Proof (*a*), (*b*), and (*c*) are obvious, and (*d*) is an immediate consequence of the Schwarz inequality. By (*d*) we have

$$\begin{aligned}|\mathbf{x}+\mathbf{y}|^2 &= (\mathbf{x}+\mathbf{y})\cdot(\mathbf{x}+\mathbf{y})\\ &= \mathbf{x}\cdot\mathbf{x}+2\mathbf{x}\cdot\mathbf{y}+\mathbf{y}\cdot\mathbf{y}\\ &\le |\mathbf{x}|^2+2|\mathbf{x}|\,|\mathbf{y}|+|\mathbf{y}|^2\\ &= (|\mathbf{x}|+|\mathbf{y}|)^2,\end{aligned}$$

so that (*e*) is proved. Finally, (*f*) follows from (*e*) if we replace $\mathbf{x}$ by $\mathbf{x}-\mathbf{y}$ and $\mathbf{y}$ by $\mathbf{y}-\mathbf{z}$.

1.38 Remarks Theorem 1.37 (*a*), (*b*), and (*f*) will allow us (see Chap. 2) to regard R^k as a metric space.

R^1 (the set of all real numbers) is usually called the line, or the real line. Likewise, R^2 is called the plane, or the complex plane (compare Definitions 1.24 and 1.36). In these two cases the norm is just the absolute value of the corresponding real or complex number.

APPENDIX

Theorem 1.19 will be proved in this appendix by constructing R from Q. We shall divide the construction into several steps.

Step 1 The members of R will be certain subsets of Q, called *cuts*. A cut is, by definition, any set $\alpha \subset Q$ with the following three properties.

(I) α is not empty, and $\alpha \neq Q$.
(II) If $p \in \alpha$, $q \in Q$, and $q < p$, then $q \in \alpha$.
(III) If $p \in \alpha$, then $p < r$ for some $r \in \alpha$.

The letters $p, q, r, \ldots$ will always denote rational numbers, and $\alpha, \beta, \gamma, \ldots$ will denote cuts.

Note that (III) simply says that α has no largest member; (II) implies two facts which will be used freely:

If $p \in \alpha$ and $q \notin \alpha$ then $p < q$.
If $r \notin \alpha$ and $r < s$ then $s \notin \alpha$.

Step 2 Define "$\alpha < \beta$" to mean: α is a proper subset of β.

Let us check that this meets the requirements of Definition 1.5.

If $\alpha < \beta$ and $\beta < \gamma$ it is clear that $\alpha < \gamma$. (A proper subset of a proper subset is a proper subset.) It is also clear that at most one of the three relations

$$\alpha < \beta, \qquad \alpha = \beta, \qquad \beta < \alpha$$

can hold for any pair α, β. To show that at least one holds, assume that the first two fail. Then α is not a subset of β. Hence there is a $p \in \alpha$ with $p \notin \beta$. If $q \in \beta$, it follows that $q < p$ (since $p \notin \beta$), hence $q \in \alpha$, by (II). Thus $\beta \subset \alpha$. Since $\beta \neq \alpha$, we conclude: $\beta < \alpha$.

Thus R is now an ordered set.

Step 3 *The ordered set R has the least-upper-bound property.*

To prove this, let A be a nonempty subset of R, and assume that $\beta \in R$ is an upper bound of A. Define γ to be the union of all $\alpha \in A$. In other words, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. We shall prove that $\gamma \in R$ and that $\gamma = \sup A$.

Since A is not empty, there exists an $\alpha_0 \in A$. This α_0 is not empty. Since $\alpha_0 \subset \gamma$, γ is not empty. Next, $\gamma \subset \beta$ (since $\alpha \subset \beta$ for every $\alpha \in A$), and therefore $\gamma \neq Q$. Thus γ satisfies property (I). To prove (II) and (III), pick $p \in \gamma$. Then $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha_1$, hence $q \in \gamma$; this proves (II). If $r \in \alpha_1$ is so chosen that $r > p$, we see that $r \in \gamma$ (since $\alpha_1 \subset \gamma$), and therefore γ satisfies (III).

Thus $\gamma \in R$.

It is clear that $\alpha \leq \gamma$ for every $\alpha \in A$.

Suppose $\delta < \gamma$. Then there is an $s \in \gamma$ and that $s \notin \delta$. Since $s \in \gamma$, $s \in \alpha$ for some $\alpha \in A$. Hence $\delta < \alpha$, and δ is not an upper bound of A.

This gives the desired result: $\gamma = \sup A$.

Step 4 If $\alpha \in R$ and $\beta \in R$ we define $\alpha + \beta$ to be the set of all sums $r + s$, where $r \in \alpha$ and $s \in \beta$.

We define 0^* to be the set of all negative rational numbers. It is clear that 0^* is a cut. *We verify that the axioms for addition* (see Definition 1.12) *hold in R, with 0^* playing the role of* 0.

(A1) We have to show that $\alpha + \beta$ is a cut. It is clear that $\alpha + \beta$ is a nonempty subset of Q. Take $r' \notin \alpha$, $s' \notin \beta$. Then $r' + s' > r + s$ for all choices of $r \in \alpha$, $s \in \beta$. Thus $r' + s' \notin \alpha + \beta$. It follows that $\alpha + \beta$ has property (I).

Pick $p \in \alpha + \beta$. Then $p = r + s$, with $r \in \alpha$, $s \in \beta$. If $q < p$, then $q - s < r$, so $q - s \in \alpha$, and $q = (q - s) + s \in \alpha + \beta$. Thus (II) holds. Choose $t \in \alpha$ so that $t > r$. Then $p < t + s$ and $t + s \in \alpha + \beta$. Thus (III) holds.

(A2) $\alpha + \beta$ is the set of all $r + s$, with $r \in \alpha$, $s \in \beta$. By the same definition, $\beta + \alpha$ is the set of all $s + r$. Since $r + s = s + r$ for all $r \in Q$, $s \in Q$, we have $\alpha + \beta = \beta + \alpha$.

(A3) As above, this follows from the associative law in Q.

(A4) If $r \in \alpha$ and $s \in 0^*$, then $r + s < r$, hence $r + s \in \alpha$. Thus $\alpha + 0^* \subset \alpha$. To obtain the opposite inclusion, pick $p \in \alpha$, and pick $r \in \alpha$, $r > p$. Then

$p - r \in 0^*$, and $p = r + (p - r) \in \alpha + 0^*$. Thus $\alpha \subset \alpha + 0^*$. We conclude that $\alpha + 0^* = \alpha$.

(A5) Fix $\alpha \in R$. Let β be the set of all p with the following property:

There exists $r > 0$ such that $-p - r \notin \alpha$.

In other words, some rational number smaller than $-p$ fails to be in α.

We show that $\beta \in R$ and that $\alpha + \beta = 0^*$.

If $s \notin \alpha$ and $p = -s - 1$, then $-p - 1 \notin \alpha$, hence $p \in \beta$. So β is not empty. If $q \in \alpha$, then $-q \notin \beta$. So $\beta \neq Q$. Hence β satisfies (I).

Pick $p \in \beta$, and pick $r > 0$, so that $-p - r \notin \alpha$. If $q < p$, then $-q - r > -p - r$, hence $-q - r \notin \alpha$. Thus $q \in \beta$, and (II) holds. Put $t = p + (r/2)$. Then $t > p$, and $-t - (r/2) = -p - r \notin \alpha$, so that $t \in \beta$. Hence β satisfies (III).

We have proved that $\beta \in R$.

If $r \in \alpha$ and $s \in \beta$, then $-s \notin \alpha$, hence $r < -s$, $r + s < 0$. Thus $\alpha + \beta \subset 0^*$.

To prove the opposite inclusion, pick $v \in 0^*$, put $w = -v/2$. Then $w > 0$, and there is an integer n such that $nw \in \alpha$ but $(n + 1)w \notin \alpha$. (Note that this depends on the fact that Q has the archimedean property!) Put $p = -(n + 2)w$. Then $p \in \beta$, since $-p - w \notin \alpha$, and

$$v = nw + p \in \alpha + \beta.$$

Thus $0^* \subset \alpha + \beta$.

We conclude that $\alpha + \beta = 0^*$.

This β will of course be denoted by $-\alpha$.

Step 5 Having proved that the addition defined in Step 4 satisfies Axioms (A) of Definition 1.12, it follows that Proposition 1.14 is valid in R, and we can prove one of the requirements of Definition 1.17:

If $\alpha, \beta, \gamma \in R$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.

Indeed, it is obvious from the definition of $+$ in R that $\alpha + \beta \subset \alpha + \gamma$; if we had $\alpha + \beta = \alpha + \gamma$, the cancellation law (Proposition 1.14) would imply $\beta = \gamma$.

It also follows that $\alpha > 0^*$ if and only if $-\alpha < 0^*$.

Step 6 Multiplication is a little more bothersome than addition in the present context, since products of negative rationals are positive. For this reason we confine ourselves first to R^+, the set of all $\alpha \in R$ with $\alpha > 0^*$.

If $\alpha \in R^+$ and $\beta \in R^+$, we define $\alpha\beta$ to be the set of all p such that $p \leq rs$ for some choice of $r \in \alpha$, $s \in \beta$, $r > 0$, $s > 0$.

We define 1^* to be the set of all $q < 1$.

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 in 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 $r \le p < s$, 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 $b - 1 \geq n(b^{1/n} - 1)$.

(*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

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