(b) Show the converse of (a) holds if $B$ is nonempty.
(c) Show that if $A$ is nonempty, each $A_i$ is nonempty. Does the converse hold?
(We will return to this question in the exercises of §19.)
(d) What is the relation between the set $A \cup B$ and the cartesian product of the sets $A_i \cup B_i$? What is the relation between the set $A \cap B$ and the cartesian product of the sets $A_i \cap B_i$?

4. Let $m, n \in \mathbb{Z}_+$. Let $X \neq \emptyset$.
   (a) If $m \leq n$, find an injective map $f : X^m \to X^n$.
   (b) Find a bijective map $g : X^m \times X^n \to X^{m+n}$.
   (c) Find an injective map $h : X^n \to X^\omega$.
   (d) Find a bijective map $k : X^n \times X^\omega \to X^\omega$.
   (e) Find a bijective map $l : X^\omega \times X^\omega \to X^\omega$.
   (f) If $A \subset B$, find an injective map $m : (A^\omega)^n \to B^\omega$.

5. Which of the following subsets of $\mathbb{R}^\omega$ can be expressed as the cartesian product of subsets of $\mathbb{R}$?
   (a) $\{x \mid x_i$ is an integer for all $i\}$.
   (b) $\{x \mid x_i \geq i$ for all $i\}$.
   (c) $\{x \mid x_i$ is an integer for all $i \geq 100\}$.
   (d) $\{x \mid x_2 = x_3\}$.

§6 Finite Sets

Finite sets and infinite sets, countable sets and uncountable sets, these are types of sets that you may have encountered before. Nevertheless, we shall discuss them in this section and the next, not only to make sure you understand them thoroughly, but also to elucidate some particular points of logic that will arise later on. First we consider finite sets.

Recall that if $n$ is a positive integer, we use $S_n$ to denote the set of positive integers less than $n$; it is called a section of the positive integers. The sets $S_n$ are the prototypes for what we call the finite sets.

Definition. A set is said to be finite if there is a bijective correspondence of $A$ with some section of the positive integers. That is, $A$ is finite if it is empty or if there is a bijection

$$f : A \to \{1, \ldots, n\}$$

for some positive integer $n$. In the former case, we say that $A$ has cardinality 0; in the latter case, we say that $A$ has cardinality $n$.

For instance, the set $\{1, \ldots, n\}$ itself has cardinality $n$, for it is in bijective correspondence with itself under the identity function.
Now note carefully: We have not yet shown that the cardinality of a finite set is uniquely determined by the set. It is of course clear that the empty set must have cardinality zero. But as far as we know, there might exist bijective correspondences of a given nonempty set $A$ with two different sets $\{1, \ldots, n\}$ and $\{1, \ldots, m\}$. The possibility may seem ridiculous, for it is like saying that it is possible for two people to count the marbles in a box and come out with two different answers, both correct. Our experience with counting in everyday life suggests that such is impossible, and in fact this is easy to prove when $n$ is a small number such as 1, 2, or 3. But a direct proof when $n$ is 5 million would be impossibly demanding.

Even empirical demonstration would be difficult for such a large value of $n$. One might, for instance, construct an experiment by taking a freight car full of marbles and hiring 10 different people to count them independently. If one thinks of the physical problems involved, it seems likely that the counters would not all arrive at the same answer. Of course, the conclusion one could draw is that at least one person made a mistake. But that would mean assuming the correctness of the result one was trying to demonstrate empirically. An alternative explanation could be that there do exist bijective correspondences between the given set of marbles and two different sections of the positive integers.

In real life, we accept the first explanation. We simply take it on faith that our experience in counting comparatively small sets of objects demonstrates a truth that holds for arbitrarily large sets as well.

However, in mathematics (as opposed to real life), one does not have to take this statement on faith. If it is formulated in terms of the existence of bijective correspondences rather than in terms of the physical act of counting, it is capable of mathematical proof. We shall prove shortly that if $n \neq m$, there do not exist bijective functions mapping a given set $A$ onto both the sets $\{1, \ldots, n\}$ and $\{1, \ldots, m\}$.

There are a number of other “intuitively obvious” facts about finite sets that are capable of mathematical proof; we shall prove some of them in this section and leave the rest to the exercises. Here is an easy fact to start with:

**Lemma 6.1.** Let $n$ be a positive integer. Let $A$ be a set; let $a_0$ be an element of $A$. Then there exists a bijective correspondence $f$ of the set $A$ with the set $\{1, \ldots, n+1\}$ if and only if there exists a bijective correspondence $g$ of the set $A - \{a_0\}$ with the set $\{1, \ldots, n\}$.

**Proof.** There are two implications to be proved. Let us first assume that there is a bijective correspondence

$$g : A - \{a_0\} \rightarrow \{1, \ldots, n\}.$$

We then define a function $f : A \rightarrow \{1, \ldots, n+1\}$ by setting

$$f(x) = g(x) \quad \text{for } x \in A - \{a_0\},$$

$$f(a_0) = n+1.$$

One checks at once that $f$ is bijective.
To prove the converse, assume there is a bijective correspondence

\[ f : A \rightarrow \{1, \ldots, n + 1\}. \]

If \( f \) maps \( a_0 \) to the number \( n - 1 \), things are especially easy; in that case, the restriction \( f|_{A - \{a_0\}} \) is the desired bijective correspondence of \( A - \{a_0\} \) with \( \{1, \ldots, n\} \). Otherwise, let \( f(a_0) = m \), and let \( a_1 \) be the point of \( A \) such that \( f(a_1) = n + 1 \). Then \( a_1 \neq a_0 \). Define a new function

\[ h : A \rightarrow \{1, \ldots, n + 1\} \]

by setting

\[
\begin{align*}
  h(a_0) &= n + 1, \\
  h(a_1) &= m, \\
  h(x) &= f(x) \quad \text{for } x \in A - \{a_0\} - \{a_1\}.
\end{align*}
\]

See Figure 6.1. It is easy to check that \( h \) is a bijection.

Now we are back in the easy case; the restriction \( h|_{A - \{a_0\}} \) is the desired bijection of \( A - \{a_0\} \) with \( \{1, \ldots, n\} \).

\[ \]

From this lemma a number of useful consequences follow:

**Theorem 6.2.** Let \( A \) be a set; suppose that there exists a bijection \( f : A \rightarrow \{1, \ldots, n\} \) for some \( n \in \mathbb{Z}_+ \). Let \( B \) be a proper subset of \( A \). Then there exists no bijection \( g : B \rightarrow \{1, \ldots, n\} \); but (provided \( B \neq \emptyset \)) there does exist a bijection \( h : B \rightarrow \{1, \ldots, m\} \) for some \( m < n \).

**Proof.** The case in which \( B = \emptyset \) is trivial, for there cannot exist a bijection of the empty set \( B \) with the nonempty set \( \{1, \ldots, n\} \).

We prove the theorem "by induction." Let \( C \) be the subset of \( \mathbb{Z}_+ \) consisting of those integers \( n \) for which the theorem holds. We shall show that \( C \) is inductive. From this we conclude that \( C = \mathbb{Z}_+ \), so the theorem is true for all positive integers \( n \).

First we show the theorem is true for \( n = 1 \). In this case \( A \) consists of a single element \( \{a\} \), and its only proper subset \( B \) is the empty set.
Now assume that the theorem is true for \( n \); we prove it true for \( n + 1 \). Suppose that \( f : A \to \{1, \ldots, n + 1\} \) is a bijection, and \( B \) is a nonempty proper subset of \( A \). Choose an element \( a_0 \) of \( B \) and an element \( a_1 \) of \( A - B \). We apply the preceding lemma to conclude there is a bijection

\[
g : A - \{a_0\} \to \{1, \ldots, n\}.
\]

Now \( B - \{a_0\} \) is a proper subset of \( A - \{a_0\} \), for \( a_1 \) belongs to \( A - \{a_0\} \) and not to \( B - \{a_0\} \). Because the theorem has been assumed to hold for the integer \( n \), we conclude the following:

1. There exists no bijection \( h : B - \{a_0\} \to \{1, \ldots, n\} \).
2. Either \( B - \{a_0\} = \emptyset \), or there exists a bijection

\[
k : B - \{a_0\} \to \{1, \ldots, p\} \quad \text{for some } p < n.
\]

The preceding lemma, combined with (1), implies that there is no bijection of \( B \) with \( \{1, \ldots, n + 1\} \). This is the first half of what we wanted to proved. To prove the second half, note that if \( B - \{a_0\} = \emptyset \), there is a bijection of \( B \) with the set \( \{1\} \); while if \( B - \{a_0\} \neq \emptyset \), we can apply the preceding lemma, along with (2), to conclude that there is a bijection of \( B \) with \( \{1, \ldots, p + 1\} \). In either case, there is a bijection of \( B \) with \( \{1, \ldots, m\} \) for some \( m < n + 1 \), as desired. The induction principle now shows that the theorem is true for all \( n \in \mathbb{Z}_+ \).

**Corollary 6.3.** If \( A \) is finite, there is no bijection of \( A \) with a proper subset of itself.

**Proof.** Assume that \( B \) is a proper subset of \( A \) and that \( f : A \to B \) is a bijection. By assumption, there is a bijection \( g : A \to \{1, \ldots, n\} \) for some \( n \). The composite \( g \circ f^{-1} \) is then a bijection of \( B \) with \( \{1, \ldots, n\} \). This contradicts the preceding theorem.

**Corollary 6.4.** \( \mathbb{Z}_+ \) is not finite.

**Proof.** The function \( f : \mathbb{Z}_+ \to \mathbb{Z}_+ - \{1\} \) defined by \( f(n) = n + 1 \) is a bijection of \( \mathbb{Z}_+ \) with a proper subset of itself.

**Corollary 6.5.** The cardinality of a finite set \( A \) is uniquely determined by \( A \).

**Proof.** Let \( m < n \). Suppose there are bijections

\[
f : A \to \{1, \ldots, n\},
g : A \to \{1, \ldots, m\}.
\]

Then the composite

\[
g \circ f^{-1} : \{1, \ldots, n\} \to \{1, \ldots, m\}
\]

is a bijection of the finite set \( \{1, \ldots, n\} \) with a proper subset of itself, contradicting the corollary just proved.
Corollary 6.6. If $B$ is a subset of the finite set $A$, then $B$ is finite. If $B$ is a proper subset of $A$, then the cardinality of $B$ is less than the cardinality of $A$.

Corollary 6.7. Let $B$ be a nonempty set. Then the following are equivalent:

1. $B$ is finite.
2. There is a surjective function from a section of the positive integers onto $B$.
3. There is an injective function from $B$ into a section of the positive integers.

Proof. (1) $\implies$ (2). Since $B$ is nonempty, there is, for some $n$, a bijective function $f : \{1, \ldots, n\} \to B$.

(2) $\implies$ (3). If $f : \{1, \ldots, n\} \to B$ is surjective, define $g : B \to \{1, \ldots, n\}$ by the equation

$$g(b) = \text{smallest element of } f^{-1}(\{b\}).$$

Because $f$ is surjective, the set $f^{-1}(\{b\})$ is nonempty; then the well-ordering property of $\mathbb{Z}_+$ tells us that $g(b)$ is uniquely defined. The map $g$ is injective, for if $b \neq b'$, then the sets $f^{-1}(\{b\})$ and $f^{-1}(\{b'\})$ are disjoint, so their smallest elements must be different.

(3) $\implies$ (1). If $g : B \to \{1, \ldots, n\}$ is injective, then changing the range of $g$ gives a bijection of $B$ with a subset of $\{1, \ldots, n\}$. It follows from the preceding corollary that $B$ is finite.

Corollary 6.8. Finite unions and finite cartesian products of finite sets are finite.

Proof. We first show that if $A$ and $B$ are finite, so is $A \cup B$. The result is trivial if $A$ or $B$ is empty. Otherwise, there are bijections $f : \{1, \ldots, m\} \to A$ and $g : \{1, \ldots, n\} \to B$ for some choice of $m$ and $n$. Define a function $h : \{1, \ldots, m+n\} \to A \cup B$ by setting $h(i) = f(i)$ for $i = 1, 2, \ldots, m$ and $h(i) = g(i-m)$ for $i = m+1, \ldots, m+n$. It is easy to check that $h$ is surjective, from which it follows that $A \cup B$ is finite.

Now we show by induction that finiteness of the sets $A_1, \ldots, A_n$ implies finiteness of their union. This result is trivial for $n = 1$. Assuming it true for $n - 1$, we note that $A_1 \cup \cdots \cup A_n$ is the union of the two finite sets $A_1 \cup \cdots \cup A_{n-1}$ and $A_n$, so the result of the preceding paragraph applies.

Now we show that the cartesian product of two finite sets $A$ and $B$ is finite. Given $a \in A$, the set $\{a\} \times B$ is finite, being in bijective correspondence with $B$. The set $A \times B$ is the union of these sets; since there are only finitely many of them, $A \times B$ is a finite union of finite sets and thus finite.

To prove that the product $A_1 \times \cdots \times A_n$ is finite if each $A_i$ is finite, one proceeds by induction. \[]
Exercises

1. (a) Make a list of all the injective maps

\[ f : \{1, 2, 3\} \rightarrow \{1, 2, 3, 4\}. \]

Show that none is bijective. (This constitutes a direct proof that a set \( A \) of cardinality three does not have cardinality four.)

(b) How many injective maps

\[ f : \{1, \ldots, 8\} \rightarrow \{1, \ldots, 10\} \]

are there? (You can see why one would not wish to try to prove directly that there is no bijective correspondence between these sets.)

2. Show that if \( B \) is not finite and \( B \subset A \), then \( A \) is not finite.

3. Let \( X \) be the two-element set \( \{0, 1\} \). Find a bijective correspondence between \( X^\omega \) and a proper subset of itself.

4. Let \( A \) be a nonempty finite simply ordered set.

   (a) Show that \( A \) has a largest element. [Hint: Proceed by induction on the cardinality of \( A \)].

   (b) Show that \( A \) has the order type of a section of the positive integers.

5. If \( A \times B \) is finite, does it follow that \( A \) and \( B \) are finite?

6. (a) Let \( A = \{1, \ldots, n\} \). Show there is a bijection of \( \mathcal{P}(A) \) with the cartesian product \( X^n \), where \( X \) is the two-element set \( X = \{0, 1\} \).

   (b) Show that if \( A \) is finite, then \( \mathcal{P}(A) \) is finite.

7. If \( A \) and \( B \) are finite, show that the set of all functions \( f : A \rightarrow B \) is finite.

§7 Countable and Uncountable Sets

Just as sections of the positive integers are the prototypes for the finite sets, the set of all the positive integers is the prototype for what we call the countably infinite sets. In this section, we shall study such sets; we shall also construct some sets that are neither finite nor countably infinite. This study will lead us into a discussion of what we mean by the process of "inductive definition."

Definition. A set \( A \) is said to be infinite if it is not finite. It is said to be countably infinite if there is a bijective correspondence

\[ f : A \rightarrow \mathbb{Z}_+. \]

Example 1. The set \( \mathbb{Z} \) of all integers is countably infinite. One checks easily that the function \( f : \mathbb{Z} \rightarrow \mathbb{Z}_+ \) defined by

\[ f(n) = \begin{cases} 
2n & \text{if } n > 0, \\
-2n + 1 & \text{if } n \leq 0
\end{cases} \]

is a bijection.
EXAMPLE 2. The product \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) is countably infinite. If we represent the elements of the product \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) by the integer points in the first quadrant, then the left-hand portion of Figure 7.1 suggests how to "count" the points, that is, how to put them in bijective correspondence with the positive integers. A picture is not a proof, of course, but this picture suggests a proof. First, we define a bijection \( f : \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow A \), where \( A \) is the subset of \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) consisting of pairs \((x, y)\) for which \( y \leq x \), by the equation

\[
f(x, y) = (x + y - 1, y).
\]

Then we construct a bijection of \( A \) with the positive integers, defining \( g : A \rightarrow \mathbb{Z}_+ \) by the formula

\[
g(x, y) = \frac{1}{2}(x - 1)x + y.
\]

We leave it to you to show that \( f \) and \( g \) are bijections.

Another proof that \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) is countably infinite will be given later.

Definition. A set is said to be **countable** if it is either finite or countably infinite. A set that is not countable is said to be **uncountable**.

There is a very useful criterion for showing that a set is countable. It is the following:

**Theorem 7.1.** Let \( B \) be a nonempty set. Then the following are equivalent:

1. \( B \) is countable.
2. There is a surjective function \( f : \mathbb{Z}_+ \rightarrow B \).
3. There is an injective function \( g : B \rightarrow \mathbb{Z}_+ \).

**Proof.** (1) \( \Rightarrow \) (2). Suppose that \( B \) is countable. If \( B \) is countably infinite, there is a bijection \( f : \mathbb{Z}_+ \rightarrow B \) by definition, and we are through. If \( B \) is finite, there is a
bijection \( h : \{1, \ldots, n\} \rightarrow B \) for some \( n \geq 1 \). (Recall that \( B \neq \emptyset \).) We can extend \( h \) to a surjection \( f : \mathbb{Z}_+ \rightarrow B \) by defining

\[
    f(i) = \begin{cases} 
        h(i) & \text{for } 1 \leq i \leq n, \\
        h(1) & \text{for } i > n.
    \end{cases}
\]

(2) \( \implies \) (3). Let \( f : \mathbb{Z}_+ \rightarrow B \) be a surjection. Define \( g : B \rightarrow \mathbb{Z}_+ \) by the equation

\[
    g(b) = \text{smallest element of } f^{-1}(\{b\}).
\]

Because \( f \) is surjective, \( f^{-1}(\{b\}) \) is nonempty; thus \( g \) is well defined. The map \( g \) is injective, for if \( b \neq b' \), the sets \( f^{-1}(\{b\}) \) and \( f^{-1}(\{b'\}) \) are disjoint, so their smallest elements are different.

(3) \( \implies \) (1). Let \( g : B \rightarrow \mathbb{Z}_+ \) be an injection; we wish to prove \( B \) is countable. By changing the range of \( g \), we can obtain a bijection of \( B \) with a subset of \( \mathbb{Z}_+ \). Thus to prove our result, it suffices to show that every subset of \( \mathbb{Z}_+ \) is countable. So let \( C \) be a subset of \( \mathbb{Z}_+ \).

If \( C \) is finite, it is countable by definition. So what we need to prove is that every infinite subset \( C \) of \( \mathbb{Z}_+ \) is countably infinite. This statement is certainly plausible. For the elements of \( C \) can easily be arranged in an infinite sequence; one simply takes the set \( \mathbb{Z}_+ \) in its usual order and “erases” all the elements of \( \mathbb{Z}_+ \) that are not in \( C \)!

The plausibility of this argument may make one overlook its informality. Providing a formal proof requires a certain amount of care. We state this result as a separate lemma, which follows.

\[ \Box \]

**Lemma 7.2.** If \( C \) is an infinite subset of \( \mathbb{Z}_+ \), then \( C \) is countably infinite.

**Proof.** We define a bijection \( h : \mathbb{Z}_+ \rightarrow C \). We proceed by induction. Define \( h(1) \) to be the smallest element of \( C \); it exists because every nonempty subset \( C \) of \( \mathbb{Z}_+ \) has a smallest element. Then assuming that \( h(1), \ldots, h(n-1) \) are defined, define

\[
    h(n) = \text{smallest element of } [C - h(\{1, \ldots, n-1\})].
\]

The set \( C - h(\{1, \ldots, n-1\}) \) is not empty; for if it were empty, then \( h : \{1, \ldots, n-1\} \rightarrow C \) would be surjective, so that \( C \) would be finite (by Corollary 6.7). Thus \( h(n) \) is well defined. By induction, we have defined \( h(n) \) for all \( n \in \mathbb{Z}_+ \).

To show that \( h \) is injective is easy. Given \( m < n \), note that \( h(m) \) belongs to the set \( h(\{1, \ldots, n-1\}) \), whereas \( h(n) \), by definition, does not. Hence \( h(n) \neq h(m) \).

To show that \( h \) is surjective, let \( c \) be any element of \( C \); we show that \( c \) lies in the image set of \( h \). First note that \( h(\mathbb{Z}_+) \) cannot be contained in the finite set \( \{1, \ldots, c\} \), because \( h(\mathbb{Z}_+) \) is infinite (since \( h \) is injective). Therefore, there is an \( n \in \mathbb{Z}_+ \), such that \( h(n) > c \). Let \( m \) be the smallest element of \( \mathbb{Z}_+ \), such that \( h(m) \geq c \). Then for all \( i < m \), we must have \( h(i) < c \). Thus, \( c \) does not belong to the set \( h(\{1, \ldots, m-1\}) \).

Since \( h(m) \) is defined as the smallest element of the set \( C - h(\{1, \ldots, m-1\}) \), we must have \( h(m) \leq c \). Putting the two inequalities together, we have \( h(m) = c \), as desired. \[ \Box \]
There is a point in the preceding proof where we stretched the principles of logic a bit. It occurred at the point where we said that "using the induction principle" we had defined the function \( h \) for all positive integers \( n \). You may have seen arguments like this used before, with no questions raised concerning their legitimacy. We have already used such an argument ourselves, in the exercises of §4, when we defined \( a^n \).

But there is a problem here. After all, the induction principle states only that if \( A \) is an inductive set of positive integers, then \( A = \mathbb{Z}_+ \). To use the principle to prove a theorem "by induction," one begins the proof with the statement "Let \( A \) be the set of all positive integers \( n \) for which the theorem is true," and then one goes ahead to prove that \( A \) is inductive, so that \( A \) must be all of \( \mathbb{Z}_+ \).

In the preceding theorem, however, we were not really proving a theorem by induction, but defining something by induction. How then should we start the proof? Can we start by saying, "Let \( A \) be the set of all integers \( n \) for which the function \( h \) is defined"? But that's silly; the symbol \( h \) has no meaning at the outset of the proof. It only takes on meaning in the course of the proof. So something more is needed.

What is needed is another principle, which we call the **principle of recursive definition.** In the proof of the preceding theorem, we wished to assert the following:

Given the infinite subset \( C \) of \( \mathbb{Z}_+ \), there is a unique function \( h : \mathbb{Z}_+ \rightarrow C \) satisfying the formula:

\[
\begin{align*}
  h(1) &= \text{smallest element of } C, \\
  h(i) &= \text{smallest element of } [C - h(\{1, \ldots, i-1\})] \quad \text{for all } i > 1.
\end{align*}
\]

The formula (*) is called a **recursion formula** for \( h \); it defines the function \( h \) in terms of itself. A definition given by such a formula is called a **recursive definition**.

Now one can get into logical difficulties when one tries to define something recursively. Not all recursive formulas make sense. The recursive formula

\[
h(i) = \text{smallest element of } [C - h(\{1, \ldots, i+1\})],
\]

for example, is self-contradictory; although \( h(i) \) necessarily is an element of the set \( h(\{1, \ldots, i+1\}) \), this formula says that it does not belong to the set. Another example is the classic paradox:

Let the barber of Seville shave every man of Seville who does not shave himself.

Who shall shave the barber?

In this statement, the barber appears twice, once in the phrase "the barber of Seville" and once as an element of the set "men of Seville"; this definition of whom the barber shall shave is a recursive one. It also happens to be self-contradictory.

Some recursive formulas do make sense, however. Specifically, one has the following principle:

**Principle of recursive definition.** Let \( A \) be a set. Given a formula that defines \( h(1) \) as a unique element of \( A \), and for \( i > 1 \) defines \( h(i) \) uniquely as an element of \( A \) in terms of the values of \( h \) for positive integers less than \( i \), this formula determines a unique function \( h : \mathbb{Z}_+ \rightarrow A \).
This principle is the one we actually used in the proof of Lemma 7.2. You can simply accept it on faith if you like. It may however be proved rigorously, using the principle of induction. We shall formulate it more precisely in the next section and indicate how it is proved. Mathematicians seldom refer to this principle specifically. They are much more likely to write a proof like our proof of Lemma 7.2 above, a proof in which they invoke the "induction principle" to define a function when what they are really using is the principle of recursive definition. We shall avoid undue pedantry in this book by following their example.

**Corollary 7.3.** A subset of a countable set is countable.

*Proof.* Suppose \( A \subset B \), where \( B \) is countable. There is an injection \( f \) of \( B \) into \( \mathbb{Z}_+ \); the restriction of \( f \) to \( A \) is an injection of \( A \) into \( \mathbb{Z}_+ \). \( \square \)

**Corollary 7.4.** The set \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) is countably infinite.

*Proof.* In view of Theorem 7.1, it suffices to construct an injective map \( f : \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \). We define \( f \) by the equation

\[
f(n, m) = 2^n 3^m.
\]

It is easy to check that \( f \) is injective. For suppose that \( 2^n 3^m = 2^p 3^q \). If \( n < p \), then \( 3^m = 2^{p-n} 3^q \), contradicting the fact that \( 3^m \) is odd for all \( m \). Therefore, \( n = p \). As a result, \( 3^m = 3^q \). Then if \( m < q \), it follows that \( 1 = 3^{q-m} \), another contradiction. Hence \( m = q \). \( \square \)

**Example 3.** The set \( \mathbb{Q}_+ \) of positive rational numbers is countably infinite. For we can define a surjection \( g : \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow \mathbb{Q}_+ \) by the equation

\[
g(n, m) = m/n.
\]

Because \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) is countable, there is a surjection \( f : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \times \mathbb{Z}_+ \). Then the composite \( g \circ f : \mathbb{Z}_+ \rightarrow \mathbb{Q}_+ \) is a surjection, so that \( \mathbb{Q}_+ \) is countable. And, of course, \( \mathbb{Q}_+ \) is infinite because it contains \( \mathbb{Z}_+ \).

We leave it as an exercise to show the set \( \mathbb{Q} \) of all rational numbers is countably infinite.

**Theorem 7.5.** A countable union of countable sets is countable.

*Proof.* Let \( \{ A_n \}_{n \in J} \) be an indexed family of countable sets, where the index set \( J \) is either \( \{1, \ldots, N\} \) or \( \mathbb{Z}_+ \). Assume that each set \( A_n \) is nonempty, for convenience; this assumption does not change anything.

Because each \( A_n \) is countable, we can choose, for each \( n \), a surjective function \( f_n : \mathbb{Z}_+ \rightarrow A_n \). Similarly, we can choose a surjective function \( g : \mathbb{Z}_+ \rightarrow J \). Now define

\[
h : \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow \bigcup_{n \in J} A_n
\]
by the equation

\[ h(k, m) = f_g(k)(m). \]

It is easy to check that \( h \) is surjective. Since \( \mathbb{Z}_+ \times \mathbb{Z}_+ \) is in bijective correspondence with \( \mathbb{Z}_+ \), the countability of the union follows from Theorem 7.1.

**Theorem 7.6.** A finite product of countable sets is countable.

**Proof.** First let us show that the product of two countable sets \( A \) and \( B \) is countable. The result is trivial if \( A \) or \( B \) is empty. Otherwise, choose surjective functions \( f : \mathbb{Z}_+ \to A \) and \( g : \mathbb{Z}_+ \to B \). Then the function \( h : \mathbb{Z}_+ \times \mathbb{Z}_+ \to A \times B \) defined by the equation \( h(n, m) = (f(n), g(m)) \) is surjective, so that \( A \times B \) is countable.

In general, we proceed by induction. Assuming that \( A_1 \times \cdots \times A_{n-1} \) is countable if each \( A_i \) is countable, we prove the same thing for the product \( A_1 \times \cdots \times A_n \). First, note that there is a bijective correspondence

\[ g : A_1 \times \cdots \times A_n \to (A_1 \times \cdots \times A_{n-1}) \times A_n \]

defined by the equation

\[ g(x_1, \ldots, x_n) = ((x_1, \ldots, x_{n-1}), x_n). \]

Because the set \( A_1 \times \cdots \times A_{n-1} \) is countable by the induction assumption and \( A_n \) is countable by hypothesis, the product of these two sets is countable, as proved in the preceding paragraph. We conclude that \( A_1 \times \cdots \times A_n \) is countable as well.

It is very tempting to assert that countable products of countable sets should be countable; but this assertion is in fact not true:

**Theorem 7.7.** Let \( X \) denote the two element set \( \{0, 1\} \). Then the set \( X^\omega \) is uncountable.

**Proof.** We show that, given any function

\[ g : \mathbb{Z}_+ \to X^\omega, \]

g is not surjective. For this purpose, let us denote \( g(n) \) as follows:

\[ g(n) = (x_{n1}, x_{n2}, x_{n3}, \ldots, x_{nm}, \ldots), \]

where each \( x_{ij} \) is either 0 or 1. Then we define an element \( y = (y_1, y_2, \ldots, y_n, \ldots) \) of \( X^\omega \) by letting

\[ y_n = \begin{cases} 0 & \text{if } x_{nn} = 1, \\ 1 & \text{if } x_{nn} = 0. \end{cases} \]
(If we write the numbers $x_{ni}$ in a rectangular array, the particular elements $x_{nn}$ appear as the diagonal entries in this array; we choose $y$ so that its $n$th coordinate differs from the diagonal entry $x_{nn}$.)

Now $y$ is an element of $X^\omega$, and $y$ does not lie in the image of $g$; given $n$, the point $g(n)$ and the point $y$ differ in at least one coordinate, namely, the $n$th. Thus, $g$ is not surjective. 

The cartesian product $[0, 1]^\omega$ is one example of an uncountable set. Another is the set $\mathcal{P}(\mathbb{Z}_+)$, as the following theorem implies:

**Theorem 7.8.** Let $A$ be a set. There is no injective map $f : \mathcal{P}(A) \to A$, and there is no surjective map $g : A \to \mathcal{P}(A)$.

**Proof.** In general, if $B$ is a nonempty set, the existence of an injective map $f : B \to C$ implies the existence of a surjective map $g : C \to B$; one defines $g(c) = f^{-1}(c)$ for each $c$ in the image set of $f$, and defines $g$ arbitrarily on the rest of $C$.

Therefore, it suffices to prove that given a map $g : A \to \mathcal{P}(A)$, the map $g$ is not surjective. For each $a \in A$, the image $g(a)$ of $a$ is a subset of $A$, which may or may not contain the point $a$ itself. Let $B$ be the subset of $A$ consisting of all those points $a$ such that $g(a)$ does not contain $a$;

$$B = \{a \mid a \in A - g(a)\}.$$ 

Now, $B$ may be empty, or it may be all of $A$, but that does not matter. We assert that $B$ is a subset of $A$ that does not lie in the image of $g$. For suppose that $B = g(a_0)$ for some $a_0 \in A$. We ask the question: Does $a_0$ belong to $B$ or not? By definition of $B$,

$$a_0 \in B \iff a_0 \in A - g(a_0) \iff a_0 \in A - B.$$ 

In either case, we have a contradiction. 

Now we have proved the existence of uncountable sets. But we have not yet mentioned the most familiar uncountable set of all—the set of real numbers. You have probably seen the uncountability of $\mathbb{R}$ demonstrated already. If one assumes that every real number can be represented uniquely by an infinite decimal (with the proviso that a representation ending in an infinite string of 9's is forbidden), then the uncountability of the reals can be proved by a variant of the diagonal procedure used in the proof of Theorem 7.7. But this proof is in some ways not very satisfying. One reason is that the infinite decimal representation of a real number is not at all an elementary consequence of the axioms but requires a good deal of labor to prove. Another reason is that the uncountability of $\mathbb{R}$ does not, in fact, depend on the infinite decimal expansion of $\mathbb{R}$ or indeed on any of the algebraic properties of $\mathbb{R}$; it depends on only the order properties of $\mathbb{R}$. We shall demonstrate the uncountability of $\mathbb{R}$, using only its order properties, in a later chapter.
Exercises

1. Show that \( \mathbb{Q} \) is countably infinite.

2. Show that the maps \( f \) and \( g \) of Examples 1 and 2 are bijections.

3. Let \( X \) be the two-element set \( \{0, 1\} \). Show there is a bijective correspondence between the set \( \mathcal{P}(\mathbb{Z}_+) \) and the cartesian product \( X^\omega \).

4. (a) A real number \( x \) is said to be \textbf{algebraic} (over the rationals) if it satisfies some polynomial equation of positive degree
\[ x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \]
with rational coefficients \( a_i \). Assuming that each polynomial equation has only finitely many roots, show that the set of algebraic numbers is countable.

(b) A real number is said to be \textbf{transcendental} if it is not algebraic. Assuming the reals are uncountable, show that the transcendental numbers are uncountable. (It is a somewhat surprising fact that only two transcendental numbers are familiar to us: \( e \) and \( \pi \). Even proving these two numbers transcendental is highly nontrivial.)

5. Determine, for each of the following sets, whether or not it is countable. Justify your answers.
   (a) The set \( A \) of all functions \( f : \{0, 1\} \rightarrow \mathbb{Z}_+ \).
   (b) The set \( B_n \) of all functions \( f : \{1, \ldots, n\} \rightarrow \mathbb{Z}_+ \).
   (c) The set \( C = \bigcup_{n \in \mathbb{Z}_+} B_n \).
   (d) The set \( D \) of all functions \( f : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \).
   (e) The set \( E \) of all functions \( f : \mathbb{Z}_+ \rightarrow \{0, 1\} \).
   (f) The set \( F \) of all functions \( f : \mathbb{Z}_+ \rightarrow \{0, 1\} \) that are "eventually zero." [We say that \( f \) is \textbf{eventually zero} if there is a positive integer \( N \) such that \( f(n) = 0 \) for all \( n \geq N \).]
   (g) The set \( G \) of all functions \( f : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \) that are eventually 1.
   (h) The set \( H \) of all functions \( f : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ \) that are eventually constant.
   (i) The set \( I \) of all two-element subsets of \( \mathbb{Z}_+ \).
   (j) The set \( J \) of all finite subsets of \( \mathbb{Z}_+ \).

6. We say that two sets \( A \) and \( B \) \textbf{have the same cardinality} if there is a bijection of \( A \) with \( B \).
   (a) Show that if \( B \subset A \) and if there is an injection
\[ f : A \rightarrow B, \]
then \( A \) and \( B \) have the same cardinality. \([\text{Hint:} \text{ Define } A_1 = A, B_1 = B, \text{ and for } n > 1, A_n = f(A_{n-1}) \text{ and } B_n = f(B_{n-1}). \text{(Recursive definition again!)}\text{ Note that } A_1 \supset B_1 \supset A_2 \supset B_2 \supset A_3 \supset \cdots. \text{ Define a bijection } h : A \rightarrow B \text{ by the rule}
\]
\[ h(x) = \begin{cases} f(x) & \text{if } x \in A_n - B_n \text{ for some } n, \\ x & \text{otherwise.} \end{cases} \]
(b) **Theorem (Schroeder-Bernstein theorem).** If there are injections \( f : A \to C \) and \( g : C \to A \), then \( A \) and \( C \) have the same cardinality.

7. Show that the sets \( D \) and \( E \) of Exercise 5 have the same cardinality.

8. Let \( X \) denote the two-element set \( \{0, 1\} \); let \( \mathcal{B} \) be the set of *countable* subsets of \( X^\omega \). Show that \( X^\omega \) and \( \mathcal{B} \) have the same cardinality.

9. (a) The formula

\[
\begin{align*}
h(1) &= 1, \\
h(2) &= 2, \\
(*) & \quad h(n) = [h(n + 1)]^2 - [h(n - 1)]^2 \quad \text{for } n \geq 2
\end{align*}
\]

is not one to which the principle of recursive definition applies. Show that nevertheless there does exist a function \( h : \mathbb{Z}_+ \to \mathbb{R} \) satisfying this formula. [**Hint:** Reformulate \((*)\) so that the principle will apply and require \( h \) to be positive.]

(b) Show that the formula \((*)\) of part (a) does not determine \( h \) uniquely. [**Hint:** If \( h \) is a positive function satisfying \((*)\), let \( f(i) = h(i) \) for \( i \neq 3 \), and let \( f(3) = -h(3) \).]

(c) Show that there is no function \( h : \mathbb{Z}_+ \to \mathbb{R} \) satisfying the formula

\[
\begin{align*}
h(1) &= 1, \\
h(2) &= 2, \\
h(n) &= [h(n + 1)]^2 + [h(n - 1)]^2 \quad \text{for } n \geq 2.
\end{align*}
\]

*§8 The Principle of Recursive Definition*

Before considering the general form of the principle of recursive definition, let us first prove it in a specific case, that of Lemma 7.2. That should make the underlying idea of the proof much clearer when we consider the general case.

So, given the infinite subset \( C \) of \( \mathbb{Z}_+ \), let us consider the following recursion formula for a function \( h : \mathbb{Z}_+ \to C \):

\[
\begin{align*}
(*) & \quad h(1) = \text{smallest element of } C, \\
& \quad h(i) = \text{smallest element of } [C - h(\{1, \ldots, i - 1\})] \quad \text{for } i > 1.
\end{align*}
\]

We shall prove that there exists a unique function \( h : \mathbb{Z}_+ \to C \) satisfying this recursion formula.

The first step is to prove that there exist functions defined on *sections* \( \{1, \ldots, n\} \) of \( \mathbb{Z}_+ \) that satisfy \((*)\):

**Lemma 8.1.** Given \( n \in \mathbb{Z}_+ \), there exists a function

\[
f : \{1, \ldots, n\} \to C
\]

that satisfies \((*)\) for all \( i \) in its domain.