CHAPTER I
THE REAL AND COMPLEX NUMBERS
DEFINITION OF THE NUMBERS 1, i, AND $\sqrt{2}$

In order to make precise sense out of the concepts we study in mathematical analysis, we must first come to terms with what the "real numbers" are. Everything in mathematical analysis is based on these numbers, and their very definition and existence is quite deep. We will, in fact, not attempt to demonstrate (prove) the existence of the real numbers in the body of this text, but will content ourselves with a careful delineation of their properties, referring the interested reader to an appendix for the existence and uniqueness proofs.

Although people may always have had an intuitive idea of what these real numbers were, it was not until the nineteenth century that mathematically precise definitions were given. The history of how mathematicians came to realize the necessity for such precision in their definitions is fascinating from a philosophical point of view as much as from a mathematical one. However, we will not pursue the philosophical aspects of the subject in this book, but will be content to concentrate our attention just on the mathematical facts. These precise definitions are quite complicated, but the powerful possibilities within mathematical analysis rely heavily on this precision, so we must pursue them. Toward our primary goals, we will in this chapter give definitions of the symbols (numbers) -1, i, and $\sqrt{2}$.

The main points of this chapter are the following:

(1) The notions of **least upper bound** (*supremum*) and **greatest lower bound** (*infimum*) of a set of numbers,
(2) The definition of the **real numbers** $\mathbb{R}$,
(3) the formula for the sum of a **geometric progression** (Theorem 1.9),
(4) the **Binomial Theorem** (Theorem 1.10), and
(5) the **triangle inequality** for complex numbers (Theorem 1.15).

THE NATURAL NUMBERS AND THE INTEGERS

We will take for granted that we understand the existence of what we call the *natural numbers,* i.e., the set $\mathbb{N}$ whose elements are the numbers $1, 2, 3, 4, \ldots$. Indeed, the two salient properties of this set are that (a) there is a frist element (the natural number 1), and (b) for each element n of this set there is a "very next" one, i.e., an immediate successor. We assume that the algebraic notions of sum and product of natural numbers is well-defined and familiar. These operations satisfy three basic relations:

BASIC ALGEBRAIC RELATIONS.

(1) (Commutativity) $n + m = m + n$ and $n \times m = m \times n$ for all $n, m \in \mathbb{N}$.
(2) (Associativity) $n + (m + k) = (n + m) + k$ and $n \times (m \times k) = (n \times m) \times k$ for all $n, m, k \in \mathbb{N}$.
(3) (Distributivity) $n \times (m + k) = n \times m + n \times k$ for all $n, m, k \in \mathbb{N}$.

We also take as given the notion of one natural number being larger than another one. $2 > 1$, $5 > 3$, $n + 1 > n$, etc. We will accept as true the **axiom of mathematical induction,** that is, the following statement:

AXIOM OF MATHEMATICAL INDUCTION. *Let S be a subset of the set $\mathbb{N}$ of natural numbers. Suppose that*

(1) $1 \in S$.

(2) *If a natural number k is in S, then the natural number $k+1$ also is in S.*

Then $S = \mathbb{N}$. That is, every natural number n belongs to S.

REMARK. The axiom of mathematical induction is for our purposes frequently employed as a method of proof. That is, if we wish to show that a certain proposition holds for all natural numbers, then we let S denote the set of numbers for which the proposition is true, and then, using the axiom of mathematical induction, we verify that S is all of $\mathbb{N}$ by showing that S satisfies both of the above conditions.

Mathematical induction can also be used as a method of definition. That is, using it, we can define an infinite number of objects $\{O_n\}$ that are indexed by the natural numbers. Think of S as the set of natural numbers for which the object O_n is defined. We check first to see that the object O_1 is defined. We check next that, if the object O_k is defined for a natural number k, then there is a prescribed procedure for defining the object O_{k+1}. So, by the axiom of mathematical induction, the object is defined for all natural numbers. This method of defining an infinite set of objects is often referred to as sl recursive definition, or *definition by recursion.*

As an example of recursive definition, let us carefully define *exponentiation.*

DEFINITION. Let a be a natural number. We define inductively natural numbers a^n as follows: $a^1 = a$, and, whenever a^k is defined, then a^{k+1} is defined to be $a \times a^k$.

. The set S of all natural numbers for which a^n is defined is therefore all of $\mathbb{N}$. For, a^1 is defined, and if a^k is defined there is a prescription for defining a^{k+1}. This "careful" definition of a^n may seem unnecessarily detailed. Why not simply define a^n as $a \times a \times a \times a \ldots \times a$ n times? The answer is that the $\ldots$, though suggestive enough, is just not mathematically precise. After all, how would you explain what $\ldots$ means? The answer to that is that you invent a recursive definition to make the intuitive meaning of the $\ldots$ mathematically precise. We will of course use the symbol $\ldots$ to simplify and shorten our notation, but keep in mind that, if pressed, we should be able to provide a careful definition.

Exercise 1.1. (a) Derive the three laws of exponents for the natural numbers: $a^{n+m} = a^n \times a^m$.

HINT: Fix a and m and use the axiom of mathematical induction.

$a^{n \times m} = (a^m)^n$.

HINT: Fix a and m and use the axiom of mathematical induction.

$(a \times b)^n = a^n \times b^n$.

HINT: Fix a and b and use the axiom of mathematical induction.

(b) Define inductively numbers $\{S_i\}$ as follows: $S_1 = 1$, and if S_k is defined, then S_{k+1} is defined to be $S_k + k + 1$. Prove, by induction, that $S_n = n(n+1)/2$. Note that we could have defined S_n using the $\ldots$ notation by $S_n = 1 + 2 + 3 + \ldots + n$.

(c) Prove that

$$1 + 4 + 9 + 16 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(d) Make a recursive definition of $n! = 1 \times 2 \times 3 \times \ldots \times n$. $n!$ is called n factorial.

There is a slightly more general statement of the axiom of mathematical induction, which is sometimes of use.

GENERAL AXIOM OF MATHEMATICAL INDUCTION. *Let S be a subset of the set $\mathbb{N}$ of natural numbers, and suppose that S satisfies the following conditions*

(1) *There exists a natural number k_0 such that $k_0 \in S$.*
(2) *If S contains a natural number k, then S contains the natural number $k+1$.*

Then S contains every natural number n that is larger than or equal to k_0.

From the fundamental set $\mathbb{N}$ of natural numbers, we construct the set $\mathbb{Z}$ of all integers. First, we simply create an additional number called 0 that satisfies the equations $0+n=n$ for all $n \in \mathbb{N}$ and $0 \times n = 0$ for all $n \in \mathbb{N}$. The word "create" is, for some mathematicians, a little unsettling. In fact, the idea of zero did not appear in mathematics until around the year 900. It is easy to see how the so-called natural numbers came by their name. Fingers, toes, trees, fish, etc., can all be counted, and the very concept of counting is what the natural numbers are about. On the other hand, one never needed to count zero fingers or fish, so that the notion of zero as a number easily could have only come into mathematics at a later time, a time when arithmetic was becoming more sophisticated. In any case, from our twenty-first century viewpoint, 0 seems very understandable, and we won't belabor the fundamental question of its existence any further here.

Next, we introduce the so-called *negative numbers*. This is again quite reasonable from our point of view. For every natural number n, we let $-n$ be a number which, when added to n, give 0. Again, the question of whether or not such negative numbers exist will not concern us here. We simply create them.

In short, we will take as given the existence of a set $\mathbb{Z}$, called the *integers*, which comprises the set $\mathbb{N}$ of natural numbers, the additional number 0, and the set $-\mathbb{N}$ of all negative numbers. We assume that addition and multiplication of integers satisfy the three basic algebraic relations of commutativity, associativity, and distributivity stated above. We also assume that the following additional relations hold:

$$(-n) \times (-k) = n \times k, \text{ and } (-n) \times k = n \times (-k) = -(n \times k)$$

for all natural numbers n and k.

THE RATIONAL NUMBERS

Next, we discuss the set $\mathbb{Q}$ of rational numbers, which we ordinarily think of as quotients k/n of integers. Of course, we do not allow the "second" element n of the quotient k/n to be 0. Also, we must remember that there isn't a 1-1 correspondence between the set $\mathbb{Q}$ of all rational numbers and the set of all such quotients k/n. Indeed, the two distinct quotients $2/3$ and $6/9$ represent the same rational number.

To be precise, the set $\mathbb{Q}$ is a collection of equivalence classes of ordered pairs (k, n) of integers, for which the second component of the pair is not 0. The equivalence relation among these ordered pairs is this:

$$(k, n) \equiv (k', n') \text{ if } k \times n' = n \times k'.$$

We will not dwell on this possibly subtle definition, but will rather accept the usual understanding of the rational numbers and their arithmetic properties. In

particular, we will represent them as quotients rather than as ordered pairs, and, if r is a rational number, we will write $r = k/n$, instead of writing r as the equivalence class containing the ordered pair (k, n). As usual, we refer to the first integer in the quotient k/n as the *numerator* and the second (nonzero) integer in the quotient k/n as the *denominator* of the quotient. The familiar definitions of sum and product for rational numbers are these:

$$\frac{k}{n} + \frac{k'}{n'} = \frac{kn' + nk'}{nn'}$$

and

$$\frac{k}{n} \times \frac{k'}{n'} = \frac{kk'}{nn'}.$$

Addition and multiplication of rational numbers satisfy the three basic algebraic relations of commutativity, associativity and distributivity stated earlier.

We note that the integers $\mathbb{Z}$ can be identified in an obvious way as a subset of the rational numbers $\mathbb{Q}$. Indeed, we identify the integer k with the quotient $k/1$. In this way, we note that $\mathbb{Q}$ contains the two numbers $0 \equiv 0/1$ and $1 \equiv 1/1$. Notice that any other quotient k/n that is equivalent to $0/1$ must satisfy $k = 0$, and any other quotient k/n that is equivalent to $1/1$ must satisfy $k = n$. Remember, $k/n \equiv k'/n'$ if and only if $kn' = k'n$.

The set $\mathbb{Q}$ has an additional property not shared by the set of integers $\mathbb{Z}$. It is this: For each nonzero element $r \in \mathbb{Q}$, there exists an element $r' \in \mathbb{Q}$ for which $r \times r' = 1$. Indeed, if $r = k/n \neq 0$, then $k \neq 0$, and we may define $r' = n/k$. Consequently, the set $\mathbb{Q}$ of all rational numbers is what is known in mathematics as a field.

DEFINITION. A *field* is a nonempty set F on which there are defined two binary operations, addition $(+)$ and multiplication $(\times)$, such that the following six axioms hold:

(1) Both addition and multiplication are commutative and associative.
(2) Multiplication is distributive over addition; i.e.,

$$x \times (y + z) = x \times y + x \times z$$

for all $x, y, z \in F$.
(3) There exists an element in F, which we will denote by 0, that is an identity for addition; i.e., $x + 0 = x$ for all $x \in F$.
(4) There exists a **nonzero** element in F, which we will denote by 1, that is an identity for multiplication; i.e., $x \times 1 = x$ for all $x \in F$.
(5) If $x \in F$, then there exists a unique element $y \in F$ such that $x + y = 0$. This element y is called the *additive inverse* of x and is denoted by $-x$.
(6) If $x \in F$ and $x \neq 0$, then there exists a unique element $y \in F$ such that $x \times y = 1$. This element y is called the *multiplicative inverse* of x and is denoted by x^{-1}.

REMARK. There are many examples of fields. (See the exercise below.) They all share certain arithmetic properties, which can be derived from the axioms above.

If x is an element of a field F, then according to one of the axioms above, we have that $1 \times x = x$. (Note that this "1" is the multiplicative identity of the field

F and not the natural number 1.) However, it is tempting to write $x + x = 2 \times x$ in the field F. The "2" here is not à priori an element of F, so that the equation $x + x = 2 \times x$ is not really justified. This is an example of a situation where a careful recursive definition can be useful.

DEFINITION. If x is an element of a field F, define inductively elements $n \cdot x \equiv nx$ of F by $1 \cdot x = x$, and, if $k \cdot x$ is defined, set $(k+1) \cdot x = x + k \cdot x$. The set S of all natural numbers n for which $n \cdot x$ is defined is therefore, by the axiom of mathematical induction, all of $\mathbb{N}$.

Usually we will write nx instead of $n \cdot x$. Of course, nx is just the element of F obtained by adding x to itself n times: $nx = x + x + x + \ldots + x$.

Exercise 1.2. (a) Justify for yourself that the set $\mathbb{Q}$ of all rational numbers is a field. That is, carefully verify that all six of the axioms hold.

(b) Let F_7 denote the seven elements $\{0, 1, 2, 3, 4, 5, 6\}$. Define addition and multiplication on F_7 as ordinary addition and multiplication mod 7. Prove that F_7 is a field. (You may assume that axioms (1) and (2) hold. Check only conditions (3)–(6).) Show in addition that $7x = 0$ for every $x \in F_7$.

(c) Let F_9 denote the set consisting of the nine elements $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Define addition and multiplication on F_9 to be ordinary addition and multiplication mod 9. Show that F_9 is not a field. Which of the axioms fail to hold?

(d) Show that the set $\mathbb{N}$ of natural numbers is not a field. Which of the field axioms fail to hold? Show that the set $\mathbb{Z}$ of all integers is not a field. Which of the field axioms fail to hold?

Exercise 1.3. Let F be any field. Verify that the following arithmetic properties hold in F.

(a) $0 \times x = 0$ for all $x \in F$.

HINT: Use the distributive law and the fact that $0 = 0 + 0$.

(b) If x and y are nonzero elements of F, then $x \times y$ is nonzero. And, the multiplicative inverse of $x \times y$ satisfies $(x \times y)^{-1} = x^{-1} \times y^{-1}$.

(c) $(-1) \times x = (-x)$ for all $x \in F$.

(d) $(-x) \times (-y) = x \times y$ for all $x, y \in F$.

(e) $x \times x - y \times y = (x - y) \times (x + y)$.

(f) $(x + y) \times (x + y) = x \times x + 2 \cdot x \times y + y \times y$.

DEFINITION. Let F be a field, and let x be a nonzero element of F.

For each natural number n, we define inductively an element x^n in F as follows: $x^1 = x$, and, if x^k is defined, set $x^{k+1} = x \times x^k$. Of course, x^n is just the product of n x's.

Define x^0 to be 1.

For each natural number n, define x^{-n} to be the multiplicative inverse $(x^n)^{-1}$ of the element x^n.

Finally, we define 0^m to be 0 for every positive integer m, and we leave 0^{-n} and 0^0 undefined.

We have therefore defined x^m for every nonzero x and every integer $m \in \mathbb{Z}$.

Exercise 1.4. Let F be a field. Derive the following laws of exponents:

(a) $x^{n+m} = x^n \times x^m$ for all nonzero elements $x \in F$ and all integers n and m.

HINT: Fix $x \in F$ and $m \in \mathbb{Z}$ and use induction to derive this law for all natural numbers n. Then use the fact that in any field $(x \times y)^{-1} = x^{-1} \times y^{-1}$.

(b) $x^{n\times m} = (x^m)^n$ for all nonzero $x \in F$ and all $n, m \in \mathbb{Z}$.
(c) $(x \times y)^n = x^n \times y^n$ for all nonzero $x, y \in F$ and all $n \in \mathbb{Z}$.

From now on, we will indicate multiplication in a field by juxtaposition; i.e., $x \times y$ will be denoted simply as xy. Also, we will use the standard fractional notation to indicate multiplicative inverses. For instance,

$$xy^{-1} = x\frac{1}{y} = \frac{x}{y}.$$

THE REAL NUMBERS

What are the real numbers? From a geometric point of view (and a historical one as well) real numbers are quantities, i.e., lengths of segments, areas of surfaces, volumes of solids, etc. For example, once we have settled on a unit of length, i.e., a segment whose length we call 1, we can, using a compass and straightedge, construct segments of any rational length k/n. In some obvious sense then, the rational numbers are real numbers. Apparently it was an intellectual shock to the Pythagoreans to discover that there are some other real numbers, the so-called irrational ones. Indeed, the square root of 2 is a real number, since we can construct a segment the square of whose length is 2 by making a right triangle each of whose legs has length 1. (By the Pythagorean Theorem of plane geometry, the square of the hypotenuse of this triangle must equal 2.) And, Pythagoras proved that there is no rational number whose square is 2, thereby establishing that there are real numbers tha are not rational. See part (c) of Exercise 1.9.

Similarly, the area of a circle of radius 1 should be a real number; i.e., π should be a real number. It wasn't until the late 1800's that Hermite showed that π is not a rational number. One difficulty is that to define π as the area of a circle of radius 1 we must first define what is meant by the " area" of a circle, and this turns out to be no easy task. In fact, this naive, geometric approach to the definition of the real numbers turns out to be unsatisfactory in the sense that we are not able to prove or derive from these first principles certain intuitively obvious arithmetic results. For instance, how can we multiply or divide an area by a volume? How can we construct a segment of length the cube root of 2? And, what about negative numbers?

Let us begin by presenting two properties we expect any set that we call the real numbers ought to possess.

Algebraic Properties

We should be able to add, multiply, divide, etc., real numbers. In short, we require the set of real numbers to be a field.

Positivity Properties

The second aspect of any set we think of as the real numbers is that it has some notion of direction, some notion of positivity. It is this aspect that will allow us to "compare" numbers, e.g., one number is larger than another. The mathematically precise way to discuss this notion is the following.

DEFINITION. A field F is called an *ordered field* if there exists a subset $P \subseteq F$ that satisfies the following two properties:

(1) If $x, y \in P$, then $x + y$ and xy are in P.

(2) If $x \in F$, then one and only one of the following three statements is true. (i) $x \in P$, (ii) $-x \in P$, and (iii) $x = 0$. (This property is known as the *law of tricotomy*.)

The elements of the set P are called *positive* elements of F, and the elements x for which $-x$ belong to P are called *negative* elements of F.

As a consequence of these properties of P, we may introduce in F a notion of order.

DEFINITION. If F is an ordered field, and x and y are elements of F, we say that $x < y$ if $y - x \in P$. We say that $x \leq y$ if either $x < y$ or $x = y$.

We say that $x > y$ if $y < x$, and $x \geq y$ if $y \leq x$.

An ordered field satisfies the familiar laws of inequalities. They are consequences of the two properties of the set P.

Exercise 1.5. Using the positivity properties above for an ordered field F, together with the axioms for a field, derive the familiar laws of inequalities:

(a) (Transitivity) If $x < y$ and $y < z$, then $x < z$.

(b) (Adding like inequalities) If $x < y$ and $z < w$, then $x + z < y + w$.

(c) If $x < y$ and $a > 0$, then $ax < ay$.

(d) If $x < y$ and $a < 0$, then $ay < ax$.

(e) If $0 < a < b$ and $0 < c < d$, then $ac < bd$.

(f) Verify parts (a) through (e) with $<$ replaced by $\leq$.

(g) If x and y are elements of F, show that one and only one of the following three relations can hold: (i) $x < y$, (ii) $x > y$, (iii) $x = y$.

(h) Suppose x and y are elements of F, and assume that $x \leq y$ and $y \leq x$. Prove that $x = y$.

Exercise 1.6. (a) If F is an ordered field, show that $1 \in P$; i.e., that $0 < 1$.
HINT: By the law of tricotomy, only one of the three possibilities holds for 1. Rule out the last two.

(b) Show that F_7 of Exercise 1.2 is not an ordered field; i.e., there is no subset $P \subseteq F_7$ such that the two positivity properties can hold.
HINT: Use part (a) and positivity property (1).

(c) Prove that $\mathbb{Q}$ is an ordered field, where the set P is taken to be the usual set of positive rational numbers. That is, P consists of those rational numbers a/b for which both a and b are natural numbers.

(d) Suppose F is an ordered field and that x is a nonzero element of F. Show that for all natural numbers n $nx \neq 0$.

(e) Show that, in an ordered field, every nonzero square is positive; i.e., if $x \neq 0$, then $x^2 \in P$.

We remarked earlier that there are many different examples of fields, and many of these are also ordered fields. Some fields, though technically different from each other, are really indistinguishable from the algebraic point of view, and we make this mathematically precise with the following definition.

DEFINITION. Let F_1 and F_2 be two ordered fields, and write P_1 and P_2 for the set of positive elements in F_1 and F_2 respectively. A 1-1 correspondence J between F_1 and F_2 is called an *isomorphism* if

(1) $J(x + y) = J(x) + J(y)$ for all $x, y \in F_1$.

(2) $J(xy) = J(x)J(y)$ for all $x, y \in F_1$.
(3) $x \in P_1$ if and only if $J(x) \in P_2$.

REMARK. In general, if A_1 and A_2 are two algebraic systems, then a 1-1 correspondence between A_1 and A_2 is called an *isomorphism* if it converts the algebraic structure on A_1 into the corresponding algebraic structure on A_2.

Exercise 1.7. (a) Let F be an ordered field. Define a function $J : \mathbb{N} \to F$ by $J(n) = n \cdot 1$. Prove that J is an isomorphism of $\mathbb{N}$ onto a subset $\widetilde{\mathbb{N}}$ of F. That is, show that this correspondence is one-to-one and converts addition and multiplication in $\mathbb{N}$ into addition and multiplication in F. Give an example to show that this result is not true if F is merely a field and not an ordered field.

(b) Let F be an ordered field. Define a function $J : \mathbb{Q} \to F$ by $J(k/n) = k \cdot 1 \times (n \cdot 1)^{-1}$. Prove that J is an isomorphism of the ordered field $\mathbb{Q}$ onto a subset $\widetilde{\mathbb{Q}}$ of the ordered field F. Conclude that every ordered field F contains a subset that is isomorphic to the ordered field $\mathbb{Q}$.

REMARK. Part (b) of the preceding exercise shows that the ordered field $\mathbb{Q}$ is the smallest possible ordered field, in the sense that every other ordered field contains an isomorphic copy of $\mathbb{Q}$. However, as mentioned earlier, the ordered field $\mathbb{Q}$ cannot suffice as the set of real numbers. There is no rational number whose square is 2, and we want the square root of 2 to be a real number. See Exercise 1.9 below.

What extra property is there about an ordered field F that will allow us to prove that numbers like $\sqrt{2}$, π, and so on are elements of F? It turns out that the extra property we need is related to a quite subtle point concerning upper and lower bounds of sets. It gives us some initial indication that the known-to-be subtle concept of a **limit** may be fundamental to our very notion of what the real numbers are.

DEFINITION. If S is a subset of an ordered field F, then an element $x \in F$ is called an *upper bound* for S if $x \geq y$ for every $y \in S$. An element z is called a *lower bound* for S if $z \leq y$ for every $y \in S$.

A subset S of an ordered field F is called *bounded above* if it has an upper bound; it is called *bounded below* if it has a lower bound; and it is called *bounded* if it has both an upper bound and a lower bound.

An element M is called the *least upper bound* or *supremum* of a set S if it is an upper bound for S and if $M \leq x$ for every other upper bound x of S. That is, M is less than or equal to any other upper bound of S.

Similarly, an element m is called the *greatest lower bound* or *infimum* of S if it is a lower bound for S and if $z \leq m$ for every other lower bound z of S. That is, m is greater than or equal to any other lower bound of S.

Clearly, the supremum and infimum of a set S are unique. For instance, if M and M' are both least upper bounds of a set S, then they are both upper bounds of S. We would then have $M \leq M'$ and $M' \leq M$. Therefore, by part (h) of Exercise 1.5, $M = M'$.

It is important to keep in mind that an upper bound of a set S need not be an element of S, and in particular, the least upper bound of S **may or may not** actually belong to S.

If M is the supremum of a set S, we denote M by $\sup S$. If m is the infimum of a set S, we denote it by $\inf S$.

Exercise 1.8. (a) Suppose S is a nonempty subset of an ordered field F and that x is an element of F. What does it mean to say that "x is not an upper bound for S?"

(b) Let F be an ordered field, and let S be the empty set, thought of as a subset of F. Prove that every element $x \in F$ is an upper bound for S and that every element $y \in F$ is a lower bound for S.
HINT: If not, then what?

(c) If $S = \emptyset$, show that S has no least upper bound and no greatest lower bound.

REMARK. The preceding exercise shows that peculiar things about upper and lower bounds happen when S is the empty set. One point is that just because a set has an upper bound does not mean it has to have a least upper bound. That is, no matter which upper bound we choose, there is always another one that is strictly smaller. This is a very subtle point, and it is in fact quite difficult to give a simple concrete example of this phenomenon. See the remark following Theorem 1.6. However, part (d) of the next exercise contains the seed of an example.

Exercise 1.9. A natural number a is called *even* if there exists a natural number c such that $a = 2c$, and a is called *odd* if there exists a natural number c such that $a = 2c + 1$.

(a) Prove by induction that every natural number is either odd or even.

(b) Prove that a natural number a is even if and only if $a^2 = a \times a$ is even.

(c) Prove that there is no element x of $\mathbb{Q}$ whose square is 2. That is, the square root of 2 is not a rational number.
HINT: Argue by contradiction. Suppose there is a rational number k/n for which $k^2/n^2 = 2$, and assume, as we may, that the natural numbers k and n have no common factor. Observe that k must be even, and then observe that n also must be even.

(d) Let S be the set of all positive rational numbers x for which $x^2 = x \times x < 2$. Prove that S has an upper bound and a lower bound. Can you determine whether or not S has a least upper bound?

The existence of least upper bounds and greatest lower bounds of bounded sets turns out to be the critical idea in defining the real numbers. It is precisely the existence of such suprema and infimas that enables us to define as real numbers quantities such as $\sqrt{2}$, π, e, and so on.

DEFINITION. An ordered field F is called *complete* if every nonempty subset S of F that has an upper bound has a least upper bound.

REMARK. Although $\mathbb{Q}$ is an ordered field, we will see that it is not a complete ordered field. In fact, the answer to part (d)(of Exercise 1.9 is no. The set described there, though bounded above, has no least upper bound. In fact, it was one of nineteenth century mathematicians' major achievements to prove the following theorem.

THEOREM 1.1. *There exists a complete ordered field.*

We leave the proof of this theorem to the appendix.

Perhaps the most reassuring result along these lines is the following companion theorem, whose proof we also leave to the appendix.

THEOREM 1.2. *If F_1 and F_2 are two complete ordered fields, then they are isomorphic.*

Taken together, the content of the two preceding theorems is that, up to isomorphism, there exists one and only one complete ordered field. For no other reason that that, this special field should be an important object in mathematics. Our definition of the real numbers is then the following:

DEFINITION. By the set $\mathbb{R}$ of *real numbers* we mean the (unique) complete ordered field.

PROPERTIES OF THE REAL NUMBERS

THEOREM 1.3. *The set $\mathbb{R}$ contains a subset that is isomorphic to the ordered field $\mathbb{Q}$ of rational numbers, and hence subsets that are isomorphic to $\mathbb{N}$ and $\mathbb{Z}$.*

REMARK. The proof of Theorem 1.3 is immediate from part (b) of Exercise 1.7. In view of this theorem, we will simply think of the natural numbers, the integers, and the rational numbers as subsets of the real numbers.

Having made a definition of the set of real numbers, it is incumbent upon us now to verify that this set $\mathbb{R}$ satisfies our intuitive notions about the reals. Indeed, we will show that $\sqrt{2}$ is an element of $\mathbb{R}$ and hence is a real number (as plane geometry indicates it should be), and we will show in later chapters that there are elements of $\mathbb{R}$ that agree with our intuition about e and π. Before we can proceed to these tasks, we must establish some special properties of the field $\mathbb{R}$. The first, the next theorem, is simply an analog for lower bounds of the least upper bound condition that comes from the completeness property.

THEOREM 1.4. *If S is a nonempty subset of $\mathbb{R}$ that is bounded below, then there exists a greatest lower bound for S.*

PROOF. Define T to be the set of all real numbers x for which $-x \in S$. That is, T is the set $-S$. We claim first that T is bounded above. Thus, let m be a lower bound for the set S, and let us show that the number $-m$ is an upper bound for T. If $x \in T$, then $-x \in S$. So, $m \leq -x$, implying that $-m \geq x$. Since this is true for all $x \in T$, the number $-m$ is an upper bound for T.

Now, by the completeness assumption, T has a least upper bound M_0. We claim that the number $-M_0$ is the greatest lower bound for S. To prove this, we must check two things. First, we must show that $-M_0$ is a lower bound for S. Thus, let y be an element of S. Then $-y \in T$, and therefore $-y \leq M_0$. Hence, $-M_0 \leq y$, showing that $-M_0$ is a lower bound for S.

Finally, we must show that $-M_0$ is the greatest lower bound for S. Thus, let m be a lower bound for S. We saw above that this implies that $-m$ is an upper bound for T. Hence, because M_0 is the least upper bound for T, we have that $-m \geq M_0$, implying that $m \leq -M_0$, and this proves that $-M_0$ is the infimum of the set S.

The following is the most basic and frequently used property of least upper bounds. It is our first glimpse of " limits." Though the argument is remarkably short and sweet, it will provide the mechanism for many of our later proofs, so master this one.

THEOREM 1.5. *Let S be a nonempty subset of $\mathbb{R}$ that is bounded above, and Let M_0 denote the least upper bound of S; i.e., $M_0 = \sup S$. Then, for any positive real number ϵ there exists an element t of S such that $t > M_0 - \epsilon$.*

PROOF. Let $\epsilon > 0$ be given. Since $M_0 - \epsilon < M_0$, it must be that $M_0 - \epsilon$ is not an upper bound for S. (M_0 is necessarily less than or equal to any other upper bound of S.) Therefore, there exists an element $t \in S$ for which $t > M_0 - \epsilon$. This is exactly what the theorem asserts.

Exercise 1.10. (a) Let S be a nonempty subset of $\mathbb{R}$ which is bounded below, and let m_0 denote the infimum of S. Prove that, for every positive δ, there exists an element s of S such that $s < m_0 + \delta$. Mimic the proof to Theorem 1.5.

(b) Let S be any bounded subset of $\mathbb{R}$, and write $-S$ for the set of negatives of the elements of S. Prove that $\sup(-S) = -\inf S$.

(c) Use part (b) to give an alternate proof of part (a) by using Theorem 1.5 and a minus sign.

Exercise 1.11. (a) Let S be the set of all real numbers x for which $x < 1$. Give an example of an upper bound for S. What is the least upper bound of S? Is $\sup S$ an element of S?

(b) Let S be the set of all $x \in \mathbb{R}$ for which $x^2 \leq 4$. Give an example of an upper bound for S. What is the least upper bound of S? Does $\sup S$ belong to S?

We show now that $\mathbb{R}$ contains elements other than the rational numbers in $\mathbb{Q}$. Of course this holds for any complete ordered field. The next theorem makes this quite explicit.

THEOREM 1.6. *If x is a positive real number, then there exists a positive real number y such that $y^2 = x$. That is, every positive real number x has a positive square root in $\mathbb{R}$. Moreover, there is only one positive square root of x.*

PROOF. Let S be the set of positive real numbers t for which $t^2 \leq x$. Then S is nonempty Indeed, If $x > 1$, then 1 is in S because $1^2 = 1 \times 1 < 1 \times x = x$. And, if $x \leq 1$, then x itself is in S, because $x^2 = x \times x \leq 1 \times x = x$.

Also, S is bounded above. In fact, the number $1 + x/2$ is an upper bound of S. Indeed, arguing by contradiction, suppose there were a t in S such that $t > 1 + x/2$. Then

$$x \geq t^2 > (1 + x/2)^2 = 1 + x + x^2/4 > x,$$

which is a contradiction. Therefore, $1 + x/2$ is an upper bound of S, and so S is bounded above.

Now let $y = \sup S$. We wish to show that $y^2 = x$. We show first that $y^2 \leq x$, and then we will show that $y^2 \geq x$. It will then follow from the tricotomy law that $y^2 = x$. We prove both these inequalities by contradiction.

So, assume first that $y^2 > x$, and write α for the positive number $y^2 - x$. Let ϵ be the positive number $\alpha/(2y)$, and, using Theorem 1.5, choose a $t \in S$ such that

$t > y - \epsilon$. Then $y + t \leq (2y)$, and $y - t < \epsilon = \alpha/2y$. So,

$$\begin{aligned}
\alpha &= y^2 - x \\
&= y^2 - t^2 + t^2 - x \\
&\leq y^2 - t^2 \\
&= (y + t)(y - t) \\
&\leq 2y(y - t) \\
&< 2y\epsilon \\
&< 2y \times \frac{\alpha}{2y} \\
&= \alpha,
\end{aligned}$$

which is a contradiction. Therefore y^2 is not greater than x.

Now we show that y^2 is not less than x. Again, arguing by contradiction, suppose it is, and let ϵ be the positive number $x - y^2$. Choose a positive number δ that is less than y and also less than $\epsilon/(3y)$. Let $s = y + \delta$. Then s is not in S, whence $s^2 > x$, so that we must have

$$\begin{aligned}
\epsilon &= x - y^2 \\
&= x - s^2 + s^2 - y^2 \\
&\leq s^2 - y^2 \\
&= (s + y)(s - y) \\
&= (2y + \delta)\delta \\
&< 3y\delta \\
&< \epsilon,
\end{aligned}$$

which again is a contradiction.

This completes the proof that $y^2 = x$; i.e., that x has a positive square root.

Finally, if y' were another positive number for which ${y'}^2 = x$, we show that $y = y'$ by ruling out the other two cases: $y < y'$ and $y > y'$. For instance, if $y < y'$, then we would have that $y^2 < {y'}^2$, giving that

$$x = y^2 < {y'}^2 = x,$$

implying that $x < x$, and this is a contradiction.

DEFINITION. If x is a positive real number, then the symbol $\sqrt{x}$ will denote the unique positive number y for which $y^2 = x$. Of course, $\sqrt{0}$ denotes the number 0.

REMARK. Part (c) of Exercise 1.9 shows that the field $\mathbb{Q}$ contains no number whose square is 2, and Theorem 1.6 shows that the field $\mathbb{R}$ does contain a number whose square is 2. We have therefore "proved" that the real numbers is a larger set than the rational numbers. It may come as a surprise to learn that we only now have been able to prove that. Look back through the chapter to be sure. It follows also that $\mathbb{Q}$ itself is not a complete ordered field. If it were, it would be isomorphic to $\mathbb{R}$, by Theorem 1.2, so that it would have to contain a square root of 2, which it does not.

DEFINITION. A real number x that is not a rational number, i.e., is not an element of the subset $\mathbb{Q}$ of $\mathbb{R}$, is called an *irrational number*.

Exercise 1.12. (a) Prove that every positive real number has exactly 2 square roots, one positive ($\sqrt{x}$) and the other negative ($-\sqrt{x}$).

(b) Prove that if x is a negative real number, then there is no real number y such that $y^2 = x$.

(c) Prove that the product of a nonzero rational number and an arbitrary irrational number must be irrational. Show by example that the sum and product of irrational numbers can be rational.

INTERVALS AND APPROXIMATION

We introduce next into the set of real numbers some geometric concepts, namely, a notion of distance between numbers. Of course this had to happen, for geometry is the very basis of mathematics.

DEFINITION. The absolute value of a real number x is denoted by $|x|$ and is defined as follows:

(i) $|0| = 0$.

(ii) If $x > 0$ then $|x| = x$.

(iii) If $x < 0$ ($-x > 0$) then $|x| = -x$.

We define the *distance* $d(x, y)$ between two real numbers x and y by $d(x, y) = |x - y|$.

Obviously, such definitions of absolute value and distance can be made in any ordered field.

Exercise 1.13. Let x and y be real numbers.

(a) Show that $|x| \geq 0$, and that $x \leq |x|$.

(b) Prove the Triangle Inequality for absolute values.

$$|x + y| \leq |x| + |y|.$$

HINT: Check the three cases $x + y > 0$, $x + y < 0$, and $x + y = 0$.

(c) Prove the so-called ‘ ‘ backward” triangle inequality.

$$|x - y| \geq ||x| - |y||.$$

HINT: Write $|x| = |(x - y) + y|$, and use part (b).

(d) Prove that $|xy| = |x||y|$.

(e) Prove that $|x| = \sqrt{x^2}$ for all real numbers x.

(f) Prove the Triangle Inequality for the distance function. That is, show that

$$d(x, y) \leq d(x, z) + d(z, y)$$

for all $x, y, z \in \mathbb{R}$.

Exercise 1.14. (a) Prove that $x = y$ if $|x - y| < \epsilon$ for every positive number ϵ.
HINT: Argue by contradiction. Suppose $x \neq y$, and take $\epsilon = |x - y|/2$.

(b) Prove that $x = y$ if and only if $x - y \leq \epsilon$ and $y - x \leq \epsilon$ for every positive ϵ.

DEFINITION. Let a and b be real numbers for which $a < b$. By the *open interval (a,b)* we mean the set of all real numbers x for which $a < x < b$, and by the *closed interval [a,b]* we mean the set of all real numbers x for which $a \leq x \leq b$.

By (a, ∞) we mean the set of all real numbers x for which $a < x$, and by $[a, \infty)$ we mean the set of all real numbers x for which $a \leq x$.

Analogously, we define $(-\infty, b)$ and $(-\infty, b]$ to be respectively the set of all real numbers x for which $x < b$ and the set of all real numbers x for which $x \leq b$.

Exercise 1.15. (a) Show that the intersection of two open intervals either is the empty set or it is again an open interval.

(b) Show that $(a, b) = (-\infty, b) \cap (a, \infty)$.

(c) Let y be a fixed real number, and let ϵ be a positive number. Show that the inequality $|x - y| < \epsilon$ is equivalent to the pair of inequalities

$$y - \epsilon < x \,\text{and}\, x < y + \epsilon;$$

i.e., show that x satisfies the first inequality if and only if it satisfies the two latter ones. Deduce that $|x - y| < \epsilon$ if and only if x is in the open interval $(y - \epsilon, y + \epsilon)$.

Here is one of those assertions that seems like an obvious fact. However, it requires a proof which we only now can give, for it depends on the completeness axiom, and in fact is false in some ordered fields.

THEOREM 1.7. *Let $\mathbb{N}$ denote the set of natural Numbers, thought of as a subset of $\mathbb{R}$. Then $\mathbb{N}$ is not bounded above.*

PROOF. Suppose false. Let M be an upper bound for the nonempty set $\mathbb{N}$, and let M_0 be the least upper bound for $\mathbb{N}$. Taking ϵ to be the positive number $1/2$, and applying Theorem 1.5, we have that there exists an element k of $\mathbb{N}$ such that $M_0 - 1/2 < k$. But then $M_0 - 1/2 + 1 < k + 1$, or, $M_0 + 1/2 < k + 1$. So $M_0 < k + 1$. But $M_0 \geq k + 1$ because M_0 is an upper bound for $\mathbb{N}$. We have thus arrived at a contradiction, and the theorem is proved.

REMARK. As mentioned above, there do exist ordered fields F in which the subset $\mathbb{N}$ **is** bounded above. Such fields give rise to what is called "nonstandard analysis," and they were first introduced by Abraham Robinson in 1966. The fact that $\mathbb{R}$ is a complete ordered field is apparently crucial to be able to conclude the intuitively clear fact that the natural numbers have no upper bound.

The next exercise presents another intuitively obvious fact, and this one is in some real sense the basis for many of our upcoming arguments about limits. It relies on the preceding theorem, is in fact just a corollary, so it has to be considered as a rather deep property of the real numbers; it is not something that works in every ordered field.

Exercise 1.16. Prove that if ϵ is a positive real number, then there exists a natural number N such that $1/N < \epsilon$.

The next theorem and exercise show that the set $\mathbb{Q}$ of rational numbers is "everywhere dense" in the field $\mathbb{R}$. That is, every real number can be approximated arbitrarily closely by rational numbers. Again, we point out that this result holds in any complete ordered field, and it is the completeness that is critical.

THEOREM 1.8. *Let $a < b$ be two real numbers. Then there exists a rational number $r = p/q$ in the open interval (a, b). In fact, there exist infinitely many rational numbers in the interval (a, b).*

PROOF. If $a < 0$ and $b > 0$, then taking $r = 0$ satisfies the first statement of the theorem. Assume first that $a \geq 0$ and $b > a$. Let n be a natural number for which $1/n$ is less than the positive number $b - a$. (Here, we are using the completeness of the field, because we are referring to Theorem 1.7, where completeness was vital.) If $a = 0$, then $b = b - a$. Setting $r = 1/n$, we would have that $a < r < b$. So, again, the first part of the theorem would be proved in that case.

Suppose then that $a > 0$, and choose the natural number q to be such that $1/q$ is less than the minimum of the two positive numbers a and $b - a$. Now, because the number aq is not an upper bound for the set $\mathbb{N}$, we may let p be the smallest natural number that is larger than aq. Set $r = p/q$.

We have first that $aq < p$, implying that $a < p/q = r$. Also, because p is the smallest natural number larger than aq, we must have that $p - 1 \leq aq$. Therefore, $(p-1)/q < a$, or $(p/q)-(1/q) < a$, implying that $r = p/q \leq a+1/q < a+(b-a) = b$. Hence, $a < r$ and $r < b$, and the first statement of the theorem is proved when both a and b are nonnegative.

If both a and b are nonpositive, then both $-b$ and $-a$ are nonnegative, and, using the first part of the proof, we can find a rational number r such that $-b < r < -a$. So, $a < -r < b$, and the first part of the theorem is proved in this case as well.

Clearly, we may replace b by r and repeat the argument to obtain another rational r_1 such that $a < r_1 < r < b$. Then, replacing b by r_1 and repeating the argument, we get a third rational r_2 such that $a < r_2 < r_1 < r < b$. Continuing this procedure would lead to an infinite number of rationals, all between a and b. This proves the second statement of the theorem.

Exercise 1.17. (a) Let $\epsilon > 0$ be given, and let k be a nonnegative integer. Prove that there exists a rational number p/q such that

$$k\epsilon < p/q < (k + 1)\epsilon.$$

(b) Let x be a positive real number and let ϵ be a positive real number. Prove that there exists a rational number p/q such that $x - \epsilon < p/q < x$. State and prove an analogous result for negative numbers x.

Exercise 1.18. (a) If a and b are real numbers with $a < b$, show that there is an irrational number x (not a rational number) between a and b, i.e., with $a < x < b$. HINT: Apply Theorem 1.8 to the numbers $a\sqrt{2}$ and $b\sqrt{2}$.

(b) Conclude that within every open interval (a, b) there is a rational number and an irrational number. Are there necessarily infinitely many rationals and irrationals in (a, b)?

The preceding exercise shows the "denseness" of the rationals and the irrationals in the reals. It is essentially clear from this that every real number is arbitrarily close to a rational number and an irrational one.

THE GEOMETRIC PROGRESSION AND THE BINOMIAL THEOREM

There are two special algebraic identities that hold in $\mathbb{R}$ (in fact in any field F whatsoever) that we emphasize. They are both proved by mathematical induction. The first is the formula for the sum of a geometric progression.

THEOREM 1.9. (Geometric Progression) Let x be a real number, and let n be a natural number. Then,

(1) If $x \neq 1$, then
$$\sum_{j=0}^{n} x^j = \frac{1-x^{n+1}}{1-x}.$$

(2) If $x = 1$, then
$$\sum_{j=0}^{n} x^j = n+1.$$

PROOF. The second claim is clear, since there are $n+1$ summands and each is equal to 1.

We prove the first claim by induction. Thus, if $n = 1$, then the assertion is true, since
$$\sum_{j=0}^{1} x^j = x^0 + x^1 = 1 + x = (1+x)\frac{1-x}{1-x} = \frac{1-x^2}{1-x}.$$

Now, supposing that the assertion is true for the natural number k, i.e., that
$$\sum_{j=0}^{k} x^j = \frac{1-x^{k+1}}{1-x},$$

let us show that the assertion holds for the natural number $k+1$. Thus
$$\begin{aligned}\sum_{j=0}^{k+1} x^j &= \sum_{j=0}^{k} x^j + x^{k+1} \\ &= \frac{1-x^{k+1}}{1-x} + x^{k+1} \\ &= \frac{1-x^{k+1}+x^{k+1}-x^{k+2}}{1-x} \\ &= \frac{1-x^{k+1+1}}{1-x},\end{aligned}$$

which completes the proof.

The second algebraic formula we wish to emphasize is the Binomial Theorem. Before stating it, we must introduce some useful notation.

DEFINITION. Let n be a natural number. As earlier in this chapter, we define $n!$ as follows:
$$n! = n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1.$$

For later notational convenience, we also define 0! to be 1.

If k is any integer for which $0 \leq k \leq n$, we define the *binomial coefficient* $\binom{n}{k}$ by
$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \times (n-1) \times (n-2) \times \ldots \times (n-k+1)}{k!}.$$

Exercise 1.19. (a) Prove that $\binom{n}{0} = 1$, $\binom{n}{1} = n$ and $\binom{n}{n} = 1$.

(b) Prove that

$$\binom{n}{k} \leq \frac{2n^k}{2^k}$$

for all natural numbers n and all integers $0 \leq k \leq n$.

(c) Prove that

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

for all natural numbers n and all integers $1 \leq k \leq n$.

THEOREM 1.10. (Binomial Theorem) If $x, y \in \mathbb{R}$ and n is a natural number, then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

PROOF. We shall prove this theorem by induction. If $n = 1$, then the assertion is true, for $(x+y)^1 = x + y$ and

$$\sum_{k=0}^{1} \binom{1}{k} x^k y^{1-k} = \binom{1}{0} x^0 y^1 + \binom{1}{1} x^1 y^0 = x + y.$$

Now, assume that the assertion holds for the natural number j; i.e.,

$$(x+y)^j = \sum_{k=0}^{j} \binom{j}{k} x^k y^{j-k},$$

and let us prove that the assertion holds for the natural number $j+1$. We will make

use of part (c) of Exercise 1.19. We have that

$$\begin{aligned}
(x+y)^{j+1} &= (x+y)(x+y)^j \\
&= (x+y)\sum_{k=0}^{j}\binom{j}{k}x^k y^{j-k} \\
&= x\sum_{k=0}^{j}\binom{j}{k}x^k y^{j-k} + y\sum_{k=0}^{j}\binom{j}{k}x^k y^{j-k} \\
&= \sum_{k=0}^{j}\binom{j}{k}x^{k+1} y^{j-k} + \sum_{k=0}^{j}\binom{j}{k}x^k y^{j+1-k} \\
&= \sum_{k=0}^{j-1}\binom{j}{k}x^{k+1} y^{j-k} + \binom{j}{j}x^{j+1}y^0 \\
&\quad + \sum_{k=1}^{j}\binom{j}{k}x^k y^{j+1-k} + \binom{j}{0}x^0 y^{j+1} \\
&= x^{j+1} + \sum_{k=1}^{j}\binom{j}{k-1}x^k y^{j+1-k} \\
&\quad + \sum_{k=1}^{j}\binom{j}{k}x^k y^{j+1-k} + y^{j+1} \\
&= x^{j+1} + \sum_{k=1}^{j}(\binom{j}{k-1} + \binom{j}{k})x^k y^{j+1-k} + y^{j+1} \\
&= x^{j+1} + \sum_{k=1}^{j}\binom{j+1}{k}x^k y^{j+1-k} + y^{j+1} \\
&= \binom{j+1}{j+1}x^{j+1}y^0 + \sum_{k=1}^{j}\binom{j+1}{k}x^k y^{j+1-k} + \binom{j+1}{0}x^0 y^{j+1} \\
&= \sum_{k=0}^{j+1}\binom{j+1}{k}x^k y^{j+1-k},
\end{aligned}$$

which shows that the assertion of the theorem holds for the natural number $j+1$. This completes the proof.

The next exercise is valid in any ordered field, but, since we are mainly interested in the order field $\mathbb{R}$, we state everything in terms of that field.

Exercise 1.20. (a) If x and y are positive real numbers, and if n and k are natural numbers with $k \le n$, show that $(x+y)^n \ge \binom{n}{k}x^k y^{n-k}$.

(b) For any positive real number x and natural number n, show that $(1+x)^n \ge 1+nx$.

(c) For any real number $x > -1$ and natural number n, prove that $(1+x)^n \ge 1+nx$.

HINT: Do not try to use the binomial theorem as in part (b); it won't work because the terms are not all positive; prove this directly by induction.

There is one more important algebraic identity, which again can be proved by induction. It is actually just a corollary of the geometric progression formula.

THEOREM 1.11. *If $x, y \in \mathbb{R}$ and n is a natural number, then*

$$x^n - y^n = (x-y)(\sum_{j=0}^{n-1} x^j y^{n-1-j}.$$

PROOF. If $n = 1$ the theorem is clear. Suppose it holds for a natural number k, and let us prove the identity for the natural number $k+1$. We have

$$\begin{aligned} x^{k+1} - y^{k+1} &= x^{k+1} - x^k y + x^k y - y^{k+1} \\ &= (x-y)x^k + y(x^k - y^k) \\ &= (x-y)x^k + y(x-y)(\sum_{j=0}^{k-1} x^j y^{k-1-j}) \\ &= (x-y)x^k + (x-y)(\sum_{j=0}^{k-1} x^j y^{k-j} \\ &= (x-y)(x^k y^{k-k} + \sum_{j=0}^{k-1} x^j y^{k-j}) \\ &= (x-y)(\sum_{j=0}^{k} x^j y^{k-j}), \end{aligned}$$

which shows that the assertion holds for the natural number $k+1$. So, by induction, the theorem is proved.

Exercise 1.21. Let x and y be real numbers.

(a) Let n be an odd natural number; i.e., $n = 2k+1$ for some natural number k. Show that

$$x^n + y^n = (x+y)(\sum_{j=0}^{n-1} (-1)^j x^j y^{n-1-j}.$$

HINT: Write $x^n + y^n = x^n - (-y)^n$.

(b) Show that $x^2 + y^2$ can not be factored into a product of the form $(ax + by)(cx + dy)$ for any choices of real numbers a, b, c, and d.

Using the Binomial Theorem together with the preceding theorem, we may now investigate the existence of nth roots of real numbers. This next theorem is definitely not valid in any ordered field, for it again depends on the completeness property.

THEOREM 1.12. *Let n be a natural number and let x be a positive real number. Then there exists a unique positive real number y such that $y^n = x$; i.e., x has a unique positive nth root.*

PROOF. Note first that if $0 \leq t < s$, then $t^n < s^n$. (To see this, argue by induction, and use part (e) of Exercise 1.5.) Using this, we mimic the proof of Theorem 1.6.

Thus, let S be the set of all positive real numbers t for which $t^n \leq x$. Then S is nonempty and bounded above. Indeed, if $x \geq 1$, then $1 \in S$, while if $x < 1$, then x itself is in S. Therefore, S is nonempty. Also, using part (b) of Exercise 1.20, we see that $1 + (x/n)$ is an upper bound for S. For, if $t > 1 + x/n$, then

$$t^n > (1 + (x/n))^n \geq 1 + n(x/n) > x.$$

Now let $y = \sup S$, and let us show that $y^n = x$. We rule out the other two possibilities. First, if $y^n > x$, let ϵ be the positive number $y^n - x$, and define ϵ' to be the positive number $\epsilon/(ny^{n-1})$. Then, using Theorem 1.5, choose $t \in S$ so that $y - \epsilon' < t \leq y$. (Theorem 1.5 is where the completeness of the ordered field $\mathbb{R}$ is crucial.) We have

$$\begin{aligned}
\epsilon &= y^n - x \\
&= y^n - t^n + t^n - x \\
&\leq y^n - t^n \\
&= (y - t)(\sum_{j=0}^{n-1} y^j t^{n-1-j}) \\
&\leq (y - t)(\sum_{j=0}^{n-1} y^j y^{n-1-j}) \\
&= (y - t)(\sum_{j=0}^{n-1} y^{n-1} \\
&< \epsilon' n y^{n-1} \\
&= \epsilon,
\end{aligned}$$

and this is a contradiction. Therefore, y^n is not greater than x.

Now, if $y^n < x$, let ϵ be the positive number $x - y^n$, and choose a $\delta > 0$ such that $\delta < 1$ and $\delta < \epsilon/(y + 1)^n$. Then, using the Binomial Theorem, we have that

$$\begin{aligned}
(y + \delta)^n &= \sum_{k=0}^{n} \binom{n}{k} y^k \delta^{n-k} \\
&= y^n + \sum_{k=0}^{n-1} \binom{n}{k} y^k \delta^{n-k} \\
&= y^n + \delta \sum_{k=0}^{n-1} \binom{n}{k} y^k \delta^{n-1-k} \\
&< y^n + \delta \sum_{k=0}^{n} \binom{n}{k} y^k 1^{n-k} \\
&= y^n + \delta(y + 1)^n \\
&= x - \epsilon + \delta(y + 1)^n \\
&< x - \epsilon + \epsilon \\
&= x,
\end{aligned}$$

implying that $y + \delta \in S$. But this is a contradiction, since $y = \sup S$. Therefore, y^n is not less than x, and so $y^n = x$.

We have shown the existence of a positive nth root of x. To see the uniqueness, suppose y and y' are two positive nth roots of x. Then

$$\begin{aligned} 0 &= y^n - {y'}^n \\ &= (y - y')(\sum_{j=0}^{n-1} y^j {y'}^{n-j-1}, \end{aligned}$$

which implies that either $y - y' = 0$ or $\sum_{j=0}^{n-1} y^j {y'}^{n-j-1} = 0$. Since this latter sum consists of positive terms, it cannot be 0, whence $y = y'$. This shows that there is but one positive nth root of x, and the theorem is proved.

Exercise 1.22. (a) Show that if $n = 2k$ is an even natural number, then every positive real number has exactly two distinct nth roots.

(b) If $n = 2k + 1$ is an odd natural number, show that every real number has exactly one nth root.

(c) If n is a natural number greater than 1, prove that there is no rational number whose nth power equals 2, i.e., the nth root of 2 is not a rational number.

THE COMPLEX NUMBERS

It is useful to build from the real numbers another number system called the *complex numbers*. Although the real numbers $\mathbb{R}$ have many of the properties we expect, i.e., every positive number has a positive square root, every number has a cube root, and so on, there are somewhat less prominent properties that $\mathbb{R}$ fails to possess. For instance, negative numbers do not have square roots. This is actually a property that is missing in any ordered field, since every square is positive in an ordered field. See part (e) of Exercise 1.6. One way of describing this shortcoming on the part of the real numbers is to note that the equation $1 + x^2 = 0$ has no solution in the real numbers. Any solution would have to be a number whose square is -1, and no real number has that property. As an initial extension of the set of real numbers, why not build a number system in which this equation has a solution?

We faced a similar kind of problem earlier on. In the set $\mathbb{N}$ there is no element j such that $j + n = n$ for all $n \in \mathbb{N}$. That is, there was no element like 0 in the natural numbers. The solution to the problem in that case was simply to "create" something called zero, and just adjoin it to our set $\mathbb{N}$. The same kind of solution exists for us now. Let us invent an additional number, this time denoted by i, which has the property that its square i^2 is -1. Because the square of any nonzero real number is positive, this new number i was traditionally referred to as an "imaginary" number. We simply adjoin this number to the set $\mathbb{R}$, and we will then have a number whose square is negative, i.e., -1. Of course, we will require that our new number system should still be a field; we don't want to give up our basic algebraic operations. There are several implications of this requirement: First of all, if y is any real number, then we must also adjoin to $\mathbb{R}$ the number $y \times i \equiv yi$, for our new number system should be closed under multiplication. Of course the square of iy will equal $i^2y^2 = -y^2$, and therefore this new number iy must also be imaginary, i.e., not a real number. Secondly, if x and y are any two real numbers,

we must have in our new system a number called $x + yi$, because our new system should be closed under addition.

DEFINITION. Let i denote an object whose square $i^2 = -1$. Let $\mathbb{C}$ be the set of all objects that can be represented in the form $z = x + yi$, where both x and y are real numbers.

Define two operations $+$ and $\times$ on $\mathbb{C}$ as follows:

$$(x + yi) + (x' + y'i) = x + x' + (y + y')i,$$

and

$$(x + iy)(x' + iy') = xx' + xiy' + iyx' + iyiy' = xx' - yy' + (xy' + yx')i.$$

THEOREM 1.13.

(1) *The two operations $+$ and $\times$ defined above are commutative and associative, and multiplication is distributive over addition.*
(2) *Each operation has an identity: $(0 + 0i)$ is the identity for addition, and $(1 + 0i)$ is the identity for multiplication.*
(3) *The set $\mathbb{C}$ with these operations is a field.*

PROOF. We leave the proofs of Parts (1) and (2) to the following exercise. To see that $\mathbb{C}$ is a field, we need to verify one final condition, and that is to show that if $z = x+yi \neq 0 = 0+0i$, then there exists a $w = u+vi$ such that $z \times w = 1 = 1+0i$. Thus, suppose $z = x + yi \neq 0$. Then at least one of the two real numbers x and y must be nonzero, so that $x^2 + y^2 > 0$. Define a complex number w by

$$w = \frac{x}{x^2 + y^2} + \frac{-y}{x^2 + y^2}i.$$

We then have

$$\begin{aligned} z \times w &= (x + yi) \times (\frac{x}{x^2 + y^2} + \frac{-y}{x^2 + y^2}i \\ &= \frac{x^2}{x^2 + y^2} - \frac{-y^2}{x^2 + y^2} + (x\frac{-y}{x^2 + y^2} + y\frac{x}{x^2 + y^2})i \\ &= \frac{x^2 + y^2}{x^2 + y^2} + \frac{0}{x^2 + y^2}i \\ &= 1 + 0i \\ &= 1, \end{aligned}$$

as desired.

Exercise 1.23. Prove parts (1) and (2) of Theorem 1.13.

One might think that these kinds of improvements of the real numbers will go on and on. For instance, we might next have to create and adjoin another object j so that the number i has a square root; i.e., so that the equation $i - z^2 = 0$ has a solution. Fortunately and surprisingly, this is not necessary, as we will see when we finally come to the Fundamental Theorem of Algebra in Chapter VII.

The subset of $\mathbb{C}$ consisting of the pairs $x + 0i$ is a perfect (isomorphic) copy of the real number system $\mathbb{R}$. We are justified then in saying that the complex number system extends the real number system, and we will say that a real number x is the same as the complex number $x + 0i$. That is, real numbers are special kinds of complex numbers. The complex numbers of the form $0 + yi$ are called *purely imaginary numbers*. Obviously, the only complex number that is both real and purely imaginary is the number $0 = 0 + 0i$. The set $\mathbb{C}$ can also be regarded as a 2-dimensional space, a plane, and it is also helpful to realize that the complex numbers form a 2-dimensional vector space over the field of real numbers.

DEFINITION. If $z = x + yi$, we say that the real number x is the *real part* of z and write $x = \Re(z)$. We say that the real number y is the *imaginary part* of z and write $y = \Im(z)$.

If $z = x + yi$ is a complex number, define the *complex conjugate* $\bar{z}$ of z by $\bar{z} = x - yi$.

The complex number i satisfies $i^2 = -1$, showing that the negative number -1 has a square root in $\mathbb{C}$, or equivalently that the equation $1 + z^2 = 0$ has a solution in $\mathbb{C}$. We have thus satisfied our initial goal of extending the real numbers. But what about other complex numbers? Do they have square roots, cube roots, nth roots? What about solutions to other kinds of equations than $1 + z^2$?

Exercise 1.24. (a) Prove that every complex number has a square root.
HINT: Let $z = a + bi$. Assume $w = x + yi$ satisfies $w^2 = z$, and just solve the two equations in two unknowns that arise.

(b) Prove that every quadratic equation $az^2 + bz + c = 0$, for a, b, and c complex numbers, has a solution in $\mathbb{C}$.
HINT: If $a = 0$, it is easy to find a solution. If $a \neq 0$, we need only find a solution to the equivalent equation

$$z^2 + \frac{b}{a}z + \frac{c}{a} = 0.$$

Justify the following algebraic manipulations, and then solve the equation.

$$\begin{aligned} z^2 + \frac{b}{a}z + \frac{c}{a} &= z^2 + \frac{b}{a}z + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a} \\ &= (z + \frac{b}{2a})^2 - \frac{b^2}{4a^2} + \frac{c}{a}. \end{aligned}$$

What about this new field $\mathbb{C}$? Does every complex number have a cube root, a fourth root, does every equation have a solution in $\mathbb{C}$? A natural instinct would be to suspect that $\mathbb{C}$ takes care of square roots, but that it probably does not necessarily have higher order roots. However, the content of the Fundamental Theorem of Algebra, to be proved in Chapter VII, is that every equation of the form $P(z) = 0$, where P is a nonconstant polynomial, has a solution in $\mathbb{C}$. This immediately implies that every complex number c has an nth root, for any solution of the equation $z^n - c = 0$ would be an nth root of c.

The fact that the Fundamental Theorem of Algebra is true is a good indication that the field $\mathbb{C}$ is a "good" field. But it's not perfect.

THEOREM 1.14. *In no way can the field $\mathbb{C}$ be made into an ordered field. That is, there exists no subset P of $\mathbb{C}$ that satisfies the two positivity axioms.*

PROOF. Suppose $\mathbb{C}$ were an ordered field, and write P for its set of positive elements. Then, since every square in an ordered field must be in P (part (e) of Exercise 1.6), we must have that $-1 = i^2$ must be in P. But, by part (a) of Exercise 1.6, we also must have that 1 is in P, and this leads to a contradiction of the law of tricotomy. We can't have both 1 and -1 in P. Therefore, $\mathbb{C}$ is not an ordered field.

Although we may not define when one complex number is smaller than another, we can define the absolute value of a complex number and the distance between two of them.

DEFINITION. If $z = x + yi$ is in $\mathbb{C}$, we define the *absolute value* of z by

$$|z| = \sqrt{x^2 + y^2}.$$

We define the *distance* $d(z, w)$ between two complex numbers z and w by $d(z, w) = |z - w|$.

If $c \in \mathbb{C}$ and $r > 0$, we define the *open disk of radius r around c*, and denote it by $B_r(c)$, by

$$B_r(c) = \{z \in \mathbb{C} : |z - c| < r\}.$$

The *closed disk* of radius r around c is denoted by $\overline{B}_r(c)$ and is defined by

$$\overline{B}_r(c) = \{z \in \mathbb{C} : |z - c| \leq r\}.$$

We also define open and closed *punctured* disks $B'_r(c)$ and $\overline{B}'_r(c)$ around c by

$$B'_r(c) = \{z : 0 < |z - c| < r\}$$

and

$$\overline{B}'_r(c) = \{z : 0 < |z - c \leq r\}.$$

These punctured disks are just like the regular disks, except that they do not contain the central point c.

More generally, if S is any subset of $\mathbb{C}$, we define the *open neighborhood of radius r around S*, denoted by $N_r(S)$, to be the set of all z such that there exists a $w \in S$ for which $|z - w| < r$. That is, $N_r(S)$ is the set of all complex numbers that are within a distance of r of the set S. We define the *closed neighborhood* of radius r around S, and denote it by $\overline{N}_r(S)$, to be the set of all $z \in \mathbb{C}$ for which there exists a $w \in S$ such that $|z - w| \leq r$.

Exercise 1.25. (a) Prove that the absolute value of a complex number z is a nonnegative real number. Show in addition that $|z|^2 = z\bar{z}$.

(b) Let x be a real number. Show that the absolute value of x is the same whether we think of x as a real number or as a complex number.

(c) Prove that $\max(|\Re(z)|, |\Im(z)|) \leq |z| \leq |\Re(z)| + |\Im(z)|$. Note that this just amounts to verifying that

$$\max(|x|, |y|) \leq \sqrt{x^2 + y^2} \leq |x| + |y|$$

for any two real numbers x and y.

(d) For any complex numbers z and w, show that $\overline{z+w} = \bar{z}+\bar{w}$, and that $\bar{\bar{z}} = z$.

(e) Show that $z + \bar{z} = 2\Re(z)$ and $z - \bar{z} = 2i\Im(z)$.

(f) If $z = a + bi$ and $w = a' + b'i$, prove that $|zw| = |z||w|$.

HINT: Just compute $|(a + bi)(a' + b'i)|^2$.

The next theorem is in a true sense the most often used inequality of mathematical analysis. We have already proved the triangle inequality for the absolute value of real numbers, and the proof was not very difficult in that case. For complex numbers, it is not at all simple, and this should be taken as a good indication that it is a deep result.

THEOREM 1.15. (Triangle Inequality) If z and z' are two complex numbers, then

$$|z + z'| \leq |z| + |z'|$$

and

$$|z - z'| \geq ||z| - |z'||.$$

PROOF. We use the results contained in Exercise 1.25.

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

The Triangle Inequality follows now by taking square roots.

REMARK. The Triangle Inequality is often used in conjunction with what's called the "add and subtract trick." Frequently we want to estimate the size of a quantity like $|z-w|$, and we can often accomplish this estimation by adding and subtracting the same thing within the absolute value bars:

$$|z - w| = |z - v + v - w| \leq |z - v| + |v - w|.$$

The point is that we have replaced the estimation problem of the possibly unknown quantity $|z - w|$ by the estimation problems of two other quantities $|z - v|$ and $|v - w|$. It is often easier to estimate these latter two quantities, usually by an ingenious choice of v of course.

Exercise 1.26. (a) Prove the second assertion of the preceding theorem.

(b) Prove the Triangle Inequality for the distance function. That is, prove that

$$d(z, w) \leq d(z, v) + d(v, w)$$

for all $z, w, v \in \mathbb{C}$.

(c) Use mathematical induction to prove that

$$|\sum_{i=1}^{n} a_i| \leq \sum_{i=1}^{n} |a_i|.$$

It may not be necessary to point out that part (b) of the preceding exercise provides a justification for the name "triangle inequality." Indeed, part (b) of that exercise is just the assertion that the length of one side of a triangle in the plane is less than or equal to the sum of the lengths of the other two sides. Plot the three points z, w, and v, and see that this interpretation is correct.

DEFINITION. A subset S of $\mathbb{C}$ is called *Bounded* if there exists a real number M such that $|z| \leq M$ for every z in S.

Exercise 1.27. Let S be a subset of $\mathbb{C}$. Let S_1 be the subset of $\mathbb{R}$ consisting of the real parts of the complex numbers in S, and let S_2 be the subset of $\mathbb{R}$ consisting of the imaginary parts of the elements of S. Prove that S is bounded if and only if S_1 and S_2 are both bounded.
HINT: Use Part (c) of Exercise 1.25.

(b) Let S be the unit circle in the plane, i.e., the set of all complex numbers $z = x + iy$ for which $|z| = 1$. Compute the sets S_1 and S_2 of part (a).

Exercise 1.28. (a) Verify that the formulas for the sum of a geometric progression and the binomial theorem (Theorems 1.9 and 1.10) are valid for complex numbers z and z'.
HINT: Check that, as claimed, the proofs of those theorems work in any field.

(b) Prove Theorem 1.11 for complex numbers z and z'.