19. Prove that if $f : A \to B$ is bijective and $g : B \to C$ is bijective, then the composite $g \circ f$ is a bijective map of A onto C.

20. Let $f : A \to B$ and $g : B \to C$ be functions.
    (a) Show that if $g \circ f$ is injective, then f is injective.
    (b) Show that if $g \circ f$ is surjective, then g is surjective.

21. Prove Theorem 1.1.14.

22. Let f, g be functions such that $(g \circ f)(x) = x$ for all $x \in D(f)$ and $(f \circ g)(y) = y$ for all $y \in D(g)$. Prove that $g = f^{-1}$.

Section 1.2 Mathematical Induction

Mathematical Induction is a powerful method of proof that is frequently used to establish the validity of statements that are given in terms of the natural numbers. Although its utility is restricted to this rather special context, Mathematical Induction is an indispensable tool in all branches of mathematics. Since many induction proofs follow the same formal lines of argument, we will often state only that a result follows from Mathematical Induction and leave it to the reader to provide the necessary details. In this section, we will state the principle and give several examples to illustrate how inductive proofs proceed.

We shall assume familiarity with the set of natural numbers:

$$\mathbb{N} := \{1, 2, 3, \cdots\},$$

with the usual arithmetic operations of addition and multiplication, and with the meaning of a natural number being less than another one. We will also assume the following fundamental property of $\mathbb{N}$.

1.2.1 Well-Ordering Property of $\mathbb{N}$ *Every nonempty subset of* $\mathbb{N}$ *has a least element.*

A more detailed statement of this property is as follows: If S is a subset of $\mathbb{N}$ and if $S \neq \emptyset$, then there exists $m \in S$ such that $m \leq k$ for all $k \in S$.

On the basis of the Well-Ordering Property, we shall derive a version of the Principle of Mathematical Induction that is expressed in terms of subsets of $\mathbb{N}$.

1.2.2 Principle of Mathematical Induction *Let S be a subset of* $\mathbb{N}$ *that possesses the two properties:*

(1) The number $1 \in S$.

(2) For every $k \in \mathbb{N}$, if $k \in S$, then $k + 1 \in S$.

Then we have $S = \mathbb{N}$.

Proof. Suppose to the contrary that $S \neq \mathbb{N}$. Then the set $\mathbb{N} \backslash S$ is not empty, so by the Well-Ordering Principle it has a least element m. Since $1 \in S$ by hypothesis (1), we know that $m > 1$. But this implies that $m - 1$ is also a natural number. Since $m - 1 < m$ and since m is the least element in $\mathbb{N}$ such that $m \notin S$, we conclude that $m - 1 \in S$.

We now apply hypothesis (2) to the element $k := m - 1$ in S, to infer that $k + 1 = (m - 1) + 1 = m$ belongs to S. But this statement contradicts the fact that $m \notin S$. Since m was obtained from the assumption that $\mathbb{N} \backslash S$ is not empty, we have obtained a contradiction. Therefore we must have $S = \mathbb{N}$. Q.E.D.

The Principle of Mathematical Induction is often set forth in the framework of properties or statements about natural numbers. If $P(n)$ is a meaningful statement about $n \in \mathbb{N}$, then $P(n)$ may be true for some values of n and false for others. For example, if $P_1(n)$ is the statement: "$n^2 = n$", then $P_1(1)$ is true while $P_1(n)$ is false for all $n > 1, n \in \mathbb{N}$. On the other hand, if $P_2(n)$ is the statement: "$n^2 > 1$", then $P_2(1)$ is false, while $P_2(n)$ is true for all $n > 1, n \in \mathbb{N}$.

In this context, the Principle of Mathematical Induction can be formulated as follows.

For each $n \in \mathbb{N}$, let $P(n)$ be a statement about n. Suppose that:

(1′) *$P(1)$ is true.*
(2′) *For every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.*

Then $P(n)$ is true for all $n \in \mathbb{N}$.

The connection with the preceding version of Mathematical Induction, given in 1.2.2, is made by letting $S := \{n \in \mathbb{N} : P(n) \text{ is true}\}$. Then the conditions (1) and (2) of 1.2.2 correspond exactly to the conditions (1′) and (2′), respectively. The conclusion that $S = \mathbb{N}$ in 1.2.2 corresponds to the conclusion that $P(n)$ is true for all $n \in \mathbb{N}$.

In (2′) the assumption "if $P(k)$ is true" is called the **induction hypothesis**. In establishing (2′), we are not concerned with the actual truth or falsity of $P(k)$, but only with the validity of the implication "if $P(k)$, then $P(k+1)$". For example, if we consider the statements $P(n)$: "$n = n + 5$", then (2′) is logically correct, for we can simply add 1 to both sides of $P(k)$ to obtain $P(k+1)$. However, since the statement $P(1)$: "$1 = 6$" is false, we cannot use Mathematical Induction to conclude that $n = n + 5$ for all $n \in \mathbb{N}$.

It may happen that statements $P(n)$ are false for certain natural numbers but then are true for all $n \geq n_0$ for some particular n_0. The Principle of Mathematical Induction can be modified to deal with this situation. We will formulate the modified principle, but leave its verification as an exercise. (See Exercise 12.)

1.2.3 Principle of Mathematical Induction (second version) *Let $n_0 \in \mathbb{N}$ and let $P(n)$ be a statement for each natural number $n \geq n_0$. Suppose that:*

be a statement for each natural number $n \geq n_0$. Suppose that:

(1) *The statement $P(n_0)$ is true.*
(2) *For all $k \geq n_0$, the truth of $P(k)$ implies the truth of $P(k+1)$.*

Then $P(n)$ is true for all $n \geq n_0$.

Sometimes the number n_0 in (1) is called the **base**, since it serves as the starting point, and the implication in (2), which can be written $P(k) \Rightarrow P(k+1)$, is called the **bridge**, since it connects the case k to the case $k+1$.

The following examples illustrate how Mathematical Induction is used to prove assertions about natural numbers.

1.2.4 Examples **(a)** For each $n \in \mathbb{N}$, the sum of the first n natural numbers is given by

$$1 + 2 + \cdots + n = \tfrac{1}{2}n(n+1).$$

To prove this formula, we let S be the set of all $n \in \mathbb{N}$ for which the formula is true. We must verify that conditions (1) and (2) of 1.2.2 are satisfied. If $n = 1$, then we have $1 = \frac{1}{2} \cdot 1 \cdot (1 + 1)$ so that $1 \in S$, and (1) is satisfied. Next, we *assume* that $k \in S$ and wish to infer from this assumption that $k + 1 \in S$. Indeed, if $k \in S$, then

$$1 + 2 + \cdots + k = \tfrac{1}{2}k(k+1).$$

If we add $k+1$ to both sides of the assumed equality, we obtain

$$\begin{aligned} 1+2+\cdots+k+(k+1) &= \tfrac{1}{2}k(k+1)+(k+1) \\ &= \tfrac{1}{2}(k+1)(k+2). \end{aligned}$$

Since this is the stated formula for $n=k+1$, we conclude that $k+1 \in S$. Therefore, condition (2) of 1.2.2 is satisfied. Consequently, by the Principle of Mathematical Induction, we infer that $S=\mathbb{N}$, so the formula holds for all $n \in \mathbb{N}$.

(b) For each $n \in \mathbb{N}$, the sum of the squares of the first n natural numbers is given by

$$1^2+2^2+\cdots+n^2 = \tfrac{1}{6}n(n+1)(2n+1).$$

To establish this formula, we note that it is true for $n=1$, since $1^2 = \frac{1}{6}\cdot 1\cdot 2\cdot 3$. If we assume it is true for k, then adding $(k+1)^2$ to both sides of the assumed formula gives

$$\begin{aligned} 1^2+2^2+\cdots+k^2+(k+1)^2 &= \tfrac{1}{6}k(k+1)(2k+1)+(k+1)^2 \\ &= \tfrac{1}{6}(k+1)(2k^2+k+6k+6) \\ &= \tfrac{1}{6}(k+1)(k+2)(2k+3). \end{aligned}$$

Consequently, the formula is valid for all $n \in \mathbb{N}$.

(c) Given two real numbers a and b, we will prove that $a-b$ is a factor of $a^n - b^n$ for all $n \in \mathbb{N}$.

First we see that the statement is clearly true for $n=1$. If we now assume that $a-b$ is a factor of $a^k - b^k$, then

$$\begin{aligned} a^{k+1} - b^{k+1} &= a^{k+1} - ab^k + ab^k - b^{k+1} \\ &= a(a^k - b^k) + b^k(a-b). \end{aligned}$$

By the induction hypothesis, $a-b$ is a factor of $a(a^k-b^k)$ and it is plainly a factor of $b^k(a-b)$. Therefore, $a-b$ is a factor of $a^{k+1}-b^{k+1}$, and it follows from Mathematical Induction that $a-b$ is a factor of a^n-b^n for all $n \in \mathbb{N}$.

A variety of divisibility results can be derived from this fact. For example, since $11-7=4$, we see that $11^n - 7^n$ is divisible by 4 for all $n \in \mathbb{N}$.

(d) The inequality $2^n > 2n+1$ is false for $n=1, 2$, but it is true for $n=3$. If we assume that $2^k > 2k+1$, then multiplication by 2 gives, when $2k+2>3$, the inequality

$$2^{k+1} > 2(2k+1) = 4k+2 = 2k+(2k+2) > 2k+3 = 2(k+1)+1.$$

Since $2k+2>3$ for all $k \geq 1$, the bridge is valid for all $k \geq 1$ (even though the statement is false for $k=1, 2$). Hence, with the base $n_0 = 3$, we can apply Mathematical Induction to conclude that the inequality holds for all $n \geq 3$.

(e) The inequality $2^n \leq (n+1)!$ can be established by Mathematical Induction.

We first observe that it is true for $n=1$, since $2^1 = 2 = 1+1$. If we assume that $2^k \leq (k+1)!$, it follows from the fact that $2 \leq k+2$ that

$$2^{k+1} = 2\cdot 2^k \leq 2(k+1)! \leq (k+2)(k+1)! = (k+2)!.$$

Thus, if the inequality holds for k, then it also holds for $k+1$. Therefore, Mathematical Induction implies that the inequality is true for all $n \in \mathbb{N}$.

(f) If $r \in \mathbb{R}$, $r \neq 1$, and $n \in \mathbb{N}$, then

$$1+r+r^2+\cdots+r^n = \frac{1-r^{n+1}}{1-r}.$$

This is the formula for the sum of the terms in a "geometric progression". It can be established using Mathematical Induction as follows. First, if $n = 1$, then $1 + r = (1 - r^2)/(1 - r)$. If we assume the truth of the formula for $n = k$ and add the term r^{k+1} to both sides, we get (after a little algebra)

$$1 + r + r^k + \cdots + r^{k+1} = \frac{1 - r^{k+1}}{1 - r} + r^{k+1} = \frac{1 - r^{k+2}}{1 - r},$$

which is the formula for $n = k + 1$. Therefore, Mathematical Induction implies the validity of the formula for all $n \in \mathbb{N}$.

[This result can also be proved without using Mathematical Induction. If we let $s_n := 1 + r + r^2 + \cdots + r^n$, then $rs_n = r + r^2 + \cdots + r^{n+1}$, so that

$$(1 - r)s_n = s_n - rs_n = 1 - r^{n+1}.$$

If we divide by $1 - r$, we obtain the stated formula.]

(g) Careless use of the Principle of Mathematical Induction can lead to obviously absurd conclusions. The reader is invited to find the error in the "proof" of the following assertion.

Claim: If $n \in \mathbb{N}$ and if the maximum of the natural numbers p and q is n, then $p = q$.

"Proof." Let S be the subset of $\mathbb{N}$ for which the claim is true. Evidently, $1 \in S$ since if $p, q \in \mathbb{N}$ and their maximum is 1, then both equal 1 and so $p = q$. Now assume that $k \in S$ and that the maximum of p and q is $k + 1$. Then the maximum of $p - 1$ and $q - 1$ is k. But since $k \in S$, then $p - 1 = q - 1$ and therefore $p = q$. Thus, $k + 1 \in S$, and we conclude that the assertion is true for all $n \in \mathbb{N}$.

(h) There are statements that are true for *many* natural numbers but that are not true for *all* of them.

For example, the formula $p(n) := n^2 - n + 41$ gives a prime number for $n = 1, 2, \cdots, 40$. However, $p(41)$ is obviously divisible by 41, so it is not a prime number. □

Another version of the Principle of Mathematical Induction is sometimes quite useful. It is called the " Principle of Strong Induction", even though it is in fact equivalent to 1.2.2.

1.2.5 Principle of Strong Induction *Let S be a subset of $\mathbb{N}$ such that*

(1″) $1 \in S$.

(2″) *For every $k \in \mathbb{N}$, if $\{1, 2, \cdots, k\} \subseteq S$, then $k + 1 \in S$.*

Then $S = \mathbb{N}$.

We will leave it to the reader to establish the equivalence of 1.2.2 and 1.2.5.

Exercises for Section 1.2

1. Prove that $1/1 \cdot 2 + 1/2 \cdot 3 + \cdots + 1/n(n + 1) = n/(n + 1)$ for all $n \in \mathbb{N}$.
2. Prove that $1^3 + 2^3 + \cdots + n^3 = \left[\frac{1}{2}n(n + 1)\right]^2$ for all $n \in \mathbb{N}$.
3. Prove that $3 + 11 + \cdots + (8n - 5) = 4n^2 - n$ for all $n \in \mathbb{N}$.
4. Prove that $1^2 + 3^2 + \cdots + (2n - 1)^2 = (4n^3 - n)/3$ for all $n \in \mathbb{N}$.
5. Prove that $1^2 - 2^2 + 3^2 + \cdots + (-1)^{n+1}n^2 = (-1)^{n+1}n(n + 1)/2$ for all $n \in \mathbb{N}$.

6. Prove that $n^3 + 5n$ is divisible by 6 for all $n \in \mathbb{N}$.
7. Prove that $5^{2n} - 1$ is divisible by 8 for all $n \in \mathbb{N}$.
8. Prove that $5^n - 4n - 1$ is divisible by 16 for all $n \in \mathbb{N}$.
9. Prove that $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9 for all $n \in \mathbb{N}$.
10. Conjecture a formula for the sum $1/1 \cdot 3 + 1/3 \cdot 5 + \cdots + 1/(2n-1)(2n+1)$, and prove your conjecture by using Mathematical Induction.
11. Conjecture a formula for the sum of the first n odd natural numbers $1 + 3 + \cdots + (2n - 1)$, and prove your formula by using Mathematical Induction.
12. Prove the Principle of Mathematical Induction 1.2.3 (second version).
13. Prove that $n < 2^n$ for all $n \in \mathbb{N}$.
14. Prove that $2^n < n!$ for all $n \geq 4$, $n \in \mathbb{N}$.
15. Prove that $2n - 3 \leq 2^{n-2}$ for all $n \geq 5$, $n \in \mathbb{N}$.
16. Find all natural numbers n such that $n^2 < 2^n$. Prove your assertion.
17. Find the largest natural number m such that $n^3 - n$ is divisible by m for all $n \in \mathbb{N}$. Prove your assertion.
18. Prove that $1/\sqrt{1} + 1/\sqrt{2} + \cdots + 1/\sqrt{n} > \sqrt{n}$ for all $n \in \mathbb{N}$.
19. Let S be a subset of $\mathbb{N}$ such that (a) $2^k \in S$ for all $k \in \mathbb{N}$, and (b) if $k \in S$ and $k \geq 2$, then $k - 1 \in S$. Prove that $S = \mathbb{N}$.
20. Let the numbers x_n be defined as follows: $x_1 := 1$, $x_2 := 2$, and $x_{n+2} := \frac{1}{2}(x_{n+1} + x_n)$ for all $n \in \mathbb{N}$. Use the Principle of Strong Induction (1.2.5) to show that $1 \leq x_n \leq 2$ for all $n \in \mathbb{N}$.

Section 1.3 Finite and Infinite Sets

When we count the elements in a set, we say "one, two, three,$\cdots$", stopping when we have exhausted the set. From a mathematical perspective, what we are doing is defining a bijective mapping between the set and a portion of the set of natural numbers. If the set is such that the counting does not terminate, such as the set of natural numbers itself, then we describe the set as being infinite.

The notions of "finite" and "infinite" are extremely primitive, and it is very likely that the reader has never examined these notions very carefully. In this section we will define these terms precisely and establish a few basic results and state some other important results that seem obvious but whose proofs are a bit tricky. These proofs can be found in Appendix B and can be read later.

1.3.1 Definition **(a)** The empty set $\emptyset$ is said to have 0 **elements.**

(b) If $n \in \mathbb{N}$, a set S is said to have n **elements** if there exists a bijection from the set $\mathbb{N}_n := \{1, 2, \cdots, n\}$ onto S.

(c) A set S is said to be **finite** if it is either empty or it has n elements for some $n \in \mathbb{N}$.

(d) A set S is said to be **infinite** if it is not finite.

Since the inverse of a bijection is a bijection, it is easy to see that a set S has n elements if and only if there is a bijection from S onto the set $\{1, 2, \cdots, n\}$. Also, since the composition of two bijections is a bijection, we see that a set S_1 has n elements if and only if there is a bijection from S_1 onto another set S_2 that has n elements. Further, a set T_1 is finite if and only if there is a bijection from T_1 onto another set T_2 that is finite.

It is now necessary to establish some basic properties of finite sets to be sure that the definitions do not lead to conclusions that conflict with our experience of counting. From the definitions, it is not entirely clear that a finite set might not have n elements for *more than one* value of n. Also it is conceivably possible that the set $\mathbb{N} := \{1, 2, 3, \cdots\}$ might be a finite set according to this definition. The reader will be relieved that these possibilities do not occur, as the next two theorems state. The proofs of these assertions, which use the fundamental properties of $\mathbb{N}$ described in Section 1.2, are given in Appendix B.

1.3.2 Uniqueness Theorem *If S is a finite set, then the number of elements in S is a unique number in $\mathbb{N}$.*

1.3.3 Theorem *The set $\mathbb{N}$ of natural numbers is an infinite set.*

The next result gives some elementary properties of finite and infinite sets.

1.3.4 Theorem **(a)** *If A is a set with m elements and B is a set with n elements and if $A \cap B = \emptyset$, then $A \cup B$ has $m + n$ elements.*

(b) *If A is a set with $m \in \mathbb{N}$ elements and $C \subseteq A$ is a set with 1 element, then $A \backslash C$ is a set with $m - 1$ elements.*

(c) *If C is an infinite set and B is a finite set, then $C \backslash B$ is an infinite set.*

Proof. (a) Let f be a bijection of $\mathbb{N}_m$ onto A, and let g be a bijection of $\mathbb{N}_n$ onto B. We define h on $\mathbb{N}_{m+n}$ by $h(i) := f(i)$ for $i = 1, \cdots, m$ and $h(i) := g(i - m)$ for $i = m + 1, \cdots, m + n$. We leave it as an exercise to show that h is a bijection from $\mathbb{N}_{m+n}$ onto $A \cup B$.

The proofs of parts (b) and (c) are left to the reader, see Exercise 2. Q.E.D.

It may seem "obvious" that a subset of a finite set is also finite, but the assertion must be deduced from the definitions. This and the corresponding statement for infinite sets are established next.

1.3.5 Theorem *Suppose that S and T are sets and that $T \subseteq S$.*

(a) *If S is a finite set, then T is a finite set.*

(b) *If T is an infinite set, then S is an infinite set.*

Proof. (a) If $T = \emptyset$, we already know that T is a finite set. Thus we may suppose that $T \neq \emptyset$. The proof is by induction on the number of elements in S.

If S has 1 element, then the only nonempty subset T of S must coincide with S, so T is a finite set.

Suppose that every nonempty subset of a set with k elements is finite. Now let S be a set having $k + 1$ elements (so there exists a bijection f of $\mathbb{N}_{k+1}$ onto S), and let $T \subseteq S$. If $f(k + 1) \notin T$, we can consider T to be a subset of $S_1 := S \backslash \{f(k + 1)\}$, which has k elements by Theorem 1.3.4(b). Hence, by the induction hypothesis, T is a finite set.

On the other hand, if $f(k + 1) \in T$, then $T_1 := T \backslash \{f(k + 1)\}$ is a subset of S_1. Since S_1 has k elements, the induction hypothesis implies that T_1 is a finite set. But this implies that $T = T_1 \cup \{f(k + 1)\}$ is also a finite set.

(b) This assertion is the contrapositive of the assertion in (a). (See Appendix A for a discussion of the contrapositive.) Q.E.D.

Countable Sets

We now introduce an important type of infinite set.

1.3.6 Definition **(a)** A set S is said to be **denumerable** (or **countably infinite**) if there exists a bijection of $\mathbb{N}$ onto S.

(b) A set S is said to be **countable** if it is either finite or denumerable.

(c) A set S is said to be **uncountable** if it is not countable.

From the properties of bijections, it is clear that S is denumerable if and only if there exists a bijection of S onto $\mathbb{N}$. Also a set S_1 is denumerable if and only if there exists a bijection from S_1 onto a set S_2 that is denumerable. Further, a set T_1 is countable if and only if there exists a bijection from T_1 onto a set T_2 that is countable. Finally, an infinite countable set is denumerable.

1.3.7 Examples **(a)** The set $E := \{2n : n \in \mathbb{N}\}$ of *even* natural numbers is denumerable, since the mapping $f : \mathbb{N} \to E$ defined by $f(n) := 2n$ for $n \in \mathbb{N}$, is a bijection of $\mathbb{N}$ onto E.

Similarly, the set $O := \{2n - 1 : n \in \mathbb{N}\}$ of *odd* natural numbers is denumerable.

(b) The set $\mathbb{Z}$ of *all* integers is denumerable.

To construct a bijection of $\mathbb{N}$ onto $\mathbb{Z}$, we map 1 onto 0, we map the set of even natural numbers onto the set $\mathbb{N}$ of positive integers, and we map the set of odd natural numbers onto the negative integers. This mapping can be displayed by the enumeration:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \cdots\}.$$

(c) The union of two disjoint denumerable sets is denumerable.

Indeed, if $A = \{a_1, a_2, a_3, \cdots\}$ and $B = \{b_1, b_2, b_3, \cdots\}$, we can enumerate the elements of $A \cup B$ as:

$$a_1, b_1, a_2, b_2, a_3, b_3, \cdots. \qquad \square$$

1.3.8 Theorem *The set* $\mathbb{N} \times \mathbb{N}$ *is denumerable.*

Informal Proof. Recall that $\mathbb{N} \times \mathbb{N}$ consists of all ordered pairs (m, n), where $m, n \in \mathbb{N}$. We can enumerate these pairs as:

$$(1, 1), \quad (1, 2), \quad (2, 1), \quad (1, 3), \quad (2, 2), \quad (3, 1), \quad (1, 4), \cdots,$$

according to increasing sum $m + n$, and increasing m. (See Figure 1.3.1.) Q.E.D.

The enumeration just described is an instance of a "diagonal procedure", since we move along diagonals that each contain finitely many terms as illustrated in Figure 1.3.1. While this argument is satisfying in that it shows exactly what the bijection of $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ should do, it is not a "formal proof", since it doesn't define this bijection precisely. (See Appendix B for a more formal proof.)

As we have remarked, the construction of an explicit bijection between sets is often complicated. The next two results are useful in establishing the countability of sets, since they do not involve showing that certain mappings are bijections. The first result may seem intuitively clear, but its proof is rather technical; it will be given in Appendix B.

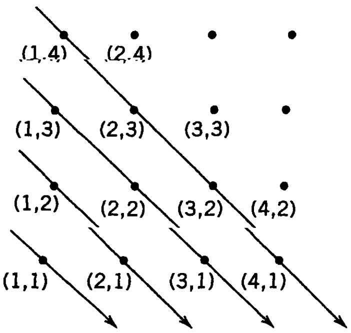

Figure 1.3.1 The set $\mathbb{N} \times \mathbb{N}$

1.3.9 Theorem *Suppose that S and T are sets and that $T \subseteq S$.*

(a) *If S is a countable set, then T is a countable set.*

(b) *If T is an uncountable set, then S is an uncountable set.*

1.3.10 Theorem *The following statements are equivalent:*

(a) *S is a countable set.*

(b) *There exists a surjection of $\mathbb{N}$ onto S.*

(c) *There exists an injection of S into $\mathbb{N}$.*

Proof. (a) $\Rightarrow$ (b) If S is finite, there exists a bijection h of some set $\mathbb{N}_n$ onto S and we define H on $\mathbb{N}$ by

$$H(k) := \begin{cases} h(k) & \text{for } k = 1, \cdots, n, \\ h(n) & \text{for } k > n. \end{cases}$$

Then H is a surjection of $\mathbb{N}$ onto S.

If S is denumerable, there exists a bijection H of $\mathbb{N}$ onto S, which is also a surjection of $\mathbb{N}$ onto S.

(b) $\Rightarrow$ (c) If H is a surjection of $\mathbb{N}$ onto S, we define $H_1 : S \to \mathbb{N}$ by letting $H_1(s)$ be the least element in the set $H^{-1}(s) := \{n \in \mathbb{N} : H(n) = s\}$. To see that H_1 is an injection of S into $\mathbb{N}$, note that if $s, t \in S$ and $n_{st} := H_1(s) = H_1(t)$, then $s = H(n_{st}) = t$.

(c) $\Rightarrow$ (a) If H_1 is an injection of S into $\mathbb{N}$, then it is a bijection of S onto $H_1(S) \subseteq \mathbb{N}$. By Theorem 1.3.9(a), $H_1(S)$ is countable, whence the set S is countable. Q.E.D.

1.3.11 Theorem *The set $\mathbb{Q}$ of all rational numbers is denumerable.*

Proof. The idea of the proof is to observe that the set $\mathbb{Q}^+$ of positive rational numbers is contained in the enumeration:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \cdots,$$

which is another "diagonal mapping" (see Figure 1.3.2). However, this mapping is not an injection, since the different fractions $\frac{1}{2}$ and $\frac{2}{4}$ represent the same rational number.

To proceed more formally, note that since $\mathbb{N} \times \mathbb{N}$ is countable (by Theorem 1.3.8), it follows from Theorem 1.3.10(b) that there exists a surjection f of $\mathbb{N}$ onto $\mathbb{N} \times \mathbb{N}$. If

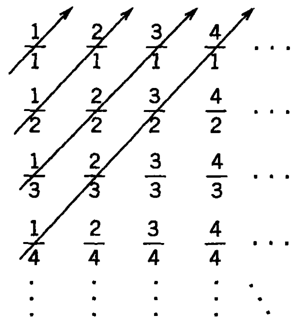

Figure 1.3.2 The set $\mathbb{Q}^+$

$g : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}^+$ is the mapping that sends the ordered pair (m, n) into the rational number having a representation m/n, then g is a surjection onto $\mathbb{Q}^+$. Therefore, the composition $g \circ f$ is a surjection of $\mathbb{N}$ onto $\mathbb{Q}^+$, and Theorem 1.3.10 implies that $\mathbb{Q}^+$ is a countable set.

Similarly, the set $\mathbb{Q}^-$ of all negative rational numbers is countable. It follows as in Example 1.3.7(b) that the set $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$ is countable. Since $\mathbb{Q}$ contains $\mathbb{N}$, it must be a denumerable set. Q.E.D.

The next result is concerned with unions of sets. In view of Theorem 1.3.10, we need not be worried about possible overlapping of the sets. Also, we do not have to construct a bijection.

1.3.12 Theorem *If A_m is a countable set for each $m \in \mathbb{N}$, then the union $A := \bigcup_{m=1}^{\infty} A_m$ is countable.*

Proof. For each $m \in \mathbb{N}$, let φ_m be a surjection of $\mathbb{N}$ onto A_m. We define $\psi : \mathbb{N} \times \mathbb{N} \to A$ by

$$\psi(m, n) := \varphi_m(n).$$

We claim that ψ is a surjection. Indeed, if $a \in A$, then there exists a least $m \in \mathbb{N}$ such that $a \in A_m$, whence there exists a least $n \in \mathbb{N}$ such that $a = \varphi_m(n)$. Therefore, $a = \psi(m, n)$.

Since $\mathbb{N} \times \mathbb{N}$ is countable, it follows from Theorem 1.3.10 that there exists a surjection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ whence $\psi \circ f$ is a surjection of $\mathbb{N}$ onto A. Now apply Theorem 1.3.10 again to conclude that A is countable. Q.E.D.

Remark A less formal (but more intuitive) way to see the truth of Theorem 1.3.12 is to enumerate the elements of A_m, $m \in \mathbb{N}$, as:

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \cdots\}, \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \cdots\}, \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \cdots\}, \\ &\cdots \quad \cdots \quad \cdots . \end{aligned}$$

We then enumerate this array using the "diagonal procedure":

$$a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, \cdots,$$

as was displayed in Figure 1.3.1.

The argument that the set $\mathbb{Q}$ of rational numbers is countable was first given in 1874 by Georg Cantor (1845–1918). He was the first mathematician to examine the concept of infinite set in rigorous detail. In contrast to the countability of $\mathbb{Q}$, he also proved the set $\mathbb{R}$ of real numbers is an uncountable set. (This result will be established in Section 2.5.)

In a series of important papers, Cantor developed an extensive theory of infinite sets and transfinite arithmetic. Some of his results were quite surprising and generated considerable controversy among mathematicians of that era. In a 1877 letter to his colleague Richard Dedekind, he wrote, after proving an unexpected theorem, "I see it, but I do not believe it".

We close this section with one of Cantor's more remarkable theorems.

1.3.13 Cantor's Theorem *If A is any set, then there is no surjection of A onto the set $\mathcal{P}(A)$ of all subsets of A.*

Proof. Suppose that $\varphi : A \to \mathcal{P}(A)$ is a surjection. Since $\varphi(a)$ is a subset of A, either a belongs to $\varphi(a)$ or it does not belong to this set. We let

$$D := \{a \in A : a \notin \varphi(a)\}.$$

Since D is a subset of A, if φ is a surjection, then $D = \varphi(a_0)$ for some $a_0 \in A$.

We must have either $a_0 \in D$ or $a_0 \notin D$. If $a_0 \in D$, then since $D = \varphi(a_0)$, we must have $a_0 \in \varphi(a_0)$, contrary to the definition of D. Similarly, if $a_0 \notin D$, then $a_0 \notin \varphi(a_0)$ so that $a_0 \in D$, which is also a contradiction.

Therefore, φ cannot be a surjection. Q.E.D.

Cantor's Theorem implies that there is an unending progression of larger and larger sets. In particular, it implies that the collection $\mathcal{P}(\mathbb{N})$ of all subsets of the natural numbers $\mathbb{N}$ *is uncountable.*

Exercises for Section 1.3

1. Prove that a nonempty set T_1 is finite if and only if there is a bijection from T_1 onto a finite set T_2.
2. Prove parts (b) and (c) of Theorem 1.3.4.
3. Let $S := \{1, 2\}$ and $T := \{a, b, c\}$.
   (a) Determine the number of different injections from S into T.
   (b) Determine the number of different surjections from T onto S.
4. Exhibit a bijection between $\mathbb{N}$ and the set of all odd integers greater than 13.
5. Give an explicit definition of the bijection f from $\mathbb{N}$ onto $\mathbb{Z}$ described in Example 1.3.7(b).
6. Exhibit a bijection between $\mathbb{N}$ and a proper subset of itself.
7. Prove that a set T_1 is denumerable if and only if there is a bijection from T_1 onto a denumerable set T_2.
8. Give an example of a countable collection of finite sets whose union is not finite.
9. Prove in detail that if S and T are denumerable, then $S \cup T$ is denumerable.
10. Determine the number of elements in $\mathcal{P}(S)$, the collection of all subsets of S, for each of the following sets:
    (a) $S := \{1, 2\}$,
    (b) $S := \{1, 2, 3\}$,
    (c) $S := \{1, 2, 3, 4\}$.
    Be sure to include the empty set and the set S itself in $\mathcal{P}(S)$.
11. Use Mathematical Induction to prove that if the set S has n elements, then $\mathcal{P}(S)$ has 2^n elements.
12. Prove that the collection $\mathcal{F}(\mathbb{N})$ of all *finite* subsets of $\mathbb{N}$ is countable.