1

THE REAL AND COMPLEX NUMBER SYSTEMS

INTRODUCTION

A satisfactory discussion of the main concepts of analysis (such as convergence, continuity, differentiation, and integration) must be based on an accurately defined number concept. We shall not, however, enter into any discussion of the axioms that govern the arithmetic of the integers, but assume familiarity with the rational numbers (i.e., the numbers of the form m/n, where m and n are integers and $n \neq 0$).

The rational number system is inadequate for many purposes, both as a field and as an ordered set. (These terms will be defined in Secs. 1.6 and 1.12.) For instance, there is no rational p such that $p^2 = 2$. (We shall prove this presently.) This leads to the introduction of so-called "irrational numbers" which are often written as infinite decimal expansions and are considered to be "approximated" by the corresponding finite decimals. Thus the sequence

$$1, 1.4, 1.41, 1.414, 1.4142, \ldots$$

"tends to $\sqrt{2}$." But unless the irrational number $\sqrt{2}$ has been clearly defined, the question must arise: Just what is it that this sequence "tends to"?

This sort of question can be answered as soon as the so-called "real number system" is constructed.

1.1 Example We now show that the equation

$$p^2 = 2 \tag{1}$$

is not satisfied by any rational p. If there were such a p, we could write $p = m/n$ where m and n are integers that are not both even. Let us assume this is done. Then (1) implies

$$m^2 = 2n^2, \tag{2}$$

This shows that m^2 is even. Hence m is even (if m were odd, m^2 would be odd), and so m^2 is divisible by 4. It follows that the right side of (2) is divisible by 4, so that n^2 is even, which implies that n is even.

The assumption that (1) holds thus leads to the conclusion that both m and n are even, contrary to our choice of m and n. Hence (1) is impossible for rational p.

We now examine this situation a little more closely. Let A be the set of all positive rationals p such that $p^2 < 2$ and let B consist of all positive rationals p such that $p^2 > 2$. We shall show that *A contains no largest number and B contains no smallest.*

More explicitly, for every p in A we can find a rational q in A such that $p < q$, and for every p in B we can find a rational q in B such that $q < p$.

To do this, we associate with each rational $p > 0$ the number

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}. \tag{3}$$

Then

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2}. \tag{4}$$

If p is in A then $p^2 - 2 < 0$, (3) shows that $q > p$, and (4) shows that $q^2 < 2$. Thus q is in A.

If p is in B then $p^2 - 2 > 0$, (3) shows that $0 < q < p$, and (4) shows that $q^2 > 2$. Thus q is in B.

1.2 Remark The purpose of the above discussion has been to show that the rational number system has certain gaps, in spite of the fact that between any two rationals there is another: If $r < s$ then $r < (r + s)/2 < s$. The real number system fills these gaps. This is the principal reason for the fundamental role which it plays in analysis.

In order to elucidate its structure, as well as that of the complex numbers, we start with a brief discussion of the general concepts of *ordered set* and *field*.

Here is some of the standard set-theoretic terminology that will be used throughout this book.

1.3 Definitions If A is any set (whose elements may be numbers or any other objects), we write $x \in A$ to indicate that x is a member (or an element) of A.

If x is not a member of A, we write: $x \notin A$.

The set which contains no element will be called the *empty set*. If a set has at least one element, it is called *nonempty*.

If A and B are sets, and if every element of A is an element of B, we say that A is a subset of B, and write $A \subset B$, or $B \supset A$. If, in addition, there is an element of B which is not in A, then A is said to be a *proper* subset of B. Note that $A \subset A$ for every set A.

If $A \subset B$ and $B \subset A$, we write $A = B$. Otherwise $A \neq B$.

1.4 Definition Throughout Chap. 1, the set of all rational numbers will be denoted by Q.

ORDERED SETS

1.5 Definition Let S be a set. An *order* on S is a relation, denoted by $<$, with the following two properties:

(i) If $x \in S$ and $y \in S$ then one and only one of the statements

$$x < y, \qquad x = y, \qquad y < x$$

is true.

(ii) If $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

The statement "$x < y$" may be read as "x is less than y" or "x is smaller than y" or "x precedes y".

It is often convenient to write $y > x$ in place of $x < y$.

The notation $x \leq y$ indicates that $x < y$ or $x = y$, without specifying which of these two is to hold. In other words, $x \leq y$ is the negation of $x > y$.

1.6 Definition An *ordered set* is a set S in which an order is defined.

For example, Q is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

1.7 Definition Suppose S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, we say that E is *bounded above*, and call β an *upper bound* of E.

Lower bounds are defined in the same way (with $\geq$ in place of $\leq$).

1.8 Definition Suppose S is an ordered set, $E \subset S$, and E is bounded above. Suppose there exists an $\alpha \in S$ with the following properties:

(i) α is an upper bound of E.
(ii) If $\gamma < \alpha$ then γ is not an upper bound of E.

Then α is called the *least upper bound of* E [that there is at most one such α is clear from (ii)] or the *supremum of* E, and we write

$$\alpha = \sup E.$$

The *greatest lower bound*, or *infimum*, of a set E which is bounded below is defined in the same manner: The statement

$$\alpha = \inf E$$

means that α is a lower bound of E and that no β with $\beta > \alpha$ is a lower bound of E.

1.9 Examples

(a) Consider the sets A and B of Example 1.1 as subsets of the ordered set Q. The set A is bounded above. In fact, the upper bounds of A are exactly the members of B. Since B contains no smallest member, *A has no least upper bound in Q.*

Similarly, B is bounded below: The set of all lower bounds of B consists of A and of all $r \in Q$ with $r \leq 0$. Since A has no lasgest member, *B has no greatest lower bound in Q.*

(b) If $\alpha = \sup E$ exists, then α may or may not be a member of E. For instance, let E_1 be the set of all $r \in Q$ with $r < 0$. Let E_2 be the set of all $r \in Q$ with $r \leq 0$. Then

$$\sup E_1 = \sup E_2 = 0,$$

and $0 \notin E_1$, $0 \in E_2$.

(c) Let E consist of all numbers $1/n$, where $n = 1, 2, 3, \ldots$. Then $\sup E = 1$, which is in E, and $\inf E = 0$, which is not in E.

1.10 Definition An ordered set S is said to have the *least-upper-bound property* if the following is true:

If $E \subset S$, E is not empty, and E is bounded above, then $\sup E$ exists in S.

Example 1.9(a) shows that Q does not have the least-upper-bound property.

We shall now show that there is a close relation between greatest lower bounds and least upper bounds, and that every ordered set with the least-upper-bound property also has the greatest-lower-bound property.

1.11 Theorem *Suppose S is an ordered set with the least-upper-bound property, $B \subset S$, B is not empty, and B is bounded below. Let L be the set of all lower bounds of B. Then*

$$\alpha = \sup L$$

exists in S, and $\alpha = \inf B$.

In particular, $\inf B$ exists in S.

Proof Since B is bounded below, L is not empty. Since L consists of exactly those $y \in S$ which satisfy the inequality $y \leq x$ for every $x \in B$, we see that *every $x \in B$ is an upper bound of L.* Thus L is bounded above. Our hypothesis about S implies therefore that L has a supremum in S; call it α.

If $\gamma < \alpha$ then (see Definition 1.8) γ is not an upper bound of L, hence $\gamma \notin B$. It follows that $\alpha \leq x$ for every $x \in B$. Thus $\alpha \in L$.

If $\alpha < \beta$ then $\beta \notin L$, since α is an upper bound of L.

We have shown that $\alpha \in L$ but $\beta \notin L$ if $\beta > \alpha$. In other words, α is a lower bound of B, but β is not if $\beta > \alpha$. This means that $\alpha = \inf B$.

FIELDS

1.12 Definition A *field* is a set F with two operations, called *addition* and *multiplication*, which satisfy the following so-called "field axioms" (A), (M), and (D):

(A) Axioms for addition

(A1) If $x \in F$ and $y \in F$, then their sum $x + y$ is in F.
(A2) Addition is commutative: $x + y = y + x$ for all $x, y \in F$.
(A3) Addition is associative: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.
(A4) F contains an element 0 such that $0 + x = x$ for every $x \in F$.
(A5) To every $x \in F$ corresponds an element $-x \in F$ such that

$$x + (-x) = 0.$$

(M) Axioms for multiplication

(M1) If $x \in F$ and $y \in F$, then their product xy is in F.
(M2) Multiplication is commutative: $xy = yx$ for all $x, y \in F$.
(M3) Multiplication is associative: $(xy)z = x(yz)$ for all $x, y, z \in F$.
(M4) F contains an element $1 \neq 0$ such that $1x = x$ for every $x \in F$.
(M5) If $x \in F$ and $x \neq 0$ then there exists an element $1/x \in F$ such that

$$x \cdot (1/x) = 1.$$

(D) The distributive law

$$x(y+z) = xy + xz$$

holds for all $x, y, z \in F$.

1.13 Remarks

(*a*) One usually writes (in any field)

$$x - y, \frac{x}{y}, x + y + z, xyz, x^2, x^3, 2x, 3x, \ldots$$

in place of

$$x + (-y), x \cdot \left(\frac{1}{y}\right), (x + y) + z, (xy)z, xx, xxx, x + x, x + x + x, \ldots.$$

(*b*) The field axioms clearly hold in Q, the set of all rational numbers, if addition and multiplication have their customary meaning. Thus Q is a field.

(*c*) Although it is not our purpose to study fields (or any other algebraic structures) in detail, it is worthwhile to prove that some familiar properties of Q are consequences of the field axioms; once we do this, we will not need to do it again for the real numbers and for the complex numbers.

1.14 Proposition *The axioms for addition imply the following statements.*

(*a*) *If* $x + y = x + z$ *then* $y = z$.
(*b*) *If* $x + y = x$ *then* $y = 0$.
(*c*) *If* $x + y = 0$ *then* $y = -x$.
(*d*) $-(-x) = x$.

Statement (*a*) is a cancellation law. Note that (*b*) asserts the uniqueness of the element whose existence is assumed in (A4), and that (*c*) does the same for (A5).

Proof If $x + y = x + z$, the axioms (A) give

$$\begin{aligned} y = 0 + y &= (-x + x) + y = -x + (x + y) \\ &= -x + (x + z) = (-x + x) + z = 0 + z = z. \end{aligned}$$

This proves (*a*). Take $z = 0$ in (*a*) to obtain (*b*). Take $z = -x$ in (*a*) to obtain (*c*).

Since $-x + x = 0$, (*c*) (with $-x$ in place of x) gives (*d*).

1.15 Proposition *The axioms for multiplication imply the following statements.*

(*a*) *If* $x \neq 0$ *and* $xy = xz$ *then* $y = z$.
(*b*) *If* $x \neq 0$ *and* $xy = x$ *then* $y = 1$.
(*c*) *If* $x \neq 0$ *and* $xy = 1$ *then* $y = 1/x$.
(*d*) *If* $x \neq 0$ *then* $1/(1/x) = x$.

The proof is so similar to that of Proposition 1.14 that we omit it.

1.16 Proposition *The field axioms imply the following statements, for any* x, y, $z \in F$.

(*a*) $0x = 0$.
(*b*) *If* $x \neq 0$ *and* $y \neq 0$ *then* $xy \neq 0$.
(*c*) $(-x)y = -(xy) = x(-y)$.
(*d*) $(-x)(-y) = xy$.

Proof $0x + 0x = (0 + 0)x = 0x$. Hence 1.14(*b*) implies that $0x = 0$, and (*a*) holds.

Next, assume $x \neq 0$, $y \neq 0$, but $xy = 0$. Then (*a*) gives

$$1 = \left(\frac{1}{y}\right)\left(\frac{1}{x}\right)xy = \left(\frac{1}{y}\right)\left(\frac{1}{x}\right)0 = 0,$$

a contradiction. Thus (*b*) holds.

The first equality in (*c*) comes from

$$(-x)y + xy = (-x + x)y = 0y = 0,$$

combined with 1.14(*c*); the other half of (*c*) is proved in the same way. Finally,

$$(-x)(-y) = -[x(-y)] = -[-(xy)] = xy$$

by (*c*) and 1.14(*d*).

1.17 Definition An *ordered field* is a *field* F which is also an *ordered set*, such that

(i) $x + y < x + z$ if $x, y, z \in F$ and $y < z$,
(ii) $xy > 0$ if $x \in F$, $y \in F$, $x > 0$, and $y > 0$.

If $x > 0$, we call x *positive*; if $x < 0$, x is *negative*.

For example, Q is an ordered field.

All the familiar rules for working with inequalities apply in every ordered field: Multiplication by positive [negative] quantities preserves [reverses] inequalities, no square is negative, etc. The following proposition lists some of these.

1.18 Proposition *The following statements are true in every ordered field.*

(*a*) *If* $x > 0$ *then* $-x < 0$, *and vice versa.*
(*b*) *If* $x > 0$ *and* $y < z$ *then* $xy < xz$.
(*c*) *If* $x < 0$ *and* $y < z$ *then* $xy > xz$.
(*d*) *If* $x \neq 0$ *then* $x^2 > 0$. *In particular,* $1 > 0$.
(*e*) *If* $0 < x < y$ *then* $0 < 1/y < 1/x$.

Proof

(*a*) If $x > 0$ then $0 = -x + x > -x + 0$, so that $-x < 0$. If $x < 0$ then $0 = -x + x < -x + 0$, so that $-x > 0$. This proves (*a*).

(*b*) Since $z > y$, we have $z - y > y - y = 0$, hence $x(z - y) > 0$, and therefore

$$xz = x(z - y) + xy > 0 + xy = xy.$$

(*c*) By (*a*), (*b*), and Proposition 1.16(*c*),

$$-[x(z - y)] = (-x)(z - y) > 0,$$

so that $x(z - y) < 0$, hence $xz < xy$.

(*d*) If $x > 0$, part (ii) of Definition 1.17 gives $x^2 > 0$. If $x < 0$, then $-x > 0$, hence $(-x)^2 > 0$. But $x^2 = (-x)^2$, by Proposition 1.16(*d*). Since $1 = 1^2$, $1 > 0$.

(*e*) If $y > 0$ and $v \leq 0$, then $yv \leq 0$. But $y \cdot (1/y) = 1 > 0$. Hence $1/y > 0$. Likewise, $1/x > 0$. If we multiply both sides of the inequality $x < y$ by the positive quantity $(1/x)(1/y)$, we obtain $1/y < 1/x$.

THE REAL FIELD

We now state the *existence theorem* which is the core of this chapter.

1.19 Theorem *There exists an ordered field* R *which has the least-upper-bound property.*

Moreover, R *contains* Q *as a subfield.*

The second statement means that $Q \subset R$ and that the operations of addition and multiplication in R, when applied to members of Q, coincide with the usual operations on rational numbers; also, the positive rational numbers are positive elements of R.

The members of R are called *real numbers*.

The proof of Theorem 1.19 is rather long and a bit tedious and is therefore presented in an Appendix to Chap. 1. The proof actually constructs R from Q.

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 $-m_2 \leq m \leq m_1$) such that

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

If we combine these inequalities, we obtain

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

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) $x(y + z) = (a, b)(c + e, d + f)$
$= (ac + ae - bd - bf, ad + af + bc + be)$
$= (ac - bd, ad + bc) + (ae - bf, af + be)$
$= xy + xz.$

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 $a^2 \leq a^2 + b^2$, hence

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

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

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

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*

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

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*) $|\mathbf{x} - \mathbf{z}| \leq |\mathbf{x} - \mathbf{y}| + |\mathbf{y} - \mathbf{z}|$.

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

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

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

(*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

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

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

$$|\mathbf{x} + \mathbf{y}|^2 + |\mathbf{x} - \mathbf{y}|^2 = 2|\mathbf{x}|^2 + 2|\mathbf{y}|^2$$

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.