A.2 Construction of the Number Systems

The purpose of this section is to provide an outline of the logical development of our number systems—the natural numbers, integers, rational numbers, real numbers, and complex numbers. At best, we hope to whet the reader's appetite. We will only rarely attempt to give proofs for our statements. However, elsewhere in the text we study general constructions which include as special cases the construction of the rational numbers from the integers and the construction of the complex numbers from the real numbers.

In Chapter 1 we take a naive approach in working with the set of integers. We have assumed that the reader is willing to accept the familiar properties of the operations of addition and multiplication. However, it is possible to derive these properties from a very short list of postulates. They are called the "Peano postulates," formulated about the turn of the last century by Giuseppe Peano (1858–1932). A similar set of axioms was stated by Richard Dedekind at about the same time. These axioms provide a description of the natural numbers (nonnegative integers $0, 1, 2, \ldots$), denoted by $\mathbb{N}$.

We have chosen to take the language and concepts of set theory as the starting point of the development of the number systems. This means that the Peano postulates must be stated in set theoretic terms alone. Intuitively, to describe the natural numbers we begin with 0 and then list successive numbers. The process that extends the set from one natural number to the next can be described as a function, which we denote by S in the postulates. We have in mind the formula $S(m) = m + 1$, although the formula does not yet make sense since $+$ has not been defined. The third postulate is a statement of the principle of mathematical induction (see Section A.4).

A.2.1 Axiom (Peano postulates). *The system $\mathbb{N}$ of natural numbers is a set $\mathbb{N}$ with a distinguished element 0 and a function S from $\mathbb{N}$ into $\mathbb{N}$ which satisfies*

(i) *$S(n) \neq 0$ for all members n of $\mathbb{N}$,*

(ii) *$S(n_1) \neq S(n_2)$ for all members $n_1 \neq n_2$ of $\mathbb{N}$, and*

(iii) *any subset $\mathbb{N}'$ of $\mathbb{N}$ which contains 0 and which contains $S(n)$ for all n in $\mathbb{N}'$ must be equal to $\mathbb{N}$.*

The function S utilized in the Peano postulates is called the **successor function**. We will use it below to define addition and multiplication of natural numbers. Note that the assumption that S is a function means that it is possible to define the composition of S with itself n times, which we denote by S^n. We define S^0 to be the identity function.

A.2.2 Definition. *With the notation of the Peano postulates, let $m, n \in \mathbb{N}$.*

We define operations of addition and multiplication on $\mathbb{N}$ as follows:

$$m + n = S^n(m) \quad \text{and} \quad m \cdot n = (S^m)^n(0).$$

We define $m \geq n$ if the equation $m = n + x$ has a solution $x \in \mathbb{N}$.

It is possible to derive the basic arithmetic and order properties of the natural numbers from the Peano postulates, but that is beyond the scope of what we have set out to do. After defining the integers $\mathbb{Z}$ in terms of $\mathbb{N}$, it is then possible to extend properties of $\mathbb{N}$ to $\mathbb{Z}$. This indication of how the properties which are listed in Section A.3 can be proved is as much detail as we can provide without digressing.

In Section 1.1 we take the well-ordering principle to be an axiom. Here we show that it is a direct consequence of the Peano postulates. In Section A.4 we show that the well-ordering principle implies the principles of mathematical induction, and so the well-ordering principle is logically equivalent to induction. The last sentence of the proof of the following theorem depends on the nontrivial fact that $\{m \in \mathbb{N} \mid n < m < S(n)\}$ is empty.

A.2.3 Theorem (Well-Ordering Principle). *Any nonempty set of natural numbers contains a smallest element.*

Proof. (Outline) Let T be a nonempty subset of $\mathbb{N}$ and let L be the set of natural numbers x such that $x \leq t$ for all $t \in T$. We cannot have $L = \mathbb{N}$ since there is some natural number t in T, and then $t + 1 = S(t)$ is not in L. (We are making use of the function S from the Peano postulates.) This means that L cannot satisfy the assumptions of postulate (iii), and since we certainly have $0 \in L$, there must be some n in L with $S(n) \notin L$. Thus we have $n \leq t$ for all $t \in T$, and to finish the proof we only need to show that $n \in T$. If this were not the case, then in fact $n < t$ for all $t \in T$, and therefore $S(n) \leq t$ for all $t \in T$, a contradiction. □

The next step is to use natural numbers to define the set of integers. We can do this by considering ordered pairs of natural numbers. We know that any negative integer can be expressed (in many ways) as a difference of natural numbers. To avoid the use of subtraction, which is as yet undefined, we consider the set $\mathbb{N} \times \mathbb{N}$, where an ordered pair (a, b) in $\mathbb{N} \times \mathbb{N}$ is thought of as representing $a - b$.

Just as with fractions, there are many ways in which a particular integer can be written as the difference of two natural numbers. For example, $(0, 2)$, $(1, 3)$, $(2, 4)$, etc., all represent what we know should be -2. We need a notion of equivalence of ordered pairs, and since we know that we should have $a - b = c - d$ if and only if $a + d = c + b$, we can avoid the use of subtraction in the definition. The formulas given below for addition and multiplication are motivated by the fact that we know that we should get $(a - b) + (c - d) = (a + c) - (b + d)$ and $(a - b)(c - d) = (ac + bd) - (ad + bc)$. If we were going to prove all of our assertions, we would have to show that the definitions of addition and multiplication of integers do not depend on the particular ordered pairs of natural numbers which we choose to represent them.

A.2.4 Definition. *The set of* ***integers****, denoted by* $\mathbb{Z}$*, is defined via the set* $\mathbb{N} \times \mathbb{N}$*, where we specify that ordered pairs* (a, b) *and* (c, d) *are equivalent if and only if* $a + d = b + c$*.*

We define addition and multiplication of ordered pairs as follows:

$$(a, b) + (c, d) = (a + c, b + d) \qquad \textit{and} \qquad (a, b)(c, d) = (ac + bd, ad + bc) \ .$$

It is possible to verify all of the properties of $\mathbb{Z}$ that are listed in Section A.3, using the above definitions and the properties of $\mathbb{N}$. Furthermore, the set $\mathbb{N}$ can be identified with the set of ordered pairs (a, b) such that $a \geq b$, and so we can view $\mathbb{N}$ as the set of nonnegative integers. The well-ordering principle can easily be extended to the statement that any set of integers that is bounded below must contain a smallest element.

The next step is to construct the set of rational numbers $\mathbb{Q}$ from the set of integers. This is a special case of a general construction given in Section 5.4, where detailed proofs are provided.

A.2.5 Definition. *The set of* ***rational numbers****, denoted by* $\mathbb{Q}$*, is defined via the set of ordered pairs* (m, n) *such that* $m, n \in \mathbb{Z}$ *and* $n > 0$*, where we agree that* (a, b) *is equivalent to* (c, d) *if and only if* $ad = bc$*. We define addition and multiplication as follows:*

$$(a, b) + (c, d) = (ad + bc, bd) \qquad \textit{and} \qquad (a, b)(c, d) = (ac, bd) \ .$$

It is more difficult to describe the construction of the set of real numbers from the set of rational numbers. The Greeks used a completely geometric approach to real numbers, and initially considered numbers to be simply the ratios of lengths of line segments. However, the length of a diagonal of a square with sides of length 1 cannot be expressed as the ratio of two integer lengths, since $\sqrt{2}$ is not a rational number. This makes it necessary to introduce irrational numbers.

A sequence $\{a_n\}_{n=1}^{\infty}$ of rational numbers is said to be a **Cauchy sequence** if for each $\epsilon > 0$ there exists N such that $|a_n - a_m| < \epsilon$ for all $n, m > N$. It is then possible to define the set of **real numbers** $\mathbb{R}$ as the set of all Cauchy sequences of rational numbers, where such sequences are considered to be equivalent if the limit of the difference of the sequences is 0. To verify all of the properties of the real numbers is then quite an involved process.

We note only a few of the properties of real numbers: $\mathbb{R}$ is a field (see Section 4.1 for the definition and properties of a field) ordered by $\leq$. The set $\mathbb{Q}$ is dense in $\mathbb{R}$, in the sense that between any two distinct real numbers there is a rational number. Any set of real numbers that has a lower bound has a greatest lower bound, and any set that has an upper bound has a least upper bound. The **Archimedean property** holds; i.e., for any two positive real numbers a, b there exists an integer n such that $na > b$.

Finally, the set $\mathbf{C}$ of **complex numbers** is described in Section A.5. One method of construction is to use Kronecker's theorem, Theorem 4.3.8. An alternative is to consider ordered pairs of real numbers. Then addition and multiplication are defined as follows:

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc) .$$

The ordered pair (a, b) is usually written $a + bi$, where $i^2 = -1$.

Detailed proofs of the assertions in this section can be found in various text books such as those by Landau and by Cohen and Ehrlich. The construction of the real numbers from the rationals is usually viewed as a part of analysis rather than algebra.

A.3 Basic Properties of the Integers

We assume that the reader is familiar with the arithmetic and order properties of the integers, and indeed, we have freely used these properties throughout the book. In the interest of completeness we now explicitly list these properties, as well as their names.

A.3.1 (Properties of Addition).
(a) Closure: *Given any two integers a and b, there is a unique integer $a + b$.*
(b) Associativity: *Given integers a, b, c, we have $(a + b) + c = a + (b + c)$.*
(c) Commutativity: *Given integers a, b, we have $a + b = b + a$.*
(d) Zero element: *There exists a unique integer 0 such that $a + 0 = a$ for any integer a.*
(e) Inverses: *Given an integer a, there exists a unique integer, denoted by $-a$, such that $a + (-a) = 0$.*

A.3.2 (Properties of Multiplication).
(a) Closure: *Given any two integers a and b, there is a unique integer $a \cdot b = ab$.*
(b) Associativity: *Given integers a, b, c, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
(c) Commutativity: *Given integers a, b, we have $a \cdot b = b \cdot a$.*
(d) Identity element: *There exists a unique integer $1 (\neq 0)$ such that $a \cdot 1 = a$ for any integer a.*

A.3.3 (Joint Property of Addition and Multiplication).
Distributivity: *Given integers a, b, c, we have $a(b + c) = ab + ac$.*

A.3.4 (Properties of Order). *There exists a subset $\mathbb{Z}^+ \subset \mathbb{Z}$, called the* set of positive integers, *which satisfies the following properties:*
(a) Closure under addition: *If $a, b \in \mathbb{Z}^+$, then $a + b \in \mathbb{Z}^+$.*
(b) Closure under multiplication: *If $a, b \in \mathbb{Z}^+$, then $ab \in \mathbb{Z}^+$.*
(c) Trichotomy: *Given $a \in \mathbb{Z}$, exactly one of the following holds:*
(i) $a \in \mathbb{Z}^+$, (ii) $a = 0$, (iii) $-a \in \mathbb{Z}^+$.

A number of these properties are redundant. Our purpose is to provide a working knowledge of the system of integers, and so we have not given the most economical list of properties. Rather than investigating the foundations of the number systems, we will be content with simply making the following statement: Together with the well-ordering principle, the above list of thirteen properties completely characterizes the set of integers.

The following proposition lists some of the usual arithmetic properties of the set of integers. These properties hold in a more general setting, which is studied in Chapter 5. We will use the notation $a - b$ for $a + (-b)$.

A.3.5 Proposition. *Let $a, b, c \in \mathbb{Z}$.*
(a) *If $a + b = a + c$, then $b = c$.*
(b) $-(-a) = a$.
(c) $a \cdot 0 = 0$.
(d) $(-a)(-b) = ab$.

We introduce the usual order symbols as follows. We say that a is greater than b, denoted by $a > b$, if $a - b \in \mathbb{Z}^+$. For $a > b$ we also write $b < a$ (read "b is less than a"), and $a \geq b$ (read "a is greater than or equal to b") denotes that $a = b$ or $a > b$. Finally, the absolute value of a, denoted by $|a|$, is equal to a if $a \in \mathbb{Z}^+$ or $a = 0$ and is equal to $-a$ if $-a \in \mathbb{Z}^+$. The proof of the next proposition is left as an exercise.

A.3.6 Proposition. *Let $a, b, c \in \mathbb{Z}$.*
(a) *If $a > 0$, then $a \geq 1$.*
(b) *If $a > b$ and $b > c$, then $a > c$.*
(c) *If $a > b$, then $a + c > b + c$.*
(d) *$a < 0$ if and only if $-a \in \mathbb{Z}^+$.*
(e) *If $a > b$ and $c > 0$, then $ac > bc$.*
(f) *If $a > b$ and $c < 0$, then $ac < bc$.*
(g) *$|a| \geq 0$, and $|a| = 0$ if and only if $a = 0$.*
(h) *If $a > 0$, then $|b| \leq a$ if and only if $-a \leq b \leq a$.*
(k) $|ab| = |a||b|$.
(m) $|a + b| \leq |a| + |b|$.
(n) *If $ab = ac$ and $a \neq 0$, then $b = c$.*

A.4 Induction

If one develops the natural numbers from the Peano postulates, then mathematical induction is taken to be one of the postulates. On the other hand, if one uses the list of properties given in Section A.3 as a starting point, then the well-ordering