The next theorem could be extracted from this construction with very little extra effort. However, we prefer to derive it from Theorem 1.19 since this provides a good illustration of what one can do with the least-upper-bound property.

1.20 Theorem

(*a*) *If* $x \in R$, $y \in R$, *and* $x > 0$, *then there is a positive integer* n *such that*

$$nx > y.$$

(*b*) *If* $x \in R$, $y \in R$, *and* $x < y$, *then there exists a* $p \in Q$ *such that* $x < p < y$.

Part (*a*) is usually referred to as the *archimedean property* of R. Part (*b*) may be stated by saying that Q is *dense* in R: Between any two real numbers there is a rational one.

Proof

(*a*) Let A be the set of all nx, where n runs through the positive integers. If (*a*) were false, then y would be an upper bound of A. But then A has a *least* upper bound in R. Put $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$, and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some positive integer m. But then $\alpha < (m + 1)x \in A$, which is impossible, since α is an upper bound of A.

(*b*) Since $x < y$, we have $y - x > 0$, and (*a*) furnishes a positive integer n such that

$$n(y - x) > 1.$$

Apply (*a*) again, to obtain positive integers m_1 and m_2 such that $m_1 > nx$, $m_2 > -nx$. Then

$$-m_2 < nx < m_1.$$

Hence there is an integer m (with $-m_2 \le m \le m_1$) such that

$$m - 1 \le nx < m.$$

If we combine these inequalities, we obtain

$$nx < m \le 1 + nx < ny.$$

Since $n > 0$, it follows that

$$x < \frac{m}{n} < y.$$

This proves (*b*), with $p = m/n$.

We shall now prove the existence of nth roots of positive reals. This proof will show how the difficulty pointed out in the Introduction (irrationality of $\sqrt{2}$) can be handled in R.

1.21 Theorem *For every real $x > 0$ and every integer $n > 0$ there is one and only one positive real y such that $y^n = x$.*

This number y is written $\sqrt[n]{x}$ or $x^{1/n}$.

Proof That there is at most one such y is clear, since $0 < y_1 < y_2$ implies $y_1^n < y_2^n$.

Let E be the set consisting of all positive real numbers t such that $t^n < x$.

If $t = x/(1 + x)$ then $0 \le t < 1$. Hence $t^n \le t < x$. Thus $t \in E$, and E is not empty.

If $t > 1 + x$ then $t^n \ge t > x$, so that $t \notin E$. Thus $1 + x$ is an upper bound of E.

Hence Theorem 1.19 implies the existence of

$$y = \sup E.$$

To prove that $y^n = x$ we will show that each of the inequalities $y^n < x$ and $y^n > x$ leads to a contradiction.

The identity $b^n - a^n = (b - a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$ yields the inequality

$$b^n - a^n < (b - a)nb^{n-1}$$

when $0 < a < b$.

Assume $y^n < x$. Choose h so that $0 < h < 1$ and

$$h < \frac{x - y^n}{n(y + 1)^{n-1}}.$$

Put $a = y$, $b = y + h$. Then

$$(y + h)^n - y^n < hn(y + h)^{n-1} < hn(y + 1)^{n-1} < x - y^n.$$

Thus $(y + h)^n < x$, and $y + h \in E$. Since $y + h > y$, this contradicts the fact that y is an upper bound of E.

Assume $y^n > x$. Put

$$k = \frac{y^n - x}{ny^{n-1}}.$$

Then $0 < k < y$. If $t \ge y - k$, we conclude that

$$y^n - t^n \le y^n - (y - k)^n < kny^{n-1} = y^n - x.$$

Thus $t^n > x$, and $t \notin E$. It follows that $y - k$ is an upper bound of E.

But $y - k < y$, which contradicts the fact that y is the *least* upper bound of E.

Hence $y^n = x$, and the proof is complete.

Corollary *If a and b are positive real numbers and n is a positive integer, then*

$$(ab)^{1/n} = a^{1/n}b^{1/n}.$$

Proof Put $\alpha = a^{1/n}$, $\beta = b^{1/n}$. Then

$$ab = \alpha^n\beta^n = (\alpha\beta)^n,$$

since multiplication is commutative. [Axiom (M2) in Definition 1.12.] The uniqueness assertion of Theorem 1.21 shows therefore that

$$(ab)^{1/n} = \alpha\beta = a^{1/n}b^{1/n}.$$

1.22 Decimals We conclude this section by pointing out the relation between real numbers and decimals.

Let $x > 0$ be real. Let n_0 be the largest integer such that $n_0 \leq x$. (Note that the existence of n_0 depends on the archimedean property of R.) Having chosen $n_0, n_1, \ldots, n_{k-1}$, let n_k be the largest integer such that

$$n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \leq x.$$

Let E be the set of these numbers

$$n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \qquad (k = 0, 1, 2, \ldots). \tag{5}$$

Then $x = \sup E$. The decimal expansion of x is

$$n_0 \cdot n_1 n_2 n_3 \cdots. \tag{6}$$

Conversely, for any infinite decimal (6) the set E of numbers (5) is bounded above, and (6) is the decimal expansion of $\sup E$.

Since we shall never use decimals, we do not enter into a detailed discussion.

THE EXTENDED REAL NUMBER SYSTEM

1.23 Definition The extended real number system consists of the real field R and two symbols, $+\infty$ and $-\infty$. We preserve the original order in R, and define

$$-\infty < x < +\infty$$

for every $x \in R$.

It is then clear that $+\infty$ is an upper bound of every subset of the extended real number system, and that every nonempty subset has a least upper bound. If, for example, E is a nonempty set of real numbers which is not bounded above in R, then $\sup E = +\infty$ in the extended real number system.

Exactly the same remarks apply to lower bounds.

The extended real number system does not form a field, but it is customary to make the following conventions:

(*a*) If x is real then

$$x + \infty = +\infty, \qquad x - \infty = -\infty, \qquad \frac{x}{+\infty} = \frac{x}{-\infty} = 0.$$

(*b*) If $x > 0$ then $x \cdot (+\infty) = +\infty$, $x \cdot (-\infty) = -\infty$.
(*c*) If $x < 0$ then $x \cdot (+\infty) = -\infty$, $x \cdot (-\infty) = +\infty$.

When it is desired to make the distinction between real numbers on the one hand and the symbols $+\infty$ and $-\infty$ on the other quite explicit, the former are called *finite*.

THE COMPLEX FIELD

1.24 Definition A *complex number* is an ordered pair (a, b) of real numbers. "Ordered" means that (a, b) and (b, a) are regarded as distinct if $a \neq b$.

Let $x = (a, b)$, $y = (c, d)$ be two complex numbers. We write $x = y$ if and only if $a = c$ and $b = d$. (Note that this definition is not entirely superfluous; think of equality of rational numbers, represented as quotients of integers.) We define

$$x + y = (a + c, b + d),$$
$$xy = (ac - bd, ad + bc).$$

1.25 Theorem *These definitions of addition and multiplication turn the set of all complex numbers into a field, with* $(0, 0)$ *and* $(1, 0)$ *in the role of* 0 *and* 1.

Proof We simply verify the field axioms, as listed in Definition 1.12. (Of course, we use the field structure of R.)

Let $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.
(A1) is clear.
(A2) $x + y = (a + c, b + d) = (c + a, d + b) = y + x$.

(A3) $(x + y) + z = (a + c, b + d) + (e, f)$
$= (a + c + e, b + d + f)$
$= (a, b) + (c + e, d + f) = x + (y + z).$

(A4) $x + 0 = (a, b) + (0, 0) = (a, b) = x.$

(A5) Put $-x = (-a, -b)$. Then $x + (-x) = (0, 0) = 0.$

(M1) is clear.

(M2) $xy = (ac - bd, ad + bc) = (ca - db, da + cb) = yx.$

(M3) $(xy)z = (ac - bd, ad + bc)(e, f)$
$= (ace - bde - adf - bcf, acf - bdf + ade + bce)$
$= (a, b)(ce - df, cf + de) = x(yz).$

(M4) $1x = (1, 0)(a, b) = (a, b) = x.$

(M5) If $x \neq 0$ then $(a, b) \neq (0, 0)$, which means that at least one of the real numbers a, b is different from 0. Hence $a^2 + b^2 > 0$, by Proposition 1.18(d), and we can define

$$\frac{1}{x} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

Then

$$x \cdot \frac{1}{x} = (a, b)\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0) = 1.$$

(D)
$$\begin{aligned} x(y + z) &= (a, b)(c + e, d + f) \\ &= (ac + ae - bd - bf, ad + af + bc + be) \\ &= (ac - bd, ad + bc) + (ae - bf, af + be) \\ &= xy + xz. \end{aligned}$$

1.26 Theorem *For any real numbers a and b we have*

$$(a, 0) + (b, 0) = (a + b, 0), \qquad (a, 0)(b, 0) = (ab, 0).$$

The proof is trivial.

Theorem 1.26 shows that the complex numbers of the form $(a, 0)$ have the same arithmetic properties as the corresponding real numbers a. We can therefore identify $(a, 0)$ with a. This identification gives us the real field as a subfield of the complex field.

The reader may have noticed that we have defined the complex numbers without any reference to the mysterious square root of -1. We now show that the notation (a, b) is equivalent to the more customary $a + bi$.

1.27 Definition $i = (0, 1).$

1.28 Theorem $i^2 = -1$.

Proof $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$.

1.29 Theorem *If a and b are real, then $(a, b) = a + bi$.*

Proof

$$\begin{aligned} a + bi &= (a, 0) + (b, 0)(0, 1) \\ &= (a, 0) + (0, b) = (a, b). \end{aligned}$$

1.30 Definition If a, b are real and $z = a + bi$, then the complex number $\bar{z} = a - bi$ is called the *conjugate* of z. The numbers a and b are the *real part* and the *imaginary part* of z, respectively.

We shall occasionally write

$$a = \mathrm{Re}(z), \qquad b = \mathrm{Im}(z).$$

1.31 Theorem *If z and w are complex, then*

(*a*) $\overline{z + w} = \bar{z} + \bar{w}$,
(*b*) $\overline{zw} = \bar{z} \cdot \bar{w}$,
(*c*) $z + \bar{z} = 2\,\mathrm{Re}(z)$, $z - \bar{z} = 2i\,\mathrm{Im}(z)$,
(*d*) *$z\bar{z}$ is real and positive (except when $z = 0$).*

Proof (*a*), (*b*), and (*c*) are quite trivial. To prove (*d*), write $z = a + bi$, and note that $z\bar{z} = a^2 + b^2$.

1.32 Definition If z is a complex number, its *absolute value* $|z|$ is the non-negative square root of $z\bar{z}$; that is, $|z| = (z\bar{z})^{1/2}$.

The existence (and uniqueness) of $|z|$ follows from Theorem 1.21 and part (*d*) of Theorem 1.31.

Note that when x is real, then $\bar{x} = x$, hence $|x| = \sqrt{x^2}$. Thus $|x| = x$ if $x \geq 0$, $|x| = -x$ if $x < 0$.

1.33 Theorem *Let z and w be complex numbers. Then*

(*a*) $|z| > 0$ *unless* $z = 0$, $|0| = 0$,
(*b*) $|\bar{z}| = |z|$,
(*c*) $|zw| = |z|\,|w|$,
(*d*) $|\mathrm{Re}\, z| \leq |z|$,
(*e*) $|z + w| \leq |z| + |w|$.

Proof (*a*) and (*b*) are trivial. Put $z = a + bi$, $w = c + di$, with a, b, c, d real. Then

$$|zw|^2 = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = |z|^2|w|^2$$

or $|zw|^2 = (|z|\,|w|)^2$. Now (*c*) follows from the uniqueness assertion of Theorem 1.21.

To prove (*d*), note that $a^2 \le a^2 + b^2$, hence

$$|a| = \sqrt{a^2} \le \sqrt{a^2 + b^2}.$$

To prove (*e*), note that $\bar{z}w$ is the conjugate of $z\bar{w}$, so that $z\bar{w} + \bar{z}w = 2\operatorname{Re}(z\bar{w})$. Hence

$$\begin{aligned}|z + w|^2 &= (z + w)(\bar{z} + \bar{w}) = z\bar{z} + z\bar{w} + \bar{z}w + w\bar{w}\\ &= |z|^2 + 2\operatorname{Re}(z\bar{w}) + |w|^2\\ &\le |z|^2 + 2|z\bar{w}| + |w|^2\\ &= |z|^2 + 2|z|\,|w| + |w|^2 = (|z| + |w|)^2.\end{aligned}$$

Now (*e*) follows by taking square roots.

1.34 Notation If $x_1, \ldots, x_n$ are complex numbers, we write

$$x_1 + x_2 + \cdots + x_n = \sum_{j=1}^{n} x_j.$$

We conclude this section with an important inequality, usually known as the *Schwarz inequality*.

1.35 Theorem *If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are complex numbers, then*

$$\left|\sum_{j=1}^{n} a_j \bar{b}_j\right|^2 \le \sum_{j=1}^{n} |a_j|^2 \sum_{j=1}^{n} |b_j|^2.$$

Proof Put $A = \Sigma|a_j|^2$, $B = \Sigma|b_j|^2$, $C = \Sigma a_j \bar{b}_j$ (in all sums in this proof, j runs over the values $1, \ldots, n$). If $B = 0$, then $b_1 = \cdots = b_n = 0$, and the conclusion is trivial. Assume therefore that $B > 0$. By Theorem 1.31 we have

$$\begin{aligned}\sum |Ba_j - Cb_j|^2 &= \sum (Ba_j - Cb_j)(B\bar{a}_j - \overline{Cb_j})\\ &= B^2 \sum |a_j|^2 - B\bar{C} \sum a_j \bar{b}_j - BC \sum \bar{a}_j b_j + |C|^2 \sum |b_j|^2\\ &= B^2 A - B|C|^2\\ &= B(AB - |C|^2).\end{aligned}$$

Since each term in the first sum is nonnegative, we see that

$$B(AB - |C|^2) \geq 0.$$

Since $B > 0$, it follows that $AB - |C|^2 \geq 0$. This is the desired inequality.

EUCLIDEAN SPACES

1.36 Definitions For each positive integer k, let R^k be the set of all ordered k-tuples

$$\mathbf{x} = (x_1, x_2, \ldots, x_k),$$

where $x_1, \ldots, x_k$ are real numbers, called the *coordinates* of $\mathbf{x}$. The elements of R^k are called points, or vectors, especially when $k > 1$. We shall denote vectors by boldfaced letters. If $\mathbf{y} = (y_1, \ldots, y_k)$ and if α is a real number, put

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_k + y_k),$$
$$\alpha\mathbf{x} = (\alpha x_1, \ldots, \alpha x_k)$$

so that $\mathbf{x} + \mathbf{y} \in R^k$ and $\alpha\mathbf{x} \in R^k$. This defines addition of vectors, as well as multiplication of a vector by a real number (a scalar). These two operations satisfy the commutative, associative, and distributive laws (the proof is trivial, in view of the analogous laws for the real numbers) and make R^k into a *vector space over the real field.* The zero element of R^k (sometimes called the *origin* or the *null vector*) is the point $\mathbf{0}$, all of whose coordinates are 0.

We also define the so-called "inner product" (or scalar product) of $\mathbf{x}$ and $\mathbf{y}$ by

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{k} x_i y_i$$

and the *norm* of $\mathbf{x}$ by

$$|\mathbf{x}| = (\mathbf{x} \cdot \mathbf{x})^{1/2} = \left(\sum_1^k x_i^2\right)^{1/2}.$$

The structure now defined (the vector space R^k with the above inner product and norm) is called euclidean k-space.

1.37 Theorem *Suppose* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in R^k$, *and* α *is real. Then*

(*a*) $|\mathbf{x}| \geq 0$;
(*b*) $|\mathbf{x}| = 0$ *if and only if* $\mathbf{x} = \mathbf{0}$;
(*c*) $|\alpha\mathbf{x}| = |\alpha|\,|\mathbf{x}|$;
(*d*) $|\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}|\,|\mathbf{y}|$;
(*e*) $|\mathbf{x} + \mathbf{y}| \leq |\mathbf{x}| + |\mathbf{y}|$;
(*f*) $|\mathbf{x} - \mathbf{z}| \leq |\mathbf{x} - \mathbf{y}| + |\mathbf{y} - \mathbf{z}|$.