollary by saying that the set of nonzero rational numbers is *closed* under multiplication; i.e., the product of numbers in this set is again in this set.

As a result of the foregoing theorems, we can assert that the nonzero rationals with *multiplication* form an Abelian group. That is, multiplication gives us a binary operation on the nonzero rationals that is associative and commutative, we have an identity element 1_Q, and we have multiplicative inverses. As in any Abelian group, the inverse of r is unique; we denote it as r^{-1}. The proof of Theorem 5QF shows that

$$[\langle a, b\rangle]^{-1} = [\langle b, a\rangle].$$

Inverses provide us with a division operation. For a nonzero rational r we can define

$$s \div r = s \cdot_Q r^{-1}.$$

Then we have

$$\begin{aligned}[\langle c, d\rangle] \div [\langle a, b\rangle] &= [\langle c, d\rangle] \cdot_Q [\langle b, a\rangle] \\ &= [\langle cb, da\rangle],\end{aligned}$$

a version of the "invert and multiply" rule for division of fractions.

The algebraic concept exemplified by the rational numbers is the concept of a *field*. To say that $\langle \mathbb{Q}, +_Q, \cdot_Q, 0_Q, 1_Q\rangle$ is a field means that it is an integral domain with the further property that multiplicative inverses exist. (Other examples of fields are provided by the real numbers and by the complex numbers.) The method we have used to extend from $\mathbb{Z}$ to $\mathbb{Q}$ can be applied to extend any integral domain to a field.

Next we want to define the ordering relation for the rational numbers. The informal calculation

$$\frac{a}{b} < \frac{c}{d} \quad \text{iff} \quad ad < cb$$

is correct if b and d are positive. There is no guarantee that denominators are always positive. But because

$$[\langle a, b\rangle] = [\langle -a, -b\rangle],$$

every rational number can be represented by some fraction with a positive denominator. (Recall that for nonzero b, either b or $-b$ is positive.) The above informal calculation then suggests that we define $<_Q$ so that

$$[\langle a, b\rangle] <_Q [\langle c, d\rangle] \quad \text{iff} \quad ad < cb$$

whenever b and d are positive. As with $<_Z$, we must verify that this condition yields a well-defined relation. The following lemma accomplishes the verification.

Lemma 5QH Assume that $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$. Further assume that b, b', d, and d' are all positive. Then

$$ad < cb \quad \text{iff} \quad a'd' < c'b'.$$

Proof The proof is the same as the proof of Lemma 5ZH, but with multiplication of integers in place of addition of natural numbers. ⊣

This lemma guarantees that when we test to see whether or not $r <_Q s$, it does not matter which fractions with positive denominators we choose from r and s.

Example To check that $0_Q <_Q 1_Q$, we choose fractions $\langle 0, 1\rangle \in 0_Q$ and $\langle 1, 1\rangle \in 1_Q$. Then since $0 \cdot 1 < 1 \cdot 1$, we do indeed have $0_Q <_Q 1_Q$. But we could also have chosen fractions $\langle 0, 4\rangle \in 0_Q$ and $\langle 3, 3\rangle \in 1_Q$. Then since $0 \cdot 3 < 3 \cdot 4$, we again find, in consistency with the first calculation, that $0_Q <_Q 1_Q$.

Theorem 5QI The relation $<_Q$ is a linear ordering on $\mathbb{Q}$.

Proof The proof is the same as the proof of Theorem 5ZI, with multiplication in place of addition. For example, to prove trichotomy, we consider rational numbers r and s. For suitable integers we can write

$$r = [\langle a, b\rangle] \qquad \text{and} \qquad s = [\langle c, d\rangle],$$

where b and d are positive. Then trichotomy for $\mathbb{Z}$ tells us that exactly one of

$$ad < cb, \qquad ad = cb, \qquad cb < ad$$

holds, whence exactly one of

$$r <_Q s, \qquad r = s, \qquad s <_Q r$$

holds. ⊣

One can check that $r <_Q 0_Q$ iff $0_Q <_Q -r$ (Exercise 12). Call q *positive* iff $0_Q <_Q q$. Then as a consequence of trichotomy, we have the fact for any rational number r, exactly one of the three alternatives

$$r \text{ is positive}, \qquad r \text{ is zero}, \qquad -r \text{ is positive}$$

holds. We can define the *absolute value* $|r|$ of r by

$$|r| = \begin{cases} -r & \text{if } -r \text{ is positive,} \\ r & \text{otherwise.} \end{cases}$$

Then $0_Q \leq_Q |r|$ for every r.

Next we prove that order is preserved by addition and by multiplication by a positive factor.

Theorem 5QJ Let r, s, and t be rational numbers.

(a) $r <_Q s$ iff $r +_Q t <_Q s +_Q t$.
(b) If t is positive, then

$$r <_Q s \quad \text{iff} \quad r \cdot_Q t <_Q s \cdot_Q t.$$

Proof Part (b) has the same proof as part (a) of Theorem 5ZJ, but with multiplication in place of addition. To prove part (a), we first write r, s, and t in the form

$$r = [\langle a, b\rangle], \qquad s = [\langle c, d\rangle], \qquad t = [\langle e, f\rangle],$$

where b, d, and f are positive. Since t is a positive rational, e is also a positive integer. Then

$$\begin{aligned} r +_Q t <_Q s +_Q t &\Leftrightarrow [\langle af + eb, bf\rangle] <_Q [\langle cf + ed, df\rangle] \\ &\Leftrightarrow (af + eb)df < (cf + ed)bf \\ &\Leftrightarrow adff + bdef < bcff + bdef \\ &\Leftrightarrow ad < bc \qquad \text{by Theorem 5ZJ} \\ &\Leftrightarrow r <_Q s \end{aligned}$$

as desired. ⊣

We have already said that the rational numbers form a field; the two preceding theorems state that $\langle \mathbb{Q}, +_Q, \cdot_Q, 0_Q, 1_Q, <_Q\rangle$ is an *ordered field*.

Theorem 5QK The following cancellation laws hold for any rational numbers.

(a) If $r +_Q t = s +_Q t$, then $r = s$.
(b) If $r \cdot_Q t = s \cdot_Q t$ and t is nonzero, then $r = s$.

Proof We can prove this as a corollary of the preceding theorem, following our past pattern. But there is now a simpler option open to us. In part (a) we add $-t$ to both sides of the given equation, and in part (b) we multiply both sides of the given equation by t^{-1}. (This proof works in any Abelian group.) ⊣

Finally, we want to show that, although $\mathbb{Z}$ is not a subset of $\mathbb{Q}$, nevertheless $\mathbb{Q}$ has a subset that is "just like" $\mathbb{Z}$. Define the embedding function $E: \mathbb{Z} \to \mathbb{Q}$ by

$$E(a) = [\langle a, 1\rangle].$$

This functions gives us an isomorphic embedding in the sense that the following theorem holds.

Theorem 5QL E is a one-to-one function from $\mathbb{Z}$ into $\mathbb{Q}$ satisfying the following conditions:

(a) $E(a + b) = E(a) +_Q E(b)$.
(b) $E(ab) = E(a) \cdot_Q E(b)$.
(c) $E(0) = 0_Q$ and $E(1) = 1_Q$.
(d) $a < b$ iff $E(a) <_Q E(b)$.

Proof Each part of the theorem can be proved by direct calculation. First we check that E is one-to-one:

$$\begin{aligned} E(a) = E(b) &\Rightarrow [\langle a, 1\rangle] = [\langle b, 1\rangle] \\ &\Rightarrow \langle a, 1\rangle \sim \langle b, 1\rangle \\ &\Rightarrow a = b. \end{aligned}$$

Parts (a), (b), and (d) are proved by the following calculations:

$$\begin{aligned} E(a) +_Q E(b) &= [\langle a, 1\rangle] +_Q [\langle b, 1\rangle] \\ &= [\langle a + b, 1\rangle] \\ &= E(a + b), \\ E(a) \cdot_Q E(b) &= [\langle a, 1\rangle] \cdot_Q [\langle b, 1\rangle] \\ &= [\langle ab, 1\rangle] \\ &= E(ab), \end{aligned}$$

$$\begin{aligned} E(a) <_Q E(b) &\Leftrightarrow [\langle a, 1\rangle] <_Q [\langle b, 1\rangle] \\ &\Leftrightarrow a \cdot 1 < b \cdot 1 \\ &\Leftrightarrow a < b. \end{aligned}$$

Finally part (c) is a restatement of the definitions of 0_Q and 1_Q. ⊣

We also obtain the following relation between fractions and division:

$$[\langle a, b\rangle] = E(a) \div E(b).$$

Since $b \neq 0$, we have $E(b) \neq 0_Q$, and so the indicated division is possible.

Henceforth we will simplify the notation by omitting the subscript "Q" on $+_Q$, $\cdot_Q$, 0_Q, and so forth. Also the product $r \cdot s$ will usually be written as just rs.

Exercises

10. Show that $r \cdot_Q 0_Q = 0_Q$ for every rational number r.

11. Give a direct proof (not using Theorem 5QF) that if $r \cdot_Q s = 0_Q$, then either $r = 0_Q$ or $s = 0_Q$.

12. Show that

$$r <_Q 0_Q \quad \text{iff} \quad 0_Q <_Q -r.$$

13. Give a new proof of the cancellation law for $+_Z$ (Corollary 5ZK(a)), using Theorem 5ZD instead of Theorem 5ZJ.

14. Show that the ordering of rationals is dense, i.e., between any two rationals there is a third one:

$$p <_Q s \quad \Rightarrow \quad (\exists r)(p <_Q r <_Q s).$$

REAL NUMBERS

The last number system that we will consider involves the set $\mathbb{R}$ of all real numbers. The ancient Pythagoreans discovered, to their dismay, that there was a *need* to go beyond the rational numbers. They found that there simply was no rational number to measure the length of the hypotenuse of a right triangle whose other two sides had unit length.

In our previous extensions of number systems, we relied on the facts that an integer could be named by a pair of natural numbers, and a rational number could be named by a pair of integers. But we *cannot* hope to name real number by a pair of rationals, because, as we will prove in Chapter 6, there are too many real numbers and not enough pairs of rationals. Hence we must look at new techniques in searching for a way to name real numbers.

Actually there are several methods that can be used successfully to construct the real numbers. One approach is to utilize decimal expansions, so that a real number is determined by an integer and an infinite sequence of digits (a function from ω into 10). This approach may be found in Claude Burrill's book, *Foundations of Real Numbers*, McGraw-Hill, 1967.

A more common method of constructing a suitable set $\mathbb{R}$ is to utilize the fact that a real number can be named by giving a sequence of rationals (a function from ω into $\mathbb{Q}$) converging to it. So one can take the set of all convergent sequences and then divide out by an equivalence relation (where two sequences are equivalent iff they converge to the same limit). But there is one hitch: The concepts of "convergent" and "equivalent" must be defined without reference to the real number to which the sequence is converging. This can be done by a technique named after Cauchy.

Define a *Cauchy sequence* to be a function s: $\omega \to \mathbb{Q}$ such that $|s_m - s_n|$ is arbitrarily small for all sufficiently large m and n; i.e.,

$$(\forall \text{ positive } \varepsilon \text{ in } \mathbb{Q})(\exists k \in \omega)(\forall m > k)(\forall n > k)\ |s_m - s_n| < \varepsilon.$$

(Here we write s_n in place of $s(n)$, as usual for ω-sequences.) The concept of a Cauchy sequence is useful here because of the theorem of calculus asserting that a sequence is convergent iff it is a Cauchy sequence.

Let C be the set of all Cauchy sequences. For r and s in C, we define r and s to be *equivalent* ($r \sim s$) iff $|r_n - s_n|$ is arbitrarily small for all sufficiently large n; i.e.,

$$(\forall \text{ positive } \varepsilon \text{ in } \mathbb{Q})(\exists k \in \omega)(\forall n > k)\ |r_n - s_n| < \varepsilon.$$

Then the quotient set $C/\sim$ is a suitable candidate for $\mathbb{R}$. (This approach to constructing $\mathbb{R}$ is due to Cantor.)

An alternative construction of $\mathbb{R}$ uses so-called *Dedekind cuts*. This is the method we follow henceforth in this section. The Cauchy sequence construction and the Dedekind cut construction each have their own advantages. The Dedekind cut construction of $\mathbb{R}$ has an initial advantage of simplicity, in that it provides a simple definition of $\mathbb{R}$ and its ordering. But multiplication of Dedekind cuts is awkward, and verification of the properties of multiplication is a tedious business. The Cauchy sequence construction of $\mathbb{R}$ also has the advantage of generality, since it can be used with an arbitrary metric space in place of $\mathbb{Q}$.

With these considerations in mind, we choose the following strategy. We will present the Dedekind cut construction, and will prove that least upper bounds exist in $\mathbb{R}$. (This is the property that distinguishes $\mathbb{R}$ from the other ordered fields.) Although we will define addition and multiplication of real numbers, we will not give complete verification of the algebraic properties. The Cauchy sequence construction may be found, among other

places, in Norman Hamilton and Joseph Landin's book, *Set Theory and the Structure of Arithmetic*, Allyn and Bacon, 1961.

The idea behind Dedekind cuts is that a real number x can be named by giving an infinite set of rationals, namely all the rationals less than x. We will in effect define x to be the set of all rationals smaller than x. To avoid circularity in the definition, we must be able to characterize the sets of rationals obtainable in this way. The following definition does the job.

Definition A *Dedekind cut* is a subset x of $\mathbb{Q}$ such that:

(a) $\varnothing \neq x \neq \mathbb{Q}$.

(b) x is "closed downward," i.e.,

$$q \in x \,\&\, r < q \;\Rightarrow\; r \in x.$$

(c) x has no largest member.

We then define the set $\mathbb{R}$ of real numbers to be the set of all Dedekind cuts. Note that there is no equivalence relation here; a real (i.e., a real number) is a cut, not an equivalence class of cuts.

The ordering on $\mathbb{R}$ is particularly simple. For x and y in $\mathbb{R}$, define

$$x <_R y \quad \text{iff} \quad x \subset y.$$

In other words, $<_R$ is the relation of being a proper subset:

$$<_R = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid x \subset y\}.$$

Theorem 5RA The relation $<_R$ is a linear ordering on $\mathbb{R}$.

Proof The relation is clearly transitive; we must show that it satisfies trichotomy on $\mathbb{R}$. So consider any x and y in $\mathbb{R}$. Obviously *at most* one of the alternatives,

$$x \subset y, \qquad x = y, \qquad y \subset x,$$

can hold, but we must prove that at least one holds. Suppose that the first two fail, i.e., that $x \not\subseteq y$. We must prove that $y \subset x$.

Since $x \not\subseteq y$ there is some rational r in the relative complement $x - y$ (see Fig. 23). Consider any $q \in y$. If $r \leq q$, then since y is closed downward,

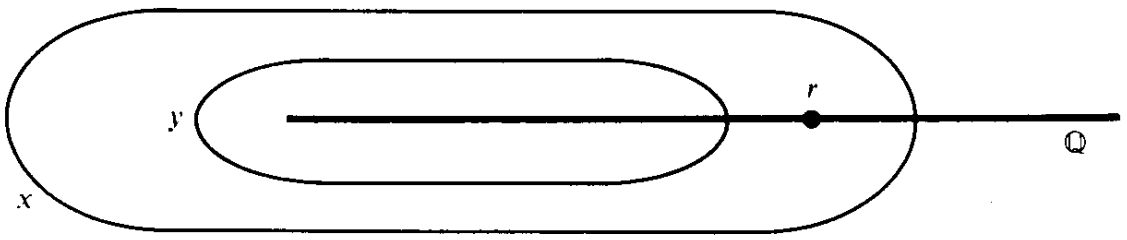

Fig. 23. The proof of Theorem 5RA.

we would have $r \in y$. But $r \notin y$, so we must have $q < r$. Since x is closed downward, it follows that $q \in x$. Since q was arbitrary (and $x \neq y$), we have $y \subset x$. ⊣

Now consider a set A of reals; a real number x is said to be an *upper bound* of A iff $y \leq_R x$ for every y in A. The number x itself might or might not belong to A. The set A is *bounded* (i.e., *bounded above*) iff there exists some upper bound of A. A *least upper bound* of A is an upper bound that is less than any other upper bound.

First consider an example not in $\mathbb{R}$, but in $\mathbb{Q}$. The set

$$\{r \in \mathbb{Q} \mid r \cdot r < 2\}$$

of rationals whose square is less than 2 is a bounded set of rationals that has no least upper bound in $\mathbb{Q}$. (We are stating this, not proving it, but it follows from the fact that $\sqrt{2}$ is irrational.) The following theorem shows that examples of this sort cannot be found in $\mathbb{R}$.

Theorem 5RB Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$.

Proof Let A be the set of real numbers in question. We will show that the least upper bound is just $\bigcup A$.

Simply by the definition of $\bigcup A$, we have $x \subseteq \bigcup A$ for all $x \in A$. Furthermore let z be any upper bound for A, so that $x \subseteq z$ for all $x \in A$. It then follows that $\bigcup A \subseteq z$; compare Exercise 5 of Chapter 2. The argument so far is not tied to $\mathbb{R}$; we have only shown that $\bigcup A$ is the least upper bound of the set A with respect to ordering by inclusion.

What remains to be shown is that $\bigcup A \in \mathbb{R}$. Because A is nonempty, it is easy to see that $\bigcup A \neq \varnothing$. Also $\bigcup A \neq \mathbb{Q}$ because $\bigcup A \subseteq z$ where z is an upper bound for A. You can easily verify (Exercise 15) that $\bigcup A$ is closed downward and has no largest element. ⊣

The foregoing theorem is important in mathematical analysis. For example, it is needed in order to prove that a continuous function on a closed interval assumes a maximum. And this in turn is used to prove the mean value theorem of calculus.

The addition operation for $\mathbb{R}$ is easily defined from addition of rationals. For reals x and y, define:

$$x +_R y = \{q + r \mid q \in x \;\&\; r \in y\}.$$

Lemma 5RC For real numbers x and y, the sum $x +_R y$ is also in $\mathbb{R}$.

Proof Clearly $x +_R y$ is a nonempty subset of $\mathbb{Q}$. To show that $x +_R y \neq \mathbb{Q}$, choose some q' in $\mathbb{Q} - x$ and r' in $\mathbb{Q} - y$. Then

$$\begin{aligned} q \in x \,\&\, r \in y &\Rightarrow q < q' \,\&\, r < r' \\ &\Rightarrow q + r < q' + r' \end{aligned}$$

so that any member $q + r$ of $x +_R y$ is strictly less than $q' + r'$. Hence $q' + r' \notin x +_R y$.

To show that $x +_R y$ is closed downward, consider any

$$p < q + r \in x +_R y$$

(where $q \in x$ and $r \in y$). Then adding $-q$ to both sides of the inequality, we have $p - q < r$. Since y is closed downward, we have $p - q \in y$. Thus we can write p as the sum

$$p = q + (p - q)$$

of q from x and $p - q$ from y; this is what we need to have $p \in x +_R y$. (*Note*: Here "$p - q$" refers to subtraction of rationals, $p + (-q)$. Earlier in this proof "$\mathbb{Q} - x$" referred to the relative complement of x in $\mathbb{Q}$. If this sort of thing happened often, we would use a different symbol "$\mathbb{Q} \setminus x$" for complements. But in fact the opportunities for confusion will be rare.)

We leave it to you to verify that $x +_R y$ has no largest member (Exercise 16). ⊣

Theorem 5RD Addition of real numbers is associative and commutative:

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

Proof Since addition of rationals is commutative, it is clear from the definition of $+_R$ that it is commutative as well. As for associativity, we have

$$\begin{aligned} (x +_R y) +_R z &= \{s + r \mid s \in x +_R y \,\&\, r \in z\} \\ &= \{(p + q) + r \mid p \in x \,\&\, q \in y \,\&\, r \in z\}, \end{aligned}$$

and a similar calculation applies to the other grouping. Thus associativity of $+_R$ follows from associativity of addition of rationals. ⊣

The zero element of $\mathbb{R}$ is defined to be the set of negative rational numbers:

$$0_R = \{r \in \mathbb{Q} \mid r < 0\}.$$

Theorem 5RE (a) 0_R is a real number.
(b) For any x in $\mathbb{R}$, we have $x +_R 0_R = x$.

Proof (a) It is easy to see that $\varnothing \neq 0_R \neq \mathbb{Q}$; for example, $-1 \in 0_R$ and $1 \notin 0_R$. And it is clear that 0_R is closed downward. The fact that 0_R has no largest member follows immediately from the density of the rationals (Exercise 14).

For part (b), we must prove that

$$\{r + s \mid r \in x \ \& \ s < 0\} = x.$$

The "$\subseteq$" inclusion holds because x is closed downward. To prove the "$\supseteq$" half, consider any p in x. Since x has no largest member, there is some r with $p < r \in x$. Let $s = p - r$. Then $s < 0$ and $p = r + s \in 0_R$. Hence both inclusions hold. ⊣

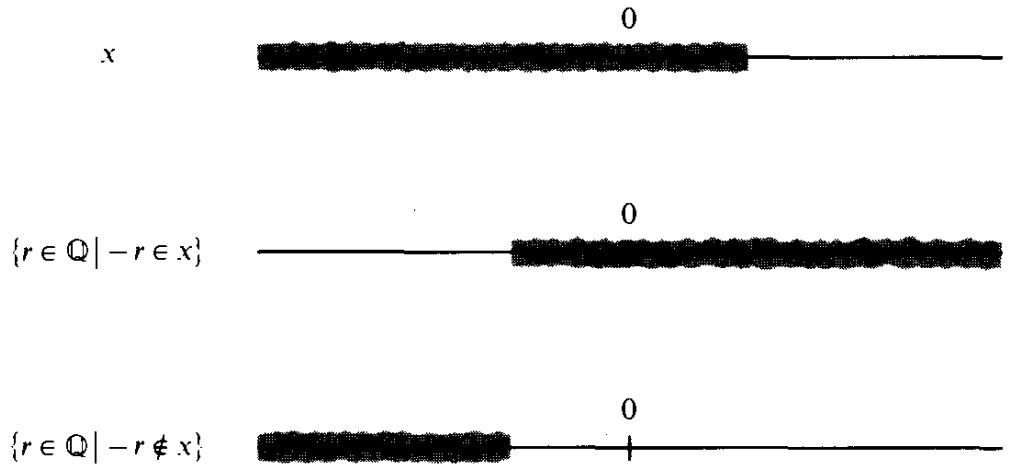

Fig. 24. Sometimes $-x$ is $\{r \in \mathbb{Q} \mid -r \notin x\}$, but not always.

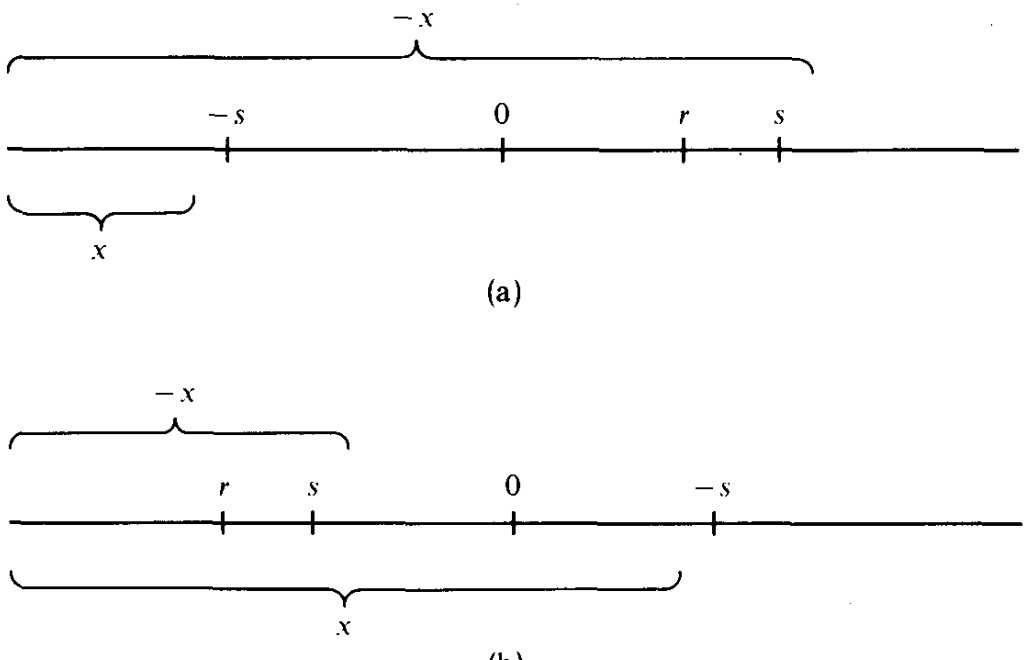

Fig. 25. In (a) x is negative; in (b) x is positive.

Before we can conclude that the real numbers form an Abelian group with $+_R$ and 0_R, we must prove that additive inverses exist. First we need to say just what set $-x$ should be (where $x \in \mathbb{R}$). We think of the real number $-x$ as the set of all smaller rational numbers. If we draw a picture as in Fig. 24, we might be tempted to think that $-x$ is the complement of $\{r \in \mathbb{Q} \mid -r \in x\}$, or in other words, that $-x$ should be $\{r \in \mathbb{Q} \mid -r \notin x\}$. This choice is not quite right, because it may have a largest element. Instead we define

$$-x = \{r \in \mathbb{Q} \mid (\exists s > r) -s \notin x\}.$$

In Fig. 25, $-x$ is illustrated as a subset of the rational number line.

Theorem 5RF For every x in $\mathbb{R}$:

(a) $-x \in \mathbb{R}$,
(b) $x +_R (-x) = 0_R$.

Proof To prove that $-x$ is a real number, we first must show that $\varnothing \neq -x \neq \mathbb{Q}$. There is some rational t with $t \notin x$; let $r = -t - 1$. Then $r \in -x$ because $r < -t$ and $-(-t) \notin x$. Hence $-x \neq \varnothing$. To show that $-x \neq \mathbb{Q}$, take any $p \in x$. We claim that $-p \notin -x$. This holds because if $s > -p$, then $-s < p \in x$, whence $-s \in x$. Hence $-p \notin -x$ and so $-x \neq \mathbb{Q}$.

It is easier to show that $-x$ is closed downward. Suppose that $q < r \in -x$. Then $(\exists s > r) -s \notin x$. Consequently $(\exists s > q) -s \notin x$, since the same s can be used. Hence $q \in -x$.

It remains to show that $-x$ has no largest element. Consider then any element r in $-x$. We know that for some $s > r$ we have $-s \notin x$. Because the rationals are densely ordered (Exercise 14), there is some p with $s > p > r$. Then $p \in -x$, and p is larger than r. This completes the proof that $-x$ is a real number.

Now we turn to part (b). By definition

$$x +_R (-x) = \{q + r \mid q \in x \;\&\; (\exists s > r) -s \notin x\}.$$

For any such member $q + r$ of this set, we have $r < s$ and $q < -s$ (lest $-s \leq q \in x$). Hence by the order-preserving property of addition,

$$q + r < (-s) + s = 0.$$

This shows that $x +_R (-x) \subseteq 0_R$.

To establish the other inclusion, consider any p in 0_R. Then $p < 0$, and so $-p$ is positive. By Exercise 19, there is some $q \in x$ for which $q + (-p \div 2) \notin x$. Let $s = (p \div 2) - q$, so that $-s \notin x$. Then p is the sum of q (which is in x) and $p - q$ (which is less than s, where $-s \notin x$). This makes p a member of $x +_R (-x)$. Thus we have both inclusions. ⊣

We have now shown that $\langle \mathbb{R}, +_R, 0_R \rangle$ is an Abelian group. As in any Abelian group, the cancellation law holds:

Corollary 5RG For any real numbers,

$$x +_R z = y +_R z \quad \Rightarrow \quad x = y.$$

Proof Simply add $-z$ to both sides of the given equation. ⊣

Next we prove that addition preserves order.

Theorem 5RH For any real numbers,

$$x <_R y \quad \Leftrightarrow \quad x +_R z <_R y +_R z.$$

Proof It is easy to prove that

(1) $$x \leq_R y \quad \Rightarrow \quad x +_R z \leq_R y +_R z,$$

because this amounts to the statement that if $x \subseteq y$, then

$$\{q + s \mid q \in x \ \& \ s \in z\} \subseteq \{r + s \mid r \in y \ \& \ s \in z\},$$

which is obvious. And by Corollary 5RG we have

(2) $$x \neq y \quad \Rightarrow \quad x +_R z \neq y +_R z,$$

which together with (1) gives the "$\Rightarrow$" half of the theorem. The "$\Leftarrow$" half then follows by trichotomy (as in the proof to Theorem 4N). ⊣

We can define the absolute value $|x|$ of a real number x to be the larger of x and $-x$. Since our ordering is inclusion, the larger of the two is just their union. Thus our definition becomes

$$|x| = x \cup -x.$$

Then by Exercise 20, $|x|$ is always nonnegative, i.e., $0_R \leq_R |x|$.

Consider now the definition of multiplication. For the product of x and y we cannot use $\{rs \mid r \in x \ \& \ s \in y\}$ (in analogy to the definition of $x +_R y$), because both x and y contain negative rationals of large magnitude. Instead we use the following variation on the above idea.

Definition (a) If x and y are nonnegative real numbers, then

$$x \cdot_R y = 0_R \cup \{rs \mid 0 \leq r \in x \ \& \ 0 \leq s \in y\}.$$

(b) If x and y are both negative real numbers, then

$$x \cdot_R y = |x| \cdot_R |y|.$$

(c) If one of the real numbers x and y is negative and one is nonnegative, then

$$x \cdot_R y = -(|x| \cdot_R |y|).$$

The facts we want to know about multiplication are gathered into the following theorem. Let $1_R = \{r \in \mathbb{Q} \mid r < 1\}$. Clearly $0_R <_R 1_R$. We will not give a proof for this theorem; a proof can be found in Appendix F of *Number Systems and the Foundations of Analysis* by Elliott Mendelson (Academic Press, 1973).

Theorem 5RI For any real numbers, the following hold:

(a) $x \cdot_R y$ is a real number.
(b) Multiplication is associative, commutative, and distributive over addition.
(c) $0_R \neq 1_R$ and $x \cdot_R 1_R = x$.
(d) For nonzero x there is a nonzero real number y with $x \cdot_R y = 1_R$.
(e) Multiplication by a positive number preserves order: If $0_R <_R z$, then

$$x <_R y \quad \Leftrightarrow \quad x \cdot_R z <_R y \cdot_R z.$$

The foregoing theorems show that, like the rationals, the reals (with $+_R$, $\cdot_R$, 0_R, 1_R, and $<_R$) form an ordered field. But unlike the rationals, the reals have the least-upper-bound property (Theorem 5RB). An ordered field is said to be *complete* iff it has the least-upper-bound property. It can be shown that the reals, in a sense, yield the *only* complete ordered field. That is, any other complete ordered field is "just like" (or more precisely, is isomorphic to) the ordered field of real numbers. For an exact statement of this theorem and for its proof, see any of the books we have referred to in this section, or p. 110 of Andrew Gleason's book, *Fundamentals of Abstract Analysis*, Addison-Wesley, 1966.

The correct embedding function E from $\mathbb{Q}$ into $\mathbb{R}$ assigns to each rational number r the corresponding real number

$$E(r) = \{q \in \mathbb{Q} \mid q < r\},$$

consisting of all smaller rationals.

Theorem 5RJ E is a one-to-one function from $\mathbb{Q}$ into $\mathbb{R}$ satisfying the following conditions:

(a) $E(r + s) = E(r) +_R E(s)$.
(b) $E(rs) = E(r) \cdot_R E(s)$.
(c) $E(0) = 0_R$ and $E(1) = 1_R$.
(d) $r < s$ iff $E(r) <_R E(s)$.

Proof First of all, we must show that $E(r)$ is a real number. Obviously $E(r)$ is a set of rationals, and it is closed downward. Furthermore $\varnothing \neq E(r) \neq \mathbb{Q}$ because $r - 1 \in E(r)$ and $r \notin E(r)$. $E(r)$ has no largest element, because if $q \in E(r)$, then by Exercise 14 there is a larger element p with $q < p < r$. Hence $E(r)$ is indeed a real number.

To show that E is one-to-one, suppose that $r \neq s$. Then one is less than the other; we may suppose that $r < s$. Then $r \in E(s)$ whereas $s \notin E(s)$. Hence $E(r) \neq E(s)$.

Next let us prove part (d), because it is easy. If $r < s$, then clearly $E(r) \subseteq E(s)$. The inclusion is proper since E is one-to-one. Thus

$$r < s \quad \Rightarrow \quad E(r) \subset E(s).$$

The converse follows from trichotomy. If $E(r) \subset E(s)$, then we cannot have $r = s$ nor $s < r$ (lest $E(s) \subset E(r)$), so we must have $r < s$.

For part (a), we have

$$\begin{aligned} E(r) +_R E(s) &= \{p + q \mid p \in E(r) \ \& \ q \in E(s)\} \\ &= \{p + q \mid p < r \ \& \ q < s\}. \end{aligned}$$

We must show that this is the same as $E(r + s)$, i.e., that

$$\{p + q \mid p < r \ \& \ q < s\} = \{t \mid t < r + s\}.$$

The "$\subseteq$" inclusion holds because by Theorem 5QJ,

$$p + q < r + q < r + s.$$

To establish the "$\supseteq$" inclusion, suppose that $t < r + s$. Let $\varepsilon = (r + s - t) \div 2$; then $\varepsilon > 0$. Define $p = r - \varepsilon$ and $q = s - \varepsilon$. Then $p < r$ and $q < s$ and $p + q = t$. Thus we can represent t as a sum in the desired form. Hence both inclusions hold.

Finally, we omit the (awkward) proof of part (b), and part (c) is only a restatement of definitions. ⊣

Exercises

15. In Theorem 5RB, show that $\bigcup A$ is closed downward and has no largest element.

16. In Lemma 5RC, show that $x +_R y$ has no largest element.

17. Assume that a is a positive integer. Show that for any integer b there is some k in ω with

$$b < a \cdot E(k).$$

18. Assume that p is a positive rational number. Show that for any rational number r there is some k in ω with

$$r < p \cdot E(E(k)).$$

(Here k is in ω, $E(k)$ is the corresponding integer, and $E(E(k))$ is the corresponding rational.)

19. Assume that p is a positive rational number. Show that for any real number x there is some rational q in x such that

$$p + q \notin x.$$

20. Show that for any real number x, we have $0_R \leq_R |x|$.

21. Show that if $x <_R y$, then there is a rational number r with

$$x <_R E(r) <_R y.$$

22. Assume that $x \in \mathbb{R}$. How do we know that $|x| \in \mathbb{R}$?

SUMMARIES

In this chapter we have given one way of constructing the real numbers as particular sets. Along the way, some concepts from abstract algebra have naturally arisen. For convenient reference, we have collected in the present section certain definitions that have played a key role in this chapter.

Integers Let m, n, p, and q be natural numbers.

$$\begin{aligned}
[\langle m, n\rangle] \sim [\langle p, q\rangle] &\Leftrightarrow m + q = p + n,\\
[\langle m, n\rangle] +_Z [\langle p, q\rangle] &= [\langle m + p, n + q\rangle],\\
-[\langle m, n\rangle] &= [\langle n, m\rangle],\\
[\langle m, n\rangle] \cdot_Z [\langle p, q\rangle] &= [\langle mp + nq, mp + np\rangle],\\
[\langle m, n\rangle] <_Z [\langle p, q\rangle] &\Leftrightarrow m + q \in p + n,\\
E(n) &= [\langle n, 0\rangle].
\end{aligned}$$

Rational numbers Let a, b, c, and d be integers with $bd \neq 0$.

$$\begin{aligned}
\langle a, b\rangle \sim \langle c, d\rangle &\Leftrightarrow ad = cb,\\
[\langle a, b\rangle] +_Q [\langle c, d\rangle] &= [\langle ad + cb, bd\rangle],\\
-[\langle a, b\rangle] &= [\langle -a, b\rangle],\\
[\langle a, b\rangle] \cdot_Q [\langle c, d\rangle] &= [\langle ac, bd\rangle],\\
[\langle a, b\rangle] <_Q [\langle c, d\rangle] &\Leftrightarrow ad < cb, \quad \text{when } b \text{ and } d \text{ are positive},\\
E(a) &= [\langle a, 1\rangle].
\end{aligned}$$

Real numbers. A real number is a set x such that $\varnothing \subset x \subset \mathbb{Q}$, x is closed downward, and x has no largest member.

$$\begin{aligned}
x <_R y &\Leftrightarrow x \subset y,\\
x +_R y &= \{q + r \mid q \in x \,\&\, r \in y\},\\
-x &= \{r \in \mathbb{Q} \mid (\exists s > r)\, -s \notin x\},\\
|x| &= x \cup -x,\\
|x| \cdot_R |y| &= 0_R \cup \{rs \mid 0 \leq r \in |x| \,\&\, 0 \leq s \in |y|\},\\
E(r) &= \{q \in \mathbb{Q} \mid q < r\}.
\end{aligned}$$

Next we turn to the definitions from abstract algebra that are relevant to the number systems in this chapter.

An *Abelian group* (in additive notation) is a triple[2] $\langle A, +, 0\rangle$ consisting of a set A, a binary operation $+$ on A, and an element ("zero") of A, such that the following conditions are met:

1. $+$ is associative and commutative.
2. 0 is an identity element, i.e., $x + 0 = x$.
3. Inverses exist, i.e., $\forall x\, \exists y\, x + y = 0$.

An Abelian group (in multiplicative notation) is a triple $\langle A, \cdot, 1\rangle$ consisting of a set A, a binary operation $\cdot$ on A, and an element 1 of A, such that the following conditions are met:

1. $\cdot$ is associative and commutative.
2. 1 is an identity element, i.e., $x \cdot 1 = x$.
3. Inverses exist, i.e., $\forall x\, \exists y\, x \cdot y = 1$.

This is, of course, the same as the preceding definition.

A *group* has the same definition, except that we do not require that the binary operation be commutative. All of the groups that we have considered have, in fact, been Abelian groups. But some of our results (e.g., the uniqueness of inverses) are correct in any group, Abelian or not.

A *commutative ring with identity* is a quintuple $\langle D, +, \cdot, 0, 1\rangle$ consisting of a set D, binary operations $+$ and $\cdot$ on D, and distinguished elements 0 and 1 of D, such that the following conditions are met:

1. $\langle D, +, 0\rangle$ is an Abelian group.
2. The operation $\cdot$ is associative and commutative, and is distributive over addition.
3. 1 is a multiplicative identity ($x \cdot 1 = x$) and $0 \neq 1$.

An *integral domain* is a commutative ring with identity with the additional property that there are no zero divisors:

4. If $x \neq 0$ and $y \neq 0$, then also $x \cdot y \neq 0$.

A *field* is a commutative ring with identity in which multiplicative inverses exist:

4′. If x is a nonzero element of D, then $x \cdot y = 1$ for some y.

Any field is also an integral domain, because condition 4′ implies condition 4 (see the proof to Corollary 5QG).

[2] It is also possible to define a group to be a pair $\langle A, +\rangle$, since the zero element turns out to be uniquely determined. We have formulated these definitions to match the exposition in this chapter.

An *ordered field* is a sextuple $\langle D, +, \cdot, 0, 1, < \rangle$ such that the following conditions are met:

1. $\langle D, +, \cdot, 0, 1 \rangle$ is a field.
2. $<$ is a linear ordering on D.
3. Order is preserved by addition and by multiplication by a positive element:

$$x < y \Leftrightarrow x + z < y + z.$$

If $0 < z$, then

$$x < y \Leftrightarrow x \cdot z < y \cdot z.$$

We can define *ordered integral domain* or even *ordered commutative ring with identity* by adjusting the first condition. A *complete ordered field* is an ordered field in which for every bounded nonempty subset of D there is a least upper bound.

The constructions in this chapter can be viewed as providing an existence proof for such fields. The conditions for a complete ordered field are not impossible to meet, for we have constructed a field meeting them.

TWO

What is a two? What are numbers? These are awkward questions; yet when we discuss numbers one might naively expect us to know what it is we are talking about.

In the Real World, we do not encounter (directly) abstract objects such as numbers. Instead we find physical objects: a number of similar apples, a ruler, partially filled containers (Fig. 26).

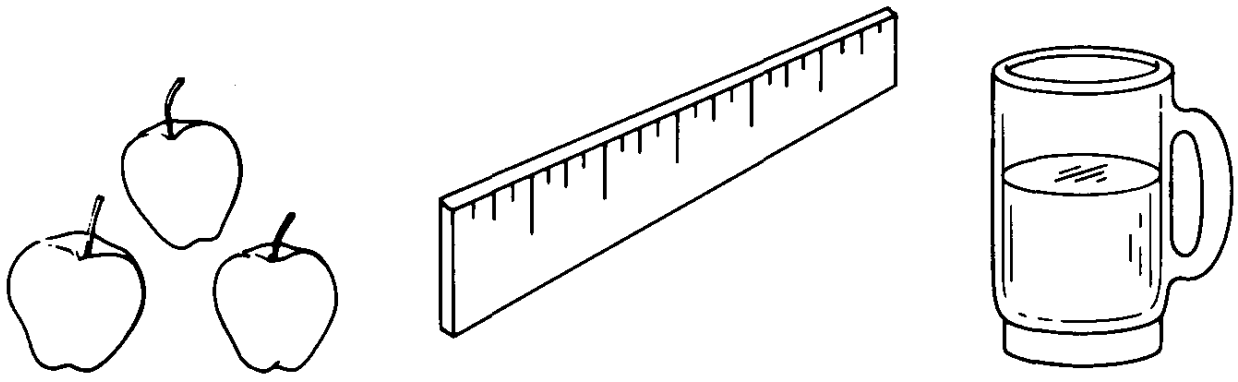

Fig. 26. A picture of the Real World.

Somehow we manage to abstract from this physical environment the concept of numbers. Not in any precise sense, of course, but we feel inwardly that we know what numbers are, or at least some numbers like 2 and 3. And we have various mental images that we use when thinking about numbers (Fig. 27).

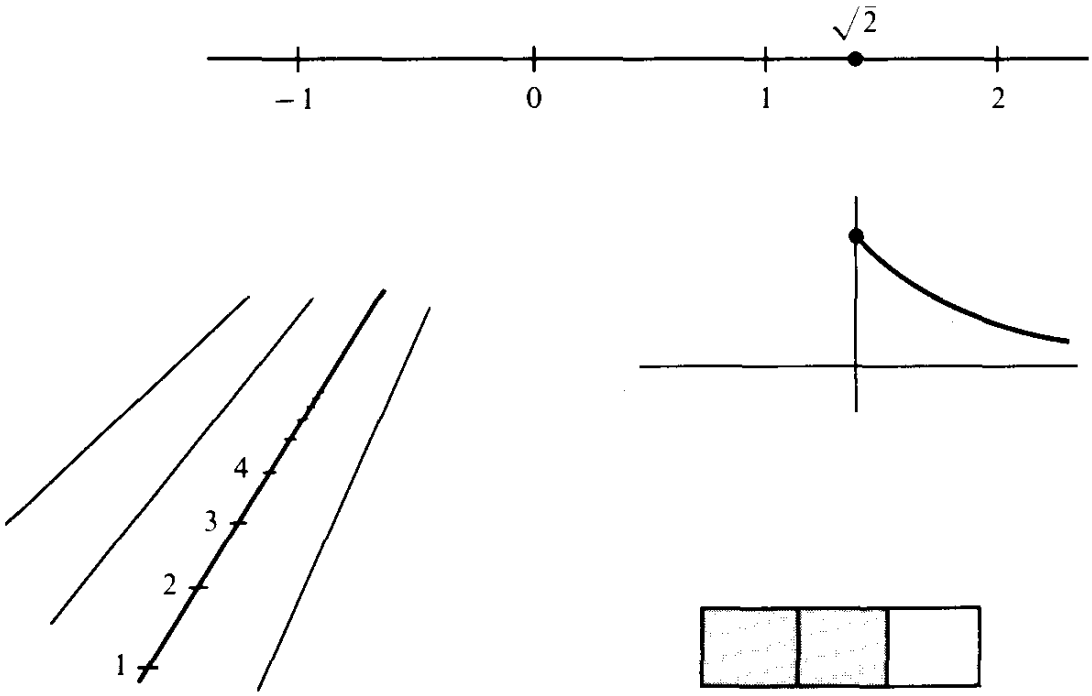

Fig. 27. Pictures of mental images.

Then at some point we acquire a mathematical education. This teaches us many formal manipulations of symbols (Fig. 28). It all seems fairly reasonable, but it can all be done without paying very much attention to what the symbols stand for. In fact computers can be programmed to carry out the manipulations without any understanding at all.

Since numbers are abstract objects (as contrasted with physical objects) it might be helpful to consider first other abstractions. Take honesty, for example. Honesty is a *property* possessed by those people whose utterances are true sentences, who do not fudge on their income tax, and so forth. By way of imitation, we can try characterizing two as the property that is true of exactly those sets that, for some distinct x and y, have as members x and y and nothing else. A slight variation on this proposal would be to eliminate sets and characterize two as the property that is true of exactly those properties that, for some distinct x and y, are true of x and y and nothing else. (This proposal is due to Frege.)

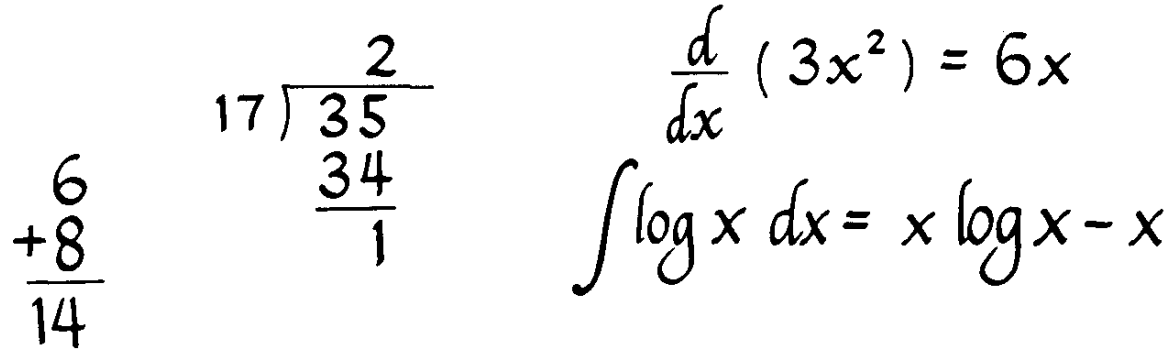

Fig. 28. Pictures of manipulated symbols.

If we define numbers in terms of properties, someone might ask us what a property is. And no matter how we define numbers, the procedure of defining one concept in terms of another cannot go on forever, producing an infinite regress of definitions. Eventually the procedure must be founded on a commonly agreed upon basis. Properties might form such a basis. For a mathematician, sets form a more workable basis.

Actually there is a close connection between properties and sets. Define the *extension* of a property to be the set of all objects of which that property is true. If a couple of properties have the same extension (i.e., if they are true of exactly the same objects), are they in fact one and the same property? Is the property of being a prime number less than 10 the same as the property of being a solution to

$$x^4 - 17x^3 + 101x^2 - 247x + 210 = 0?$$

If you answer "yes," then one says that you are thinking of properties *extensionally*, whereas if you answer "no," then you are thinking of properties *intensionally*. Both alternatives are legitimate, as long as the choice of alternatives is made clear. Either way, sets are the extensions of properties. (All sets are obtainable in this way; the set x is the extension of the property of belonging to x.)

We can recast Frege's proposal in terms of sets as follows: Two is the set having as members exactly those sets that, for some distinct x and y, have as members x and y and nothing else. But in Zermelo–Fraenkel set theory, there is no such set. (For the number one, you should check Exercise 8 of Chapter 2.) Our response to this predicament was to select artificially one particular set $\{\varnothing, \{\varnothing\}\}$ as a paradigm. Now $\{\varnothing, \{\varnothing\}\}$ is very different from the property that is true of exactly those sets that, for some distinct x and y, have as members x and y and nothing else, but it serves as an adequate substitute. Then rapidly one thing led to another, until we had the complete ordered field of real numbers. And as we have mentioned, one complete ordered field is very much like any other.

But let us back up a little. In mathematics there are two ways to introduce new objects:

(i) The new objects might be defined in terms of other already known objects.

(ii) The new objects can be introduced as primitive notions and axioms can be adopted to describe the notions. (This is not so much a way of answering foundational questions about the objects as it is a way of circumventing them.)

In constructing real numbers as certain sets we have selected the first path. The axiomatic approach would regard the definition of a complete

ordered field as *axioms* concerning the real number system (as a primitive notion). On the other hand, for sets themselves we have followed (with stripes) the axiomatic method.

But what about the Real World and those mental images? And the manipulated symbols? We want not just any old concept of number, but a concept that accurately reflects our experiences with apples and rulers and containers, and accurately mirrors our mental images. This is not a precise criterion, since it demands that a precise mathematical concept be compared with informal and intuitive ideas. And consequently the question whether our concept is indeed accurate must be evaluated on informal grounds. Throughout this chapter our formulation of definitions has been motivated ultimately by our intuitive ideas. Is there any way we could have gone wrong?

Yes, we could have gone wrong. In seeking a number system applicable to problems dealing with physical objects and physical space, we might have been guided by erroneous ideas. There is always the possibility that lines in the Real World do not really resemble $\mathbb{R}$. For example, over very short distances, space might be somehow quantized instead of being continuous. (Experimental evidence forced us to accept the fact that matter is quantized; experimental evidence has not *yet* forced us to accept similar ideas about space.) Or over very large distances, space might not be Euclidean (a possibility familiar to science-fiction buffs). In such events, mathematical theorems about $\mathbb{R}$, while still true of $\mathbb{R}$, would be less interesting, as they might be inapplicable to certain problems in the Real World.

Mathematical concepts are useful in solving problems from the Real World to the extent that the concepts accurately reflect the essential features of those problems. The process of solving a problem mathematically has three parts (Fig. 29). We begin with a Real World problem. Then we need to model the original problem by a mathematical problem. This typically requires simplifying or idealizing some aspects of the original problem. (For example, we might decide to ignore air resistance or friction.) The middle step in the process consists of finding a mathematical solution to the mathematical problem. The final step is to interpret the mathematical solution in terms of the original problem. The middle step in this process is called "pure mathematics," and the entire process is called "applied mathematics."

We have, for example, all been given problems such as: If Johnny has six pennies and steals eight more, how many does he have? We first convert this to the mathematical problem: $6 + 8 = ?$ Then by pure mathematics (addition, in this case) we obtain 14 as the solution. Finally, we decide that Johnny has fourteen pennies.

The mathematical modeling of a Real World problem is not always this

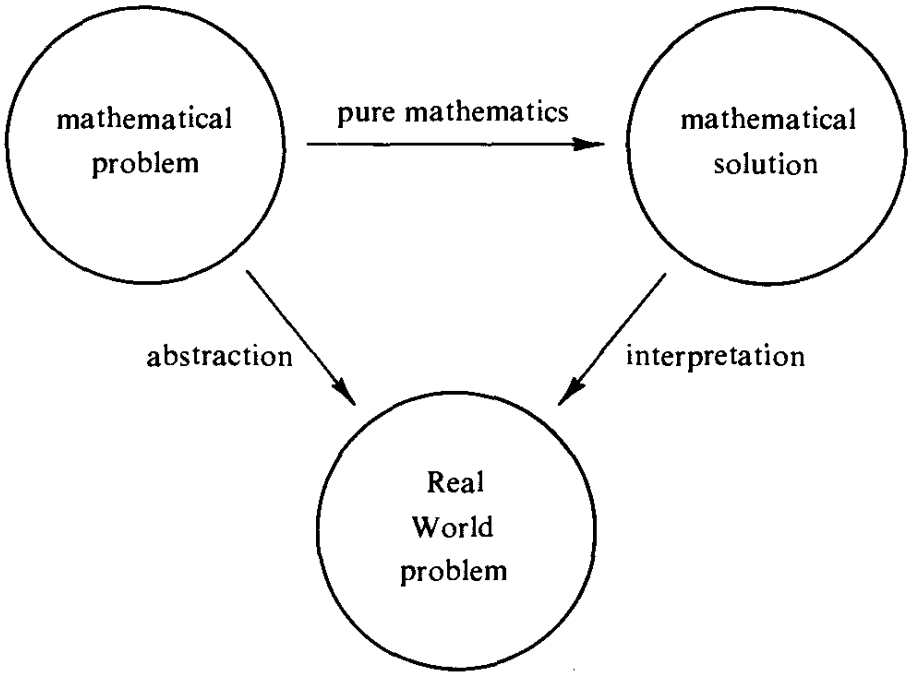

Fig. 29. Applied mathematics.

straightforward. When we try to interpret our mathematical solution in terms of the original problem, we might discover that it just does not fit. If we start with six blobs of water and add eight more blobs, we may end up with only four or five rather large puddles. This outcome does not shake our faith in arithmetic at all. It does show that we need to revise the model and try again (perhaps by measuring volume instead of counting blobs). From the vast array of mathematical concepts we must select those (if any!) that accurately model the essential feature of the problem to be solved.