ANALYSIS

An Introduction

RICHARD BEALS
Yale University

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2004

Printed in the United States of America

Typeface Times 11/14 pt. *System* LaTeX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data

Beals, Richard, 1938–
Analysis : an introduction / Richard Beals.
p. cm.
Includes bibliographical references and index.
ISBN 0-521-84072-4 – ISBN 0-521-60047-2 (pbk.)
1. Mathematical analysis. I. Title.
QA300.B4124 2004
515–dc22 2004040687

ISBN 0 521 84072 4 hardback
ISBN 0 521 60047 2 paperback

Contents

1

Introduction

The properties of the real numbers are the basis for the careful development of the topics of analysis. The purpose of this chapter is to engage in a preliminary and rather informal discussion of these properties and to sketch a construction that justifies assuming that the properties are satisfied. Along the way we introduce standard notation for various sets of numbers.

1A. Notation and Motivation

First, we use $\mathbb{N}$ to denote the set of *natural numbers* or *positive integers*:

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

In this set there are two basic algebraic operations, *addition* and *multiplication*. Each of these operations assigns to a pair of positive integers p, q an integer, respectively, the *sum* $p + q$ and the *product* $p \cdot q$ or simply pq. Further operations, such as powers, may be defined from these. There are then many facts, such as

$$1+2=3, \quad 1+2+4=7, \quad 1+2+4+8=15, \quad 1+2+4+8+16=31, \quad \dots.$$

More interesting, from a mathematical point of view, are general statements, like

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1, \qquad \text{all } n \in \mathbb{N}. \tag{1}$$

Within $\mathbb{N}$, there is also an *order relation*, denoted $<$, defined as follows. If m and n are elements of $\mathbb{N}$, then $m < n$ if and only if there is $p \in \mathbb{N}$ such that $m + p = n$. If so, we also write $n > m$. It is easy to convince oneself that this has the properties that *define* an "order relation" – given elements m, n of $\mathbb{N}$, exactly one of the following is true:

$$m < n, \qquad \text{or} \qquad n < m, \qquad \text{or} \qquad m = n. \tag{2}$$

Moreover, the relation is transitive:

$$m < n, \quad n < p \quad \Rightarrow \quad m < p. \tag{3}$$

(The one-sided arrow $\Rightarrow$ means "implies.")

Implicit in this discussion is the following fact: Given positive integers p and q, the equation $p + r = q$ does not generally have a solution r in $\mathbb{N}$; the necessary and sufficient condition is that $p < q$. Of course one can get around this difficulty by introducing $\mathbb{Z}$, the set

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

of all *integers*. The operations of addition and multiplication extend to this larger set, as does the order relation. Within this larger set one can make new statements, such as

$$1 - 2 + 2^2 - 2^3 + 2^4 - \cdots + (-2)^n = \frac{1 - (-2)^{n+1}}{3}. \tag{4}$$

The left side of this equation is clearly an integer, so the right side must also be an integer, despite the fact that not every integer is divisible by 3.

A more general way to put the statement about divisibility is this: Given integers p and q, the equation $qr = p$ does not generally have a solution r in the set $\mathbb{Z}$. To remedy this we must enlarge our set once more and go to $\mathbb{Q}$, the set

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

of *rational numbers*. The operations of addition and multiplication extend to the larger set, as does the order relation. Here we may make a statement that generalizes (1)–(3):

$$1 + r + r^2 + r^3 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r} \qquad \text{if } r \in \mathbb{Q} \quad \text{and} \quad r \neq 1. \tag{5}$$

The identities (1)–(5) are purely algebraic. The last one leads to a kind of statement that has a different character. Suppose that r is "small": Specifically, suppose that $|r| < 1$. Then successive powers of r get smaller and smaller, so that one might be tempted to write

$$1 + r + r^2 + r^3 + \cdots = \frac{1}{1 - r}, \qquad \text{if } r \in \mathbb{Q} \quad \text{and} \quad |r| < 1. \tag{6}$$

Here the ellipsis $\cdots$ means that the addition on the left is imagined to be carried out for *all* powers of r, that is, there are infinitely many summands. The reader may or may not feel that it is clear what the left side means and why it is equal to the right side; these points will be discussed in much detail in Chapter 4.

Consider two more examples of statements like (6):

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \cdots = s_1; \tag{7}$$

$$1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \frac{1}{11} - \frac{1}{6} + \cdots = s_2. \tag{8}$$

Note that the second (formal) sum has exactly the same summands as the first, except that they are written in a different order. We know that addition is associative and commutative, so it would seem that if the sums mean anything, then clearly $s_1 = s_2$. Now group the terms in (7):

$$\begin{aligned} s_1 &= 1 - \left(\frac{1}{2} - \frac{1}{3}\right) - \left(\frac{1}{4} - \frac{1}{5}\right) - \left(\frac{1}{6} - \frac{1}{7}\right) - \cdots \\ &= 1 - \frac{1}{2 \cdot 3} - \frac{1}{4 \cdot 5} - \frac{1}{6 \cdot 7} - \cdots. \end{aligned} \tag{9}$$

Each expression in parentheses is positive, so we should have $s_1 < 1$. Similarly, in (8),

$$\begin{aligned} s_2 &= 1 + \left(\frac{1}{3} - \frac{1}{2} + \frac{1}{5}\right) + \left(\frac{1}{7} - \frac{1}{4} + \frac{1}{9}\right) + \left(\frac{1}{11} - \frac{1}{6} + \frac{1}{13}\right) + \cdots \\ &= 1 + \frac{1}{2 \cdot 3 \cdot 5} + \frac{1}{4 \cdot 7 \cdot 9} + \frac{1}{6 \cdot 11 \cdot 13} + \cdots. \end{aligned} \tag{10}$$

Each expression in parentheses is positive, so we should have $s_2 > 1$. It is tempting to conclude that *either* the processes we are describing do not make sense *or* that there is some subtle flaw in the argument that purports to show that $s_1 \neq s_2$. However, the processes *do* make sense, and there is no flaw in the argument. In fact, in Chapter 4, Section D, we will show how to prove that

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \cdots = \log 2;$$

$$1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \cdots = \frac{3}{2} \log 2,$$

where $\log 2$ means the natural logarithm. In Chapter 5, Section D, we will show how to obtain different proofs of these identities. (We also present an argument for the "identity"

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + \cdots = -\frac{1}{12},$$

but this last should not be taken too seriously.)

There are a number of points to be made in this connection:

- Care must be taken with infinite repetition of algebraic operations.
- When care is taken, the results may be paradoxical but they are consistent, and often important.
- The addition of rational numbers can lead to an irrational sum, when it is extended to the case of infinitely many summands. Here is another example, also proved later:

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \frac{1}{36} + \cdots = \frac{\pi^2}{6}. \tag{11}$$

Let us pause to examine (11). Without worrying, at the moment, about the equality between the left and right sides, consider how one might conclude that the left side should have some meaning. The sequence of rational numbers

$$r_1 = 1, \qquad r_2 = 1 + \frac{1}{4}, \qquad r_3 = 1 + \frac{1}{4} + \frac{1}{9}, \qquad r_4 = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16}, \qquad \ldots$$

is *increasing*: $r_1 < r_2 < r_3 < \ldots$. We show later that this sequence is *bounded above*; in fact, $r_n < 2$ for every n. There is a standard representation of rationals as points on a line. We might expect geometrically that there is a unique point on the line with the property that, as n increases, the rationals r_n come arbitrarily close to this point. [Warning: Statements like "come arbitrarily close" need, eventually, to be made precise.] Then the left-hand side of (11) should be taken to mean the number that corresponds to this point. Thus, to be sure that things like the left side of (11) have a meaning, we want to be sure that *any bounded, increasing sequence of numbers has a limit*. (This is one version of what can be called the "no-gap" property of the real numbers. Starting in Chapter 2 we will take as basic a different, but equivalent, version, the "Least Upper Bound Property." See Figure 1.)

Another example of a bounded, increasing sequence is

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad 3.14159, \quad \ldots.$$

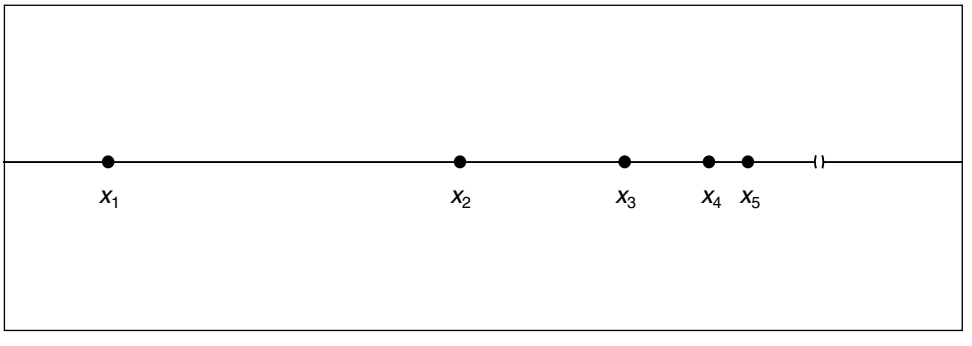

Figure 1. Heading for a gap.

Assuming that this sequence is headed where we expect, the limit π is known not to be a rational number. What justification do we have for asserting the existence of such numbers, and for thinking that we can add and multiply them in the usual ways, with the usual rules, such as $(x + y) + z = x + (y + z)$, without encountering a contradiction? These questions will be discussed in the next two sections.

Exercises

1. Prove the identity (1) by induction on n.
2. Prove by induction that the numerator in the right side of (4) is always divisible by 3.
3. (a) Prove the identity (5) by induction.
   (b) Give a second proof of the identity (5).
4. Derive and prove a general form for the expressions in parentheses in the sum (9), thus verifying that these expressions are positive.
5. Derive and prove a general form for the expressions in parentheses in the sum (10), thus verifying that these expressions are positive.

1B*. The Algebra of Various Number Systems

We begin by examining the "usual rules." The basic properties of addition and multiplication in $\mathbb{N}$ can be summarized in the following axioms (statements of properties). It is understood for the moment that m, n, and p denote arbitrary elements of $\mathbb{N}$.

A1: Associativity of addition. $(m + n) + p = m + (n + p)$.

A2: Commutativity of addition. $m + n = n + m$.

M1: Associativity of multiplication. $(mn)p = m(np)$.

M2: Commutativity of multiplication. $mn = nm$.

D: Distributive law(s). $m(n + p) = mn + mp; \quad (m + n)p = mp + np$.

[Note that either part of D follows from the other part, together with M2.]

The order relation in $\mathbb{N}$ has the defining characteristics of an order relation. Again m and n denote arbitrary elements of $\mathbb{N}$,

O1: Trichotomy. *Exactly one of the following is true:* $m < n$, $n < m$, *or* $m = n$.

O2: Transitivity. *If* $m < n$ *and* $n < p$, *then* $m < p$.

The order relation has connections with addition and with multiplication:

$$m < m + n; \qquad m < n \quad \Rightarrow \quad mp < np, \qquad \text{all } m, n, p \in \mathbb{N}. \tag{12}$$

We shall take the positive integers and these properties for granted. One can then *construct* the set of all integers as follows. The *ingredients* are all the formal expressions $m - n$, where m and n are positive integers. This formal expression can be thought of as representing the "solution" x of the equation $n + x = m$. We do not want to consider these as all representing different things (consider $1 - 1$ and $2 - 2$), so we *identify* the expressions $m - n$ and $m' - n'$ under a certain condition:

$$m - n \equiv m' - n' \qquad \text{if } m + n' = n + m'. \tag{13}$$

The set $\mathbb{Z}$ may be thought of, for now, as the set of such expressions, subject to the "identification" rule (13).

Addition and multiplication of these expressions are *defined* by

$$(m - n) + (p - q) = (m + n) - (p + q); \tag{14}$$

$$(m - n) \cdot (p - q) = (mp + nq) - (mq + np). \tag{15}$$

These rules associate to any pair of such expressions an expression of the same form. It can be checked that

$$\begin{aligned} &\text{if } m - n \equiv m' - n' \text{ and } p - q \equiv p' - q', \text{ then} \\ &(m - n) + (p - q) \equiv (m' - n') + (p' - q') \text{ and} \\ &(m - n) \cdot (p - q) \equiv (m' - n') \cdot (p' - q'). \end{aligned} \tag{16}$$

Therefore, the operations (14) and (15) are compatible with the "identifications" and may be considered as operations in $\mathbb{Z}$.

The order relation may be extended to $\mathbb{Z}$, using the definition

$$m - n < p - q \qquad \text{if } m + q < n + p. \tag{17}$$

This order relation is also compatible with the identification:

$$\begin{aligned} &\text{if } m - n \equiv m' - n' \text{ and } p - q \equiv p' - q', \text{ then} \\ &(m - n) < (p - q) \Rightarrow m' - n' < (p' - q'). \end{aligned} \tag{18}$$

If we identify a positive integer m with (any and all of) the expressions $(m + n) - n$, $n \in \mathbb{N}$, then the operations (14) and (15) are compatible with the operations in $\mathbb{N}$, so $\mathbb{N}$ may be considered as a certain *subset* of $\mathbb{Z}$. The properties A1, A2, M1, M2, D, O1, 02 can be proved for $\mathbb{Z}$, using the properties for $\mathbb{N}$ and the definitions. The important point is that $\mathbb{Z}$ has additional properties, also provable, that are not true for $\mathbb{N}$. (At the risk of introducing confusion, we now let z denote an arbitrary element of $\mathbb{Z}$.)

A3: Neutral element for addition. *There is an element* 0 *with the property that* $z + 0 = z$, *all* $z \in \mathbb{Z}$.

A4: Additive inverses. *For each* $z \in \mathbb{Z}$ *there is an element* $-z$ *with the property that* $z + (-z) = 0$.

The role of the neutral element is played by any of the expressions $m - m$, and the role of the additive inverse of $m - n$ is played by $n - m$, or by any other expression $n' - m'$ with the property that $m + n' = n + m'$.

(Any set A that has an operation of addition that satisfies A1–A4 is called a *commutative group*. If A also has an operation of multiplication and satisfies M1, M4, and D as well, then it is called a *commutative ring*. If one drops the commutativity of multiplication, M2, one has a plain *ring*.)

There is an interplay between the order relation and the algebraic operations in $\mathbb{Z}$, summarized in two properties that can be derived using (some of) A1–A4, M1, M2, D, O1, O2, and (12).

O3: Order and addition. *If* $m < n$, *then* $m + p < n + p$.

O4: Order and multiplication. *If* $m < n$ *and* $p > 0$, *then* $mp < np$.

This type of method can be extended to a construction of the rational numbers as well. Consider expressions of the form m/n, where n is a positive integer and m is any integer; this expression represents the "solution" x of the equation $nx = m$. Again it is necessary to introduce an identification:

$$m/n \equiv m'/n' \qquad \text{if } mn' = nm'. \tag{19}$$

The set $\mathbb{Q}$ of rational numbers can be thought of as the set of expressions $m - n$, subject to this identification rule.

Addition and multiplication in $\mathbb{Q}$ are *defined* by

$$\frac{m}{n} + \frac{p}{q} = \frac{mq + pn}{nq} \tag{20}$$

$$\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}, \tag{21}$$

and the order relation is defined by

$$\frac{m}{n} < \frac{p}{q} \qquad \text{if } mq < np. \tag{22}$$

The operations (20) and (21) and the order (22) are compatible with the identification rule (19), so the operations and order may be viewed as being defined in $\mathbb{Q}$.

We may consider $\mathbb{Z}$ as a *subset* of $\mathbb{Q}$ by identifying $m \in \mathbb{Z}$ with the expressions mn/n, where n belongs to $\mathbb{N}$. The operations and order in $\mathbb{Z}$ are consistent with those in $\mathbb{Q}$ under this identification. The set $\mathbb{Q}$ with the operations (20), (21), and the order relation (22) has all the preceding properties A1–A4, M1, M2, D, 01–O4. Again, there are new algebraic properties. Here r denotes an element of $\mathbb{Q}$:

M3: Neutral element for multiplication. *There is an element* $\mathbf{1}$ *such that* $r \cdot \mathbf{1} = r$*, all* r.

M4: Multiplicative inverses. *For each* $r \neq 0$*, there is an element* r^{-1} *such that* $r \cdot r^{-1} = \mathbf{1}$.

In fact, the multiplicative neutral element is represented by any n/n, the rational that is identified with the integer 1. A multiplicative inverse of m/n is n/m if $m > 0$, or $(m/n)^{-1} = (-n)/(-m)$ if $m < 0$.

There is another important property to be noted concerning $\mathbb{Q}$.

O5: The Archimedean property. *If* r *and* s *are positive rationals, then there is a positive integer* N *such that* $Nr > s$.

(If we think of s as the amount of water in a bathtub and r as the capacity of a teaspoon, this says that we can bail the water from the bathtub with the teaspoon in at most N steps. Of course N may be large.) To verify O5, suppose that $r = m/n$ and $s = p/q$. Then $Nr = (Nm)/n$, and, in view of (22), we need to find N so that Nmq is larger than np. Obviously $N = np + 1$ will do.

As we have noted, we need to go from $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$ in order to guarantee that simple algebraic equations like $a + x = b$ and $ax = b$ have solutions. However, $\mathbb{Q}$ is still not rich enough to do more interesting algebra. *In fact, the equation* $r^2 = 2$ *does not have a solution* $r \in \mathbb{Q}$. Suppose that it *did* have a solution $r = p/q$, where p and q are integers and q is positive. We may assume that r is in lowest terms, that is, that p and q have *no common factors*. Then $p^2 = 2q^2$, so p is even. Thus, $p = 2m$ with m an integer. Then $4m^2 = 2q^2$, so $2m^2 = q^2$, so q is also even, and so p and q have the common factor 2, a contradiction.

Now it is possible to find an increasing sequence of rationals

$$1, \quad 1.4, \quad 1.41, \quad 1.414, \quad 1.4142, \quad 1.41421, \quad 1.414213, \quad \ldots$$

whose squares get "arbitrarily close" to 2. (The reader is invited to formulate a more precise form of this statement.) As before, we would like to be able to assert that (a) this sequence has a number x as it limit and (b) $x^2 = 2$.

Note what has happened in this section: In effect, we took the positive integers $\mathbb{Z}$ and their operations as raw material and sketched how to *construct* the remaining integers and the rationals. The construction allows us to *prove* the various algebraic and order properties of $\mathbb{Z}$ and $\mathbb{Q}$ from properties of $\mathbb{N}$. In the next section we sketch a construction of the real numbers from the rationals, in order to fill in the gaps like $\sqrt{2}$ and π.

Exercises

1. Prove the assertion (16).
2. Use the definition (14) and the identification (13) to prove A1 and A2 for the integers $\mathbb{Z}$.
3. Use the definition (15) and the identification (13) to prove M1 and M2 for the integers $\mathbb{Z}$.
4. Verify A3 and A4 for the integers $\mathbb{Z}$.
5. Prove from axioms A1–A4 that 0 is unique: If $z + 0' = z$, then $0' = 0$.
6. Prove from A1–A4 that, given integers m and n, the equation $m + x = n$ has a unique solution $x \in \mathbb{Z}$.
7. Use (12) and the remaining axioms for $\mathbb{Z}$ to prove O3 and O4 for $\mathbb{Z}$.
8. Prove the analogue of assertion (16) for the rationals $\mathbb{Q}$.
9. Use the definition (20) and the identification (19) to prove A1 and A2 for $\mathbb{Q}$.
10. Use the definition (21) and the identification (19) to prove M1 and M2 for $\mathbb{Q}$.
11. Use axioms A, M, and D to prove that $r \cdot 0 = 0$.
12. Prove from axioms A, M, and D that, for any rationals r, s, if $r \neq 0$, then the equation $rx = s$ has a unique rational solution x.
13. Prove that there is no rational r such that $r^2 = 3$.
14. Prove that there is no rational r such that $r^3 = 2$.

1C*. The Line and Cuts

The usual geometric representation of the various number systems above uses a horizontal line. Imagine such a line with one point marked as the origin. Choose a unit of length, and march to the right from the origin in steps of unit length, denoting the corresponding points as $1, 2, 3, \ldots$. Similarly, points obtained by going to the left from the origin in steps of unit length are denoted $-1, -2, -3, \ldots$. This gives us a representation of $\mathbb{Z}$. The order relation $p < q$ has the geometric meaning that p is to the left of q. The distance between p and q is the absolute value $|p - q|$. Points corresponding to the remaining rationals are easily introduced: If we divide the interval with endpoints 3 and 4 into five equal subintervals, the first of these has endpoints 3 and $3 + 1/5 = 16/5$ and so on.

The integers $\mathbb{Z}$ determine a partition of the line into disjoint half-open intervals I_n, where $I_n = [n, n + 1)$ consists of all points that lie at or to the right of n but

strictly to the left of $n+1$. Given a point x of the line, the *integral part* of x, denoted $[x]$, is the unique integer $[x] = n$ such that x belongs to I_n: The point x is at or to the right of the integer n, and its distance from n is less than 1. It is important to note that this may be sharpened if we proceed to the rationals: *Each point x on the line may be approached as closely as we like by rational points.* In fact, partition the interval with endpoints $[x]$ and $[x]+1$ into 10^k equal subintervals. The point x lies in one of these subintervals and is therefore at distance less than 10^{-k} from one of the endpoints of that subinterval, which are rational numbers.

The preceding is the basis for one of the first *constructions* of the reals, due to Dedekind. We want the reals to account for all points on the line, and we want the line to have no gaps: Any sequence of points moving to the right, but staying to the left of some fixed point, should have a limit. We also want to extend the algebraic operations and the order relation to this full set of points, again so that $<$ means "to the left of."

Our starting point for this process can only be the rationals themselves; they must be the scaffolding on which the real numbers are constructed. In order to see how to proceed, we begin by *imagining that the goal has already been accomplished*. Then, for any point x in the line, we could associate to the point, or real number, x a *set* S of rationals – *all rationals that lie strictly to left of* x. If x and x' are distinct points, then there is a rational r strictly between them. (Choose k so large that $1/10^k$ is smaller than the distance between x and x', and look at the rational points $m/10^k$, $m \in \mathbb{Z}$.) Therefore, the set S that corresponds to x and the set S' that corresponds to x' are different: r belongs to S' but not to S. Notice also that the set S that corresponds to x has the following properties:

(C1) S is not empty and is not all of $\mathbb{Q}$.
(C2) If r is in S, s is in $\mathbb{Q}$, and $s < r$, then s is in S.
(C3) S has no largest element.

We call a subset of the rationals that has these three properties, (C1), (C2), and (C3), a *cut*. (Actually, Dedekind considered both S and the set T consisting of all rationals to the right of x; the pair together partitions the rationals not equal to x into two subsets that correspond to the act of cutting the line at the point x.)

Now, conversely, suppose that S is a cut, a subset of the rationals that has the three properties (C1), (C2), and (C3). Then we expect there to be a unique point x such that S consists precisely of the rationals strictly to the left of x. To see this, construct a sequence of rationals as follows. Conditions (C1) and (C2) imply that there is a largest integer r_0 such that $r_0 \in S$. Then $r_0 + 1$ is not in S. Next, there is an integer p, $0 \le p \le 9$ such that

$$r_1 = r_0 + \frac{p}{10} \in S, \qquad r_0 + \frac{p+1}{10} \notin S.$$

Continuing in this way, we can produce a sequence of rationals r_n such that $r_0 \leq r_1 \leq r_2 \leq \ldots$ and

$$r_n \in S, \qquad r_n + \frac{1}{10^n} \notin S.$$

Because of the no-gap condition, we expect this sequence to have a limit x. (In fact, the r_n's are successive parts of what should be the decimal expansion of x.) A bit of thought shows that a rational should belong to S if and only if it is smaller than some r_n, which is true if and only if is to the left of x.

Our discussion to this point says that *if* we had attained our goal, *then* there would be a 1–1 correspondence between real numbers on one hand and cuts on the other. We now *turn the procedure around*. We take as our *objects* the cuts themselves – the subsets of $\mathbb{Q}$ that satisfy (C1), (C2), and (C3). One can introduce algebraic operations and an order relation among the cuts and demonstrate the properties listed in the previous section. For example, the *sum* of two cuts S and S' is defined to be the set of rationals

$$S + S' = \{s = r + r' : r \in S,\ r' \in S'\}. \tag{23}$$

The rational r can be identified with the cut it induces, which we denote by r^*:

$$r^* = \{s \in \mathbb{Q} : s < r\}. \tag{24}$$

In particular, 0^* turns out to be the neutral element for addition of cuts, and 1^* the neutral element for multiplication of cuts.

The order relation is simple: If S and S' are cuts, then we set $S < S'$ if $S \subset S'$ and $S \neq S'$. (The notation $S' \subset S$ means that S' is a subset of S, but not necessarily a proper subset.)

Defining multiplication of cuts is a bit tricky. (The obvious simple adaptation of the sum rule has a problem: The product of two very negative numbers is very positive.) The usual practice is to start by finding a good definition for $S \cdot S'$ when S and S' are both positive, that is, $0^* < S, 0^* < S'$. [The reader may try to find such a definition and to verify the multiplicative and distributive properties M1–M4, D; see the exercises.]

One can verify that the set of all cuts, with the indicated addition and order relation (and the multiplication to which we have merely alluded), satisfies all the properties listed in the previous section. Of course $\mathbb{Q}$ already had all these properties. The key here is that *the set of all cuts satisfies the no-gap condition.* We do not verify this in detail here, because we have not yet defined what we mean for a sequence to have a limit, but it is easy to specify what the limit is. Suppose that $\{S_n\}$ is a sequence of cuts that is increasing and bounded above:

$$S_1 \subset S_2 \subset S_3 \subset \ldots \subset S_n \subset T, \qquad \text{all } n, \tag{25}$$

for some fixed cut T. Then one can show that the union

$$S = \bigcup_{n=1}^{\infty} S_n = S_1 \cup S_2 \cup S_3 \cup \cdots \tag{26}$$

is a cut and should be considered to be the limit of the cuts S_n.

The same idea leads to the proof of a second version of the no-gap condition, the Least Upper Bound Property, stated in the next chapter. Thus, what we have done in this section is to indicate how one can, starting with $\mathbb{Q}$, construct a collection of objects $\mathbb{R}$ that satisfies all the conditions listed in the next section and that contains (a copy of) $\mathbb{Q}$ itself.

Exercises

1. Suppose that S and S' are two cuts. Prove that either $S \subset S'$ or $S' \subset S$, or $S = S'$.
2. Suppose that S and S' are cuts. Prove that $S + S'$ is a cut, that is, that it is a subset of the rationals that has the three properties (C1), (C2), and (C3).

3–6. Prove some or all of the addition properties A1–A4 for cuts.

7. Check the compatibility of addition for rationals and the corresponding cuts: $(r + s)^* = r^* + s^*$.
8. Define the product of positive cuts. Check that your definition gives a cut, and that $S \cdot 1^* = \alpha$ for every nonnegative cut S.
9. Check the compatibility of multiplication for positive rationals and the corresponding cuts.

10–12. Prove some or all of M1, M2, and D for positive cuts.

13. Define the absolute value $|S|$ of a cut and use it to extend the definition of the product to any two cuts. (Hint: Define the product with 0^* separately.)

14–18. Prove some or all of axioms M and D for arbitrary cuts.

19. Suppose that $S_1, S_2, \ldots$ and T are cuts that satisfy (25). Prove that the set S in (26) is a cut, and that it is the smallest cut such that every S_n is smaller than S.
20. Another approach to constructing the reals is to take all formal decimal expansions. (To remove ambiguities like 1 versus .9999 . . . , we could take *nonterminating* formal decimal expansions.) Discuss the difficulties in defining the algebraic operations. For example, what would be the first term in the decimal expansion corresponding to

$$.997999194\ldots + .002000805\ldots\ ?$$

Is there some stage (preferably specifiable in advance) at which you would be sure to have enough information to know whether the sum is greater than 1?

1D. Proofs, Generalizations, Abstractions, and Purposes

Why do we want proofs? Consider assertions like (4). This is actually an infinite family of assertions, one for each positive integer n. Any single one of these

assertions could be checked by performing the required arithmetic. If one checked the first thousand or so, one might become quite confident of the rest, but that is not sufficient for mathematical *certainty*. (There are statements that are valid up to very large integers but not for all integers. A simple example: "n is not divisible by 10^{100}.") Certainty can be established in at least two ways. One way is by *mathematical induction*: Statement (4) is clearly true if $n = 1$, and by adding $(-2)^{n+1}$ to each side and regrouping the right side one obtains the truth of each subsequent statement from the truth of the one that precedes it. Since the first statement is true, so is the second; since the second statement is true, so is the third; and so on. On the other hand, (4) is a special case of the more general sequence of statements (5). Now (5) can also be proved by mathematical induction. *Another way* to prove (5) for any given positive integer n is to multiply both sides by $1 - r$.

Not only do general statements like (5) need to be proved if we are to rely on them, but, as we have just remarked, there may be more than one way to prove such a statement. In addition to general techniques that work in many cases, like mathematical induction, there are specialized tricks that may give more insight into particular problems. We can deduce (4) as a special case of (5) – but only if (5) has been soundly demonstrated. Because of the cumulative nature of mathematics, we want to be very careful about each step we take.

What makes a proof a proof? A proof is simply an argument that is designed to convince, to leave no doubt. A proof by induction is very convincing if it is carried out carefully – and if the listener or the reader is familiar with the technique and has confidence in it. Such a proof demands some sophistication of both the presenter and the presentee. The second proof of (5) mentioned above is clear and convincing to anyone who is comfortable with algebraic manipulation, and may even suggest how (5) was discovered.

How does one learn to "do" proofs? By observation and practice, practice, practice.

The purpose of this book is to proceed along the path from properties of the number system to the most important results from calculus of one variable, with each step justified, and with enough side excursions to keep the walk interesting. *Definitions* are crucial. They give precise meaning to the terms we use. Many results follow fairly directly from the definitions and a bit of logical thinking. One thing to keep in mind: *The more general the statement of a result*, typically *the simpler its proof must be*. The reason is that the proof cannot take advantage of any of those features of special examples that have been abstracted (i.e., removed) in defining the general concepts.

Proving the equality of real numbers (or of sets) is often best accomplished by proving two inequalities: We may prove that number a = number b or that set

$A =$ set B by proving

$$a \leq b \qquad \text{and} \qquad b \leq a,$$

or

$$A \subset B \qquad \text{and} \qquad B \subset A.$$

In some brief excursions, in order to get some more interesting results or examples, we will break the logical development and use things like the integral and the natural logarithm before they have been introduced rigorously. No circularity is involved: These results will not be used to develop the later theory.

Exercise

1. Another way to show equality: Prove that the real numbers a and b are equal if and only if, for each positive real ε, the absolute value $|a - b|$ satisfies $|a - b| < \varepsilon$.