Then the axioms (M) and (D) of Definition 1.12 hold, with R^+in place of F, and with 1^* in the role of 1 .

The proofs are so similar to the ones given in detail in Step 4 that we omit them.

Note, in particular, that the second requirement of Definition 1.17 holds: If $\alpha > 0^*$ and $\beta > 0^*$ then $\alpha\beta > 0^*$.

Step 7 We complete the definition of multiplication by setting $\alpha 0^* = 0^*\alpha = 0^*$, and by setting

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta) & \text{if } \alpha < 0^*, \beta < 0^* \\ -[(-\alpha)\beta] & \text{if } \alpha < 0^*, \beta > 0^* \\ -[\alpha \cdot (-\beta)] & \text{if } \alpha > 0^*, \beta < 0^* \end{cases}$$

The products on the right were defined in Step 6.
Having proved (in Step 6) that the axioms (M) hold R^+, it is now perfectly simple to prove them in R, by repeated application of the identity $\gamma = -(-\gamma)$ which is part of Proposition 1.14. (See Step 5.)

The proof of the distributive law

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$$

breaks into cases. For instance, suppose $\alpha > 0^*, \beta < 0^*, \beta + \gamma > 0^*$. Then $\gamma = (\beta + \gamma) + (-\beta)$, and (since we already know that the distributive law holds in R^+)

$$\alpha\gamma = \alpha(\beta + \gamma) + \alpha \cdot (-\beta).$$

But $\alpha \cdot (-\beta) = -(\alpha\beta)$. Thus

$$\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma).$$

The other cases are handled in the same way.
We have now completed the proof that R is an ordered field with the least-upper-bound property.

Step 8 We associate with each $r \in Q$ the set r^* which consists of all $p \in Q$ such that $p < r$. It is clear that each r^* is a cut; that is, $r^* \in R$. These cuts satisfy the following relations:
(a) $r^* + s^* = (r + s)^*$,
(b) $r^*s^* = (rs)^*$,
(c) $r^* < s^*$ if and only if $r < s$.

To prove (a), choose $p \in r^* + s^*$. Then $p = u + v$, where $u < r, v < s$. Hence $p < r + s$, which says that $p \in (r + s)^*$.

Conversely, suppose $p \in (r + s)^*$. Then $p < r + s$. Choose t so that $2t = r + s - p$, put

$$r' = r - t, s' = s - t$$

Then $r' \in r^*, s' \in s^*$, and $p = r' + s'$, so that $p \in r^* + s^*$.
This proves (a). The proof of (b) is similar.
If $r < s$ then $r \in s^*$, but $r \notin r^*$; hence $r^* < s^*$.
If $r^* < s^*$, then there is a $p \in s^*$ such that $p \notin r^*$. Hence $r \leq p < s$, so that $r < s$.

This proves (c).
Step 9 We saw in Step 8 that the replacement of the rational numbers r by the corresponding "rational cuts" $r^* \in R$ preserves sums, products, and order. This fact may be expressed by saying that the ordered field Q is isomorphic to the ordered field Q^* whose elements are the rational cuts. Of course, r^* is by no means the same as r, but the properties we are concerned with (arithmetic and order) are the same in the two fields.

It is this identification of Q with Q^* which allows us to regard Q as a subfield of R.

The second part of Theorem 1.19 is to be understood in terms of this identification. Note that the same phenomenon occurs when the real numbers are regarded as a subfield of the complex field, and it also occurs at a much more elementary level, when the integers are identified with a certain subset of Q.

It is a fact, which we will not prove here, that any two ordered fields with the least-upper-bound property are isomorphic. The first part of Theorem 1.19 therefore characterizes the real field R completely.

The books by Landau and Thurston cited in the Bibliography are entirely devoted to number systems. Chapter 1 of Knopp's book contains a more leisurely description of how R can be obtained from Q. Another construction, in which each real number is defined to be an equivalence class of Cauchy sequences of rational numbers (see Chap. 3), is carried out in Sec. 5 of the book by Hewitt and Stromberg.

The cuts in Q which we used here were invented by Dedekind. The construction of R from Q by means of Cauchy sequences is due to Cantor. Both Cantor and Dedekind published their constructions in 1872.

EXERCISES

Unless the contrary is explicitly stated, all numbers that are mentioned in these exercises are understood to be real.

1. If r is rational ($r \neq 0$) and x is irrational, prove that $r + x$ and rx are irrational.

2. Prove that there is no rational number whose square is 12 .

3. Prove Proposition 1.15.

4. Let E be a nonempty subset of an ordered set; suppose α is a lower bound of E and β is an upper bound of E. Prove that $\alpha \leq \beta$.

5. Let A be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that

$$\inf A = -\sup(-A)$$

6. Fix $b > 1$.
(a) If m, n, p, q are integers, $n > 0, q > 0$, and $r = m/n = p/q$, prove that

$$(b^m)^{1/n} = (b^p)^{1/q}$$

Hence it makes sense to define $b^r = (b^m)^{1/n}$.
(b) Prove that $b^{r+s} = b^r b^s$ if r and s are rational.
(c) If x is real, define $B(x)$ to be the set of all numbers b^t, where t is rational and $t \leq x$. Prove that

$$b^r = \sup B(r)$$

when r is rational. Hence it makes sense to define

$$b^x = \sup B(x)$$

for every real x.
(d) Prove that $b^{x+y} = b^x b^y$ for all real x and y.
7. Fix $b > 1, y > 0$, and prove that there is a unique real x such that $b^x = y$, by completing the following outline. (This x is called the logarithm of y to the base b.)
(a) For any positive integer $n, b^n - 1 \geq n(b-1)$.
(b) Hence $b - 1 \geq n\left(b^{1/n} - 1\right)$.
(c) If $t > 1$ and $n > (b-1)/(t-1)$, then $b^{1/n} < t$.
(d) If w is such that $b^w < y$, then $b^{w+(1/n)} < y$ for sufficiently large n; to see this, apply part (c) with $t = y \cdot b^{-w}$.
(e) If $b^w > y$, then $b^{w-(1/n)} > y$ for sufficiently large n.
(f) Let A be the set of all w such that $b^w < y$, and show that $x = \sup A$ satisfies $b^x = y$.
(g) Prove that this x is unique.
8. Prove that no order can be defined in the complex field that turns it into an ordered field. Hint: -1 is a square.
9. Suppose $z = a + bi, w = c + di$. Define $z < w$ if $a < c$, and also if $a = c$ but $b < d$. Prove that this turns the set of all complex numbers into an ordered set. (This type of order relation is called a dictionary order, or lexicographic order, for obvious reasons.) Does this ordered set have the least-upper-bound property?
10. Suppose $z = a + bi, w = u + iv$, and

$$a = \left(\frac{|w| + u}{2}\right)^{1/2}, \quad b = \left(\frac{|w| - u}{2}\right)^{1/2}$$

Prove that $z^2 = w$ if $v \geq 0$ and that $(\bar{z})^2 = w$ if $v \leq 0$. Conclude that every complex number (with one exception!) has two complex square roots.

11. If z is a complex number, prove that there exists an $r \geq 0$ and a complex number w with $|w| = 1$ such that $z = rw$. Are w and r always uniquely determined by z ?

12. If $z_1, \ldots, z_n$ are complex, prove that

$$|z_1 + z_2 + \cdots + z_n| \leq |z_1| + |z_2| + \cdots + |z_n|\,.$$

13. If x, y are complex, prove that

$$||x| - |y|| \leq |x - y|.$$

14. If z is a complex number such that $|z| = 1$, that is, such that $z\bar{z} = 1$, compute

$$|1 + z|^2 + |1 - z|^2$$

15. Under what conditions does equality hold in the Schwarz inequality?

16. Suppose $k \geq 3, \mathbf{x}, \mathbf{y} \in R^k, |\mathbf{x} - \mathbf{y}| = d > 0$, and $r > 0$. Prove:
(a) If $2r > d$, there are infinitely many $\mathbf{z} \in R^k$ such that

$$|\mathbf{z} - \mathbf{x}| = |\mathbf{z} - \mathbf{y}| = r$$

(b) If $2r = d$, there is exactly one such $\mathbf{z}$.
(c) If $2r < d$, there is no such $\mathbf{z}$.
How must these statements be modified if k is 2 or 1 ?

17. Prove that

$$|x + y|^2 + |x - y|^2 = 2|x|^2 + 2|y|^2$$

if $\mathbf{x} \in R^k$ and $\mathbf{y} \in R^k$. Interpret this geometrically, as a statement about parallelograms.

18. If $k \geq 2$ and $\mathbf{x} \in R^k$, prove that there exists $\mathbf{y} \in R^k$ such that $\mathbf{y} \neq \mathbf{0}$ but $\mathbf{x} \cdot \mathbf{y} = 0$.
Is this also true if $k = 1$?

19. Suppose $\mathbf{a} \in R^k, \mathbf{b} \in R^k$. Find $\mathbf{c} \in R^k$ and $r > 0$ such that

$$|\mathbf{x} - \mathbf{a}| = 2|\mathbf{x} - \mathbf{b}|$$

if and only if $|\mathbf{x} - \mathbf{c}| = r$.
(Solution: $3\mathbf{c} = 4\mathbf{b} - \mathbf{a}, 3r = 2|\mathbf{b} - \mathbf{a}|$.)

20. With reference to the Appendix, suppose that property (III) were omitted from the definition of a cut. Keep the same definitions of order and addition. Show that the resulting ordered set has the least-upper-bound property, that addition satisfies axioms (A1) to (A4) (with a slightly different zero-element!) but that (A5) fails.

2

BASIC TOPOLOGY

FINITE, COUNTABLE, AND UNCOUNTABLE SETS

We begin this section with a definition of the function concept.

2.1 Definition Consider two sets A and B, whose elements may be any objects whatsoever, and suppose that with each element x of A there is associated, in some manner, an element of B, which we denote by $f(x)$. Then f is said to be a function from A to B (or a mapping of A into B). The set A is called the domain of f (we also say f is defined on A), and the elements $f(x)$ are called the values of f. The set of all values of f is called the range of f.

2.2 Definition Let A and B be two sets and let f be a mapping of A into B. If $E \subset A, f(E)$ is defined to be the set of all elements $f(x)$, for $x \in E$. We call $f(E)$ the image of E under f. In this notation, $f(A)$ is the range of f. It is clear that $f(A) \subset B$. If $f(A) = B$, we say that f maps A onto B. (Note that, according to this usage, onto is more specific than into.)

If $E \subset B, f^{-1}(E)$ denotes the set of all $x \in A$ such that $f(x) \in E$. We call $f^{-1}(E)$ the inverse image of E under f. If $y \in B, f^{-1}(y)$ is the set of all $x \in A$