Chapter 1

Natural Numbers

“In die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.” “God made the natural numbers; all else is the work of man.” Leopold Kronecker (1886)

In mathematics, the natural numbers 1, 2, 3, ... are, arguably, the most familiar objects. Moreover, the system of natural numbers is fundamental in constructing other number systems and developing advanced concepts in mathematics. The main question addressed in this chapter is: How do we define the natural numbers?

There are two principally different approaches to the problem of defining natural numbers.

First, there is an axiomatic approach. In the framework of this approach, three compelling axioms called the “Peano Axioms” are introduced. It is also postulated that there exists an algebraic structure satisfying these axioms. Next all basic properties of natural numbers are deduced from these axioms. Under this approach you are not told what the natural numbers are but rather what you can do with them.

Second, the natural numbers can be constructed as sets using concepts and tools of set theory. An algebraic structure based on these numbers satisfies the Peano Axioms.

We begin by introducing a Peano system as an algebraic structure satisfying three axioms in Section 1.1. In the three consequent sections, main elements of what is usually called the “Peano arithmetic” are presented. Operations of addition and multiplication, order relations, and their properties are introduced in these sections.

In Section 1.5, we prove that any two Peano systems are isomorphic, that is, they are indistinguishable in some precise sense. The proof of this important fact is
more involved than proofs in the previous sections. The reader may find it better to skip the proof and return to it after studying the reminder of this chapter.

A particular set-theoretic model of natural numbers is presented in Section 1.6. It is, arguably, the most popular model among other models suggested for the natural numbers.

Recursion is a common method of defining terms in mathematics and computer science. It is also known as the method of “inductive definition”. The “Recursion Theorem” and its applications are subjects of Section 1.7, which is followed by Section 1.8 where we discuss the main instances of “proofs by mathematical induction”.

Number systems considered in the book are based on algebraic structures satisfying certain conditions. The Peano system \( \langle N, s, 1 \rangle \) is one of these systems. Two other examples of algebraic structures are introduced in Section 1.9.

In this and the consequent chapters, we use the word “informally” when we present facts or examples which cannot be described within the context of the formal material under consideration. The purpose of these insertions is to provide the reader with an intuitive background of formal theories.

1.1. Peano Systems

Informally, we “construct” the list of natural numbers

\[ 1, 2, 3, \ldots \]

by starting with number 1 and taking successive successors, 2, 3, and so on. Here, a successor of a natural number \( n \) is the “next” natural number \( n + 1 \). One can also argue that this list is infinite because “we can always add 1 to a natural number and obtain the next natural number”. The notions of “1” and “successor” are undefined primitive concepts of the theory that is presented in this and the next three sections.

**Definition 1.1.** Let \( N \) be a nonempty set, 1 an element of \( N \), and \( s \) a function from \( N \) into \( N, s : N \to N \). A triple \( \langle N, s, 1 \rangle \) is said to be an algebraic structure. The set \( N \) and the element 1 are called the underlying set and the distinguished element of the algebraic structure \( \langle N, s, 1 \rangle \), respectively.

An algebraic structure \( \langle N, s, 1 \rangle \) is called a Peano system if the following conditions are satisfied:

\[ \text{P1. } s(a) \neq 1 \text{ for all } a \in N. \]

\[ \text{P2. } s(a) = s(b) \text{ implies } a = b \text{ for all } a, b \in N. \]

\[ \text{P3. (Axiom of Induction) If } M \text{ is a subset of } N \text{ such that } \]
\[ \qquad \text{a) } 1 \in M, \text{ and } \]
\[ \qquad \text{b) } a \in M \text{ implies } s(a) \in M, \]
\[ \text{then } M = N. \]

If \( \langle N, s, 1 \rangle \) is a Peano system, then \( s \) is called the successor function. Conditions P1–P3 are called Peano Axioms.
1.1. Peano Systems

Note that 1 is merely a symbol for the distinguished element of a Peano system. A different symbol may be selected for a distinguished element of an algebraic structure.

Example 1.2. a) Let \( N = \{a\} \) be a singleton. Clearly, \( a \) is the only choice for the distinguished element and \( s \) must be the identity function in the algebraic structure \( \langle N, s, a \rangle \). This structure satisfies Peano Axioms \( \text{P2} \) and \( \text{P3} \), but does not satisfy Axiom \( \text{P1} \).

b) Let \( N = \{a, b\} \) be a pair and \( s : N \rightarrow N \) a constant function: \( s(x) = b \) for all \( x \in N \). Then \( \langle N, s, a \rangle \) is an algebraic structure satisfying Peano Axioms \( \text{P1} \) and \( \text{P3} \), but not \( \text{P2} \).

c) For \( N = \{a, b\} \), let \( s : N \rightarrow N \) be defined by \( s(a) = b, s(b) = a \). The algebraic structure \( \langle N, s, a \rangle \) satisfies Axioms \( \text{P2} \) and \( \text{P3} \). It does not satisfy Axiom \( \text{P1} \).

Informal examples of Peano systems are found in Exercise 4. We call these examples “informal” because they use number systems that themselves form the subject matter of this book. Formal examples will be given in Section 1.6.

Let \( \langle N, s, 1 \rangle \) be a Peano system. The following two theorems are the first illustrations of the methods that are used in establishing properties of Peano systems.

Theorem 1.3. \( s \) is a bijection from \( N \) onto \( N \setminus \{1\} \).

Proof. By Axiom \( \text{P1} \), \( 1 \notin s(N) \), and by Axiom \( \text{P2} \), \( s \) is a one-to-one function. To prove that \( s \) is a bijection we need to show that \( s(N) = N \setminus \{1\} \).

Let \( M = s(N) \cup \{1\} \). Clearly, \( 1 \in M \). If \( a \in M \), then \( a \in N \) because \( M \subseteq N \). Therefore, \( s(a) \in s(N) \subseteq M \). By Axiom \( \text{P3} \), \( M = N \), that is, \( s(N) \cup \{1\} = N \). Because \( 1 \notin s(N) \) we have \( s(N) = N \setminus \{1\} \), as required.

Theorem 1.3 asserts that any element of the set \( N \) different from 1 is a successor of another element of \( N \). Put it differently: every element \( b \neq 1 \) in \( N \) has a predecessor in \( N \), that is, an element \( a \) such that \( b = s(a) \).

Theorem 1.4. For every \( a \in N \), \( s(a) \neq a \).

Proof. Let \( M = \{a \in N : s(a) \neq a\} \). By Axiom \( \text{P1} \), \( 1 \in M \). By Axiom \( \text{P2} \), \( a \neq b \) implies \( s(a) \neq s(b) \) for all \( a, b \in N \). Therefore, \( s(a) \neq a \) implies \( s(s(a)) \neq s(a) \) for all \( a \in N \). Hence, \( s(a) \in M \) for every \( a \in M \). By the Axiom of Induction (Axiom \( \text{P3} \)), \( M = N \), that is, \( s(a) \neq a \) for all \( a \in N \).

Two remarks are in order. First, we define the subset \( M \) of the set \( N \) in the proof of Theorem 1.4 by means of the Axiom of Specification (Axiom A.3 in Section A.1). This is how most of sets are defined in the rest of the book.

Second, it is clear that the Axiom of Induction is crucial for the proofs of the two foregoing theorems. It also plays an instrumental role in establishing most results in this chapter.

Because the natural numbers are necessary for the development of other number systems, we adopt a simple assumption.
**Axiom 1.1.** (Axiom of Infinity.) There exists a Peano system.

It follows from Theorem 1.3 that the set \( N \) in a Peano system \( \langle N, s, 1 \rangle \) is an infinite set (cf. Section A.4). Thus Axiom 1.1 implies existence of infinite sets. (For this reason it is called “Axiom of Infinity”.)

### 1.2. Addition

In this and the next two sections, \( \langle N, s, 1 \rangle \) is a fixed Peano system. (Such a system exists by the Axiom of Infinity.)

As in some other places in the book, we begin this section with an informal discussion based on the reader’s prior experience with the natural numbers \( 1, 2, 3 \ldots \). An interpretation for the components of the Peano system \( \langle N, s, 1 \rangle \) is that the underlying set \( N \) is the set \( \{1, 2, 3, \ldots, n, \ldots\} \), the successor \( s(n) \) of \( n \) is the next number following \( n \), that is, \( n + 1 \), and the distinguished element is the natural number 1. By applying these interpretations and usual properties of the addition operation, we obtain the identities

\[
    n + 1 = s(n),
\]

for all natural numbers \( n \), and

\[
    n + s(m) = n + (m + 1) = (n + m) + 1 = s(n + m),
\]

for all natural numbers \( n \) and \( m \).

In a formal setting, the following theorem asserts that the two displayed identities completely characterize a binary operation on the underlying set \( N \) of the Peano system \( \langle N, s, 1 \rangle \).

**Theorem 1.5.** There exists a unique binary operation \( + \) on \( N \) such that

\[
    (1.1) \quad a + 1 = s(a), \quad \text{for all } a \in N
\]

and

\[
    (1.2) \quad a + s(b) = s(a + b), \quad \text{for all } a, b \in N.
\]

The unique binary operation \( + \), existence of which is asserted by Theorem 1.5, is called the operation of addition (on the underlying set \( N \)). The element \( a + b \) of \( N \) obtained by addition of \( b \) to \( a \) is called the sum of elements \( a \) and \( b \). Elements \( a \) and \( b \) in the sum \( a + b \) are called summands.

The ensuing proof of Theorem 1.5 is a more intricate application of the Axiom of Induction (Axiom P3) than in the proofs of Theorems 1.3 and 1.4. This is mainly due to the fact that we have to deal with two “arguments”, \( a \) and \( b \), of the operation of addition.

The key idea of the proof is to define the sum \( a + b \) “piecewise”, for a fixed \( a \) and an arbitrary \( b \) in the set \( N \). For this, we write \( a + b = f_a(b) \) where, for every \( a \in N \), \( f_a \) is a function \( f_a : N \to N \), and recast conditions (1.1) and (1.2), respectively, as follows:

\[
    (1.3) \quad f_a(1) = s(a), \quad \text{for every } a \in N,
\]
and

\[(1.4) \quad f_a(s(b)) = s(f_a(b)), \quad \text{for all } b \in N.\]

First we prove two lemmas which we need in the proof of Theorem 1.5.

**Lemma 1.6** (Uniqueness). *For every* \(a \in N\), *there is no more than one function* \(f_a\) *satisfying conditions (1.3) and (1.4).*

**Proof.** Suppose that for some \(a \in N\) there are functions \(f_a\) and \(g_a\) that satisfy conditions (1.3) and (1.4). Consider the set

\[M = \{b \in N : f_a(b) = g_a(b)\}.\]

We use the Axiom of Induction to show that \(M = N\), that is, the functions \(f_a\) and \(g_a\) are equal.

We have

\[f_a(1) \text{ by (1.3)} \quad \overset{\Rightarrow}{=} \quad f_a(s(a)) \text{ by (1.3)} \quad \overset{\Rightarrow}{=} \quad g_a(1).\]

Hence, \(1 \in M\).

Suppose \(b \in M\), so \(f_a(b) = g_a(b)\). Then

\[f_a(s(b)) \text{ by (1.4)} \quad \overset{\Rightarrow}{=} \quad f_a(s(f_a(b))) = s(g_a(b)) \text{ by (1.4)} \quad \overset{\Rightarrow}{=} \quad g_a(s(b)).\]

Therefore, \(s(b) \in M\). By the Axiom of Induction, \(M = N\). \(\square\)

**Lemma 1.7** (Existence). *For every* \(a \in N\), *there exists a function* \(f_a\) *satisfying conditions (1.3) and (1.4).*

**Proof.** Let \(M\) be the set of all elements \(a \in N\) for which there exists (a unique, by Lemma 1.6) function \(f_a : N \to N\) satisfying conditions (1.3) and (1.4).

For \(a = 1\), we verify that the function \(f_1\) defined by \(f_1(b) = s(b)\) for \(b \in N\), satisfies conditions (1.3) and (1.4):

\[f_1(1) = s(1),\]

so (1.3) holds, and

\[f_1(s(b)) = s(s(b)) = s(f_1(b)),\]

so (1.4) holds. Thus, \(1 \in M\).

Suppose now that \(a \in M\), that is, there is a unique function \(f_a\) satisfying conditions (1.3) and (1.4). We verify that the function \(f_{s(a)}\) defined by

\[(1.5) \quad f_{s(a)}(b) = s(f_a(b))\]

satisfies conditions (1.3) and (1.4):

\[f_{s(a)}(1) \text{ by (1.5)} \quad \overset{\Rightarrow}{=} \quad s(f_a(1)) \text{ by (1.3)} \quad \overset{\Rightarrow}{=} \quad f_a(s(a)),\]

so (1.3) holds for \(f_{s(a)}\), and

\[f_{s(a)}(s(b)) \text{ by (1.5)} \quad \overset{\Rightarrow}{=} \quad s(f_a(s(b))) \text{ by (1.4)} \quad \overset{\Rightarrow}{=} \quad f_a(s(f_a(b))) \text{ by (1.5)} \quad \overset{\Rightarrow}{=} \quad s(f_{s(a)}(b)),\]

so (1.4) holds for \(f_{s(a)}\). Thus, \(s(a) \in M\).

By the Axiom of Induction, \(M = N\), and the result follows. \(\square\)
Note that, informally, (1.5) has its roots in the identity
\[(m + 1) + n = (m + n) + 1\]
for the natural numbers \(m\) and \(n\).

Now we proceed with the proof of Theorem 1.5.

**Proof.** By Lemmas 1.6 and 1.7, for every \(a \in N\), there exists a unique function \(f_a : N \to N\) satisfying conditions (1.3) and (1.4). It is clear that the binary operation \(+\) on \(N\) defined by
\[a + b = f_a(b),\quad \text{for all } a, b \in N,\]
satisfies conditions (1.1) and (1.2).

Suppose that there is another binary operation, \(\oplus\), on \(N\) satisfying conditions (1.1) and (1.2), so
\[a \oplus 1 = s(a),\quad \text{for all } a \in N\]
and
\[a \oplus s(b) = s(a \oplus b),\quad \text{for all } a, b \in N.\]
We define \(g_a(b) = a \oplus b\) for \(a, b \in N\). The functions \(f_a\) and \(g_a\) satisfy conditions (1.3) and (1.4) for every \(a \in N\). By Lemma 1.6, \(g_a = f_a\) for all \(a \in N\), so \(a \oplus b = a + b\) for all \(a, b \in N\).

The assertion of Theorem 1.5 follows. \(\square\)

The next two theorems establish two main properties of the operation of addition.

**Theorem 1.8** (Associative Law of Addition).
\[(a + b) + c = a + (b + c)\]
for all \(a, b, c \in N\).

**Proof.** Let us fix elements \(a\) and \(b\) in \(N\), and let \(M\) be the set of all elements \(c\) in \(N\) for which (1.6) holds. We use the Axiom of Induction to prove that \(M = N\).

By conditions (1.1) and (1.2),
\[(a + b) + 1 = s(a + b) = a + s(b) = a + (b + 1).\]
Hence, \(1 \in M\).

Suppose (1.6) holds for some \(c \in M\). We have
\[(a + b) + s(c) = s((a + b) + c)\]
\[= s(a + (b + c)) = a + s(b + c) = a + (b + s(c)),\]
by (1.2) and (1.6). Hence, \(s(c) \in M\).

By the Axiom of Induction, (1.6) holds for all \(c \in N\). Because \(a\) and \(b\) are arbitrary elements of \(N\), the assertion of the theorem holds for all elements \(a, b,\) and \(c\) of the set \(N\). \(\square\)
From the Associative Law of Addition it follows that it does not matter how parentheses are inserted into the expression 
\[ a + b + c, \]
and hence they are often omitted (cf. Exercise 5).

**Theorem 1.9 (Commutative Law of Addition).**

(1.7) 
\[ a + b = b + a \]
for all \( a, b \in N \).

**Proof.** First, we use the Axiom of Induction to show that the equality 
\[ a + 1 = 1 + a \]
holds for all \( a \in N \).

Let \( M = \{a \in N : a + 1 = 1 + a\} \). Clearly, the displayed equality holds for \( a = 1 \), hence, \( 1 \in M \). Suppose that it holds for some \( a \in M \), that is, \( a + 1 = 1 + a \). Then we have
\[ s(a) + 1 = (a + 1) + 1 = (1 + a) + 1 = s(1 + a) = 1 + s(a), \]
by conditions (1.1) and (1.2). Therefore, \( s(a) \in M \). It follows that \( M = N \), that is, \( a + 1 = 1 + a \) for all \( a \in N \).

Next, we fix \( a \in N \) and consider the set 
\[ M = \{b \in N : a + b = b + a\}. \]

The element 1 belongs to \( M \) by the first part of the proof. Suppose \( b \) is an element of the set \( M \), that is, \( a + b = b + a \). In the following chain of equalities we use the identities from Theorem 1.5, the first part of the proof, and the Associative Law of Addition:
\[ a + s(b) = a + (b + 1) = (a + b) + 1 \]
\[ = 1 + (a + b) = 1 + (b + a) = (1 + b) + a \]
\[ = (b + 1) + a = s(b) + a. \]
Thus, \( s(b) \in M \). By the Axiom of Induction, (1.7) holds for every \( b \in N \). Because \( a \) is an arbitrary element of \( N \), (1.7) holds for all \( a, b \in N \). \( \square \)

We need the result of Lemma 1.10 to establish a fundamental property of the addition operation known as the *Trichotomy Law of Addition*.  

**Lemma 1.10.** For all \( a, b \in N \), 
\[ a + b \neq b. \]

**Proof.** Fix \( a \in N \) and define \( M = \{b \in N : a + b \neq b\} \). We have \( 1 \in M \) because, by (1.1) and Axiom P1,
\[ a + 1 = s(a) \neq 1. \]

Suppose \( b \in M \), that is, \( a + b \neq b \). Then we have 
\[ a + s(b) = s(a + b) \neq s(b), \]
by \((1.2)\) and Axiom \(\textbf{P2}\). Hence, \(b \in M\) implies \(s(b) \in M\). By the Axiom of Induction, \(M = N\). Because \(a\) is an arbitrary element of \(N\), we conclude that \(a + b \neq b\) for all \(a, b \in N\).

\[\square\]

**Theorem 1.11** (Trichotomy Law of Addition). For any two elements \(a\) and \(b\) in \(N\), one and only one of the following statements holds:

1) \(a = b\).

2) There is \(m \in N\) such that \(a = b + m\).

3) There is \(n \in N\) such that \(b = a + n\).

**Proof.** By Lemma 1.10, cases 1) and 2), as well as 1) and 3), are mutually exclusive. By the same lemma, cases 2) and 3) are mutually exclusive, because otherwise we would have

\[a = b + m = (a + n) + m = a + (n + m),\]

by the Associative Law of Addition.

Therefore we can have at most one of the cases 1), 2), or 3). Let us fix \(a\) and let \(M\) be the set of all elements \(b\) for which one (and only one) of these cases holds.

In order to show that \(M = N\), we use the Axiom of Induction.

For \(b = 1\), we have case 1) if \(a = 1\). If \(a \neq 1\), then, by Theorem 1.3, there is \(m \in N\) such that \(a = s(m)\). Therefore, by property (1.1) and the Commutative Law of Addition,

\[a = s(m) = m + 1 = 1 + m,\]

that is, the statement in case 2) holds. It follows that \(1 \in M\).

Let \(b\) be an element of \(M\), that is, one and only one of the statements 1), 2), or 3) of the theorem holds. We consider the three possibilities separately.

Case \(a = b\). We have

\[s(b) = b + 1 = a + 1,\]

so we have case 3) for \(s(b)\).

Case \(a = b + m\). If \(m = 1\), then \(a = b + 1 = s(b)\), so we have case 1) for \(s(b)\). Otherwise, by Theorem 1.3, there is \(k \in N\) such that \(m = s(k)\). Then, by applying property (1.1) and the Commutativity and Associativity Laws of Addition, we have

\[a = b + s(k) = b + (k + 1) = b + (1 + k) = (b + 1) + k = s(b) + k,\]

which is case 2) for \(s(b)\).

Case \(b = a + n\). By property (1.2), we have

\[s(b) = s(a + n) = a + s(n),\]

that is, case 3) for \(s(b)\).

In all three cases, we demonstrated that \(s(b) \in M\). By the Axiom of Induction, \(M = N\). Because \(a\) is an arbitrary element of \(N\), the assertion of the theorem follows. \[\square\]
1.3. Multiplication

In this section we often use properties of the operation of addition without explicitly referring to them.

Informally, we have the following properties of products of natural numbers:

\[ m \cdot 1 = m \]

and

\[ m \cdot (n + 1) = m \cdot n + m. \]

It turns out that these properties completely characterize a binary operation on the underlying set \( N \) of a Peano system \( \langle N, s, 1 \rangle \).

**Theorem 1.12.** There exists a unique binary operation \( \cdot \) on \( N \) such that

\[ a \cdot 1 = a, \quad \text{for all } a \in N \]  

and

\[ a \cdot s(b) = (a \cdot b) + a, \quad \text{for all } a, b \in N. \]

The unique binary operation \( \cdot \), the existence of which is asserted in Theorem 1.12, is called the operation of multiplication. The symbol \( \cdot \) is read times, and the element \( a \cdot b \) of \( N \) is called the product of \( a \) and \( b \). In what follows, we often write \( ab \) for \( a \cdot b \) and omit parentheses following the standard order of operations rules known from elementary algebra.

We use the same method as in the proof of Theorem 1.5, that is, we write \( a \cdot b = f_a(b) \) where, for every \( a \in N \), \( f_a \) is a function from \( N \) into \( N \). (Note that, of course, this function is not the same as in the previous section.) Then conditions (1.8) and (1.9) can be cast as follows (cf. (1.3) and (1.4), respectively).

For every \( a \in N \):

\[ f_a(1) = a \]  

and

\[ f_a(s(b)) = f_a(b) + a, \quad \text{for all } b \in N. \]

We prove two lemmas similar to the uniqueness and existence lemmas (Lemmas 1.6 and 1.7, respectively) established for the addition operation.

**Lemma 1.13** (Uniqueness). For every \( a \in N \), there is no more than one function \( f_a \) satisfying conditions (1.10) and (1.11).

**Proof.** Suppose \( f_a \) and \( g_a \) are functions satisfying conditions (1.10) and (1.11) for some \( a \in N \). Let

\[ M = \{ b \in M : f_a(b) = g_a(b) \}. \]

We have \( 1 \in M \) because

\[ f_a(1) = a = g_a(1), \]

by (1.10).
Suppose \( b \in M \), that is, \( f_a(b) = g_a(b) \). Then we have
\[
f_a(s(b)) = f_a(b) + a = g_a(b) + a = g_a(s(b)),
\]
by (1.11). Hence, \( s(b) \in M \).

By the Axiom of Induction, \( M = N \), hence the functions \( f_a \) and \( g_a \) are identical. \( \square \)

**Lemma 1.14** (Existence). For every \( a \in N \), there exist a function \( f_a \) satisfying conditions (1.10) and (1.11).

**Proof.** Let \( M \) be the set of all elements \( a \in N \) for which there exists (a unique, by Lemma 1.13) function \( f_a : N \to N \) satisfying condition (1.10) and condition (1.11).

For \( a = 1 \), we verify that the function \( f_1 \) defined by \( f_1(b) = b \) for \( b \in N \), satisfies conditions (1.10) and (1.11):
\[
f_1(1) = 1,
\]
so (1.10) holds, and
\[
f_1(s(b)) = s(b) = b + 1 = f_1(b) + 1,
\]
so (1.11) holds. Thus, \( 1 \in M \).

Suppose now that \( a \in M \), that is, there exists a unique function \( f_a \) satisfying conditions (1.10) and (1.11). We verify that the function \( f_{s(a)} \) defined by
\[
f_{s(a)}(b) = f_a(b) + b, \quad \text{for all } b \in N,
\]
satisfies conditions (1.10) and (1.11):
\[
f_{s(a)}(1) = f_a(1) + 1 = a + 1 = s(a),
\]
so (1.10) holds, and
\[
f_{s(a)}(s(b)) \overset{(1.12)}{=} f_a(s(b)) + s(b) \overset{(1.11) \text{ for } f_a}{=} f_a(b) + a + s(b)
\]
\[
= f_a(b) + s(a + b) = f_a(b) + s(b + a)
\]
\[
= f_a(b) + b + s(a) \overset{(1.11) \text{ for } f_a}{=} f_a(s(a)) + s(a),
\]
so (1.11) holds. Hence, \( a \in M \) implies \( s(a) \in M \).

By the Axiom of Induction, \( M = N \), and the result follows. \( \square \)

Note that, informally, we obtain (1.12) from the usual distributivity property
\[
(m + 1) \cdot n = m \cdot n + n,
\]
for natural numbers \( m \) and \( n \).

As in the proof of Theorem 1.5 the assertion of Theorem 1.12 follows immediately from Lemmas 1.13 and 1.14 (cf. Exercise 7).

**Theorem 1.15** (Right Distributive Law).

(1.13) \((a + b)c = ac + bc,
\)
for all \( a, b, c \in N \).
1.3. Multiplication

Proof. Let us fix \( a, b \in \mathbb{N} \) and define \( M = \{ c \in \mathbb{N} : (a + b)c = ac + bc \} \).

We have
\[
(a + b) \cdot 1 \quad \text{by (1.8)} \quad a + b \quad \text{by (1.8)} \quad a \cdot 1 + b \cdot 1.
\]
Hence, \( 1 \in M \).

Suppose \( c \in M \), that is, \( (a + b)c = ac + bc \). Then, by using the Associativity and Commutativity Laws of Addition, we obtain
\[
(a + b)s(c) \quad \text{by (1.9)} \quad (a + b)c + (a + b) = (ac + bc) + (a + b)
\]
\[
= (ac + a) + (bc + b) \quad \text{by (1.9)} \quad as(c) + bs(c).
\]
Hence, \( s(c) \in M \). By the Axiom of Induction, \( M = \mathbb{N} \). Because \( a \) and \( b \) are arbitrary elements of \( \mathbb{N} \), (1.13) holds for all \( a, b, c \in \mathbb{N} \). \( \square \)

Theorem 1.16 (Commutative Law of Multiplication).

(1.14)
\[ ab = ba, \]
for all \( a, b \in \mathbb{N} \).

Proof. First, we use the Axiom of Induction to prove the claim for \( a = 1 \). Let \( M = \{ b \in \mathbb{N} : 1 \cdot b = b \cdot 1 \} \). Clearly, \( 1 \in M \). If \( 1 \cdot b = b \cdot 1 \), then
\[
1 \cdot s(b) \quad \text{by (1.9)} \quad 1 \cdot b + 1 = b \cdot 1 + 1 \quad \text{by (1.8)} \quad b + 1 = s(b) \quad \text{by (1.8)} \quad s(b) \cdot 1.
\]
Hence, \( s(b) \in M \), that is, \( M = \mathbb{N} \). It follows that \( 1 \cdot b = b \cdot 1 \) for all \( b \in \mathbb{N} \).

Now we use the Axiom of Induction again to prove that \( ab = ba \) for a fixed \( b \in \mathbb{N} \). Let \( M = \{ a \in \mathbb{N} : ab = ba \} \). In the foregoing paragraph, we proved that \( 1 \in M \). If \( a \in M \), then \( ab = ba \) and we obtain, using the Right Distributive Law,
\[
s(a)b = (a + 1)b = ab + 1 \cdot b = ba + b \cdot 1 \quad \text{by (1.8)} \quad ba + b \quad \text{by (1.9)} \quad bs(a).
\]
Therefore, \( s(a) \in M \), and the claim of the theorem follows. \( \square \)

The result of the next theorem is an immediate consequence of two previous theorems.

Theorem 1.17 (Left Distributive Law).

(1.15)
\[ c(a + b) = ca + cb, \]
for all \( a, b, c \in \mathbb{N} \).

Theorem 1.18 (Associative Law of Multiplication).

(1.16)
\[ (ab)c = a(bc), \]
for all \( a, b, c \in \mathbb{N} \).

Proof. Let us fix \( a, b \in \mathbb{N} \) and consider the set
\[
M = \{ c \in \mathbb{N} : (ab)c = a(bc) \}.
\]
By (1.8), \( (ab) \cdot 1 = ab = a(b \cdot 1) \), so \( 1 \in M \).
1. Natural Numbers

Suppose \( c \in M \), that is, \((ab)c = a(bc)\). Then, by the Left Distributive Law, we have
\[
(ab)s(c) = (ab)c + ab = a(bc) + ab = a(bc + b) \quad \text{by (1.9) } a(bs(c)).
\]
It follows that \( s(c) \in M \). Hence, by the Axiom of Induction, \( M = N \). Because \( a \) and \( b \) are arbitrary elements of \( N \), the result follows. \( \Box \)

1.4. Order

Definition 1.19. For any \( a, b \in N \), we put:
\[
\begin{align*}
  a < b & \quad \text{if there is } n \in N \text{ such that } b = a + n, \\
  a \leq b & \quad \text{if } a < b \text{ or } a = b, \\
  a > b & \quad \text{if } b < a, \\
  a \geq b & \quad \text{if } b \leq a.
\end{align*}
\]
The binary relations \(<, \leq, >, \geq\) are called order relations on \( N \).

From Theorem 1.11 we immediately obtain the following result (cf. Exercise 13).

Theorem 1.20 (Trichotomy Law for \(<\)). For any \( a, b \in N \), exactly one of the three cases
\[
a < b, \quad a = b, \quad b < a
\]
holds.

Another important property of the relation \(<\) is its transitivity.

Theorem 1.21 (Transitive Law for \(<\)). For any \( a, b, c \in N \),
\[
\text{if } \ a < b \text{ and } b < c, \text{ then } a < c.
\]
Proof. If \( a < b \) and \( b < c \), then, by (1.17), there are elements \( p \) and \( q \) of \( N \) such that \( b = a + p \) and \( c = b + q \). Hence, \( c = (a + p) + q = a + (p + q) \), and the result follows from the definition of \(<\) (cf. (1.17)). \( \Box \)

Because the relation \(<\) is transitive and satisfies the Trichotomy Law, it is a linear order (cf. Section A.3) on the set \( N \).

Theorem 1.22. For any \( a, b, c \in N \), if \( a < b \), then
\[
a + c < b + c \quad \text{and} \quad ac < bc.
\]
Proof. Because \( a < b \), there is \( n \in N \) such that \( b = a + n \). Hence, by the Associative and Commutative Laws,
\[
b + c = (a + n) + c = a + n + c = (a + c) + n,
\]
so \( a + c < b + c \).

Furthermore, by applying the Right Distributive Law,
\[
bc = (a + n)c = ac + nc.
\]
Therefore, \( ac < bc \). \( \Box \)
Recall that \( s(a) = a+1 \) for any \( a \in \mathbb{N} \), by (1.1). The following theorem justifies the name “successor” for \( s(a) \).

**Theorem 1.23.** For any \( a \in \mathbb{N} \), there is no element \( b \in N \) such that
\[
a < b < a+1.
\]
(We write \( a < b < c \) if \( a < b \) and \( b < c \).)

**Proof.** The proof is by contradiction. Suppose there is \( b \) such that \( a < b \) and \( b < a+1 \). We have \( b = a + n \) for some \( n \in \mathbb{N} \), because \( a < b \).

Suppose that \( n = 1 \). Then we have \( a + 1 = b < a + 1 \), which contradicts the Trichotomy Law (Theorem 1.20).

If \( n \neq 1 \), then there is \( m \) such that \( n = s(m) = m + 1 \), so
\[
b = a + n = a + (m + 1) = (a + 1) + m.
\]
This implies \( a + 1 < b \), which contradicts our assumption that \( b < a + 1 \) (again by the Trichotomy Law). \( \square \)

**Definition 1.24.** Let \( M \) be a nonempty subset of \( \mathbb{N} \). An element \( a \in M \) is called a *least* element of \( M \) if \( a \leq b \) for all \( b \in M \). Likewise, \( a \in M \) is a *greatest* element of \( M \) if \( a \geq b \) for all \( b \in M \).

If a subset of the set \( \mathbb{N} \) has a least (or greatest) element, then this element is unique (cf. Exercise 15).

Note that 1 is the least element of \( \mathbb{N} \) (cf. Exercise 17a)). On the other hand, there is no greatest element of \( \mathbb{N} \) because \( a + 1 > a \) for any \( a \in \mathbb{N} \) (cf. Exercise 16).

**Theorem 1.25** (Well-Ordering Principle). Any nonempty subset of \( \mathbb{N} \) has a least element.

**Proof.** Let \( P \) be a nonempty subset of \( \mathbb{N} \). We define
\[
M = \{ a \in \mathbb{N} : a \leq b, \text{ for all } b \in P \}.
\]
The set \( M \) is not empty because \( 1 \in M \) (cf. Exercise 17a). Furthermore, \( M \neq \mathbb{N} \). Indeed, for any \( b \in P \), \( b + 1 > b \), so \( b + 1 \notin M \).

It follows that there is \( a \in M \) such that \( s(a) = a + 1 \notin M \), because otherwise we would have \( M = \mathbb{N} \), by the Axiom of Induction.

The element \( a \) belongs to the set \( P \). Indeed, otherwise, \( a < b \) for all \( b \in P \) which implies (by Exercise 17b) \( a + 1 \leq b \) for all \( b \in P \). But this contradicts our choice of \( a \).

Because \( a \in M \) and \( a \in P \), it is a least element of \( P \). \( \square \)

### 1.5. Isomorphism of Peano Systems

Let \( \mathbb{N} \) be a set, \( s \) a function from \( \mathbb{N} \) into \( \mathbb{N} \), and 1 an element of \( \mathbb{N} \). Recall (cf. Definition 1.1) that a triple \( \langle \mathbb{N}, s, 1 \rangle \) is called an *algebraic structure* on the underlying set \( \mathbb{N} \) with a *distinguished element* \( 1 \in \mathbb{N} \). A *Peano system* is an algebraic structure satisfying axioms \( \text{P1–P3} \).
**Definition 1.26.** Two algebraic structures \( \langle N, s, 1 \rangle \) and \( \langle N', s', 1' \rangle \) are said to be *isomorphic* if there is a bijection, that is, a one-to-one and onto function \( f : N \rightarrow N' \) such that
\[
\begin{align*}
1.18 & \quad f(1) = 1', \\
1.19 & \quad f(s(a)) = s'(f(a)), \quad \text{for all } a \in N.
\end{align*}
\]
The function \( f \) is said to be an *isomorphism* of \( \langle N, s, 1 \rangle \) onto \( \langle N', s', 1' \rangle \).

The identity in (1.19) is illustrated by the diagram:
\[
\begin{array}{ccc}
N & \xrightarrow{f} & N' \\
\downarrow s & & \downarrow s' \\
N & \xrightarrow{f} & N'
\end{array}
\]

Because functions \( s, s', \) and \( f \) satisfy the identities in (1.19), the diagram is said to be *commutative*.

The proof of the following theorem is straightforward and left as an exercise (cf. Exercise 23).

**Theorem 1.27.** A bijection \( f : N \rightarrow N' \) is an isomorphism of \( \langle N, s, 1 \rangle \) onto \( \langle N', s', 1' \rangle \) if and only if
\[
\begin{align*}
b = s(a) & \quad \text{implies} \quad f(b) = s'(f(a)) \quad \text{for all } a, b \in N \\
b' = s'(a') & \quad \text{implies} \quad f^{-1}(b') = s(f^{-1}(a')) \quad \text{for all } a', b' \in N'.
\end{align*}
\]

The following example illustrates the role of Axiom P3 in the definition of a Peano system.

**Example 1.28.** Let \( \langle N, s, 1 \rangle \) be an algebraic structure satisfying Axioms P1 and P2. The function \( s \) is a one-to-one function from \( N \) into \( N \setminus \{1\} \), that is, it is a bijection from \( N \) onto \( s(N) \) which is a proper subset of \( N \). Hence, \( N \) is an infinite set (cf. Theorem 1.3). Let \( Q \) be a nonempty set such that \( N \cap Q = \emptyset \) and let \( N' = N \cup Q \). Consider an algebraic structure \( \langle N', s', 1 \rangle \) with the underlying set \( N' \), the same distinguished element 1, and the function \( s' : N' \rightarrow N' \) defined by
\[
s'(a) = \begin{cases} 
s(a), & \text{for } a \in N; \\
a, & \text{for } a \in Q.
\end{cases}
\]
It is not difficult to verify that the new structure satisfies Axioms P1 and P2 and is not isomorphic to the structure \( \langle N, s, 1 \rangle \) (cf. Exercise 24). Therefore, there are infinitely many nonisomorphic algebraic structures satisfying Axioms P1 and P2.

It is clear that Axiom P3 played a central role in establishing main results in Sections 1.1–1.4, where fundamentals of the Peano arithmetic are presented. In view of Example 1.28, it is not surprising that the Axiom of Induction (Axiom P3) also plays a crucial role in the proof of the next theorem.

**Theorem 1.29.** Any two Peano systems \( \langle N, s, 1 \rangle \) and \( \langle N', s', 1' \rangle \) are isomorphic.
1.5. Isomorphism of Peano Systems

Before presenting the proof of the theorem, we reformulate conditions (1.18) and (1.19) in order to give the reader a clue to the construction in the proof.

Recall that, by definition, a function \( f : \mathbb{N} \to \mathbb{N}' \) is a subset of the Cartesian product \( \mathbb{N} \times \mathbb{N}' \) with the property:

for every \( a \in \mathbb{N} \) there is a unique \( a' \in \mathbb{N}' \) such that \( (a, a') \in f \),

and that in this case we write \( a' = f(a) \) (cf. Section A.4).

In a set-theoretic notation, conditions (1.18) and (1.19) can be rewritten as follows:

(1.20) \( (1, 1') \in f \),

(1.21) \( (a, a') \in f \) implies \( (s(a), s'(a')) \in f \), \( \text{for all } a \in \mathbb{N}, a' \in \mathbb{N}' \),

respectively.

Now we proceed with the proof of Theorem 1.29.

Proof. Let us consider the family \( \mathcal{H} \) of subsets \( h \subseteq \mathbb{N} \times \mathbb{N}' \) such that

(1.22) \( (1, 1') \in h \),

(1.23) \( (a, a') \in h \) implies \( (s(a), s'(a')) \in h \), \( \text{for all } a \in \mathbb{N}, a' \in \mathbb{N}' \),

(cf. conditions (1.20) and (1.21)).

Note that the family \( \mathcal{H} \) is not empty because \( \mathbb{N} \times \mathbb{N}' \in \mathcal{H} \). We define \( f = \bigcap_{h \in \mathcal{H}} h \).

It is not difficult to see that \( f \in \mathcal{H} \), so \( f \) is the minimum set in \( \mathcal{H} \) with respect to the inclusion relation \( \subseteq \).

We want to show that \( f \) is the required isomorphism of the two Peano systems.

First, we prove that \( f \) is a function from \( \mathbb{N} \) into \( \mathbb{N}' \).

Let

\[ M = \{ a \in \mathbb{N} : \text{there is a unique } a' \in \mathbb{N}' \text{ such that } (a, a') \in f \} . \]

We use the Axiom of Induction to show that \( M = \mathbb{N} \) as required.

For this, we first show that \( 1 \in M \).

By (1.22), \( (1, 1') \in h \) for all \( h \in \mathcal{H} \). Hence, \( (1, 1') \in f \). Suppose there is \( b' \in \mathbb{N}' \) such that \( b' \neq 1' \) and \( (1, b') \in f \). Consider the set

\[ h' = f \setminus \{(1, b')\} . \]

It is clear that \( (1, 1') \in h' \), so (1.22) holds for \( h' \). Inasmuch as (1.23) holds for \( f \), it also holds for \( h' \), because \( (s(a), s'(a')) \neq (1, b') \) for any \( a \in \mathbb{N} \) and \( a' \in \mathbb{N}' \) (by Axiom P1, \( s(a) \neq 1 \) for any \( a \in \mathbb{N} \)). It follows that \( h' \in \mathcal{H} \), which contradicts the definition of \( f \) because \( h' \) is a proper subset of \( f \). We proved that \( 1 \in M \).

Now we prove that \( a \in M \) implies \( s(a) \in M \).

Let \( a \in M \), that is, there is a unique \( a' \in \mathbb{N}' \) such that \( (a, a') \in f \). By (1.23), \( (s(a), s'(a')) \in f \). Suppose there is \( b' \in \mathbb{N}' \) such that \( b' \neq s'(a') \) and \( (s(a), b') \in f \). Consider the set

\[ h' = f \setminus \{(s(a), b')\} . \]
It is clear that \((1,1') \in h'\), so \((1.22)\) holds for \(h'\). Next, we prove that \((1.23)\) also holds for \(h'\).

The proof is by contradiction. Suppose that there is a pair \((c,c') \in h'\) such that \((s(c),s'(c')) \notin h'\). Because \(h' \subseteq f\) and \(f\) satisfies condition \((1.23)\), we must have \((s(c),s'(c')) = (s(a),b')\). Then, \(s(c) = s(a)\) which implies \(c = a\), by Axiom \(\text{P2}\). By the assumption, there is a unique \(a' \in N'\) such that \((a,a') \in f\). Because \((c,c') \in h' \subseteq f\) and \(c = a\), we have \(c' = a'\). Therefore, \(b' = s'(c') = s'(a')\), which contradicts our assumption that \(b' \neq s'(a')\). We showed that for any pair \((c,c') \in h'\), the pair \((s(c),s'(c'))\) also belongs to \(h'\), so \((1.23)\) holds for \(h'\).

It follows that \(h'\) satisfies conditions \((1.22)\) and \((1.23)\). This contradicts the definition of the set \(f\) because \(h'\) is a proper subset of \(f\). Thus, \(s(a) \in M\).

By the Axiom of Induction, \(M = N\), that is, \(f\) is a function, \(f : N \to N'\). Note that \(f\) satisfies conditions \((1.20)\) and \((1.21)\) and therefore conditions \((1.18)\) and \((1.19)\).

It remains to show that \(f\) is a one-to-one function from \(N\) onto \(N'\), that is, for every \(a' \in N'\) there is a unique \(a \in N\) such that \((a,a') \in f\). We use conditions \((1.18)\) and \((1.19)\), and again the Axiom of Induction.

Let us define

\[ M = \{a' \in N' : \text{there is a unique } a \in N \text{ such that } f(a) = a'\}. \]

Suppose that there is a \(a \neq 1\) in \(N\) such that \(f(a) = 1'\). Then \(a = s(b)\) for some \(b \in N\), and we have, by \((1.19)\),

\[ 1' = f(a) = f(s(b)) = s'(f(b)), \]

which contradicts Axiom \(\text{P1}\). Because, \(f(1) = 1'\), by \((1.18)\), we conclude that \(1' \in M\).

Now suppose \(a' \in M\), so there is a unique \(a \in N\) such that \(f(a) = a'\). We proceed to show that there is a unique element \(b \in N\) such that \(f(b) = s'(a')\).

First, note that such an element exists because, by \((1.19)\),

\[ f(s(a)) = s'(f(a)) = s'(a'), \]

so we can take \(s(a)\) for \(b\).

Suppose \(f(b) = s'(a')\) for some \(b \neq s(a)\). Observe that \(b \neq 1\), because otherwise we would have \(1' = f(1) = s'(a')\), contradicting Axiom \(\text{P1}\). Therefore, there exists \(c \in N\) such that \(b = s(c)\). Thus, by \((1.19)\),

\[ s'(a') = f(b) = f(s(c)) = s'(f(c)). \]

By Axiom \(\text{P2}\), \(a' = f(c)\). By our assumption about \(a' \in M\), it follows that \(c = a\), that is, \(b = s(a)\). Hence, \(b = s(a)\) is the unique element in \(N\) such that \(f(b) = s'(a')\).

By Axiom of Induction, \(M = N'\), and the result follows. \(\square\)

The assertion of the following theorem is useful for showing that an algebraic structure is a Peano system.

**Theorem 1.30.** Let \(\langle N, s, 1 \rangle\) be a Peano system and let \(\langle N', s', 1' \rangle\) be an algebraic structure which is isomorphic to \(\langle N, s, 1 \rangle\). Then \(\langle N', s', 1' \rangle\) itself is a Peano system.
Proof. Let \( f : N \rightarrow N' \) be an isomorphism of algebraic structures \( \langle N, s, 1 \rangle \) and \( \langle N', s', 1' \rangle \). We verify that the Peano axioms hold for \( \langle N', s', 1' \rangle \) by using the characterizations of \( f \) in Theorem 1.27.

**Axiom P1.** Suppose \( s'(a') = 1' \). Then we have
\[
1 = f^{-1}(1') = s(f^{-1}(a')),
\]
which contradicts Axiom P1 for the Peano system \( \langle N, s, 1 \rangle \). Thus, \( s'(a') \neq 1' \) for all \( a' \in N' \).

**Axiom P2.** Suppose \( s'(a') = s'(b') \). Then, by Theorem 1.27, we have
\[
s(f^{-1}(a')) = s(f^{-1}(b')).
\]
By Axiom P2 for the Peano system \( \langle N, s, 1 \rangle \), we have \( f^{-1}(a') = f^{-1}(b') \), which implies \( a' = b' \) inasmuch as \( f \) is a bijection.

**Axiom P3.** Let \( M' \) be a subset of \( N' \) such that \( 1' \in N' \) and \( a' \in M' \) implies \( s'(a') \in M' \). Let \( M = f^{-1}(M') \). We have \( 1 \in M \) because \( 1 = f^{-1}(1') \) and \( 1' \in M' \). Furthermore, let \( a' \in M' \). We have \( a = f^{-1}(a') \in M \). By Theorem 1.27,
\[
f^{-1}(s'(a')) = s(f^{-1}(a')) = s(a).
\]
We have \( f^{-1}(s'(a')) \in M \) because \( (s'(a') \in M' \). Hence, \( s(a) \in M \). By Axiom P3 for the Peano system \( \langle N, s, 1 \rangle \), we have \( M = N \). It follows that
\[
M' = f(M) = f(N) = N'.
\]
Therefore, Axiom P3 holds for \( \langle N', s', 1' \rangle \). \( \square \)

### 1.6. A Set-Theoretic Model

According to the Axiom of Infinity, there exists at least one Peano system \( \langle N, s, 1 \rangle \). By Theorem 1.29, any two Peano systems are isomorphic. In this sense, there is “essentially” only one Peano system. In this section, we present a set-theoretic model of a Peano system.

For every set \( x \) we define the successor \( s(x) \) of \( x \) to be the set
\[
(1.24) \quad x \cup \{x\}.
\]
(As in Section A.1, we use small letters as symbols for some sets.) In other words, we expand the set \( x \) by adding the singleton \( \{x\} \) to \( x \). To construct natural numbers as sets, we need to start with a set representing number 1. An obvious possibility is to set \( 1 = \emptyset \) and define
\[
2 = s(1) = 1 \cup \{1\} = \emptyset \cup \{1\} = \{1\},
\]
\[
3 = s(2) = 2 \cup \{2\} = \{1\} \cup \{2\} = \{1, 2\},
\]
\[
4 = s(3) = 3 \cup \{3\} = \{1, 2\} \cup \{3\} = \{1, 2, 3\},
\]
and so on. The “and so on” means that we adopt the usual notation for natural numbers, so, for instance, we use numerals such as “6” or “1013” without any further explanation.

However, there is a big problem with this “and so on”, because from what was said it does not follow that this construction can be carried out ad infinitum. To
justify this process, we need another form of the Axiom of Infinity (cf. Axiom 1.1) now in the framework of set theory.

**Axiom 1.2 (Axiom of Infinity).** There exists a set containing the empty set $\emptyset$ and the successor of each of its elements.

We say that a set $A$ is *inductive* if $\emptyset \in A$ and if $x \cup \{x\} \in A$ whenever $x \in A$. Thus, Axiom 1.2 says that there exists an inductive set $A$. It is not difficult to show that the intersection of any family of inductive sets is itself an inductive set (cf. Exercise 27). Specifically, the intersection of all inductive sets included in the inductive set $A$ is an inductive set. We denote this set by $\mathbb{N}$ and use this notation throughout the book. The set $\mathbb{N}$ is a subset of any inductive set $B$. Indeed, if $B$ is an inductive set, then the set $A \cap B$ is an inductive subset of $A$. Hence, by definition, $\mathbb{N} \subseteq A \cap B \subseteq B$. Therefore, $\mathbb{N}$ is the minimum inductive set.

By definition, a *natural number* is an element of the set $\mathbb{N}$. It is clear, that sets 1, 2, 3, and 4 defined above are natural numbers (cf. Exercise 28). The notation $\mathbb{N} = \{1, 2, 3, \ldots\}$ is used very often. In this notation, ellipses $\ldots$ stand for “and so on” in our informal definition. Note that according to our definition, natural numbers are sets.

In the rest of this section, we show that the triple $(\mathbb{N}, s, 1)$, where the function $s$ is given by (1.24), is a Peano system, that is, that Axioms $P1$–$P3$ of Section 1.1 are satisfied.

**Axiom $P3$.** A subset $M$ of $\mathbb{N}$ satisfying conditions $P3a)$ and $P3b)$ is an inductive set. Hence, by the minimality property of $\mathbb{N}$, we have $M = \mathbb{N}$.

**Axiom $P1$.** Let $n$ be a natural number. The natural number $s(n) = n \cup \{n\}$ contains the element $\{n\} \neq \emptyset$. Therefore, $s(n) \neq 1 = \emptyset$.

**Axiom $P2$.** We need to prove that $m = n$ whenever $s(m) = s(n)$. For this we use the result of the following theorem.

**Theorem 1.31.** Let $n$ be a natural number. Every element $x$ of $n$ is a proper subset of $n$, that is,

$$x \in n \quad \text{implies} \quad x \subseteq n \text{ and } x \neq n, \quad \text{for every } x \in n.$$  

**Proof.** We define

$$M = \{n \in \mathbb{N} : x \subseteq n \text{ and } x \neq n, \text{ for every } x \in n\}$$

and use Axiom $P3$.

We have $1 \in M$ vacuously because $1 = \emptyset$ does not have proper subsets.

Let $n \in M$ and let $x \in n \cup \{n\}$ be an element of $s(n)$. Then either $x \in n$, or $x = n$. If $x \in n$, then $x \subseteq n$ and $x \neq n$, because $n \in M$. Hence, $x$ is a proper subset of $s(n) = n \cup \{n\}$. This is trivially true if $x = n$.

By Axiom $P3$, $M = \mathbb{N}$, hence the required result follows. \[ \square \]

Now we can validate Axiom $P2$ as follows. Suppose $s(m) = s(n)$, that is, $m \cup \{m\} = n \cup \{n\}$, for natural numbers $m$ and $n$. If $m \neq n$, then we must have
1.7. Recursion

$m \in n$ and $n \in m$. By Theorem 1.31, $m$ is a proper subset of $n$ and $n$ is a proper subset of $m$, which is impossible. This contradiction shows that $m = n$.

We proved that $(\mathbb{N},s,1)$, where $\mathbb{N}$ is the set of natural numbers, $s$ is the successor function defined by (1.24), and $1 = \emptyset$, is a Peano system. By Theorem 1.29, any other Peano system is isomorphic to $(\mathbb{N},s,1)$. For this reason, we use only this Peano system in the rest of the book.

CONVENTION. When we use the symbols $\mathbb{N}$, $s$, 1, we usually omit the explicit reference to the system $(\mathbb{N},s,1)$. Furthermore, we often write $n + 1$ for $s(n)$ (cf. Theorem 1.5).

Informal examples of Peano systems are presented in Exercise 4. Now we can give formal (that is, not involving any external structures) examples of these systems.

**Example 1.32.** (1) Let $m \in \mathbb{N}$ be a natural number and let

$$N = \{ n \in \mathbb{N} : n \geq m \}.$$

We denote the number $m$ by the symbol 1 and let $s$ be the operation of adding the natural number 1. The algebraic structure $(N,s,1)$ is a Peano system (cf. Exercise 39).

(2) Let $N$ be the set of even natural numbers (cf. Exercises 11 and 46). The symbol 1 denotes the number 2. Let $s$ be the operation of adding 2. The algebraic structure $(N,s,1)$ is a Peano system (cf. Exercise 39).

1.7. Recursion

In high school, a student has learned the definitions of the $n$th power of a real number $x$:

$$x^1 = x, \quad x^n = x \cdot x \cdot \cdots \cdot x, \quad \text{for } n > 1, \ n \in \mathbb{N},$$

and the sum of the arithmetic progression:

$$1 + 2 + 3 + \cdots + n, \quad \text{for } n > 1, \ n \in \mathbb{N}.$$

Clearly, one cannot write explicitly the product of $n$ factors or the sum of $n$ terms. To define the meaning of the above expressions, a so-called recursive form of a definition is invoked. For example, for a natural number $x$, the power $x^n$ is defined as follows:

$$x^1 = x,$$

$$x^{n+1} = x^n \cdot x, \quad \text{for every } n \in \mathbb{N}.$$

However, it is not immediately evident that this construction can be carried out ad infinitum and produce a unique correspondence $n \mapsto x^n$ (for a given $x \in \mathbb{N}$). Definitions of this kind are justified by the following theorem.

**Theorem 1.33** (Recursion Theorem). Let $S$ be a nonempty set, $c$ be a fixed element of $S$, and $g$ be a function $g : \mathbb{N} \times S \to S$. There exists a unique function $f : \mathbb{N} \to S$
such that

\begin{align}
(1.25) & \quad f(1) = c, \\
(1.26) & \quad f(s(n)) = g(n, f(n)), \quad \text{for all } n \in \mathbb{N}.
\end{align}

As in the proof of Theorem 1.29, we consider \( f \) as a subset of the Cartesian product \( \mathbb{N} \times S \) satisfying conditions

\begin{align}
(1.27) & \quad (1, c) \in f, \\
(1.28) & \quad (n, a) \in f \text{ implies } (s(n), g(n, a)) \in f, \text{ for all } n \in \mathbb{N}, a \in S.
\end{align}

which are equivalent (cf. Exercise 40) to conditions (1.25) and (1.26), respectively (cf. conditions (1.22) and (1.23)).

Now we prove Theorem 1.33.

**Proof.** (Existence.) Let \( \mathcal{H} \) be the family of subsets \( h \) of \( \mathbb{N} \times S \) such that

\begin{align}
(1.29) & \quad (1, c) \in h, \\
(1.30) & \quad (n, a) \in h \text{ implies } (s(n), g(n, a)) \in h, \text{ for all } n \in \mathbb{N}, a \in S.
\end{align}

This family is not empty because \( \mathbb{N} \times S \in \mathcal{H} \). We define

\[
\forall \, h \in \mathcal{H} \quad f = \bigcap h.
\]

It is clear that \( f \) satisfies conditions (1.29) and (1.30), so \( f \in \mathcal{H} \). Note that \( f \) is the minimum element of the family \( \mathcal{H} \) with respect to the inclusion relation \( \subseteq \) (cf. proof of Theorem 1.29).

We need to show that \( f \) is a function from \( \mathbb{N} \) into \( S \), that is, for every \( n \in \mathbb{N} \) there is a unique element \( a \in S \) such that \((n, a) \in f\).

Let

\[
M = \{ n \in \mathbb{N} : (n, a) \in f \text{ for exactly one } a \in S \}.
\]

To show that \( f \) is a function from \( \mathbb{N} \) into \( S \), it suffices to prove that \( M = \mathbb{N} \).

First, we show that \( 1 \in M \). Clearly, \((1, c) \in f \). Suppose that there is \( a \neq c \) in \( S \) such that we also have \((1, a) \in f \). Let \( h = f \setminus \{(1, a)\} \). This set belongs to the family \( \mathcal{H} \). Indeed, \((1, c) \in h \) because \( a \neq c \). For any \((n, b) \in h\) we have

\[
(s(n), g(n, b)) \neq (1, a),
\]

because \( s(n) \neq 1 \) (by Axiom P1). Inasmuch as \((s(n), g(n, b)) \in f \) (because \( f \in \mathcal{H} \)), we have \((s(n), g(n, b)) \in h = f \setminus \{(1, a)\} \). We proved that \( h \in \mathcal{H} \), which contradicts the minimality property of \( f \). It follows that \( a = c \), that is, \( c \) is the unique element of \( S \) such that \((1, c) \in f \). Hence, \( 1 \in M \).

Now we show that \( n \in M \) implies \( s(n) \in M \). If \( n \in M \), then there is a unique \( a \in S \) such that \((n, a) \in f \). Because \( f \in \mathcal{H} \), we have

\[
(s(n), g(n, a)) \in f.
\]

Suppose that there is \( b \neq g(n, a) \) in \( S \) such that \((s(n), b) \in f \) and define

\[
h = f \setminus \{(s(n), b)\}.
\]

We show that \( h \in \mathcal{H} \). First, observe that \((1, c) \in h \) because \((1, c) \in f \) and \((1, c) \neq (s(n), b) \) (since \( 1 \neq s(n) \) by Axiom P1). Now suppose \((m, d) \in h \) and
(s(m), g(m, d)) = (s(n), b), that is, s(m) = s(n) and g(m, d) = b. Because, s(m) = s(n), we have m = n by Axiom **P2**. Because (m, d) ∈ h ⊆ f, m = n, and n ∈ M, we have d = a. It follows that b = g(n, a), which contradicts our assumption that b \(\neq\) g(n, a). Hence, g(n, a) is the unique element in S such that (s(n), g(n, a)) ∈ f, so s(n) ∈ M.

By the Axiom of Induction (Axiom **P3**), it follows that M = N, that is, f is indeed a function from \(\mathbb{N}\) into S.

(Uniqueness.) We prove now that the function f defined by (1.31) is a unique function satisfying conditions (1.25) and (1.26).

Suppose that there is another function f′ satisfying the same conditions as f. Consider the set

\[ M = \{ n \in \mathbb{N} : f(n) = f'(n) \} \]

We have 1 ∈ M, because f(1) = c = f′(1).

Suppose n ∈ M, that is, f(n) = f′(n). Then, by (1.26),

\[ f(s(n)) = g(n, f(n)) = g(n, f'(n)) = f'(s(n)), \]

so s(n) ∈ M. The Axiom of Induction implies that M = N, that is, functions f and f′ are equal. □

The function f, whose existence and uniqueness is asserted in Theorem 1.33, is said to be defined **recursively** by conditions (1.25) and (1.26). In the next two examples, S = \(\mathbb{N}\), c is a fixed natural number, and f is the function from Theorem 1.33.

**Example 1.34.** Let g(n, a) = a · c. Then the function f is defined by

\[ f(1) = c, \]
\[ f(n + 1) = f(n) · c, \quad \text{for every } n \in \mathbb{N}. \]

This is a recursive definition of the exponential function \(c^n\). It is easy to verify that \(c^2 = c · c, c^3 = c · c · c,\) and so on.

**Example 1.35.** Let d be a natural number and g(n, a) = a + d. We have

\[ f(1) = c, \]
\[ f(n + 1) = f(n) + d, \quad \text{for every } n \in \mathbb{N}. \]

Here we obtained a recursive definition of the arithmetic progression:

\[ c, c + d, c + 2d, c + 3d, \ldots. \]

Note the order of operations in the above expressions—we write, for instance, \(c + 2d\) for \(c + (2 · d)\) (cf. Exercise 47).

The next example gives a different definition of the exponential function (cf. Example 1.34).

**Example 1.36.** Let us define functions h on \(\mathbb{N}\) and g on \(\mathbb{N} \times \mathbb{N}\) by h(m) = m and g(m, n) = n · m, respectively. By the result of Exercise 43, there exists a unique
function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, which we denote $f(m, n) = m^n$, that satisfies conditions:

\[
m^{1} = m, \quad \text{for any } m \in \mathbb{N}, \\
m^{n+1} = (m^n) \cdot m, \quad \text{for any } m, n \in \mathbb{N}.
\]

The Recursion Theorem and its other forms (cf. Exercises 42 and 43) have many applications in mathematics. As an example we consider the concept of extended sum.

**Definition 1.37.** A *sequence* in a set $S$ is a function $h$ from the set of natural numbers $\mathbb{N}$ into the set $S$. This sequence is also denoted by

\[(h(1), h(2), \ldots, h(k), \ldots) \quad \text{or by} \quad (h(k))_{k \in \mathbb{N}}.\]

Elements of a sequence are called its *terms*. If the $k$th term $h(k)$ is denoted by $x_k$, then we also denote the sequence by $(x_1, x_2, \ldots, x_k, \ldots)$ or by $(x_k)_{k \in \mathbb{N}}$.

Let $(x, y) \mapsto x \oplus y$ be a binary operation on $S$ (that is, a mapping from $S \times S$ into $S$). In order to define expressions of the form

\[x_1 \oplus x_2 \oplus \cdots \oplus x_n,
\]

we use the Recursive Theorem. Note that we write $n + 1$ for $s(n)$ below.

**Definition 1.38.** Let $\oplus$ be a binary operation on $S$ and let $(x_1, x_2, \ldots, x_k, \ldots)$ be a sequence of elements of $S$. For every $n \in \mathbb{N}$ we denote by

\[
\sum_{k=1}^{n} x_k
\]

the element of $S$ uniquely determined by the following conditions:

\[
\sum_{k=1}^{1} x_k = x_1, \quad (1.32)
\]

\[
\sum_{k=1}^{n+1} x_k = \left( \sum_{k=1}^{n} x_k \right) \oplus x_{n+1}. \quad (1.33)
\]

In words, $\sum_{k=1}^{n} x_k$ is the (generalized) sum of the first $n$ terms of the sequence $(x_1, x_2, \ldots, x_k, \ldots)$.

This definition is justified as follows. Let $h : \mathbb{N} \to S$ be the function that defines the sequence $(x_1, x_2, \ldots, x_k, \ldots)$, that is, $x_k = h(k)$ for every $k \in \mathbb{N}$. We set $c = x_1$ and define a function $g : \mathbb{N} \times S \to S$ by

\[g(n, a) = a \oplus h(n + 1), \quad \text{for all } n \in \mathbb{N} \text{ and } a \in S.
\]

By the Recursion Theorem, there is a unique function $f : \mathbb{N} \to S$ such that $f(1) = c$ and $f(n + 1) = g(n, f(n))$ for all $n \in \mathbb{N}$. One can immediately verify that

\[
\sum_{k=1}^{n} x_k = f(n), \quad \text{for } n \in \mathbb{N},
\]

satisfies conditions (1.32) and (1.33).
In the rest of this section, $S$ is the set of natural numbers $\mathbb{N}$.

As an immediate application of Definition 1.38, we consider the case when $\oplus$ is the addition operation on $\mathbb{N}$. For example, let us compute the sum $\sum_{k=1}^{3} x_k$:

$$\sum_{k=1}^{3} x_k = (\sum_{k=1}^{2} x_k) + x_3 = \left( \left( \sum_{k=1}^{1} x_k \right) + x_2 \right) + x_3 = (x_1 + x_2) + x_3.$$  

By the Associative Law of Addition, we can write

$$\sum_{k=1}^{3} x_k = x_1 + x_2 + x_3.$$

We obtain another application of Definition 1.38 by considering the set of natural numbers with the multiplication operation on it. It is customary to use the symbol $\prod$ for $\sum$ in this case. Thus $\prod_{k=1}^{n} x_k$ is the natural number uniquely determined by the conditions:

$$\prod_{k=1}^{1} x_k = x_1,$$

$$\prod_{k=1}^{n+1} x_k = \left( \prod_{k=1}^{n} x_k \right) \cdot x_{n+1}, \quad \text{for every } n \in \mathbb{N}.$$  

**Example 1.39.** The product of the first $n$ natural numbers is the *factorial* function $n!$:

$$\prod_{k=1}^{n} k = n!.$$  

The function $n!$ is also defined recursively by

$$1! = 1,$$

$$(n + 1)! = n! \cdot (n + 1), \quad \text{for every } n \in \mathbb{N}.$$  

**Example 1.40.** Let $c$ be a natural number. It can be easily verified that

$$\prod_{k=1}^{n} c = c^n$$

(cf. Example 1.34).

Very often, the generalized sums and products are written in the following forms:

$$\sum_{k=1}^{n} x_k = x_1 + x_2 + \cdots + x_n \quad \text{and} \quad \prod_{k=1}^{n} x_k = x_1 \cdot x_2 \cdot \cdots \cdot x_n,$$

respectively.

Some important properties of generalized sums and products are found in Exercises 48–50.
1.8. Mathematical Induction

The Axiom of Induction (Axiom P3) played a central role in establishing properties of natural numbers in this chapter. It is also the basis of an important proof method called Proof by Induction.

We begin with an example.

Example 1.41. Suppose that we want to prove that

$$2^n > n,$$

for every $n \in \mathbb{N}$.

It is not difficult to verify that the inequality holds for small natural numbers. Indeed,

$$2^1 = 2 > 1, \quad 2^2 = 4 > 2, \quad 2^3 = 8 > 3, \quad \ldots .$$

To prove the inequality for all natural numbers $n$, we use the Axiom of Induction. Let $M$ be the set of all natural numbers $n$ for which the inequality $2^n > n$ holds. Clearly, $1 \in M$. Suppose $k \in M$, that is, $2^k > k$. We have

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot k = k + k \geq k + 1.$$ 

Hence, $s(k) = k + 1 \in M$. By the Axiom of Induction, $M = \mathbb{N}$, so the inequality $2^n > n$ holds for every natural number $n$.

The argument in the foregoing paragraph can be presented in a different way. Let $P(n)$ be the property of a natural number $n$ stating that $n < 2^n$. Then (cf. the Axiom of Specification, Section A.1)

$$M = \{n \in \mathbb{N} : P(n) \text{ is true}\}.$$ 

We proved that $n < 2^n$ holds for all $n \in \mathbb{N}$ by showing that

(i) $P(1)$ is true, and

(ii) $P(k)$ is true implies $P(k + 1)$ is true, for all $k \in \mathbb{N}$.

In fact, this is quite a general way of using the Axiom of Induction as the following theorem demonstrates.

Theorem 1.42 (Principle of Mathematical Induction). Let $(\mathbb{N}, s, 1)$ be a Peano system and $P(a)$ be a property pertinent to an element $a \in \mathbb{N}$. If

1. $P(1)$ is true, and
2. $P(a)$ is true implies $P(s(a))$ is true, for all $a \in \mathbb{N},$

then $P(a)$ is true for every element $a \in \mathbb{N}$.

Proof. By the Axiom of Specification (cf. Section A.1), the set

$$M = \{a \in \mathbb{N} : P(a) \text{ is true}\}$$

exists and uniquely defined. By (1.34), $1 \in M$, and by (1.35), $a \in M$ implies $s(a) \in M$. Hence, by the Axiom of Induction, $M = \mathbb{N}$, that is, $P(a)$ is true for all $a \in \mathbb{N}$. □

The case of the Peano system $(\mathbb{N}, s, 1)$ is a typical application of the Principle of Mathematical Induction (cf. Example 1.41). In order to prove that a certain property $P(n)$ is true for every natural number $n$ by the method of mathematical
induction, we first check that $P(1)$ is true (cf. (1.34)). This is called the **base case**. Next comes the **induction step**, that is, we assume that $P(k)$ is true for some $k \in \mathbb{N}$ (the **induction hypothesis**) and show that $P(k+1)$ is true as well (cf. (1.35)).

It is important to realize that the validity of the induction step does not necessarily depend on the truth of $P(k)$. This is why the statement “$P(k)$ is true” is called a hypothesis. The next example illustrates the point.

**Example 1.43.** Let $P(n)$ be the statement “$n = n + 1$”. Suppose “$k = k + 1$” is true for some natural number $k$. Then

$$k + 1 = (k + 1) + 1.$$ 

We proved that the truth of $P(k)$ does imply the truth of $P(k+1)$. However, it is clear that both statements are false.

Example 1.43 also demonstrates the importance of the base case. Indeed, $P(1)$ does not hold.

We emphasize one more time that in the inductive step we only prove the implication:

“if $P(k)$ is true for some $k \in \mathbb{N}$, then $P(k+1)$ is true”

without establishing the truthfulness of either $P(k)$ or $P(k+1)$.

**Figure 1.** Sums of consecutive odd numbers.

**Example 1.44.** The drawings in Fig. 1 are geometric “proofs” of the equalities:

$$1 + 3 = 2^2, \quad 1 + 3 + 5 = 3^2, \quad 1 + 3 + 5 + 7 = 4^2.$$ 

These equalities suggest the identity

$$\sum_{i=1}^{n}(2i-1) = n^2, \quad \text{for all } n \in \mathbb{N},$$

which we want to prove by induction. In this context, the property $P(n)$ of a natural number $n$ is “$\sum_{i=1}^{n}(2i-1) = n^2$”. For the base case, $P(1)$ is true because $1 = 1^2$. Suppose that

$$\sum_{i=1}^{k}(2i-1) = k^2 \quad \text{holds for some } k \in \mathbb{N}.$$ 

We have

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + (2k+1) = k^2 + 2k + 1 = (k+1)^2$$
(cf. Exercise 10), that is, \( P(k + 1) \) is true. By the Principle of Mathematical Induction, \( P(n) \) is true for every \( n \in \mathbb{N} \).

Sometimes the following form of the Principle of Mathematical Induction is more useful.

**Theorem 1.45.** Let \( P(n) \) be a property pertinent to a natural number \( n \) and \( m \) be a natural number. If
\[
(1.36) \quad P(m) \text{ is true, and}
\]
\[
(1.37) \quad P(k) \text{ is true implies } P(k + 1) \text{ is true, for all } k \geq m,
\]
then \( P(n) \) is true for every \( n \in \mathbb{N} \) such that \( n \geq m \).

**Proof.** It suffices to apply the result of Theorem 1.42 to the Peano system \( \langle N, s, 1 \rangle \) with \( N = \{ n \in \mathbb{N} : n \geq m \} \), \( s : n \mapsto n + 1 \), and the symbol “1” standing for the natural number \( m \). \( \Box \)

As in the case of ordinary induction (Theorem 1.42), the proof of the statement \( P(m) \) (1.36) is called the *base step* of the induction, and the proof of the implication in (1.37) is called the *induction step*.

**Example 1.46.** We use Theorem 1.45 to prove that
\[
2^n > 2n + 1, \quad \text{for all } n \geq 3.
\]
In this case, the property \( P(n) \) states that \( 2^n > 2n + 1 \). The base case, \( P(3) \), holds because \( 2^3 = 8 > 7 = 2 \cdot 3 + 1 \).

Suppose \( 2^k > 2k + 1 \) for some natural number \( k \geq 3 \). Then we have
\[
2^{k+1} = 2 \cdot 2^k = 2^k + 2^k > (2k + 1) + 2 = 2(k + 1) + 1,
\]
by the induction hypothesis and the inequality \( 2^k = 2 \cdot 2^{k-1} > 2 \) which obviously holds for \( k \geq 3 \). This completes the induction step of the proof.

Note that the statements \( P(1) \) (\( 2 > 3 \)) and \( P(2) \) (\( 4 > 5 \)) are false.

In some problems, the following principle of induction is more potent.

**Theorem 1.47** (Strong Principle of Induction). Let \( P(n) \) be a property pertinent to a natural number \( n \) and let \( q \) be a fixed natural number. If, for each \( m \in \mathbb{N} \), \( P(k) \) is true for all \( q \leq k < m \) implies \( P(m) \) is true, then \( P(n) \) is true for every natural number \( n \geq q \).

**Proof.** Let \( N = \{ n \in \mathbb{N} : n \geq q \} \). We note that \( P(q) \) is true because the induction hypothesis
\[
"P(k) \text{ is true for } q \leq k < q"
\]
is vacuous. Hence, the set \( A = \{ n \in N : P(n) \text{ is true} \} \) contains number \( q \). Suppose \( A \neq N \). Then the set \( B = N \setminus A \) is not empty. By the Well-Ordering Principle (Theorem 1.25), \( B \) has the least element, say, \( m \). Note that \( m > q \) because \( q \notin B \). Therefore, all numbers \( k < m \) belong to the set \( A \). By the induction hypothesis, \( P(m) \) is true, so \( m \in A \). Because we cannot have \( m \in B \) and \( m \in A \), we obtained a contradiction which completes the proof. \( \Box \)
Example 1.48. A natural number \( n \) is said to be \textit{composite} if it is a product of two natural numbers each of which is different from 1. A natural number \( p > 1 \) is said to be \textit{prime} if it is not composite. We use the method of strong induction with \( q = 2 \) to show that any natural number greater than 1 is either prime or a product of prime numbers.

The property \( P(n) \) states “\( n > 1 \) is either prime or a product of primes”. Suppose \( P(k) \) is true for all \( 2 \leq k < m \). There are two mutually exclusive cases:

Case 1. \( m \) is a prime number. Then \( P(m) \) is true and we are done.

Case 2. \( m \) is a composite number. Then it is a product of two natural numbers each of which is different from 1. By the induction hypothesis each of these two numbers is a product of primes. It follows that \( m \) itself is a product of primes, that is, \( P(m) \) holds.

By Theorem 1.47, the result follows.

More examples of the method of mathematical induction are found at the end of this chapter in the Exercises section (Exercises 53–61).

1.9. Algebraic Structures

An algebraic structure was defined in Section 1.1 as a triple \( \langle N, s, 1 \rangle \), where \( N \) is a nonempty set, \( s \) is a function \( s : N \rightarrow N \), and 1 is a distinguished element of the set \( N \). The structure \( \langle N, s, 1 \rangle \) is an instance of a general notion of an algebraic structure. In abstract algebra, an algebraic structure is a nonempty set endowed with a family of operations and relations on it. For example, in the structure \( \langle N, s, 1 \rangle \), the function \( s \) is an unary operation on \( N \), and the distinguished element 1 is a nullary operation on \( N \), “select 1” (cf. Section A.4). An example of a different kind of algebraic structure is the pair \( \langle N, + \rangle \), where \( + \) is the addition operation on the set of natural numbers \( N \). In abstract algebra, \( \langle N, + \rangle \) is an instance of a \textit{commutative semigroup}. The algebraic structure \( \langle N, \cdot, 1 \rangle \) is an example of a \textit{commutative monoid}. Here are the formal definitions:

Definition 1.49. Let \( S \) be a set and \( \circ \) be a binary operation on \( S \). The pair \( \langle S, \circ \rangle \) is said to be a \textit{semigroup} if \( \circ \) is an associative operation, that is,

\[
(a \circ b) \circ c = a \circ (b \circ c),
\]

for all \( a, b, c \in S \).

If \( e \in S \) is an element such that

\[
e \circ a = a \circ e,
\]

for all \( a \in S \),

then the algebraic structure \( \langle S, \circ, e \rangle \) is called a \textit{monoid} with the \textit{identity element} \( e \).

If, in addition, \( \circ \) is a commutative operation, that is,

\[
a \circ b = b \circ a,
\]

for all \( a, b \in S \),

then the structures \( \langle S, \circ \rangle \) and \( \langle S, \circ, e \rangle \) are called a \textit{commutative semigroup} and a \textit{commutative monoid}, respectively.

It can be readily verified that the algebraic structures \( \langle N, + \rangle \) and \( \langle N, \cdot, 1 \rangle \) are indeed instances of a commutative semigroup and a commutative monoid, respectively (cf. Exercise 64).
1. Natural Numbers

We do not give a formal definition of an algebraic structure here. However, more examples of algebraic structures are found in the rest of the book.

Notes

Kronecker’s dictum in the epigraph to this chapter is a quotation from Heinrich Weber’s necrologue to Leopold Kronecker (1823–1891) which appeared in Weber (1893). One may consider the Axiom of Infinity (Axiom 1.1) as a formalization of Kronecker’s dictum.

Peano Axioms were first formulated by Richard Dedekind (1831–1913) in 1887 (see English translation in Dedekind, 1963). Giuseppe Peano (1858–1932) said as much in the preamble of his 1889 paper.

Peano Axioms, P1–P3, “characterize the natural numbers, in the sense that all reasoning about natural numbers may be reduced or rewritten in such a way that the only assumptions one needs are the Peano axioms” (Gowers, 2008, p. 259). Thus our approach to the natural numbers is not constructive. We do not tell the reader what the numbers are, but rather explain what one can do with them. This “axiomatic definition” of the natural numbers is similar to the definitions in the Euclidean geometry where points and lines are defined by their properties rather than constructively.

Conditions (1.1), (1.2) and (1.8), (1.9) serve as “inductive definitions” of the operations of addition and multiplication, respectively. These and only these conditions are used in establishing all properties of the unique operations “+” and “·”. An important remark is in order. The proofs of Theorems 1.5–1.9 and 1.12–1.18 use only the Axiom of Induction (Axiom P3). Therefore the operations of addition and multiplications are uniquely defined by conditions (1.1), (1.2) and (1.8), (1.9) in algebraic structures more general than Peano systems. An algebraic structure \( \langle N, s, 1 \rangle \) is called a induction system (alternatively, a recursion system) if it satisfies the Axiom of Induction. Clearly, a Peano system is an induction system. However, the converse is not true as illustrated by Example 1.2. The results of Theorems 1.5–1.9 and 1.12–1.18 hold in any induction system (cf. Exercises 65–67).

Note that we make no assumptions about the nature of the set \( S \) in the Recursion Theorem (Theorem 1.33). Hence examples considered in Section 1.7 are valid in all number systems presented later in the book.

Formally, we should use a different symbol for the function \( \sum_{k=1}^{n} x_k \) in Definition 1.38. A possible choice is the notation \( \oplus \) for the operation \( \Box \) and

\[
\bigoplus_{k=1}^{n} x_k \quad \text{for} \quad \sum_{k=1}^{n} x_k.
\]

However, in the rest of the book only the usual operations of addition and multiplication on numbers are used, so the usage in Definition 1.38 should not produce any confusion.

As opposed to the axiomatic method used to develop elements of Peano arithmetic in Sections 1.1–1.3, the natural numbers are constructed from sets in Section 1.6. The method was suggested by John von Neumann (1903–1957) in his paper “Zur Einführung der transfiniten Zahlen” published in 1923 in the journal
Acta Universitatis Szegediensis (Hungary). Because all Peano systems are isomorphic (Theorem 1.29), one can consider $\langle N, s, 1 \rangle$ as a “typical” system of natural numbers that exists by virtue of the Axiom of Infinity.

One should not confuse the method of mathematical induction with the method of “inductive reasoning”. The latter derives informally general propositions from specific examples. Consider, for instance, the trinomial

$$n^2 + n + 41,$$

where $n$ is a natural number. It can be verified that the value of this trinomial is a prime number for $n = 1, 2, 3, \ldots, 39$. However, this “experiment” being long and probably convincing does not prove the general proposition. Indeed,

$$40^2 + 40 + 41 = 1681 = 41^2,$$

which is not a prime number. (This example was known to Leonhard Euler (1707–1783).) An even more impressive illustration of inductive reasoning which leads to a wrong conclusion is given by the binomial $991n^2 + 1$. By experimenting with small natural numbers, one can come to the conjecture that the value of this binomial is not a square of a natural number. Even if you continue this experiment for several years without a computer, you will not produce a counterexample to this conjecture. It is not surprising because the smallest number $n$ for which the binomial is a square is

$$n = 12 055 735 790 331 359 447 442 538 767.$$

Note that there is no base case in the Strong Principle of Induction. One may say that the base case is “absorbed” into the inductive step. The induction hypothesis “$P(k)$ is true for $q \leq k < q$” in the proof of Theorem 1.47 is vacuous for $k = q$, because it is the implication

$$q \leq q < q \quad \text{implies} \quad P(q),$$

which is vacuously true ($q < q$ is false).

Of course, mathematical induction is a powerful tool. However, it is clear that one does not need it to prove, say, the proposition “$n^2 \geq 1$ for all $n \in \mathbb{N}$”. Sometimes a different method could achieve the same goal. Consider, for instance, the inequality $2^n > n$ from Example 1.41. It is a straightforward Calculus exercise to show that the function $f(x) = 2^x - x$ is increasing over the interval $[1, \infty)$. Because $f(1) = 1 > 0$, it follows that $f(x) > 0$ for all $x \geq 1$. Hence, $2^x > x$ for all real numbers $x \geq 1$.

---

### Exercises

1. Let $\langle N, s, 1 \rangle$ be a Peano system. We define:

$$N' = N \setminus \{1\}, \quad s' = s|_{N'}, \quad 1' = s(1).$$

Show that $\langle N', s', 1' \rangle$ is a Peano system.

2. Let $\langle N, s, 1 \rangle$ be a Peano system and $a$ an element of $N$ such that $a \neq 1$ and $a \neq s(1)$. Prove that there exists an element $b \in N$ such that $a = s(s(b))$. 

3. Let $\langle N, s, 1 \rangle$ be a Peano system. We define:

$$
2 = s(1), \quad 3 = s(s(1)), \quad 4 = s(s(s(1))), \quad 5 = s(s(s(s(1)))).
$$

Show that

a) $5 \neq 1$,

b) $3 \neq 5$,

c) $5 = s(s(3))$.

Prove that for all $a, b \in N$,

$$
a + b = 2 \quad \text{if and only if} \quad a = 1, \ b = 1.
$$

4. (Informal.) Determine whether the following triples $\langle N, s, 1 \rangle$ are Peano systems:

a) $N$ is the set of all integers greater than 100, “1” stands for the integer 101, and $s(x) = x + 1$ for any integer $x$ in $N$.

b) $N$ is the set of all integers, “1” stands for the ordinary integer 1, and $s(x) = x + 1$ for all integers $x$.

c) $N$ stands for the set of all fractions of the form $1/2^n$, where $n$ is a non-negative integer, “1” stands for the ordinary integer 1, and $s(x) = \frac{1}{2}x$ for all $x \in N$.

In Exercises 5–21, we assume that a Peano system $\langle N, s, 1 \rangle$ is given.

5. Write down all possible ways of inserting parentheses in

$$a + b + c + d$$

and verify that they yield the same result.

6. (Cancellation Law of Addition): Prove that for any $a, b, c \in N$,

$$a + c = b + c \quad \text{implies} \quad a = b.$$

7. Finish the proof of Theorem 1.12.

8. Prove that for all $a, b \in N$,

$$a \cdot b = 1 \quad \text{if and only if} \quad a = 1, \ b = 1.$$

9. (Cancellation Law of Multiplication): Prove that for any $a, b, c \in N$,

$$a \cdot c = b \cdot c \quad \text{implies} \quad a = b.$$

10. We define $a^2 = a \cdot a$. Prove that

$$
(a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2, \quad \text{for all} \ a, b \in N.
$$

(Here, $2 = s(1)$, cf. Exercise 3.)

11. An element $a \in N$ is said to be even if there is $b \in N$ such that $a = 2 \cdot b$; it is said to be odd if $a = 1$ or $a = 2 \cdot b + 1$ for some $b \in N$. Prove that:

\begin{itemize}
  \item[a)] Every element in $N$ either even or odd.
  \item[b)] No element in $N$ is both even and odd.
  \item[c)] $a^2 = a \cdot a$ is even if and only if $a$ is even.
  \item[d)] $a^2$ is odd if and only if $a$ is odd.
  \item[e)] The sum and product of two even elements is even.
  \item[f)] The sum of two odd elements is even.
  \item[g)] The product of two odd elements is odd.
  \item[h)] If $a$ is odd and $b$ is even, then $a + b$ is odd and $a \cdot b$ is even.
\end{itemize}
12. Let \( a < b \). Show that there is a unique element \( c \in N \) such that \( b = a + c \) (cf. (1.17)). This number is called the difference of \( b \) and \( a \) and denoted by \( b - a \).

13. Prove Theorem 1.20.

14. Show that, for any \( a, b, c \in N \), the relation \( \leq \) has the following properties:
   a) (Reflexivity): \( a \leq a \).
   b) (Connectivity): Either \( a \leq b \) or \( b \leq a \) (or both).
   c) (Antisymmetry): If \( a \leq b \) and \( b \leq a \), then \( a = b \).
   d) (Transitivity): If \( a \leq b \) and \( b \leq c \), then \( a \leq c \).

15. Show that if a set \( M \subseteq N \) has a least (greatest) element, then this element is unique.

16. Prove that \( N \) does not have a greatest element.

17. Show that, for any \( a, b, c, d \in N \),
   a) \( a \geq 1 \),
   b) if \( a < b \), then \( a + 1 \leq b \),
   c) if \( a < b + 1 \), then \( a \leq b \),
   d) if \( a > b \), or \( a = b \), or \( a < b \), then

   \[
   a + c > b + c, \text{ or } a + c = b + c, \text{ or } a + c < b + c,
   \]

   respectively,
   e) the converse of b) holds,
   f) If \( a > b \), \( c > d \), then \( a + c > b + d \).

18. Show that, for any \( a, b, c, d \in N \),
   a) \( a \leq 1 \) if and only if \( a = 1 \),
   b) \( a < s(b) \) if and only if \( a \leq b \),
   c) \( a < b \) if and only if \( s(a) \leq b \),
   d) if \( a + c < b + d \), then \( a < b \) or \( c < d \).

19. Let symbols 1, 2, 3, 4, 5 be as defined in Exercise 3. Show that

   \[
   1 < 2 < 3 < 4 < 5.
   \]

20. A subset \( M \) of the set \( N \) is said to be bounded if there is \( a \in N \) such that

   \[
   b \leq a, \quad \text{for all } b \in M.
   \]

   Prove that a bounded subset of \( N \) has a greatest element.

21. A binary relation \( \prec \) on the set \( N \times N \) which is defined by

   \[
   (a, b) \prec (c, d) \quad \text{if and only if} \quad \text{either } a < c \text{ or } (a = c \text{ and } b < d)
   \]

   is called a lexicographic order on \( N \times N \). Show that \( \prec \) is a linear order on \( N \times N \) and every nonempty subset of \( N \times N \) has a minimum element with respect to \( \prec \).

22. Describe all nonisomorphic algebraic structures on a 2-element set (a pair) (cf. Example 1.2 b) and c)).

23. Prove Theorem 1.27.

24. Show that the structures \( \langle N, s, 1 \rangle \) and \( \langle N', s', 1 \rangle \) of Example 1.28 satisfy axioms \( P1 \) and \( P2 \) but are not isomorphic.
25. Let \( \langle N, s, 1 \rangle \) and \( \langle N', s', 1 \rangle \) be Peano systems. By Theorem 1.29, there exists an isomorphism \( f : N \to N' \). Prove that \( f \) is unique.

26. Let \( \langle N, s, 1 \rangle \) be an algebraic structure (cf. the first paragraph in Section 1.5). Prove that \( \langle N, s, 1 \rangle \) is a Peano system if and only if for any set \( S \), any element \( c \in S \), and any function \( g : S \to S \), there is a unique function \( f : N \to S \) such that \( f(1) = c \) and \( f(s(a)) = g(f(a)) \) for all \( a \in N \). (MacLane, S. and Birkhoff, G., Algebra, Macmillan, New York, 1967, pp. 67–70.)

27. Prove that the intersection of any family of inductive sets is an inductive set itself.

28. Prove that sets 1, 2, and 3 are natural numbers.

29. Show that \( n/\in n \) for all natural numbers.

30. Prove that for every natural number \( n \), either \( n = 1 \), or \( 1 \in n \).

31. Prove that for all natural numbers \( n \), either \( n = 1 \), or \( n = s(k) \) for some \( k \in \mathbb{N} \).

32. Let \( m, n \in \mathbb{N} \). Prove that \( m \) is a proper subset of \( n \) if and only if \( m \in n \).

33. Show that if \( m \in n \), then either \( s(m) = n \), or else \( s(m) \in n \).

34. Show that for all \( m, n \in \mathbb{N} \), there are three mutually exclusive possibilities:

\[
m \in n, \quad m = n, \quad n \in m.
\]

35. Let \( m, n \in \mathbb{N} \). Prove that \( m \) is a proper subset of \( n \) if and only if \( s(m) \) is a proper subset of \( s(n) \).

36. Show that for all \( m, n \in \mathbb{N} \), there are three mutually exclusive possibilities:

\[
m \subset n, \quad m = n, \quad n \subset m,
\]

where \( \subset \) stands for proper inclusion.

37. Let \( n \) be a natural number and \( E \) be a nonempty subset of \( n \). Show that there is \( k \in E \) such that \( k \in m \) whenever \( m \) is an element of \( E \) distinct from \( k \).

38. For \( m, n \in \mathbb{N} \), the interval \( [m, n] \) is the subset of \( \mathbb{N} \) defined by

\[
[m, n] = \{ k \in \mathbb{N} : k \geq m \text{ and } k \leq n \}.
\]

Show that

a) \( [m, n] = \emptyset \) if and only if \( n < m \).

b) If \( m \leq n \), then \( m \in [m, n] \) and \( n \in [m, n] \).

c) \( [1, n] = s(n) \).

d) \( n \in [1, n] \) if and only if \( n \neq 1 \).

e) \([1, m] = [1, n]\) if and only if \( m = n \).

f) If \( m \leq n \), then \( [m, n] \subseteq [m, k] \) if and only if \( n \leq k \).

39. Justify statements in Example 1.32.

40. Prove that condition (1.28) is equivalent to condition (1.26).

41. Deduce the results of Theorems 1.5 and 1.12 from Theorem 1.33.

42. Let \( \langle \mathbb{N}, s, 1 \rangle \) be a Peano system with the underlying set \( \mathbb{N} \), \( S \) a set with a fixed element \( c \in S \), and \( g \) a function \( g : S \to S \). Prove that there exists a unique
function \( f : \mathbb{N} \to S \) such that
\[
\begin{align*}
  f(1) &= c, \\
  f(s(n)) &= g(f(n)), \quad \text{for all } n \in \mathbb{N}.
\end{align*}
\]

43. Let \( \langle \mathbb{N}, s, 1 \rangle \) be a Peano system with the underlying set \( \mathbb{N} \) and let \( g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) and \( h : \mathbb{N} \to \mathbb{N} \) be functions. Prove that there exists a unique function \( f : \mathbb{N} \times \mathbb{N} \to S \) such that
\[
\begin{align*}
  f(n, 1) &= h(n), \quad \text{for any } n \in \mathbb{N}, \\
  f(m, s(n)) &= g(m, f(m, n)), \quad \text{for any } m, n \in \mathbb{N}.
\end{align*}
\]

44. Establish the main properties of the exponential function:
\[
\begin{align*}
  a) \quad &1^n = 1, \\
  b) \quad &n^k \cdot n^m = n^{k+m}, \\
  c) \quad &(n^m)^k = n^{mk}, \\
  d) \quad &(m \cdot n)^k = m^k \cdot n^k,
\end{align*}
\]
for any \( m, n, k \in \mathbb{N} \).

45. Show that, for any \( m, n, k \in \mathbb{N} \),
\[
\begin{align*}
  a) \quad &m < n \text{ if and only if } m^k < n^k, \\
  b) \quad &k > 1 \text{ if and only if } n < k^n, \\
  c) \quad &(1+k)^n \geq 1 + (n \cdot k), \\
  d) \quad &n \leq m^n.
\end{align*}
\]

46. (Even and odd numbers.) Show that for each \( n \in \mathbb{N} \) either \( n = 1 \) or there is a unique \( k \in \mathbb{N} \) such that \( n = 2 \cdot k \) or there is a unique \( k \in \mathbb{N} \) such that \( n = (2 \cdot k) + 1 \).

47. Find a recursive definition for a function \( f : \mathbb{N} \to \mathbb{N} \) such that \( f(1) = 1 \) and for all \( n \in \mathbb{N}, f(2n) = 2 \) and \( f(2n + 1) = 1 \). (Note that we write \( 2n \) for \( 2 \cdot n \) and \( 2n + 1 \) for \( (2 \cdot n) + 1 \).)

48. Let \( (x_k)_{k \in \mathbb{N}} \) be a sequence of elements in \( \mathbb{N} \). Show that for any \( n \) and \( m \) in \( \mathbb{N} \) we have
\[
\begin{align*}
  \sum_{k=1}^{n+m} x_k &= \left( \sum_{k=1}^{n} x_k \right) + \left( \sum_{k=1}^{m} x_{n+k} \right), \\
  \prod_{k=1}^{n+m} x_k &= \left( \prod_{k=1}^{n} x_k \right) \cdot \left( \prod_{k=1}^{m} x_{n+k} \right).
\end{align*}
\]

49. Let \( (x_k)_{k \in \mathbb{N}} \) and \( (y_k)_{k \in \mathbb{N}} \) be sequences of elements in \( \mathbb{N} \). Show that for any \( n \in \mathbb{N} \):
\[
\begin{align*}
  \left( \sum_{k=1}^{n} x_k \right) + \left( \sum_{k=1}^{n} y_k \right) &= \sum_{k=1}^{n} (x_k + y_k), \\
  \left( \prod_{k=1}^{n} x_k \right) \cdot \left( \prod_{k=1}^{n} y_k \right) &= \prod_{k=1}^{n} (x_k \cdot y_k).
\end{align*}
\]
50. (Generalized Distributive Law.) Let \((x_k)_{k \in \mathbb{N}}\) be a sequence of elements in \(\mathbb{N}\) and let \(m\) be a natural number. Show that for any \(n \in \mathbb{N}\) we have
\[
\left( \sum_{k=1}^{n} x_k \right) \cdot m = \sum_{k=1}^{n} (x_k \cdot m).
\]

51. Let \((x_k)_{k \in \mathbb{N}}\) and \((y_k)_{k \in \mathbb{N}}\) be sequences of elements in \(\mathbb{N}\). Prove that if \(x_k = y_k\) for all \(k \in \mathbb{N}\), then
\[
\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} y_k \quad \text{and} \quad \prod_{k=1}^{n} x_k = \prod_{k=1}^{n} y_k, \quad \text{for any} \ n \in \mathbb{N}.
\]

52. Let \(n\) be a natural number greater than 1. Show that
\[
a + a + \cdots + a = n \cdot a,
\]
for every \(a \in \mathbb{N}\).

53. Prove that:
   
   a) \(2(1 + 2 + \cdots + n) = n(n+1)\), for all \(n \in \mathbb{N}\).
   
   b) \(6(1^2 + 2^2 + \cdots + n^2) = n(n+1)(2n+1)\), for all \(n \in \mathbb{N}\).
   
   c) \(1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1\), for all \(n \in \mathbb{N}\).
   
   d) \(\sum_{k=1}^{n} k^3 = \left[ \sum_{k=1}^{n} k \right]^2\), for all \(n \in \mathbb{N}\).
   
   e) \(3 \sum_{k=1}^{n} k(k+1) = n(n+1)(n+2)\), for all \(n \in \mathbb{N}\).

54. Prove that
\[
\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1,
\]
for all \(n \in \mathbb{N}\).

55. For \(n \in \mathbb{N}\), prove that the number of different subsets of an \(n\)-element set is \(2^n\).

56. For \(n \in \mathbb{N}\), we denote \(A_n = 11^{n+1} + 12^{2n-1}\). Prove that for every \(n \in \mathbb{N}\), the number \(A_n\) is divisible by 133, that is, there is a natural number \(B_n\) such that \(A_n = 133 \cdot B_n\).

57. Prove that the sum of three consecutive cubes of natural numbers is divisible by 9.

58. Prove that \(n\) distinct points on a straight line divide the line into \(n+1\) intervals.

59. A finite family of lines in the plane is said to be in a general position if every two lines intersect and no more than two pass through the same point. Show that a family of \(n\) lines in a general position divides the plane into
\[
1 + \sum_{k=1}^{n} k
\]
regions.

60. Show that the sum of angles of a convex \(n\)-gon is \((n-2)180^\circ\). (For the definition of the difference \(n - 2\), see Exercise 12).
61. It can be shown that any simple (not necessarily convex) \( n \)-gon (\( n \geq 3 \)) has at least one diagonal that lies completely within the \( n \)-gon. Assuming that it is known, show that any \( n \)-gon can be subdivided into exactly \( n - 2 \) triangles so that every triangle vertex is one of the original vertices of the \( n \)-gon.

62. Use mathematical induction to show that each integer greater than 7 is a sum of a nonnegative multiple of 3 and a nonnegative multiple of 5.

63. Find the error in the following inductive “proof” that all natural numbers are equal:

Let \( M \) be the set of all \( n \in \mathbb{N} \) such that \( n \) equals all natural numbers between 1 and \( n \) (including 1 and \( n \)). Then 1 \( \in \) \( M \). Now suppose all natural numbers up to and including \( k \) are in \( M \). Then \( k = k - 1 \). By adding 1 to both sides we obtain \( k + 1 = k \). Therefore, by the principle of mathematical induction, \( M \) contains all natural numbers, and so all natural numbers are equal.

64. Show that the algebraic structures \( \langle \mathbb{N}, + \rangle \) and \( \langle \mathbb{N}, \cdot, 1 \rangle \) are a commutative semigroup and a commutative monoid, respectively.

65. The algebraic structures in Example 1.2 b) and c) are induction systems (cf. definition on page 28). Determine the (unique) addition and multiplication operations on these systems using conditions (1.1), (1.2) and (1.8), (1.9), respectively. Then write the addition and multiplication tables for these induction systems.

66. Describe all nonisomorphic induction systems on a 2-element set.

67. Let \( s : N \rightarrow N \) be a function on \( N = \{a, b, c, d\} \) defined by:

\[
\begin{align*}
    s(a) &= b, & s(b) &= c, & s(c) &= d, & s(d) &= a.
\end{align*}
\]

Show that \( \langle N, s, a \rangle \) is an induction system and use conditions (1.1), (1.2) and (1.8), (1.9) to complete the addition and multiplication tables for this system:

\[
\begin{array}{c|cccc}
+ & a & b & c & d \\
\hline
a & b & c & d & a \\
b & c & d & a & b \\
c & d & a & b & c \\
d & a & b & c & d \\
\end{array}
\quad\text{and}\quad
\begin{array}{c|cccc}
\cdot & a & b & c & d \\
\hline
a & a & b & c & d \\
b & b & \text{-----} & \text{-----} & \text{-----} \\
c & \text{-----} & \text{-----} & \text{-----} & \text{-----} \\
d & \text{-----} & \text{-----} & \text{-----} & \text{-----} \\
\end{array}
\]

Show that there is no “exponentiation” operation \( (x, y) \mapsto x^y \) on \( N \) that satisfies the conditions:

\[
\begin{align*}
    x^a &= x, & \text{for any } x \in N, \\
    x^{s(y)} &= (x^y) \cdot x, & \text{for any } x, y \in N.
\end{align*}
\]

(cf. Example 1.36).