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 $n \in \mathbb{N}$, $n > 1$.
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, . . . ," 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 $\mathbb{N}_n := \{1, 2, \ldots, n\}$ 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 $\{1, 2, \ldots, n\}$. 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 $\mathbb{N} := \{1, 2, 3, \ldots\}$ 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 $i = 1, \ldots, m$ and $h(i) := g(i - m)$ for $i = m + 1, \ldots, m + n$. 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:

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

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

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

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

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:

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

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.

The bijection indicated by the diagram can be derived as follows. We first notice that the first diagonal has one point, the second diagonal has two points, and so on, with k points in the kth diagonal. Applying the formula in Example 1.2.4(a), we see that the total number of points in diagonals 1 through k is given by

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

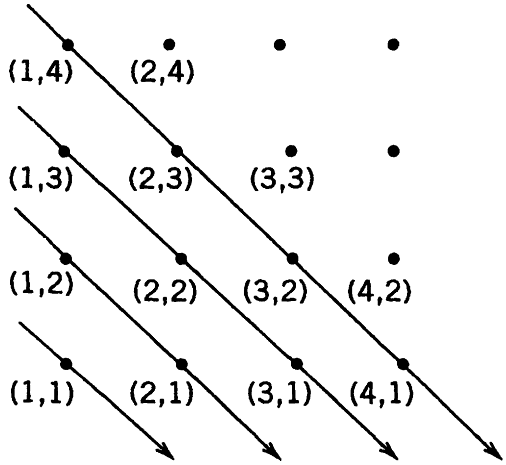


Figure 1.3.1 The set $\mathbb{N} \times \mathbb{N}$

The point (m, n) lies in the kth diagonal when $k = m + n - 1$, and it is the mth point in that diagonal as we move downward from left to right. (For example, the point (3, 2) lies in the 4th diagonal since $3 + 2 - 1 = 4$, and it is the 3rd point in that diagonal.) Therefore, in the counting scheme displayed by Figure 1.3.1, we count the point (m, n) by first counting the points in the first $k - 1 = m + n - 2$ diagonals and then adding m. Therefore, the counting function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is given by

$$\begin{aligned} h(m, n) &:= \psi(m + n - 2) + m \\ &= \tfrac{1}{2}(m + n - 2)(m + n - 1) + m. \end{aligned}$$

For example, the point (3, 2) is counted as number $h(3, 2) = \frac{1}{2} \cdot 3 \cdot 4 + 3 = 9$, as shown by Figure 1.3.1. Similarly, the point (17, 25) is counted as number $h\,(17, 25) = \psi(40) + 17 = 837$.

This geometric argument leading to the counting formula has been suggestive and convincing, but it remains to be proved that h is, in fact, a bijection of $\mathbb{N} \times \mathbb{N}$ onto $\mathbb{N}$. A detailed proof is given in Appendix B.

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.

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) ⇒ (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

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

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) ⇒ (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) ⇒ (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:

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

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.

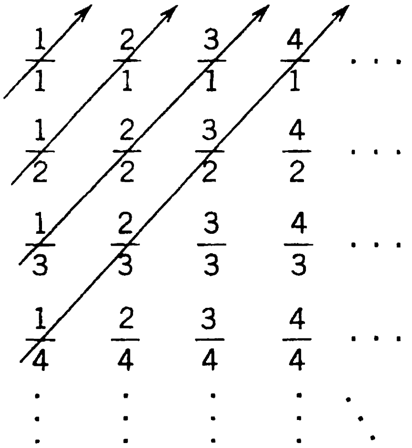


Figure 1.3.2 The set $\mathbb{Q}^+$

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 $g : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}^+$ 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 $m \in N$, 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 $\beta : \mathbb{N} \times \mathbb{N} \to A$ by

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

We claim that β 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, $a = \beta\,(m, n)$.

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 $\beta \circ f$ 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:

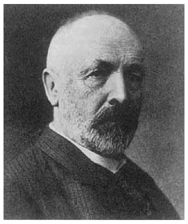
$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \ldots\}, \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \ldots\}, \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \ldots\}, \\ &\cdots \quad \cdots \quad \cdots. \end{aligned}$$

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

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

as was displayed in Figure 1.3.1.

Georg Cantor



Georg Cantor (1845–1918) was born in St. Petersburg, Russia. His father, a Danish businessman working in Russia, moved the family to Germany several years later. Cantor studied briefly at Zurich, then went to the University of Berlin, the best in mathematics at the time. He received his doctorate in 1869, and accepted a position at the University of Halle, where he worked alone on his research, but would occasionally travel the seventy miles to Berlin to visit colleagues.

Cantor is known as the founder of modern set theory and he was the first to study the concept of infinite set in rigorous detail. In 1874 he proved that $\mathbb{Q}$ is countable and, in contrast, that $\mathbb{R}$ is uncountable (see Section 2.5), exhibiting two kinds of infinity. In a series of papers he developed a general theory of infinite sets, including some surprising results. In 1877 he proved that the two-dimensional unit square in the plane could be put into one-one correspondence with the unit interval on the line, a result he sent in a letter to his colleague Richard Dedekind in Berlin, writing "I see it, but I do not believe it." Cantor's Theorem on sets of subsets shows there are many different orders of infinity and this led him to create a theory of "transfinite" numbers that he published in 1895 and 1897. His work generated considerable controversy among mathematicians of that era, but in 1904, London's Royal Society awarded Cantor the Sylvester Medal, its highest honor.

Beginning in 1884, he suffered from episodes of depression that increased in severity as the years passed. He was hospitalized several times for nervous breakdowns in the Halle Nervenklinik and spent the last seven months of his life there.

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. (a) If (m, n) is the 6th point down the 9th diagonal of the array in Figure 1.3.1, calculate its number according to the counting method given for Theorem 1.3.8.
    (b) Given that $h(m, 3) = 19$, find m.
11. 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 $\mathcal{P}(S)$.
12. Use Mathematical Induction to prove that if the set S has n elements, then $\mathcal{P}(S)$ has 2^n elements.
13. Prove that the collection $\mathcal{F}(\mathbb{N})$ of all *finite* subsets of $\mathbb{N}$ is countable.

APPENDIX B

FINITE AND COUNTABLE SETS

We will establish the results that were stated in Section 1.3 without proof. The reader should refer to that section for the definitions.

The first result is sometimes called the "Pigeonhole Principle." It may be interpreted as saying that if m pigeons are put into n pigeonholes and if $m > n$, then at least two pigeons must share one of the pigeonholes. This is a frequently used result in combinatorial analysis. It yields many useful consequences.

B.1 Theorem *Let $m, n \in \mathbb{N}$ with $m > n$. Then there does not exist an injection from $\mathbb{N}_m$ into $\mathbb{N}_n$.*

Proof. We will prove this by induction on n.

If $n = 1$ and if g is any map of $\mathbb{N}_m (m > 1)$ into $\mathbb{N}_1$, then it is clear that $g(1) = \cdots = g(m) = 1$, so that g is not injective.

Assume that $k > 1$ is such that if $m > k$, there is no injection from $\mathbb{N}_m$ into $\mathbb{N}_k$. We will show that if $m > k + 1$, there is no function $h : \mathbb{N}_m \to \mathbb{N}_{k+1}$ that is an injection.

Case 1: If the range $h(\mathbb{N}_m) \subseteq \mathbb{N}_k \subset \mathbb{N}_{k+1}$, then the induction hypothesis implies that h is not an injection of $\mathbb{N}_m$ into $\mathbb{N}_k$, and therefore into $\mathbb{N}_{k+1}$.

Case 2: Suppose that $h(\mathbb{N}_m)$ is not contained in $\mathbb{N}_k$. If more than one element in $\mathbb{N}_m$ is mapped into $k + 1$, then h is not an injection. Therefore, we may assume that a single $p \in \mathbb{N}_m$ is mapped into $k + 1$ by h. We now define $h_1 : \mathbb{N}_{m-1} \to \mathbb{N}_k$ by

$$h_1(q) := \begin{cases} h(q) & \text{if } q = 1, \ldots, p-1, \\ h(q+1) & \text{if } q = p, \ldots, m-1. \end{cases}$$

Since the induction hypothesis implies that h_1 is not an injection into $\mathbb{N}_k$, it is easily seen that h is not an injection into $\mathbb{N}_{k+1}$. Q.E.D.

We now show that a finite set determines a unique number in $\mathbb{N}$.

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

Proof. If the set S has m elements, there exists a bijection f_1 of $\mathbb{N}_m$ onto S. If S also has n elements, there exists a bijection f_2 of $\mathbb{N}_n$ onto S. If $m > n$, then (by Exercise 21 of Section 1.1) $f_2^{-1} \circ f_1$, is a bijection of $\mathbb{N}_m$ onto $\mathbb{N}_n$, which contradicts Theorem B.1. If $n > m$, then $f_1^{-1} \circ f_2$ is a bijection of $\mathbb{N}_n$ onto $\mathbb{N}_m$, which contradicts Theorem B.1. Therefore we have $m = n$. Q.E.D.

B.2 Theorem *If $n \in \mathbb{N}$, there does not exist an injection from $\mathbb{N}$ into $\mathbb{N}_n$.*

Proof. Assume that $f : \mathbb{N} \to \mathbb{N}_n$ is an injection, and let $m := n + 1$. Then the restriction of f to $\mathbb{N}_m \subset \mathbb{N}$ is also an injection into $\mathbb{N}_n$. But this contradicts Theorem B.1. Q.E.D.

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

Proof. If $\mathbb{N}$ is a finite set, there exists some $n \in \mathbb{N}$ and a bijection f of $\mathbb{N}_n$ onto $\mathbb{N}$. In this case the inverse function f^{-1} is a bijection (and hence an injection) of $\mathbb{N}$ onto $\mathbb{N}_n$. But this contradicts Theorem B.2. Q.E.D.

We will next establish Theorem 1.3.8. In connection with the array displayed in Figure 1.3.1, the function h was defined by $h(m,n) = \psi(m+n-2)+m$, where $\psi(k) = 1+2+\cdots+k = \frac{1}{2}k(k+1)$. We now prove that the function h is a bijection.

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

Proof. We will show that the function h is a bijection.

(a) We first show that h is injective. If $(m,n) \neq (m',n')$, then either (i) $m+n \neq m'+n'$, or (ii) $m+n = m'+n'$ and $m \neq m'$.

In case (i), we may suppose $m+n < m'+n'$. Then, using formula (1), the fact that ψ is increasing, and $m' > 0$, we have

$$\begin{aligned} h(m,n) &= \psi(m+n-2)+m \leq \psi(m+n-2)+(m+n-1) \\ &= \psi(m+n-1) \leq \psi(m'+n'-2) \\ &< \psi(m'+n'-2)+m' = h(m',n'). \end{aligned}$$

In case (ii), if $m+n = m'+n'$ and $m \neq m'$, then

$$h(m,n)-m = \psi(m+n-2) = \psi(m'+n'-2) = h(m',n')-m',$$

whence $h(m,n) \neq h(m',n')$.

(b) Next we show that h is surjective.

Clearly $h(1,1) = 1$. If $p \in \mathbb{N}$ with $p \geq 2$, we will find a pair $(m_p,n_p) \in \mathbb{N}\times\mathbb{N}$ with $h(m_p,n_p) = p$. Since $p < \psi(p)$, then the set $E_p := \{k \in \mathbb{N} : p \leq \psi(k)\}$ is nonempty.

Using the Well-Ordering Property 1.2.1, we let $k_p > 1$ be the least element in E_p. (This means that p lies in the k_pth diagonal.) Since $p \geq 2$, it follows from equation (1) that

$$\psi(k_p-1) < p \leq \psi(k_p) = \psi(k_p-1)+k_p.$$

Let $m_p := p-\psi(k_p-1)$ so that $1 \leq m_p \leq k_p$, and let $n_p := k_p-m_p+1$ so that $1 \leq n_p \leq k_p$ and $m_p+n_p-1 = k_n$. Therefore,

$$h(m_p,n_p) = \psi(m_p+n_p-2)+m_p = \psi(k_p-1)+m_p = p.$$

Thus h is a bijection and $\mathbb{N}\times\mathbb{N}$ is denumerable. Q.E.D.

The next result is crucial in proving Theorems 1.3.9 and 1.3.10.

B.3 Theorem *If $A \subseteq \mathbb{N}$ and A is infinite, there exists a function $\varphi : \mathbb{N} \to A$ such that $\varphi(n+1) > \varphi(n) \geq n$ for all $n \in \mathbb{N}$. Moreover, φ is a bijection of $\mathbb{N}$ onto A.*

Proof. Since A is infinite, it is not empty. We will use the Well-Ordering Property 1.2.1 of $\mathbb{N}$ to give a recursive definition of φ.

Since $A \neq 0$, there is a least element of A, which we define to be $\varphi(1)$; therefore, $\varphi(1) \geq 1$.

Since A is infinite, the set $A_1 := A\backslash\{\varphi(1)\}$ is not empty, and we define $\varphi(2)$ to be least element of A_1. Therefore $\varphi(2) > \varphi(1) \geq 1$, so that $\varphi(2) \geq 2$.

Suppose that φ has been defined to satisfy $\varphi(n+1) > \varphi(n) \geq n$ for $n = 1, \ldots, k-1$, whence $\varphi(k) > \varphi(k-1) \geq k-1$ so that $\varphi(k) \geq k$. Since the set A is infinite, the set

$$A_k := A \backslash \{\varphi(1), \ldots, \varphi(k)\}$$

is not empty and we define $\varphi(k+1)$ to be the least element in A_k. Therefore $\varphi(k+1) > \varphi(k)$, and since $\varphi(k) \geq k$, we also have $\varphi(k+1) \geq k+1$. Therefore, φ is defined on all of $\mathbb{N}$.

We claim that φ is an injection. If $m > n$, then $m = n + r$ for some $r \in \mathbb{N}$. If $r = 1$, then $\varphi(m) = \varphi(n+1) > \varphi(n)$. Suppose that $\varphi(n+k) > \varphi(n)$; we will show that $\varphi(n + (k+1)) > \varphi(n)$. Indeed, this follows from the fact that $\varphi(n + (k+1)) = \varphi((n + k) + 1) > \varphi(n+k) > \varphi(n)$. Since $\varphi(m) > \varphi(n)$ whenever $m > n$, it follows that φ is an injection.

We claim that φ is a surjection of $\mathbb{N}$ onto A. If not, the set $\tilde{A} := A \backslash \varphi(\mathbb{N})$ is not empty, and we let p be the least element in $\tilde{A}$. We claim that p belongs to the set $\{\varphi(1), \ldots, \varphi(p)\}$. Indeed, if this is not true, then

$$p \in A \backslash \{\varphi(1), \ldots, \varphi(p)\} = A_p,$$

so that $\varphi(p+1)$, being the least element in A_p, must satisfy $\varphi(p+1) \leq p$. But this contradicts the fact that $\varphi(p+1) > \varphi(p) \geq p$. Therefore $\tilde{A}$ is empty and φ is a surjection onto A. Q.E.D.

B.4 Theorem *If $A \subseteq \mathbb{N}$, then A is countable.*

Proof. If A is finite, then it is countable, so it suffices to consider the case that A is infinite. In this case, Theorem B.3 implies that there exists a bijection φ of $\mathbb{N}$ onto A, so that A is denumerable and, therefore, countable. Q.E.D.

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.*

Proof. (a) If S is a finite set, it follows from Theorem 1.3.5(a) that T is finite, and therefore countable. If S is denumerable, then there exists a bijection ψ of S onto $\mathbb{N}$. Since $\psi(S) \subseteq \mathbb{N}$, Theorem B.4 implies that $\psi(S)$ is countable. Since the restriction of ψ to T is a bijection onto $\psi(T)$ and $\psi(T) \subseteq \mathbb{N}$ is countable, it follows that T is also countable.

(b) This assertion is the contrapositive of the assertion in (a). Q.E.D.

then for any $\varepsilon > 0$, there exists an $m \in \mathbb{N}$ such that $0 \le \eta - \xi \le b_m - a_m < \varepsilon$. Since this holds for all $\varepsilon > 0$, it follows from Theorem 2.1.9 that $\eta - \xi = 0$. Therefore, we conclude that $\xi = \eta$ is the only point that belongs to I_n for every $n \in \mathbb{N}$. Q.E.D.

The Uncountability of $\mathbb{R}$

The concept of a countable set was discussed in Section 1.3 and the countability of the set $\mathbb{Q}$ of rational numbers was established there. We will now use the Nested Interval Property to prove that the set $\mathbb{R}$ is an *uncountable* set. The proof was given by Georg Cantor in 1874 in the first of his papers on infinite sets. He later published a proof that used decimal representations of real numbers, and that proof will be given later in this section.

2.5.4 Theorem *The set $\mathbb{R}$ of real numbers is not countable.*

Proof. We will prove that the unit interval $I := [0, 1]$ is an uncountable set. This implies that the set $\mathbb{R}$ is an uncountable set, for if $\mathbb{R}$ were countable, then the subset I would also be countable. (See Theorem 1.3.9(a).)

The proof is by contradiction. If we assume that I is countable, then we can enumerate the set as $I = \{x_1, x_2, \ldots, x_n, \ldots\}$. We first select a closed subinterval I_1 of I such that $x_1 \notin I_1$, then select a closed subinterval I_2 of I_1 such that $x_2 \notin I_2$, and so on. In this way, we obtain nonempty closed intervals

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$$

such that $I_n \subseteq I$ and $x_n \notin I_n$ for all n. The Nested Intervals Property 2.5.2 implies that there exists a point $\xi \in I$ such that $\xi \in I_n$ for all n. Therefore $\xi \neq x_n$ for all $n \in \mathbb{N}$, so the enumeration of I is not a complete listing of the elements of I, as claimed. Hence, I is an uncountable set. Q.E.D.

The fact that the set $\mathbb{R}$ of real numbers is uncountable can be combined with the fact that the set $\mathbb{Q}$ of rational numbers is countable to conclude that the set $\mathbb{R}\backslash\mathbb{Q}$ of irrational numbers is uncountable. Indeed, since the union of two countable sets is countable (see 1.3.7(c)), if $\mathbb{R}\backslash\mathbb{Q}$ is countable, then since $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R}\backslash\mathbb{Q})$, we conclude that $\mathbb{R}$ is also a countable set, which is a contradiction. Therefore, the set of irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ is an uncountable set.

Note: The set of real numbers can also be divided into two subsets of numbers called algebraic numbers and transcendental numbers. A real number is called *algebraic* if it is a solution of a polynomial equation $P(x) = 0$ where all the coefficients of the polynomial P are integers. A real number is called *transcendental* if it is not an algebraic number. It can be proved that the set of algebraic numbers is countably infinite, and consequently the set of transcendental numbers is uncountable. The numbers π and e are transcendental numbers, but the proofs of these facts are very deep. For an introduction to these topics, we refer the interested reader to the book by Ivan Niven listed in the References.

†Binary Representations

We will digress briefly to discuss informally the binary (and decimal) representations of real numbers. It will suffice to consider real numbers between 0 and 1, since the representations for other real numbers can then be obtained by adding a positive or negative number.

† The remainder of this section can be omitted on a first reading.