

CHAPTER 7

FUNCTIONS

Functions are ubiquitous in mathematics and computer science. That means you can hardly take two steps in these subjects without running into one. In this book we have previously discussed truth tables and input/output tables (which can be regarded as Boolean functions), sequences (which are functions defined on sets of integers), *mod* and *div* (which are functions defined on Cartesian products of integers), and floor and ceiling (which are functions from \mathbf{R} to \mathbf{Z}).

In this chapter we consider an additional wide variety of functions, focusing on those defined on discrete sets (such as finite sets or sets of integers). We then look at properties of functions such as one-to-one and onto, existence of inverse functions, and the interaction of composition of functions and the properties of one-to-one and onto. We end the chapter with the surprising result that there are different sizes of infinite sets and give an application to computability.

7.1 Functions Defined on General Sets

The theory that has had the greatest development in recent times is without any doubt the theory of functions. — Vito Volterra, 1888

As used in ordinary language, the word *function* indicates dependence of one varying quantity on another. If your teacher tells you that your grade in a course will be a function of your performance on the exams, you interpret this to mean that the teacher has some rule for translating exam scores into grades. To each collection of exam scores there corresponds a certain grade.

In Section 1.3 we defined a function as a certain type of relation. In this chapter we focus on the more dynamic way functions are used in mathematics. The following is a restatement of the definition of function that includes additional terminology associated with the concept.

• **Definition**

A **function f from a set X to a set Y** , denoted $f: X \rightarrow Y$, is a relation from X , the **domain**, to Y , the **co-domain**, that satisfies two properties: (1) every element in X is related to some element in Y , and (2) no element in X is related to more than one element in Y . Thus, given any element x in X , there is a unique element in Y that is related to x by f . If we call this element y , then we say that “ f sends x to y ” or “ f maps x to y ” and write $x \xrightarrow{f} y$ or $f: x \rightarrow y$. The unique element to which f sends x is denoted

$f(x)$ and is called

**f of x , or
the output of f for the input x , or
the value of f at x , or
the image of x under f .**

The set of all values of f taken together is called the *range of f* or the *image of X under f* . Symbolically,

$$\text{range of } f = \text{image of } X \text{ under } f = \{y \in Y \mid y = f(x), \text{ for some } x \text{ in } X\}.$$



Caution! Use $f(x)$ to refer to the value of the function f at x . Generally avoid using $f(x)$ to refer to the function f itself.



Stock Montage

Johann Peter Gustav Lejeune Dirichlet (1805–1859)

Given an element y in Y , there may exist elements in X with y as their image. If $f(x) = y$, then x is called a **preimage of y** or an **inverse image of y** . The set of all inverse images of y is called the *inverse image of y* . Symbolically,

$$\text{the inverse image of } y = \{x \in X \mid f(x) = y\}.$$

In some mathematical contexts, the notation $f(x)$ is used to refer both to the value of f at x and to the function f itself. Because using the notation this way can lead to confusion, we avoid it whenever possible. In this book, unless explicitly stated otherwise, the symbol $f(x)$ always refers to the value of the function f at x and not to the function f itself.

The concept of function was developed over a period of centuries. A definition similar to that given above was first formulated for sets of numbers by the German mathematician Lejeune Dirichlet (DEER-ish-lay) in 1837.

Arrow Diagrams

Recall from Section 1.3 that if X and Y are finite sets, you can define a function f from X to Y by drawing an arrow diagram. You make a list of elements in X and a list of elements in Y , and draw an arrow from each element in X to the corresponding element in Y , as shown in Figure 7.1.1.

This arrow diagram does define a function because

1. Every element of X has an arrow coming out of it.
2. No element of X has two arrows coming out of it that point to two different elements of Y .

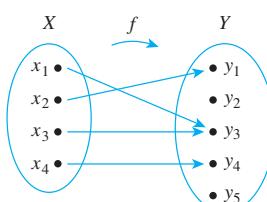


Figure 7.1.1

Example 7.1.1 Functions and Nonfunctions

Which of the arrow diagrams in Figure 7.1.2 define functions from $X = \{a, b, c\}$ to $Y = \{1, 2, 3, 4\}$?

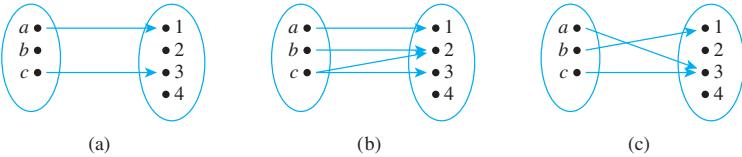


Figure 7.1.1

Solution Only (c) defines a function. In (a) there is an element of X , namely b , that is not sent to any element of Y ; that is, there is no arrow coming out of b . And in (b) the element c is not sent to a *unique* element of Y ; that is, there are two arrows coming out of c , one pointing to 2 and the other to 3. ■

Example 7.1.2 A Function Defined by an Arrow Diagram

Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Define a function f from X to Y by the arrow diagram in Figure 7.1.3.

- Write the domain and co-domain of f .
- Find $f(a)$, $f(b)$, and $f(c)$.
- What is the range of f ?
- Is c an inverse image of 2? Is b an inverse image of 3?
- Find the inverse images of 2, 4, and 1.
- Represent f as a set of ordered pairs.

Solution

- domain of $f = \{a, b, c\}$, co-domain of $f = \{1, 2, 3, 4\}$
- $f(a) = 2$, $f(b) = 4$, $f(c) = 2$
- range of $f = \{2, 4\}$
- Yes, No
- inverse image of 2 = $\{a, c\}$
inverse image of 4 = $\{b\}$
inverse image of 1 = \emptyset (since no arrows point to 1)
- $\{(a, 2), (b, 4), (c, 2)\}$

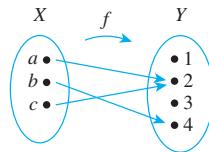


Figure 7.1.1

In Example 7.1.2 there are no arrows pointing to the 1 or the 3. This illustrates the fact that although each element of the domain of a function must have an arrow pointing out from it, there can be elements of the co-domain to which no arrows point. Note also that there are two arrows pointing to the 2—one coming from a and the other from c .

In Section 1.3 we gave a test for determining whether two functions with the same domain and co-domain are equal, saying that the test results from the definition of a function as a binary relation. We formalize this justification in Theorem 7.1.1.

Theorem 7.1.1 A Test for Function Equality

If $F: X \rightarrow Y$ and $G: X \rightarrow Y$ are functions, then $F = G$ if, and only if, $F(x) = G(x)$ for all $x \in X$.

Proof:

Note So $(x, y) \in F \Leftrightarrow y = F(x)$ and $(x, y) \in G \Leftrightarrow y = G(x)$.

Suppose $F: X \rightarrow Y$ and $G: X \rightarrow Y$ are functions, that is, F and G are binary relations from X to Y that satisfy the two additional function properties. Then F and G are subsets of $X \times Y$, and for (x, y) to be in F means that y is the unique element related to x by F , which we denote as $F(x)$. Similarly, for (x, y) to be in G means that y is the unique element related to x by G , which we denote as $G(x)$.

Now suppose that $F(x) = G(x)$ for all $x \in X$. Then if x is any element of X ,

$$(x, y) \in F \Leftrightarrow y = F(x) \Leftrightarrow y = G(x) \Leftrightarrow (x, y) \in G \quad \text{because } F(x) = G(x)$$

So F and G consist of exactly the same elements and hence $F = G$.

Conversely, if $F = G$, then for all $x \in X$,

$$y = F(x) \Leftrightarrow (x, y) \in F \Leftrightarrow (x, y) \in G \Leftrightarrow y = G(x) \quad \text{because } F \text{ and } G \text{ consist of exactly the same elements}$$

Thus, since both $F(x)$ and $G(x)$ equal y , we have that

$$F(x) = G(x).$$

Example 7.1.3 Equality of Functions

- a. Let $J_3 = \{0, 1, 2\}$, and define functions f and g from J_3 to J_3 as follows: For all x in J_3 ,

$$f(x) = (x^2 + x + 1) \bmod 3 \quad \text{and} \quad g(x) = (x + 2)^2 \bmod 3.$$

Does $f = g$?

- b. Let $F: \mathbf{R} \rightarrow \mathbf{R}$ and $G: \mathbf{R} \rightarrow \mathbf{R}$ be functions. Define new functions $F + G: \mathbf{R} \rightarrow \mathbf{R}$ and $G + F: \mathbf{R} \rightarrow \mathbf{R}$ as follows: For all $x \in \mathbf{R}$,

$$(F + G)(x) = F(x) + G(x) \quad \text{and} \quad (G + F)(x) = G(x) + F(x).$$

Does $F + G = G + F$?

Solution

- a. Yes, the table of values shows that $f(x) = g(x)$ for all x in J_3 .

x	$x^2 + x + 1$	$f(x) = (x^2 + x + 1) \bmod 3$	$(x + 2)^2$	$g(x) = (x + 2)^2 \bmod 3$
0	1	$1 \bmod 3 = 1$	4	$4 \bmod 3 = 1$
1	3	$3 \bmod 3 = 0$	9	$9 \bmod 3 = 0$
2	7	$7 \bmod 3 = 1$	16	$16 \bmod 3 = 1$

- b. Again the answer is yes. For all real numbers x ,

$$\begin{aligned} (F + G)(x) &= F(x) + G(x) && \text{by definition of } F + G \\ &= G(x) + F(x) && \text{by the commutative law for addition of real numbers} \\ &= (G + F)(x) && \text{by definition of } G + F \end{aligned}$$

Hence $F + G = G + F$. ■

Examples of Functions

The following examples illustrate some of the wide variety of different types of functions.

Example 7.1.4 The Identity Function on a Set

Given a set X , define a function I_X from X to X by

$$I_X(x) = x \quad \text{for all } x \text{ in } X.$$

The function I_X is called the **identity function on X** because it sends each element of X to the element that is identical to it. Thus the identity function can be pictured as a machine that sends each piece of input directly to the output chute without changing it in any way.

Let X be any set and suppose that a_{ij}^k and $\phi(z)$ are elements of X . Find $I_X(a_{ij}^k)$ and $I_X(\phi(z))$.

Solution Whatever is input to the identity function comes out unchanged, so $I_X(a_{ij}^k) = a_{ij}^k$ and $I_X(\phi(z)) = \phi(z)$. ■

Example 7.1.5 Sequences

The formal definition of sequences specifies that an infinite sequence is a function defined on the set of integers that are greater than or equal to a particular integer. For example, the sequence denoted

$$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \dots, \frac{(-1)^n}{n+1}, \dots$$

can be thought of as the function f from the nonnegative integers to the real numbers that associates $0 \rightarrow 1, 1 \rightarrow -\frac{1}{2}, 2 \rightarrow \frac{1}{3}, 3 \rightarrow -\frac{1}{4}, 4 \rightarrow \frac{1}{5}$, and, in general, $n \rightarrow \frac{(-1)^n}{n+1}$.

In other words, $f: \mathbf{Z}^{nonneg} \rightarrow \mathbf{R}$ is the function defined as follows:

$$\text{Send each integer } n \geq 0 \text{ to } f(n) = \frac{(-1)^n}{n+1}.$$

In fact, there are many functions that can be used to define a given sequence. For instance, express the sequence above as a function from the set of *positive* integers to the set of real numbers.

Solution Define $g: \mathbf{Z}^+ \rightarrow \mathbf{R}$ by $g(n) = \frac{(-1)^{n+1}}{n}$, for each $n \in \mathbf{Z}^+$. Then $g(1) = 1, g(2) = -\frac{1}{2}, g(3) = \frac{1}{3}$, and in general

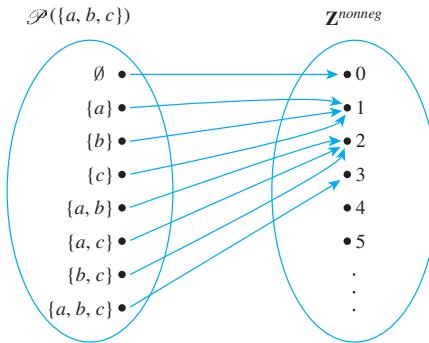
$$g(n+1) = \frac{(-1)^{n+2}}{n+1} = \frac{(-1)^n}{n+1} = f(n).$$

Example 7.1.6 A Function Defined on a Power Set

Recall from Section 6.1 that $\mathcal{P}(A)$ denotes the set of all subsets of the set A . Define a function $F: \mathcal{P}(\{a, b, c\}) \rightarrow \mathbf{Z}^{nonneg}$ as follows: For each $X \in \mathcal{P}(\{a, b, c\})$,

$$F(X) = \text{the number of elements in } X.$$

Draw an arrow diagram for F .

Solution

■

Example 7.1.7 Functions Defined on a Cartesian Product

Define functions $M: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R}$ and $R: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$ as follows: For all ordered pairs (a, b) of integers,

Note It is customary to omit one set of parentheses when referring to functions defined on Cartesian products. For example, we write $M(a, b)$ rather than $M((a, b))$.

$$M(a, b) = ab \quad \text{and} \quad R(a, b) = (-a, b).$$

Then M is the multiplication function that sends each pair of real numbers to the product of the two, and R is the reflection function that sends each point in the plane that corresponds to a pair of real numbers to the mirror image of the point across the vertical axis. Find the following:

- | | | |
|----------------|---|----------------------------|
| a. $M(-1, -1)$ | b. $M\left(\frac{1}{2}, \frac{1}{2}\right)$ | c. $M(\sqrt{2}, \sqrt{2})$ |
| d. $R(2, 5)$ | e. $R(-2, 5)$ | f. $R(3, -4)$ |

Solution

- | | | |
|-------------------|--------------------------|----------------------------------|
| a. $(-1)(-1) = 1$ | b. $(1/2)(1/2) = 1/4$ | c. $\sqrt{2} \cdot \sqrt{2} = 2$ |
| d. $(-2, 5)$ | e. $(-(-2), 5) = (2, 5)$ | f. $(-3, -4)$ |

■

• Definition Logarithms and Logarithmic Functions

Note It is not obvious, but it is true, that for any positive real number x there is a unique real number y such that $b^y = x$. Most calculus books contain a discussion of this result.

Let b be a positive real number with $b \neq 1$. For each positive real number x , the **logarithm with base b of x** , written $\log_b x$, is the exponent to which b must be raised to obtain x . Symbolically,

$$\log_b x = y \Leftrightarrow b^y = x.$$

The **logarithmic function with base b** is the function from \mathbf{R}^+ to \mathbf{R} that takes each positive real number x to $\log_b x$.

Example 7.1.8 The Logarithmic Function with Base b

Find the following:

- | | | | |
|-------------------------------|-------------------------------------|-------------------|--|
| a. $\log_3 9$ | b. $\log_2\left(\frac{1}{2}\right)$ | c. $\log_{10}(1)$ | d. $\log_2(2^m)$ (m is any real number) |
| e. $2^{\log_2 m}$ ($m > 0$) | | | |

Solution

- a. $\log_3 9 = 2$ because $3^2 = 9$.
- b. $\log_2 \left(\frac{1}{2}\right) = -1$ because $2^{-1} = \frac{1}{2}$.
- c. $\log_{10}(1) = 0$ because $10^0 = 1$.
- d. $\log_2(2^m) = m$ because the exponent to which 2 must be raised to obtain 2^m is m .
- e. $2^{\log_2 m} = m$ because $\log_2 m$ is the exponent to which 2 must be raised to obtain m . ■

Recall from Section 5.9 that if S is a nonempty, finite set of characters, then a **string over S** is a finite sequence of elements of S . The number of characters in a string is called the **length** of the string. The **null string over S** is the “string” with no characters. It is usually denoted ϵ and is said to have length 0.

Example 7.1.9 Encoding and Decoding Functions

Digital messages consist of finite sequences of 0's and 1's. When they are communicated across a transmission channel, they are frequently coded in special ways to reduce the possibility that they will be garbled by interfering noise in the transmission lines. For example, suppose a message consists of a sequence of 0's and 1's. A simple way to encode the message is to write each bit three times. Thus the message

00101111

would be encoded as

000000111000111111111111.

The receiver of the message decodes it by replacing each section of three identical bits by the one bit to which all three are equal.

Let A be the set of all strings of 0's and 1's, and let T be the set of all strings of 0's and 1's that consist of consecutive triples of identical bits. The encoding and decoding processes described above are actually functions from A to T and from T to A . The encoding function E is the function from A to T defined as follows: For each string $s \in A$,

$E(s)$ = the string obtained from s by replacing each bit of s by the same bit written three times.

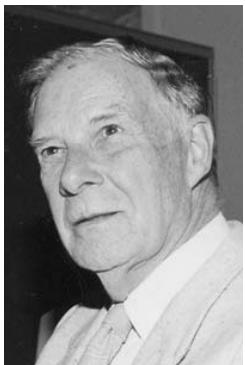
The decoding function D is defined as follows: For each string $t \in T$,

$D(t)$ = the string obtained from t by replacing each consecutive triple of three identical bits of t by a single copy of that bit.

The advantage of this particular coding scheme is that it makes it possible to do a certain amount of error correction when interference in the transmission channels has introduced errors into the stream of bits. If the receiver of the coded message observes that one of the sections of three consecutive bits that should be identical does not consist of identical bits, then one bit differs from the other two. In this case, if errors are rare, it is likely that the single bit that is different is the one in error, and this bit is changed to agree with the other two before decoding. ■

Example 7.1.10 The Hamming Distance Function

The Hamming distance function, named after the computer scientist Richard W. Hamming, is very important in coding theory. It gives a measure of the “difference” between two strings of 0's and 1's that have the same length. Let S_n be the set of all strings of 0's



Courtesy of U.S. Naval Academy

Richard Hamming
(1915–1998)**Solution**

- a. 3 b. 4

■

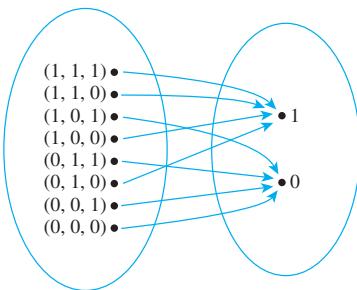
Boolean Functions

In Section 2.4 we showed how to find input/output tables for certain digital logic circuits. Any such input/output table defines a function in the following way: The elements in the input column can be regarded as ordered tuples of 0's and 1's; the set of all such ordered tuples is the domain of the function. The elements in the output column are all either 0 or 1; thus $\{0, 1\}$ is taken to be the co-domain of the function. The relationship is that which sends each input element to the output element in the same row. Thus, for instance, the input/output table of Figure 7.1.4(a) defines the function with the arrow diagram shown in Figure 7.1.4(b).

More generally, the input/output table corresponding to a circuit with n input wires has n input columns. Such a table defines a function from the set of all n -tuples of 0's and 1's to the set $\{0, 1\}$.

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

(a)



(b)

Figure 7.1.2 Two Representations of a Boolean Function**• Definition**

An (n -place) **Boolean function** f is a function whose domain is the set of all ordered n -tuples of 0's and 1's and whose co-domain is the set $\{0, 1\}$. More formally, the domain of a Boolean function can be described as the Cartesian product of n copies of the set $\{0, 1\}$, which is denoted $\{0, 1\}^n$. Thus $f: \{0, 1\}^n \rightarrow \{0, 1\}$.

Example 7.1.11 A Boolean Function

Consider the three-place Boolean function defined from the set of all 3-tuples of 0's and 1's to $\{0, 1\}$ as follows: For each triple (x_1, x_2, x_3) of 0's and 1's,

$$f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \bmod 2.$$

Describe f using an input/output table.

Solution

$$f(1, 1, 1) = (1 + 1 + 1) \bmod 2 = 3 \bmod 2 = 1$$

$$f(1, 1, 0) = (1 + 1 + 0) \bmod 2 = 2 \bmod 2 = 0$$

The rest of the values of f can be calculated similarly to obtain the following table.

Input			Output
x_1	x_2	x_3	$(x_1 + x_2 + x_3) \bmod 2$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

Checking Whether a Function Is Well Defined

It can sometimes happen that what appears to be a function defined by a rule is not really a function at all. To give an example, suppose we wrote, “Define a function $f: \mathbf{R} \rightarrow \mathbf{R}$ by specifying that for all real numbers x ,

$$f(x) \text{ is the real number } y \text{ such that } x^2 + y^2 = 1.$$

There are two distinct reasons why this description does not define a function. For almost all values of x , either (1) there is no y that satisfies the given equation or (2) there are two different values of y that satisfy the equation. For instance, when $x = 2$, there is no real number y such that $2^2 + y^2 = 1$, and when $x = 0$, both $y = -1$ and $y = 1$ satisfy the equation $0^2 + y^2 = 1$. In general, we say that a “function” is **not well defined** if it fails to satisfy at least one of the requirements for being a function.

Example 7.1.12 A Function That Is Not Well Defined

Recall that \mathbf{Q} represents the set of all rational numbers. Suppose you read that a function $f: \mathbf{Q} \rightarrow \mathbf{Z}$ is to be defined by the formula

$$f\left(\frac{m}{n}\right) = m \quad \text{for all integers } m \text{ and } n \text{ with } n \neq 0.$$

That is, the integer associated by f to the number $\frac{m}{n}$ is m . Is f well defined? Why?

Solution The function f is not well defined. The reason is that fractions have more than one representation as quotients of integers. For instance, $\frac{1}{2} = \frac{3}{6}$. Now if f were a function,

then the definition of a function would imply that $f\left(\frac{1}{2}\right) = \left(\frac{3}{6}\right)$ since $\frac{1}{2} = \frac{3}{6}$. But applying the formula for f , you find that

$$f\left(\frac{1}{2}\right) = 1 \quad \text{and} \quad f\left(\frac{3}{6}\right) = 3,$$

and so

$$f\left(\frac{1}{2}\right) \neq f\left(\frac{3}{6}\right).$$

This contradiction shows that f is not well defined and, therefore, is not a function. ■

Note that the phrase *well-defined function* is actually redundant; for a function to be well defined really means that it is worthy of being called a function.

Functions Acting on Sets

Given a function from a set X to a set Y , you can consider the set of images in Y of all the elements in a subset of X and the set of inverse images in X of all the elements in a subset of Y .

• Definition

Note For $y \in Y$, $f^{-1}(y) = f^{-1}(\{y\})$.

If $f: X \rightarrow Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

$$f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \text{ in } A\}$$

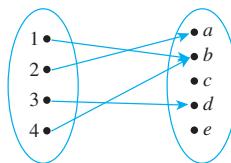
and

$$f^{-1}(C) = \{x \in X \mid f(x) \in C\}.$$

$f(A)$ is called the **image of A** , and $f^{-1}(C)$ is called the **inverse image of C** .

Example 7.1.13 The Action of a Function on Subsets of a Set

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$, and define $F: X \rightarrow Y$ by the following arrow diagram:



Let $A = \{1, 4\}$, $C = \{a, b\}$, and $D = \{c, e\}$. Find $F(A)$, $F(X)$, $F^{-1}(C)$, and $F^{-1}(D)$.

Solution

$$F(A) = \{b\} \quad F(X) = \{a, b, d\} \quad F^{-1}(C) = \{1, 2, 4\} \quad F^{-1}(D) = \emptyset$$

Example 7.1.14 Interaction of a Function with Union

Let X and Y be sets, let F be a function from X to Y , and let A and B be any subsets of X . Prove that $F(A \cup B) \subseteq F(A) \cup F(B)$.

Solution

The fact that X , Y , F , A , and B were formally introduced prior to the word “Prove” allows you to regard their existence and relationships as part of your background knowledge. Thus to prove that $F(A \cup B) \subseteq F(A) \cup F(B)$, you only need show that if y is any element in $F(A \cup B)$, then y is an element of $F(A) \cup F(B)$.

Proof:

Suppose $y \in F(A \cup B)$. [We must show that $y \in F(A) \cup F(B)$.] By definition of function, $y = F(x)$ for some $x \in A \cup B$. By definition of union, $x \in A$ or $x \in B$.

Case 1, $x \in A$: In this case, $y = F(x)$ for some x in A . Hence $y \in F(A)$, and so by definition of union, $y \in F(A) \cup F(B)$.

Case 2, $x \in B$: In this case, $y = F(x)$ for some x in B . Hence $y \in F(B)$, and so by definition of union, $y \in F(A) \cup F(B)$.

Thus in either case $y \in F(A) \cup F(B)$ [as was to be shown]. ■

Exercise 38 asks you to prove the opposite containment from the one in example 7.1.14. Taken together, the example and the solution to the exercise establish the full equality that $F(A \cup B) = F(A) \cup F(B)$.

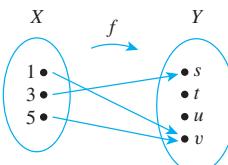
Test Yourself

Answers to Test Yourself questions are located at the end of each section.

1. Given a function f from a set X to a set Y , $f(x)$ is _____.
2. Given a function f from a set X to a set Y , if $f(x) = y$, then y is called _____ or _____ or _____.
3. Given a function f from a set X to a set Y , the range of f (or the image of X under f) is _____.
4. Given a function f from a set X to a set Y , if $f(x) = y$, then x is called _____ or _____.
5. Given a function f from a set X to a set Y , if $y \in Y$, then $f^{-1}(y) = _____$ and is called _____.
6. Given functions f and g from a set X to a set Y , $f = g$ if, and only if, _____.
7. Given positive real numbers x and b with $b \neq 1$, $\log_b x = _____$.
8. Given a function f from a set X to a set Y and a subset A of X , $f(A) = _____$.
9. Given a function f from a set X to a set Y and a subset C of Y , $f^{-1}(C) = _____$.

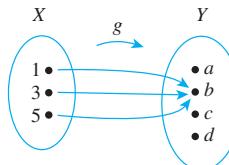
Exercise Set 7.1*

1. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$. Define $f: X \rightarrow Y$ by the following arrow diagram.



- a. Write the domain of f and the co-domain of f .
b. Find $f(1)$, $f(3)$, and $f(5)$.
c. What is the range of f ?
d. Is 3 an inverse image of s ? Is 1 an inverse image of u ?
e. What is the inverse image of s ? of u ? of v ?
f. Represent f as a set of ordered pairs.

2. Let $X = \{1, 3, 5\}$ and $Y = \{a, b, c, d\}$. Define $g: X \rightarrow Y$ by the following arrow diagram.



- a. Write the domain of g and the co-domain of g .
b. Find $g(1)$, $g(3)$, and $g(5)$.
c. What is the range of g ?
d. Is 3 an inverse image of a ? Is 1 an inverse image of b ?
e. What is the inverse image of b ? of c ?
f. Represent g as a set of ordered pairs.

*For exercises with blue numbers or letters, solutions are given in Appendix B. The symbol **H** indicates that only a hint or a partial solution is given. The symbol ***** signals that an exercise is more challenging than usual.

3. Indicate whether the statements in parts (a)–(d) are true or false. Justify your answers.
- If two elements in the domain of a function are equal, then their images in the co-domain are equal.
 - If two elements in the co-domain of a function are equal, then their preimages in the domain are also equal.
 - A function can have the same output for more than one input.
 - A function can have the same input for more than one output.
4. a. Find all functions from $X = \{a, b\}$ to $Y = \{u, v\}$.
 b. Find all functions from $X = \{a, b, c\}$ to $Y = \{u\}$.
 c. Find all functions from $X = \{a, b, c\}$ to $Y = \{u, v\}$.
5. Let I_Z be the identity function defined on the set of all integers, and suppose that e , b_i^{jk} , $K(t)$, and u_{kj} all represent integers. Find
- $I_Z(e)$
 - $I_Z(b_i^{jk})$
 - $I_Z(K(t))$
 - $I_Z(u_{kj})$
6. Find functions defined on the set of nonnegative integers that define the sequences whose first six terms are given below.
- $1, -\frac{1}{3}, \frac{1}{5}, -\frac{1}{7}, \frac{1}{9}, -\frac{1}{11}$
 - $0, -2, 4, -6, 8, -10$
7. Let $A = \{1, 2, 3, 4, 5\}$ and define a function $F: \mathcal{P}(A) \rightarrow \mathbf{Z}$ as follows: For all sets X in $\mathcal{P}(A)$,
- $$F(X) = \begin{cases} 0 & \text{if } X \text{ has an even number of elements} \\ 1 & \text{if } X \text{ has an odd number of elements.} \end{cases}$$
- Find the following:
- $F(\{1, 3, 4\})$
 - $F(\emptyset)$
 - $F(\{2, 3\})$
 - $F(\{2, 3, 4, 5\})$
8. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define a function $F: J_5 \rightarrow J_5$ as follows: For each $x \in J_5$, $F(x) = (x^3 + 2x + 4) \bmod 5$. Find the following:
- $F(0)$
 - $F(1)$
 - $F(2)$
 - $F(3)$
 - $F(4)$
9. Define a function $S: \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ as follows: For each positive integer n ,
- $$S(n) = \text{the sum of the positive divisors of } n.$$
- Find the following:
- $S(1)$
 - $S(15)$
 - $S(17)$
 - $S(5)$
 - $S(18)$
 - $S(21)$
10. Let D be the set of all finite subsets of positive integers. Define a function $T: \mathbf{Z}^+ \rightarrow D$ as follows: For each positive integer n , $T(n) =$ the set of positive divisors of n . Find the following:
- $T(1)$
 - $T(15)$
 - $T(17)$
 - $T(5)$
 - $T(18)$
 - $T(21)$
11. Define $F: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z} \times \mathbf{Z}$ as follows: For all ordered pairs (a, b) of integers, $F(a, b) = (2a + 1, 3b - 2)$. Find the following:
- $F(4, 4)$
 - $F(2, 1)$
 - $F(3, 2)$
 - $F(1, 5)$
12. Define $G: J_5 \times J_5 \rightarrow J_5 \times J_5$ as follows: For all $(a, b) \in J_5 \times J_5$,
- $$G(a, b) = ((2a + 1) \bmod 5, (3b - 2) \bmod 5).$$
- Find the following:
- $G(4, 4)$
 - $G(2, 1)$
 - $G(3, 2)$
 - $G(1, 5)$
13. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define functions $f: J_5 \rightarrow J_5$ and $g: J_5 \rightarrow J_5$ as follows: For each $x \in J_5$,
- $$f(x) = (x + 4)^2 \bmod 5 \text{ and } g(x) = (x^2 + 3x + 1) \bmod 5.$$
- Is $f = g$? Explain.
14. Let $J_5 = \{0, 1, 2, 3, 4\}$, and define functions $h: J_5 \rightarrow J_5$ and $k: J_5 \rightarrow J_5$ as follows: For each $x \in J_5$,
- $$h(x) = (x + 3)^3 \bmod 5 \text{ and } k(x) = (x^3 + 4x^2 + 2x + 2) \bmod 5.$$
- Is $h = k$? Explain.
15. Let F and G be functions from the set of all real numbers to itself. Define the product functions $F \cdot G: \mathbf{R} \rightarrow \mathbf{R}$ and $G \cdot F: \mathbf{R} \rightarrow \mathbf{R}$ as follows: For all $x \in \mathbf{R}$,
- $$(F \cdot G)(x) = F(x) \cdot G(x)$$
- $$(G \cdot F)(x) = G(x) \cdot F(x)$$
- Does $F \cdot G = G \cdot F$? Explain.
16. Let F and G be functions from the set of all real numbers to itself. Define new functions $F - G: \mathbf{R} \rightarrow \mathbf{R}$ and $G - F: \mathbf{R} \rightarrow \mathbf{R}$ as follows: For all $x \in \mathbf{R}$,
- $$(F - G)(x) = F(x) - G(x)$$
- $$(G - F)(x) = G(x) - F(x)$$
- Does $F - G = G - F$? Explain.
17. Use the definition of logarithm to fill in the blanks below.
- $\log_2 8 = 3$ because _____.
 - $\log_5 \left(\frac{1}{25}\right) = 2$ because _____.
 - $\log_4 4 = 1$ because _____.
 - $\log_3 (3^n) = n$ because _____.
 - $\log_4 1 = 0$ because _____.
18. Find exact values for each of the following quantities. Do not use a calculator.
- $\log_3 81$
 - $\log_2 1024$
 - $\log_3 \left(\frac{1}{27}\right)$
 - $\log_{10} \left(\frac{1}{10}\right)$
 - $\log_3 3$
 - $\log_2 (2^k)$
19. Use the definition of logarithm to prove that for any positive real number b with $b \neq 1$, $\log_b b = 1$.
20. Use the definition of logarithm to prove that for any positive real number b with $b \neq 1$, $\log_b 1 = 0$.
21. If b is any positive real number with $b \neq 1$ and x is any real number, b^{-x} is defined as follows: $b^{-x} = \frac{1}{b^x}$. Use this definition and the definition of logarithm to prove that $\log_b \left(\frac{1}{u}\right) = -\log_b(u)$ for all positive real numbers u and b , with $b \neq 1$.

- H 22.** Use the unique factorization for the integers theorem (Section 4.3) and the definition of logarithm to prove that $\log_3(7)$ is irrational.
- 23.** If b and y are positive real numbers such that $\log_b y = 3$, what is $\log_{1/b}(y)$? Why?
- 24.** If b and y are positive real numbers such that $\log_b y = 2$, what is $\log_{b^2}(y)$? Why?
- 25.** Let $A = \{2, 3, 5\}$ and $B = \{x, y\}$. Let p_1 and p_2 be the **projections of $A \times B$ onto the first and second coordinates**. That is, for each pair $(a, b) \in A \times B$, $p_1(a, b) = a$ and $p_2(a, b) = b$.
- Find $p_1(2, y)$ and $p_1(5, x)$. What is the range of p_1 ?
 - Find $p_2(2, y)$ and $p_2(5, x)$. What is the range of p_2 ?
- 26.** Observe that *mod* and *div* can be defined as functions from $\mathbf{Z}^{nonneg} \times \mathbf{Z}^+$ to \mathbf{Z} . For each ordered pair (n, d) consisting of a nonnegative integer n and a positive integer d , let
- $$\begin{aligned} mod(n, d) &= n \text{ mod } d \text{ (the nonnegative remainder obtained when } n \text{ is divided by } d\text{).} \\ div(n, d) &= n \text{ div } d \text{ (the integer quotient obtained when } n \text{ is divided by } d\text{).} \end{aligned}$$
- Find each of the following:
- $mod(67, 10)$ and $div(67, 10)$
 - $mod(59, 8)$ and $div(59, 8)$
 - $mod(30, 5)$ and $div(30, 5)$
- 27.** Let S be the set of all strings of a 's and b 's.
- Define $f: S \rightarrow \mathbf{Z}$ as follows: For each string s in S
- $$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s \\ 0 \quad \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$
- Find $f(aba)$, $f(bbab)$ and $f(b)$. What is the range of f ?
- Define $g: S \rightarrow S$ as follows: For each string s in S ,
- $$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$
- Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g ?
- 28.** Consider the coding and decoding functions E and D defined in Example 7.1.9.
- Find $E(0110)$ and $D(111111000111)$.
 - Find $E(1010)$ and $D(000000111111)$.
- 29.** Consider the Hamming distance function defined in Example 7.1.10.
- Find $H(10101, 00011)$
 - Find $H(00110, 10111)$.
- 30.** Draw arrow diagrams for the Boolean functions defined by the following input/output tables.
- a.**
- | Input | | Output |
|----------|----------|----------|
| P | Q | R |
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |
- b.**
- | Input | | | Output |
|----------|----------|----------|----------|
| P | Q | R | S |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 |
- 31.** Fill in the following table to show the values of all possible two-place Boolean functions.
- | Input | f_1 | f_2 | f_3 | f_4 | f_5 | f_6 | f_7 | f_8 | f_9 | f_{10} | f_{11} | f_{12} | f_{13} | f_{14} | f_{15} | f_{16} |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|
| 1 1 | | | | | | | | | | | | | | | | |
| 1 0 | | | | | | | | | | | | | | | | |
| 0 1 | | | | | | | | | | | | | | | | |
| 0 0 | | | | | | | | | | | | | | | | |
- 32.** Consider the three-place Boolean function f defined by the following rule: For each triple (x_1, x_2, x_3) of 0's and 1's,
- $$f(x_1, x_2, x_3) = (4x_1 + 3x_2 + 2x_3) \text{ mod } 2.$$
- Find $f(1, 1, 1)$ and $f(0, 0, 1)$.
 - Describe f using an input/output table.
- 33.** Student A tries to define a function $g: \mathbf{Q} \rightarrow \mathbf{Z}$ by the rule
- $$g\left(\frac{m}{n}\right) = m - n, \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$
- Student B claims that g is not well defined. Justify student B's claim.
- 34.** Student C tries to define a function $h: \mathbf{Q} \rightarrow \mathbf{Q}$ by the rule
- $$h\left(\frac{m}{n}\right) = \frac{m^2}{n}, \text{ for all integers } m \text{ and } n \text{ with } n \neq 0.$$
- Student D claims that h is not well defined. Justify student D's claim.

- 35.** Let $J_5 = \{0, 1, 2, 3, 4\}$. Then $J_5 - \{0\} = \{1, 2, 3, 4\}$. Student A tries to define a function $R: J_5 - \{0\} \rightarrow J_5 - \{0\}$ as follows: For each $x \in J_5 - \{0\}$,

$R(x)$ is the number y so that $(xy) \bmod 5 = 1$.

Student B claims that R is not well defined. Who is right: student A or student B? Justify your answer.

- 36.** Let $J_4 = \{0, 1, 2, 3\}$. Then $J_4 - \{0\} = \{1, 2, 3\}$. Student C tries to define a function $S: J_4 - \{0\} \rightarrow J_4 - \{0\}$ as follows: For each $x \in J_4 - \{0\}$,

$S(x)$ is the number y so that $(xy) \bmod 4 = 1$.

Student F claims that S is not well defined. Who is right: student C or student D? Justify your answer.

- 37.** On certain computers the integer data type goes from $-2, 147, 483, 648$ through $2, 147, 483, 647$. Let S be the set of all integers from $-2, 147, 483, 648$ through $2, 147, 483, 647$. Try to define a function $f: S \rightarrow S$ by the rule $f(n) = n^2$ for each n in S . Is f well defined? Why?

- 38.** Let $X = \{a, b, c\}$ and $Y = \{r, s, t, u, v, w\}$. Define $f: X \rightarrow Y$ as follows: $f(a) = v$, $f(b) = v$, and $f(c) = t$.

- Draw an arrow diagram for f .
- Let $A = \{a, b\}$, $C = \{t\}$, $D = \{u, v\}$, and $E = \{r, s\}$. Find $f(A)$, $f(X)$, $f^{-1}(C)$, $f^{-1}(D)$, $f^{-1}(E)$, and $f^{-1}(Y)$.

- 39.** Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$. Define $g: X \rightarrow Y$ as follows: $g(1) = a$, $g(2) = a$, $g(3) = a$, and $g(4) = d$.

- Draw an arrow diagram for g .
- Let $A = \{2, 3\}$, $C = \{a\}$, and $D = \{b, c\}$. Find $g(A)$, $g(X)$, $g^{-1}(C)$, $g^{-1}(D)$, and $g^{-1}(Y)$.

- H 40.** Let X and Y be sets, let A and B be any subsets of X , and let F be a function from X to Y . Fill in the blanks in the following proof that $F(A) \cup F(B) \subseteq F(A \cup B)$.

Proof: Let y be any element in $F(A) \cup F(B)$. [We must show that y is in $F(A \cup B)$.] By definition of union, (a).

Case 1, $y \in F(A)$: In this case, by definition of $F(A)$, $y = F(x)$ for (b) $x \in A$. Since $A \subseteq A \cup B$, it follows from the definition of union that $x \in \underline{(c)}$. Hence, $y = F(x)$ for some $x \in A \cup B$, and thus, by definition of $F(A \cup B)$, $y \in \underline{(d)}$.

Case 2, $y \in F(B)$: In this case, by definition of $F(B)$, (e) $x \in B$. Since $B \subseteq A \cup B$ it follows from the definition of union that (f).

Therefore, regardless of whether $y \in F(A)$ or $y \in F(B)$, we have that $y \in F(A \cup B)$ [as was to be shown].

In 41–49 let X and Y be sets, let A and B be any subsets of X , and let C and D be any subsets of Y . Determine which of the properties are true for all functions F from X to Y and which are false for at least one function F from X to Y . Justify your answers.

- If $A \subseteq B$ then $F(A) \subseteq F(B)$.
- $F(A \cap B) \subseteq F(A) \cap F(B)$
- $F(A) \cap F(B) \subseteq F(A \cap B)$
- For all subsets A and B of X , $F(A - B) = F(A) - F(B)$.
- For all subsets C and D of Y , if $C \subseteq D$, then

$$F^{-1}(C) \subseteq F^{-1}(D).$$

- H 46.** For all subsets C and D of Y ,

$$F^{-1}(C \cup D) = F^{-1}(C) \cup F^{-1}(D).$$

- For all subsets C and D of Y ,

$$F^{-1}(C \cap D) = F^{-1}(C) \cap F^{-1}(D).$$

- For all subsets C and D of Y ,

$$F^{-1}(C - D) = F^{-1}(C) - F^{-1}(D).$$

- $F(F^{-1}(C)) \subseteq C$

- Given a set S and a subset A , the **characteristic function of A** , denoted χ_A , is the function defined from S to \mathbf{Z} with the property that for all $u \in S$,

$$\chi_A(u) = \begin{cases} 1 & \text{if } u \in A \\ 0 & \text{if } u \notin A. \end{cases}$$

Show that each of the following holds for all subsets A and B of S and all $u \in S$.

- $\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$
- $\chi_{A \cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$

Each of exercises 51–53 refers to the Euler phi function, denoted ϕ , which is defined as follows: For each integer $n \geq 1$, $\phi(n)$ is the number of positive integers less than or equal to n that have no common factors with n except ± 1 . For example, $\phi(10) = 4$ because there are four positive integers less than or equal to 10 that have no common factors with 10 except ± 1 ; namely, 1, 3, 7, and 9.

- Find each of the following:
 - $\phi(15)$
 - $\phi(2)$
 - $\phi(5)$
 - $\phi(12)$
 - $\phi(11)$
 - $\phi(1)$
- Prove that if p is a prime number and n is an integer with $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1}$.

- Prove that there are infinitely many integers n for which $\phi(n)$ is a perfect square.

Answers for Test Yourself

1. the unique output element in Y that is related to x by f
2. the value of f at x ; the image of x under f ; the output of f for the input x
3. the set of all y in Y such that $f(x) = y$
4. an inverse image of y under f ; a preimage of y
5. $\{x \in X \mid f(x) = y\}$; the inverse image of y
6. $f(x) = g(x)$ for all $x \in X$
7. the exponent to which b must be raised to obtain x
(Or: the real number y such that $x = b^y$)
8. $\{y \in Y \mid y = f(x)$ for some $x \in A\}$ (Or: $\{f(x) \mid x \in A\}$)
9. $\{x \in X \mid f(x) \in C\}$

7.2 One-to-One and Onto, Inverse Functions

Don't accept a statement just because it is printed. — Anna Pell Wheeler, 1883–1966

In this section we discuss two important properties that functions may satisfy: the property of being *one-to-one* and the property of being *onto*. Functions that satisfy both properties are called *one-to-one correspondences* or *one-to-one onto functions*. When a function is a one-to-one correspondence, the elements of its domain and co-domain match up perfectly, and we can define an *inverse function* from the co-domain to the domain that “undoes” the action of the function.

One-to-One Functions

In Section 7.1 we noted that a function may send several elements of its domain to the same element of its co-domain. In terms of arrow diagrams, this means that two or more arrows that start in the domain can point to the same element in the co-domain. On the other hand, if no two arrows that start in the domain point to the same element of the co-domain then the function is called *one-to-one* or *injective*. For a one-to-one function, each element of the range is the image of at most one element of the domain.

• Definition

Let F be a function from a set X to a set Y . F is **one-to-one** (or **injective**) if, and only if, for all elements x_1 and x_2 in X ,

if $F(x_1) = F(x_2)$, then $x_1 = x_2$,
or, equivalently, if $x_1 \neq x_2$, then $F(x_1) \neq F(x_2)$.

Symbolically,

$$F: X \rightarrow Y \text{ is one-to-one} \Leftrightarrow \forall x_1, x_2 \in X, \text{ if } F(x_1) = F(x_2) \text{ then } x_1 = x_2.$$

To obtain a precise statement of what it means for a function *not* to be one-to-one, take the negation of one of the equivalent versions of the definition above. Thus:

$$\text{A function } F: X \rightarrow Y \text{ is not one-to-one} \Leftrightarrow \exists \text{ elements } x_1 \text{ and } x_2 \text{ in } X \text{ with } F(x_1) = F(x_2) \text{ and } x_1 \neq x_2.$$

That is, if elements x_1 and x_2 can be found that have the same function value but are not equal, then F is not one-to-one.

In terms of arrow diagrams, a one-to-one function can be thought of as a function that separates points. That is, it takes distinct points of the domain to distinct points of the co-domain. A function that is not one-to-one fails to separate points. That is, at least two points of the domain are taken to the same point of the co-domain. This is illustrated in Figure 7.2.1 on the next page.

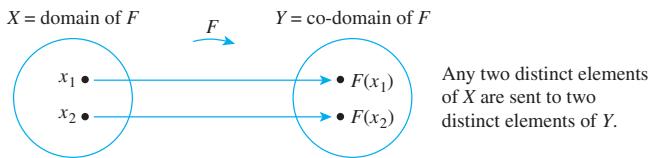


Figure 7.2.1(a) A One-to-One Function Separates Points

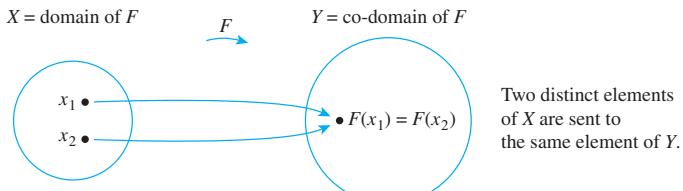


Figure 7.2.1(b) A Function That Is Not One-to-One Collapses Points Together

Example 7.2.1 Identifying One-to-One Functions Defined on Finite Sets

- a. Do either of the arrow diagrams in Figure 7.2.2 define one-to-one functions?

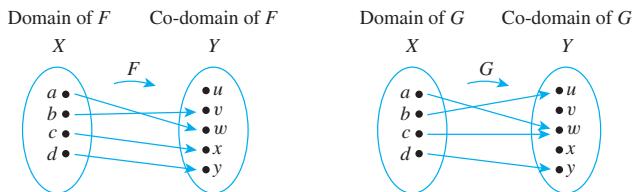


Figure 7.2.2

- b. Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$. Define $H: X \rightarrow Y$ as follows: $H(1) = c$, $H(2) = a$, and $H(3) = d$. Define $K: X \rightarrow Y$ as follows: $K(1) = d$, $K(2) = b$, and $K(3) = d$. Is either H or K one-to-one?

Solution

- a. F is one-to-one but G is not. F is one-to-one because no two different elements of X are sent by F to the same element of Y . G is not one-to-one because the elements a and c are both sent by G to the same element of Y : $G(a) = G(c) = w$ but $a \neq c$.
- b. H is one-to-one but K is not. H is one-to-one because each of the three elements of the domain of H is sent by H to a different element of the co-domain: $H(1) \neq H(2)$, $H(1) \neq H(3)$, and $H(2) \neq H(3)$. K , however, is not one-to-one because $K(1) = K(3) = d$ but $1 \neq 3$. ■

Consider the problem of writing a computer algorithm to check whether a function F is one-to-one. If F is defined on a finite set and there is an independent algorithm to compute values of F , then an algorithm to check whether F is one-to-one can be written as follows: Represent the domain of F as a one-dimensional array $a[1], a[2], \dots, a[n]$ and use a nested loop to examine all possible pairs $(a[i], a[j])$, where $i < j$. If there is a pair $(a[i], a[j])$ for which $F(a[i]) = F(a[j])$ and $a[i] \neq a[j]$, then F is not one-to-one. If, however, all pairs have been examined without finding such a pair, then F is one-to-one. You are asked to write such an algorithm in exercise 57 at the end of this section.

One-to-One Functions on Infinite Sets

Now suppose f is a function defined on an infinite set X . By definition, f is one-to-one if, and only if, the following universal statement is true:

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

Thus, to prove f is one-to-one, you will generally use the method of direct proof:

suppose x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$

and **show** that $x_1 = x_2$.

To show that f is *not* one-to-one, you will ordinarily

find elements x_1 and x_2 in X so that $f(x_1) = f(x_2)$ but $x_1 \neq x_2$.

Example 7.2.2 Proving or Disproving That Functions Are One-to-One

Define $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules

$$f(x) = 4x - 1 \quad \text{for all } x \in \mathbf{R}$$

$$\text{and} \quad g(n) = n^2 \quad \text{for all } n \in \mathbf{Z}.$$

- Is f one-to-one? Prove or give a counterexample.
- Is g one-to-one? Prove or give a counterexample.

Solution It is usually best to start by taking a positive approach to answering questions like these. Try to prove the given functions are one-to-one and see whether you run into difficulty. If you finish without running into any problems, then you have a proof. If you do encounter a problem, then analyzing the problem may lead you to discover a counterexample.

- The function $f: \mathbf{R} \rightarrow \mathbf{R}$ is defined by the rule

$$f(x) = 4x - 1 \quad \text{for all real numbers } x.$$

To prove that f is one-to-one, you need to prove that

$$\forall \text{ real numbers } x_1 \text{ and } x_2, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

Substituting the definition of f into the outline of a direct proof, you

suppose x_1 and x_2 are any real numbers such that $4x_1 - 1 = 4x_2 - 1$,

and **show** that $x_1 = x_2$.

Can you reach what is to be shown from the supposition? Of course. Just add 1 to both sides of the equation in the supposition and then divide both sides by 4.

This discussion is summarized in the following formal answer.

Answer to (a):

If the function $f: \mathbf{R} \rightarrow \mathbf{R}$ is defined by the rule $f(x) = 4x - 1$, for all real numbers x , then f is one-to-one.

Proof:

Suppose x_1 and x_2 are real numbers such that $f(x_1) = f(x_2)$. [We must show that $x_1 = x_2$.] By definition of f ,

$$4x_1 - 1 = 4x_2 - 1.$$

Adding 1 to both sides gives

$$4x_1 = 4x_2,$$

and dividing both sides by 4 gives

$$x_1 = x_2,$$

which is what was to be shown.

- b. The function $g: \mathbf{Z} \rightarrow \mathbf{Z}$ is defined by the rule

$$g(n) = n^2 \quad \text{for all integers } n.$$

As above, you start as though you were going to prove that g is one-to-one. Substituting the definition of g into the outline of a direct proof, you

suppose n_1 and n_2 are integers such that $n_1^2 = n_2^2$,

and

try to show that $n_1 = n_2$.

Can you reach what is to be shown from the supposition? No! It is quite possible for two numbers to have the same squares and yet be different. For example, $2^2 = (-2)^2$ but $2 \neq -2$.

Thus, in trying to prove that g is one-to-one, you run into difficulty. But analyzing this difficulty leads to the discovery of a counterexample, which shows that g is not one-to-one.

This discussion is summarized as follows:

Answer to (b):

If the function $g: \mathbf{Z} \rightarrow \mathbf{Z}$ is defined by the rule $g(n) = n^2$, for all $n \in \mathbf{Z}$, then g is not one-to-one.

Counterexample:

Let $n_1 = 2$ and $n_2 = -2$. Then by definition of g ,

$$\begin{aligned} g(n_1) &= g(2) = 2^2 = 4 \quad \text{and also} \\ g(n_2) &= g(-2) = (-2)^2 = 4. \end{aligned}$$

Hence

$$g(n_1) = g(n_2) \quad \text{but} \quad n_1 \neq n_2,$$

and so g is not one-to-one.

Application: Hash Functions

Imagine a set of student records, each of which includes the student's social security number, and suppose the records are to be stored in a table in which a record can be located if the social security number is known. One way to do this would be to place the record with social security number n into position n of the table. However, since social security numbers have nine digits, this method would require a table with 999,999,999 positions. The problem is that creating such a table for a small set of records would be very wasteful of computer memory space. **Hash functions** are functions defined from larger to smaller sets of integers, frequently using the *mod* function, which provide part of the solution to this problem. We illustrate how to define and use a *hash* function with a very simple example.

Example 7.2.3 A Hash Function

Suppose there are no more than seven student records. Define a function *Hash* from the set of all social security numbers (ignoring hyphens) to the set $\{0, 1, 2, 3, 4, 5, 6\}$ as follows:

$$\text{Hash}(n) = n \bmod 7 \quad \text{for all social security numbers } n.$$

To use your calculator to find $n \bmod 7$, use the formula $n \bmod 7 = n - 7 \cdot (n \text{ div } 7)$. (See Section 4.4.) In other words, divide n by 7, multiply the integer part of the result by 7, and subtract that number from n . For instance, since $328343419/7 = 46906202.71\dots$,

$$\text{Hash}(328343419) = 328343419 - (7 \cdot 46906202) = 5.$$

As a first approximation to solving the problem of storing the records, try to place the record with social security number n in position $\text{Hash}(n)$. For instance, if the social security numbers are 328-34-3419, 356-63-3102, 223-79-9061, and 513-40-8716, the positions of the records are as shown in Table 7.2.1.

The problem with this approach is that *Hash* may not be one-to one; *Hash* might assign the same position in the table to records with different social security numbers. Such an assignment is called a **collision**. When collisions occur, various **collision resolution methods** are used. One of the simplest is the following: If, when the record with social security number n is to be placed, position $\text{Hash}(n)$ is already occupied, start from that position and search downward to place the record in the first empty position that occurs, going back up to the beginning of the table if necessary. To locate a record in the table from its social security number, n , you compute $\text{Hash}(n)$ and search downward from that position to find the record with social security number n . If there are not too many collisions, this is a very efficient way to store and locate records.

Suppose the social security number for another record to be stored is 908-37-1011. Find the position in Table 7.2.1 into which this record would be placed.

Solution When you compute *Hash* you find that $\text{Hash}(908-37-1011) = 2$, which is already occupied by the record with social security number 513-40-8716. Searching downward from position 2, you find that position 3 is also occupied but position 4 is free.



Therefore, you place the record with social security number n into position 4. ■

Onto Functions

It was noted in Section 7.1 that there may be an element of the co-domain of a function that is not the image of any element in the domain. On the other hand, *every* element of a function's co-domain may be the image of some element of its domain. Such a function is called *onto* or *surjective*. When a function is onto, its range is equal to its co-domain.

- **Definition**

Let F be a function from a set X to a set Y . F is **onto** (or **surjective**) if, and only if, given any element y in Y , it is possible to find an element x in X with the property that $y = F(x)$.

Symbolically:

$$F: X \rightarrow Y \text{ is onto} \Leftrightarrow \forall y \in Y, \exists x \in X \text{ such that } F(x) = y.$$

To obtain a precise statement of what it means for a function *not* to be onto, take the negation of the definition of onto:

$$F: X \rightarrow Y \text{ is not onto} \Leftrightarrow \exists y \text{ in } Y \text{ such that } \forall x \in X, F(x) \neq y.$$

That is, there is some element in Y that is *not* the image of *any* element in X .

In terms of arrow diagrams, a function is onto if each element of the co-domain has an arrow pointing to it from some element of the domain. A function is not onto if at least one element in its co-domain does not have an arrow pointing to it. This is illustrated in Figure 7.2.3.

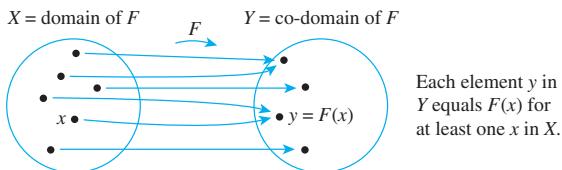


Figure 7.2.3(a) A Function That Is Onto

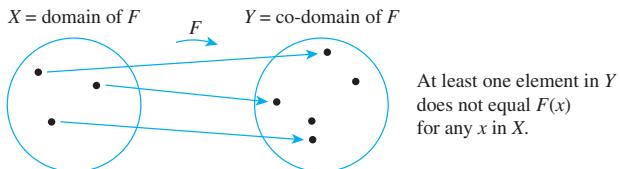


Figure 7.2.3(b) A Function That Is Not Onto

Example 7.2.4 Identifying Onto Functions Defined on Finite Sets

- a. Do either of the arrow diagrams in Figure 7.2.4 define onto functions?

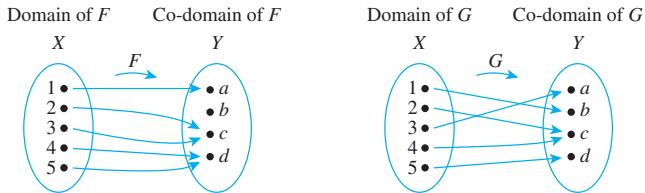


Figure 7.2.4

- b. Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$. Define $H: X \rightarrow Y$ as follows: $H(1) = c$, $H(2) = a$, $H(3) = c$, $H(4) = b$. Define $K: X \rightarrow Y$ as follows: $K(1) = c$, $K(2) = b$, $K(3) = b$, and $K(4) = c$. Is either H or K onto?

Solution

- a. F is not onto because $b \neq F(x)$ for any x in X . G is onto because each element of Y equals $G(x)$ for some x in X : $a = G(3)$, $b = G(1)$, $c = G(2) = G(4)$, and $d = G(5)$.
- b. H is onto but K is not. H is onto because each of the three elements of the co-domain of H is the image of some element of the domain of H : $a = H(2)$, $b = H(4)$, and $c = H(1) = H(3)$. K , however, is not onto because $a \neq K(x)$ for any x in $\{1, 2, 3, 4\}$.

■

It is possible to write a computer algorithm to check whether a function F is onto, provided F is defined from a finite set X to a finite set Y and there is an independent algorithm to compute values of F . Represent X and Y as one-dimensional arrays $a[1], a[2], \dots, a[n]$ and $b[1], b[2], \dots, b[m]$, respectively, and use a nested loop to pick each element y of Y in turn and search through the elements of X to find an x such that y is the image of x . If any search is unsuccessful, then F is not onto. If each such search is successful, then F is onto. You are asked to write such an algorithm in exercise 58 at the end of this section.

Onto Functions on Infinite Sets

Now suppose F is a function from a set X to a set Y , and suppose Y is infinite. By definition, F is onto if, and only if, the following universal statement is true:

$$\forall y \in Y, \exists x \in X \text{ such that } F(x) = y.$$

Thus to prove F is onto, you will ordinarily use the method of generalizing from the generic particular:

suppose that y is any element of Y

and show that there is an element x of X with $F(x) = y$.

To prove F is *not* onto, you will usually

find an element y of Y such that $y \neq F(x)$ for *any* x in X .

Example 7.2.5 Proving or Disproving That Functions Are Onto

Define $f: \mathbf{R} \rightarrow \mathbf{R}$ and $h: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules

$$f(x) = 4x - 1 \quad \text{for all } x \in \mathbf{R}$$

and $h(n) = 4n - 1 \quad \text{for all } n \in \mathbf{Z}$.

- a. Is f onto? Prove or give a counterexample.
 b. Is h onto? Prove or give a counterexample.

Solution

- a. The best approach is to start trying to prove that f is onto and be alert for difficulties that might indicate that it is not. Now $f: \mathbf{R} \rightarrow \mathbf{R}$ is the function defined by the rule

$$f(x) = 4x - 1 \quad \text{for all real numbers } x.$$

To prove that f is onto, you must prove

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y.$$

Substituting the definition of f into the outline of a proof by the method of generalizing from the generic particular, you

suppose y is a real number

and **show** that there exists a real number x such that $y = 4x - 1$.



Caution! This scratch work only proves what x has to be if it exists. The scratch work does not prove that x exists.

Scratch Work: If such a real number x exists, then

$$\begin{aligned} 4x - 1 &= y \\ 4x &= y + 1 \quad \text{by adding 1 to both sides} \\ x &= \frac{y+1}{4} \quad \text{by dividing both sides by 4.} \end{aligned}$$

Thus if such a number x exists, it must equal $(y+1)/4$. Does such a number exist? Yes. To show this, let $x = (y+1)/4$, and then make sure that (1) x is a real number and that (2) f really does send x to y . The following formal answer summarizes this process.

Answer to (a):

If $f: \mathbf{R} \rightarrow \mathbf{R}$ is the function defined by the rule $f(x) = 4x - 1$ for all real numbers x , then f is onto.

Proof:

Let $y \in \mathbf{R}$. [We must show that $\exists x \in \mathbf{R}$ such that $f(x) = y$.] Let $x = (y+1)/4$. Then x is a real number since sums and quotients (other than by 0) of real numbers are real numbers. It follows that

$$\begin{aligned} f(x) &= f\left(\frac{y+1}{4}\right) && \text{by substitution} \\ &= 4 \cdot \left(\frac{y+1}{4}\right) - 1 && \text{by definition of } f \\ &= (y+1) - 1 = y && \text{by basic algebra.} \end{aligned}$$

[This is what was to be shown.]

- b. The function $h: \mathbf{Z} \rightarrow \mathbf{Z}$ is defined by the rule

$$h(n) = 4n - 1 \quad \text{for all integers } n.$$

To prove that h is onto, it would be necessary to prove that

$$\forall \text{ integers } m, \exists \text{ an integer } n \text{ such that } h(n) = m.$$

Substituting the definition of h into the outline of a proof by the method of generalizing from the generic particular, you

suppose m is any integer

and **try to show** that there is an integer n with $4n - 1 = m$.

Can you reach what is to be shown from the supposition? No! If $4n - 1 = m$, then

$$n = \frac{m+1}{4} \quad \text{by adding 1 and dividing by 4.}$$

But n must be an integer. And when, for example, $m = 0$, then

$$n = \frac{0+1}{4} = \frac{1}{4},$$

which is *not* an integer.

Thus, in trying to prove that h is onto, you run into difficulty, and this difficulty reveals a counterexample that shows h is not onto.

This discussion is summarized in the following formal answer.

Answer to (b):

If the function $h: \mathbf{Z} \rightarrow \mathbf{Z}$ is defined by the rule $h(n) = 4n - 1$ for all integers n , then h is not onto.

Counterexample:

The co-domain of h is \mathbf{Z} and $0 \in \mathbf{Z}$. But $h(n) \neq 0$ for any integer n . For if $h(n) = 0$, then

$$4n - 1 = 0 \quad \text{by definition of } h$$

which implies that

$$4n = 1 \quad \text{by adding 1 to both sides}$$

and so

$$n = \frac{1}{4} \quad \text{by dividing both sides by 4.}$$

But $1/4$ is not an integer. Hence there is no integer n for which $f(n) = 0$, and thus f is not onto.

Relations between Exponential and Logarithmic Functions

Note That the quantity b^x is a real number for any real number x follows from the least-upper-bound property of the real number system. (See Appendix A.)

For positive numbers $b \neq 1$, the **exponential function with base b** , denoted \exp_b , is the function from \mathbf{R} to \mathbf{R}^+ defined as follows: For all real numbers x ,

$$\exp_b(x) = b^x$$

where $b^0 = 1$ and $b^{-x} = 1/b^x$.

When working with the exponential function, it is useful to recall the laws of exponents from elementary algebra.

Laws of Exponents

If b and c are any positive real numbers and u and v are any real numbers, the following laws of exponents hold true:

$$b^u b^v = b^{u+v} \quad 7.2.1$$

$$(b^u)^v = b^{uv} \quad 7.2.2$$

$$\frac{b^u}{b^v} = b^{u-v} \quad 7.2.3$$

$$(bc)^u = b^u c^u \quad 7.2.4$$

In Section 7.1 the logarithmic function with base b was defined for any positive number $b \neq 1$ to be the function from \mathbf{R}^+ to \mathbf{R} with the property that for each positive real number x ,

$\log_b(x) =$ the exponent to which b must be raised to obtain x .

Or, equivalently, for each positive real number x and real number y ,

$$\log_b x = y \Leftrightarrow b^y = x.$$

It can be shown using calculus that both the exponential and logarithmic functions are one-to-one and onto. Therefore, by definition of one-to-one, the following properties hold true:

For any positive real number b with $b \neq 1$,

$$\text{if } b^u = b^v \text{ then } u = v \text{ for all real numbers } u \text{ and } v, \quad 7.2.5$$

and

$$\text{if } \log_b u = \log_b v \text{ then } u = v \text{ for all positive real numbers } u \text{ and } v. \quad 7.2.6$$

These properties are used to derive many additional facts about exponents and logarithms. In particular we have the following properties of logarithms.

Theorem 7.2.1 Properties of Logarithms

For any positive real numbers b, c and x with $b \neq 1$ and $c \neq 1$:

a. $\log_b(xy) = \log_b x + \log_b y$

b. $\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y$

c. $\log_b(x^a) = a \log_b x$

d. $\log_c x = \frac{\log_b x}{\log_b c}$

Theorem 7.2.1(d) is proved in the next example. You are asked to prove the remainder of the theorem in exercises 33–35 at the end of this section.

Example 7.2.6 Using the One-to-Oneness of the Exponential Function

Use the definition of logarithm, the laws of exponents, and the one-to-oneness of the exponential function (property 7.2.5) to prove part (d) of Theorem 7.2.1: For any positive real numbers b , c , and x , with $b \neq 1$ and $c \neq 1$,

$$\log_c x = \frac{\log_b x}{\log_b c}.$$

Solution Suppose positive real numbers b , c , and x are given. Let

$$(1) \quad u = \log_b c \quad (2) \quad v = \log_c x \quad (3) \quad w = \log_b x.$$

Then, by definition of logarithm,

$$(1') \quad c = b^u \quad (2') \quad x = c^v \quad (3') \quad x = b^w.$$

Substituting (1') into (2') and using one of the laws of exponents gives

$$x = c^v = (b^u)^v = b^{uv} \quad \text{by 7.2.2}$$

But by (3), $x = b^w$ also. Hence

$$b^{uv} = b^w,$$

and so by the one-to-oneness of the exponential function (property 7.2.5),

$$uv = w.$$

Substituting from (1), (2), and (3) gives that

$$(\log_b c)(\log_c x) = \log_b x.$$

And dividing both sides by $\log_b c$ (which is nonzero because $c \neq 1$) results in

$$\log_c x = \frac{\log_b x}{\log_b c}. \quad \blacksquare$$

Example 7.2.7 Computing Logarithms with Base 2 on a Calculator

In computer science it is often necessary to compute logarithms with base 2. Most calculators do not have keys to compute logarithms with base 2 but do have keys to compute logarithms with base 10 (called **common logarithms** and often denoted simply log) and logarithms with base e (called **natural logarithms** and usually denoted ln). Suppose your calculator shows that $\ln 5 \cong 1.609437912$ and $\ln 2 \cong 0.6931471806$. Use Theorem 7.2.1(d) to find an approximate value for $\log_2 5$.

Solution By Theorem 7.2.1(d),

$$\log_2 5 = \frac{\ln 5}{\ln 2} \cong \frac{1.609437912}{0.6931471806} \cong 2.321928095. \quad \blacksquare$$

One-to-One Correspondences

Consider a function $F: X \rightarrow Y$ that is both one-to-one and onto. Given any element x in X , there is a unique corresponding element $y = F(x)$ in Y (since F is a function). Also given any element y in Y , there is an element x in X such that $F(x) = y$ (since F is onto) and there is only one such x (since F is one-to-one). Thus, a function that is one-to-one and onto sets up a pairing between the elements of X and the elements of Y that matches

each element of X with exactly one element of Y and each element of Y with exactly one element of X . Such a pairing is called a *one-to-one correspondence* or *bijection* and is illustrated by the arrow diagram in Figure 7.2.5. One-to-one correspondences are often used as aids to counting. The pairing of Figure 7.2.5, for example, shows that there are five elements in the set X .

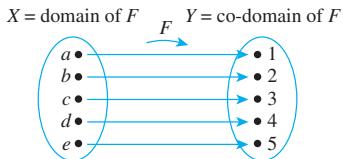


Figure 7.2.5 An Arrow Diagram for a One-to-One Correspondence

• **Definition**

A **one-to-one correspondence** (or **bijection**) from a set X to a set Y is a function $F: X \rightarrow Y$ that is both one-to-one and onto.

Example 7.2.8 A Function from a Power Set to a Set of Strings

Let $\mathcal{P}(\{a, b\})$ be the set of all subsets of $\{a, b\}$ and let S be the set of all strings of length 2 made up of 0's and 1's. Then $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ and $S = \{00, 01, 10, 11\}$. Define a function h from $\mathcal{P}(\{a, b\})$ to S as follows: Given any subset A of $\{a, b\}$, a is either in A or not in A , and b is either in A or not in A . If a is in A , write a 1 in the first position of the string $h(A)$. If a is not in A , write a 0 in the first position of the string $h(A)$. Similarly, if b is in A , write a 1 in the second position of the string $h(A)$. If b is not in A , write a 0 in the second position of the string $h(A)$. This definition is summarized in the following table.

Subset of $\{a, b\}$	Status of a	Status of b	String in S
\emptyset	not in	not in	00
$\{a\}$	in	not in	10
$\{b\}$	not in	in	01
$\{a, b\}$	in	in	11

Is h a one-to-one correspondence?

Solution The arrow diagram shown in Figure 7.2.6 shows clearly that h is a one-to-one correspondence. It is onto because each element of S has an arrow pointing to it. It is one-to-one because each element of S has no more than one arrow pointing to it.

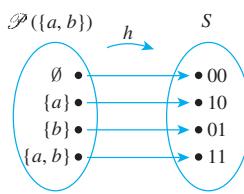


Figure 7.2.6

Example 7.2.9 A String-Reversing Function

Let T be the set of all finite strings of x 's and y 's. Define $g: T \rightarrow T$ by the rule:
For all strings $s \in T$,

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Is g a one-to-one correspondence from T to itself?

Solution The answer is yes. To show that g is a one-to-one correspondence, it is necessary to show that g is one-to-one and onto.

To see that g is one-to-one, suppose that for some strings s_1 and s_2 in T , $g(s_1) = g(s_2)$. [We must show that $s_1 = s_2$.] Now to say that $g(s_1) = g(s_2)$ is the same as saying that the string obtained by writing the characters of s_1 in reverse order equals the string obtained by writing the characters of s_2 in reverse order. But if s_1 and s_2 are equal when written in reverse order, then they must be equal to start with. In other words, $s_1 = s_2$ [as was to be shown].

To show that g is onto, suppose t is a string in T . [We must find a string s in T such that $g(s) = t$.] Let $s = g(t)$. By definition of g , $s = g(t)$ is the string in T obtained by writing the characters of t in reverse order. But when the order of the characters of a string is reversed once and then reversed again, the original string is recovered. Thus

$$\begin{aligned} g(s) &= g(g(t)) = \text{the string obtained by writing the characters of } t \text{ in reverse order and then writing those characters in reverse order again} \\ &= t. \end{aligned}$$

This is what was to be shown. ■

Example 7.2.10 A Function of Two Variables

Define a function $F: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$ as follows: For all $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$F(x, y) = (x + y, x - y).$$

Is F a one-to-one correspondence from $\mathbf{R} \times \mathbf{R}$ to itself?

Solution The answer is yes. To show that F is a one-to-one correspondence, you need to show both that F is one-to-one and that F is onto.

Proof that F is one-to-one: Suppose that (x_1, y_1) and (x_2, y_2) are any ordered pairs in $\mathbf{R} \times \mathbf{R}$ such that

$$F(x_1, y_1) = F(x_2, y_2).$$

[We must show that $(x_1, y_1) = (x_2, y_2)$.] By definition of F ,

$$(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2).$$

For two ordered pairs to be equal, both the first and second components must be equal. Thus x_1 , y_1 , x_2 , and y_2 satisfy the following system of equations:

$$x_1 + y_1 = x_2 + y_2 \tag{1}$$

$$x_1 - y_1 = x_2 - y_2 \tag{2}$$

Adding equations (1) and (2) gives that

$$2x_1 = 2x_2, \quad \text{and so} \quad x_1 = x_2.$$

Substituting $x_1 = x_2$ into equation (1) yields

$$x_1 + y_1 = x_1 + y_2, \quad \text{and so} \quad y_1 = y_2.$$



Caution! This scratch work only shows what (r, s) has to be if it exists. The scratch work does not prove that (r, s) exists.

Thus, by definition of equality of ordered pairs, $(x_1, y_1) = (x_2, y_2)$ [as was to be shown].

Scratch Work for the Proof that F is onto: To prove that F is onto, you suppose you have any ordered pair in the co-domain $\mathbf{R} \times \mathbf{R}$, say (u, v) , and then you show that there is an ordered pair in the domain that is sent to (u, v) by F . To do this, you suppose temporarily that you have found such an ordered pair, say (r, s) . Then

$$F(r, s) = (u, v) \quad \begin{array}{l} \text{because you are supposing that} \\ F \text{ sends } (r, s) \text{ to } (u, v), \end{array}$$

and

$$F(r, s) = (r + s, r - s) \quad \text{by definition of } F.$$

Equating the right-hand sides gives

$$(r + s, r - s) = (u, v).$$

By definition of equality of ordered pairs this means that

$$r + s = u \quad (1)$$

$$r - s = v \quad (2)$$

Adding equations (1) and (2) gives

$$2r = u + v, \quad \text{and so} \quad r = \frac{u+v}{2}.$$

Subtracting equation (2) from equation (1) yields

$$2s = u - v, \quad \text{and so} \quad s = \frac{u-v}{2}.$$

Thus, if F sends (r, s) to (u, v) , then $r = (u + v)/2$ and $s = (u - v)/2$. To turn this scratch work into a proof, you need to make sure that (1) $\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ is in the domain of F , and (2) that F really does send $\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ to (u, v) .

Proof that F is onto: Suppose (u, v) is any ordered pair in the co-domain of F . [We will show that there is an ordered pair in the domain of F that is sent to (u, v) by F .] Let

$$r = \frac{u+v}{2} \quad \text{and} \quad s = \frac{u-v}{2}.$$

Then (r, s) is an ordered pair of real numbers and so is in the domain of F . In addition:

$$\begin{aligned} F(r, s) &= F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) && \text{by definition of } F \\ &= \left(\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}\right) && \text{by substitution} \\ &= \left(\frac{u+v+u-v}{2}, \frac{u+v-u+v}{2}\right) \\ &= \left(\frac{2u}{2}, \frac{2v}{2}\right) \\ &= (u, v) && \text{by algebra.} \end{aligned}$$

[This is what was to be shown.] ■

Inverse Functions

If F is a one-to-one correspondence from a set X to a set Y , then there is a function from Y to X that “undoes” the action of F ; that is, it sends each element of Y back to the element of X that it came from. This function is called the *inverse function* for F .

Theorem 7.2.2

Suppose $F: X \rightarrow Y$ is a one-to-one correspondence; that is, suppose F is one-to-one and onto. Then there is a function $F^{-1}: Y \rightarrow X$ that is defined as follows:

Given any element y in Y ,

$$F^{-1}(y) = \text{that unique element } x \text{ in } X \text{ such that } F(x) \text{ equals } y.$$

In other words,

$$F^{-1}(y) = x \Leftrightarrow y = F(x).$$

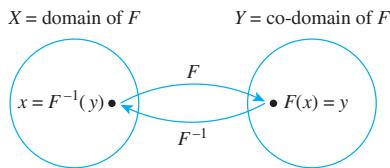
The proof of Theorem 7.2.2 follows immediately from the definition of one-to-one and onto. Given an element y in Y , there is an element x in X with $F(x) = y$ because F is onto; x is unique because F is one-to-one.

• Definition

The function F^{-1} of Theorem 7.2.2 is called the **inverse function** for F .

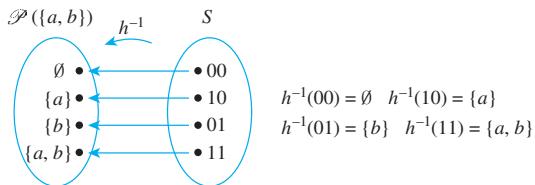
Note that according to this definition, the logarithmic function with base $b > 0$ is the inverse of the exponential function with base b .

The diagram that follows illustrates the fact that an inverse function sends each element back to where it came from.

**Example 7.2.11 Finding an Inverse Function for a Function Given by an Arrow Diagram**

Define the inverse function for the one-to-one correspondence h given in Example 7.2.8.

Solution The arrow diagram for h^{-1} is obtained by tracing the h -arrows back from S to $\mathcal{P}(\{a, b\})$ as shown below.

**Example 7.2.12 Finding an Inverse Function for a Function Given in Words**

Define the inverse function for the one-to-one correspondence g given in Example 7.2.9.

Solution The function $g: T \rightarrow T$ is defined by the rule

For all strings t in T ,

$$g(t) = \text{the string obtained by writing the characters of } t \text{ in reverse order.}$$

Now if the characters of t are written in reverse order and then written in reverse order again, the original string is recovered. Thus given any string t in T ,

$$\begin{aligned}g^{-1}(t) &= \text{the unique string that, when written}\\&\quad \text{in reverse order, equals } t \\&= \text{the string obtained by writing the}\\&\quad \text{characters of } t \text{ in reverse order} \\&= g(t).\end{aligned}$$

Hence $g^{-1}: T \rightarrow T$ is the same as g , or, in other words, $g^{-1} = g$. ■

Example 7.2.13 Finding an Inverse Function for a Function Given by a Formula

The function $f: \mathbf{R} \rightarrow \mathbf{R}$ defined by the formula

$$f(x) = 4x - 1 \quad \text{for all real numbers } x$$

was shown to be one-to-one in Example 7.2.2 and onto in Example 7.2.5. Find its inverse function.

Solution For any [particular but arbitrarily chosen] y in \mathbf{R} , by definition of f^{-1} ,

$$f^{-1}(y) = \text{that unique real number } x \text{ such that } f(x) = y.$$

But

$$\begin{aligned}f(x) &= y \\ \Leftrightarrow 4x - 1 &= y \quad \text{by definition of } f \\ \Leftrightarrow x &= \frac{y+1}{4} \quad \text{by algebra.}\end{aligned}$$

$$\text{Hence } f^{-1}(y) = \frac{y+1}{4}. \quad \blacksquare$$

The following theorem follows easily from the definitions.

Theorem 7.2.3

If X and Y are sets and $F: X \rightarrow Y$ is one-to-one and onto, then $F^{-1}: Y \rightarrow X$ is also one-to-one and onto.

Proof:

F^{-1} is one-to-one: Suppose y_1 and y_2 are elements of Y such that $F^{-1}(y_1) = F^{-1}(y_2)$. [We must show that $y_1 = y_2$.] Let $x = F^{-1}(y_1) = F^{-1}(y_2)$. Then $x \in X$, and by definition of F^{-1} ,

$$F(x) = y_1 \quad \text{since } x = F^{-1}(y_1)$$

$$\text{and} \quad F(x) = y_2 \quad \text{since } x = F^{-1}(y_2).$$

Consequently, $y_1 = y_2$ since each is equal to $F(x)$. This is what was to be shown.

F^{-1} is onto: Suppose $x \in X$. [We must show that there exists an element y in Y such that $F^{-1}(y) = x$.] Let $y = F(x)$. Then $y \in Y$, and by definition of F^{-1} , $F^{-1}(y) = x$. This is what was to be shown.

Example 7.2.14 Finding an Inverse Function for a Function of Two Variables

Define the inverse function $F^{-1} : \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$ for the one-to-one correspondence given in Example 7.2.10.

Solution

The solution to Example 7.2.10 shows that $F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = (u, v)$. Because F is one-to-one, this means that

$\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ is the unique ordered pair in the domain of F that is sent to (u, v) by F .

Thus, F^{-1} is defined as follows: For all $(u, v) \in \mathbf{R} \times \mathbf{R}$,

$$F^{-1}(u, v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right).$$



Test Yourself

1. If F is a function from a set X to a set Y , then F is one-to-one if, and only if, _____.
2. If F is a function from a set X to a set Y , then F is not one-to-one if, and only if, _____.
3. If F is a function from a set X to a set Y , then F is onto if, and only if, _____.
4. If F is a function from a set X to a set Y , then F is not onto if, and only if, _____.
5. The following two statements are _____:

$$\forall u, v \in U, \text{ if } H(u) = H(v) \text{ then } u = v.$$

$$\forall u, v \in U, \text{ if } u \neq v \text{ then } H(u) \neq H(v).$$
6. Given a function $F: X \rightarrow Y$ and an infinite set X , to prove that F is one-to-one, you suppose that _____ and then you show that _____.
7. Given a function $F: X \rightarrow Y$ and an infinite set X , to prove that F is onto, you suppose that _____ and then you show that _____.
8. Given a function $F: X \rightarrow Y$, to prove that F is not one-to-one, you _____.
9. Given a function $F: X \rightarrow Y$, to prove that F is not onto, you _____.
10. A one-to-one correspondence from a set X to a set Y is a _____ that is _____.
11. If F is a one-to-one correspondence from a set X to a set Y and y is in Y , then $F^{-1}(y)$ is _____.

Exercise Set 7.2

1. The definition of one-to-one is stated in two ways:

$$\forall x_1, x_2 \in X, \text{ if } F(x_1) = F(x_2) \text{ then } x_1 = x_2$$

$$\text{and } \forall x_1, x_2 \in X, \text{ if } x_1 \neq x_2 \text{ then } F(x_1) \neq F(x_2).$$

Why are these two statements logically equivalent?

2. Fill in each blank with the word *most* or *least*.

- A function F is one-to-one if, and only if, each element in the co-domain of F is the image of at _____ one element in the domain of F .
- A function F is onto if, and only if, each element in the co-domain of F is the image of at _____ one element in the domain of F .

- H 3.** When asked to state the definition of one-to-one, a student replies, “A function f is one-to-one if, and only if, every element of X is sent by f to exactly one element of Y .” Give a counterexample to show that the student’s reply is incorrect.

- H 4.** Let $f: X \rightarrow Y$ be a function. True or false? A sufficient condition for f to be one-to-one is that for all elements y in Y , there is at most one x in X with $f(x) = y$.

- H 5.** All but two of the following statements are correct ways to express the fact that a function f is onto. Find the two that are incorrect.

- f is onto \Leftrightarrow every element in its co-domain is the image of some element in its domain.
 - f is onto \Leftrightarrow every element in its domain has a corresponding image in its co-domain.
 - f is onto $\Leftrightarrow \forall y \in Y, \exists x \in X$ such that $f(x) = y$.
 - f is onto $\Leftrightarrow \forall x \in X, \exists y \in Y$ such that $f(x) = y$.
 - f is onto \Leftrightarrow the range of f is the same as the co-domain of f .
6. Let $X = \{1, 5, 9\}$ and $Y = \{3, 4, 7\}$.
- Define $f: X \rightarrow Y$ by specifying that
$$f(1) = 4, \quad f(5) = 7, \quad f(9) = 4.$$

Is f one-to-one? Is f onto? Explain your answers.

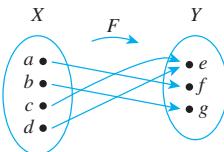
- b. Define $g: X \rightarrow Y$ by specifying that

$$g(1) = 7, \quad g(5) = 3, \quad g(9) = 4.$$

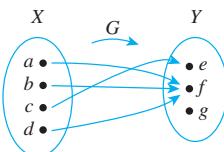
Is g one-to-one? Is g onto? Explain your answers.

7. Let $X = \{a, b, c, d\}$ and $Y = \{e, f, g\}$. Define functions F and G by the arrow diagrams below.

Domain of F Co-domain of F



Domain of G Co-domain of G

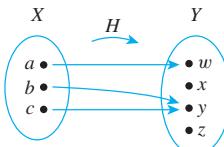


- a. Is F one-to-one? Why or why not? Is it onto? Why or why not?

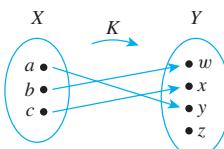
- b. Is G one-to-one? Why or why not? Is it onto? Why or why not?

8. Let $X = \{a, b, c\}$ and $Y = \{w, x, y, z\}$. Define functions H and K by the arrow diagrams below.

Domain of H Co-domain of H



Domain of K Co-domain of K



- a. Is H one-to-one? Why or why not? Is it onto? Why or why not?

- b. Is K one-to-one? Why or why not? Is it onto? Why or why not?

9. Let $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$, and $Z = \{1, 2\}$.

- a. Define a function $f: X \rightarrow Y$ that is one-to-one but not onto.
 b. Define a function $g: X \rightarrow Z$ that is onto but not one-to-one.
 c. Define a function $h: X \rightarrow X$ that is neither one-to-one nor onto.
 d. Define a function $k: X \rightarrow X$ that is one-to-one and onto but is not the identity function on X .

10. a. Define $f: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rule $f(n) = 2n$, for all integers n .

(i) Is f one-to-one? Prove or give a counterexample.

(ii) Is f onto? Prove or give a counterexample.

- b. Let $2\mathbf{Z}$ denote the set of all even integers. That is, $2\mathbf{Z} = \{n \in \mathbf{Z} \mid n = 2k, \text{ for some integer } k\}$. Define $h: \mathbf{Z} \rightarrow 2\mathbf{Z}$ by the rule $h(n) = 2n$, for all integers n . Is h onto? Prove or give a counterexample.

- H 11. a. Define $g: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rule $g(n) = 4n - 5$, for all integers n .

(i) Is g one-to-one? Prove or give a counterexample.

(ii) Is g onto? Prove or give a counterexample.

- b. Define $G: \mathbf{R} \rightarrow \mathbf{R}$ by the rule $G(x) = 4x - 5$ for all real numbers x . Is G onto? Prove or give a counterexample.

12. a. Define $F: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rule $F(n) = 2 - 3n$, for all integers n .

(i) Is F one-to-one? Prove or give a counterexample.

(ii) Is F onto? Prove or give a counterexample.

- b. Define $G: \mathbf{R} \rightarrow \mathbf{R}$ by the rule $G(x) = 2 - 3x$ for all real numbers x . Is G onto? Prove or give a counterexample.

13. a. Define $H: \mathbf{R} \rightarrow \mathbf{R}$ by the rule $H(x) = x^2$, for all real numbers x .

(i) Is H one-to-one? Prove or give a counterexample.

(ii) Is H onto? Prove or give a counterexample.

- b. Define $K: \mathbf{R}^{nonneg} \rightarrow \mathbf{R}^{nonneg}$ by the rule $K(x) = x^2$, for all nonnegative real numbers x . Is K onto? Prove or give a counterexample.

14. Explain the mistake in the following “proof.”

Theorem: The function $f: \mathbf{Z} \rightarrow \mathbf{Z}$ defined by the formula $f(n) = 4n + 3$, for all integers n , is one-to-one.

“Proof: Suppose any integer n is given. Then by definition of f , there is only one possible value for $f(n)$, namely, $4n + 3$. Hence f is one-to-one.”

In each of 15–18 a function f is defined on a set of real numbers. Determine whether or not f is one-to-one and justify your answer.

15. $f(x) = \frac{x+1}{x}$, for all real numbers $x \neq 0$

16. $f(x) = \frac{x}{x^2 + 1}$, for all real numbers x

17. $f(x) = \frac{3x-1}{x}$, for all real numbers $x \neq 0$

18. $f(x) = \frac{x+1}{x-1}$, for all real numbers $x \neq 1$

19. Referring to Example 7.2.3, assume that records with the following social security numbers are to be placed in sequence into Table 7.2.1. Find the position into which each record is placed.

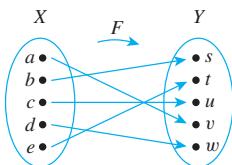
- a. 417-30-2072 b. 364-98-1703 c. 283-09-0787

- 20.** Define Floor: $\mathbf{R} \rightarrow \mathbf{Z}$ by the formula $\text{Floor}(x) = \lfloor x \rfloor$, for all real numbers x .
- Is Floor one-to-one? Prove or give a counterexample.
 - Is Floor onto? Prove or give a counterexample.
- 21.** Let S be the set of all strings of 0's and 1's, and define $l: S \rightarrow \mathbf{Z}^{\text{nonneg}}$ by
- $$l(s) = \text{the length of } s, \quad \text{for all strings } s \in S.$$
- Is l one-to-one? Prove or give a counterexample.
 - Is l onto? Prove or give a counterexample.
- 22.** Let S be the set of all strings of 0's and 1's, and define $D: S \rightarrow \mathbf{Z}$ as follows: For all $s \in S$,
- $$D(s) = \text{the number of 1's in } s \text{ minus the number of 0's in } s.$$
- Is D one-to-one? Prove or give a counterexample.
 - Is D onto? Prove or give a counterexample.
- 23.** Define $F: \mathcal{P}(\{a, b, c\}) \rightarrow \mathbf{Z}$ as follows: For all A in $\mathcal{P}(\{a, b, c\})$,
- $$F(A) = \text{the number of elements in } A.$$
- Is F one-to-one? Prove or give a counterexample.
 - Is F onto? Prove or give a counterexample.
- 24.** Let S be the set of all strings of a 's and b 's, and define $N: S \rightarrow \mathbf{Z}$ by
- $$N(s) = \text{the number of } a\text{'s in } s, \quad \text{for all } s \in S.$$
- Is N one-to-one? Prove or give a counterexample.
 - Is N onto? Prove or give a counterexample.
- 25.** Let S be the set of all strings in a 's and b 's, and define $C: S \rightarrow S$ by
- $$C(s) = as, \quad \text{for all } s \in S.$$
- (C is called **concatenation** by a on the left.)
- Is C one-to-one? Prove or give a counterexample.
 - Is C onto? Prove or give a counterexample.
- 26.** Define $S: \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ by the rule: For all integers n , $S(n) =$ the sum of the positive divisors of n .
- Is S one-to-one? Prove or give a counterexample.
 - Is S onto? Prove or give a counterexample.
- H 27.** Let D be the set of all finite subsets of positive integers, and define $T: \mathbf{Z}^+ \rightarrow D$ by the rule: For all integers n , $T(n) =$ the set of all of the positive divisors of n .
- Is T one-to-one? Prove or give a counterexample.
 - Is T onto? Prove or give a counterexample.
- 28.** Define $G: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$ as follows:
- $$G(x, y) = (2y, -x) \text{ for all } (x, y) \in \mathbf{R} \times \mathbf{R}.$$
- Is G one-to-one? Prove or give a counterexample.
 - Is G onto? Prove or give a counterexample.
- 29.** Define $H: \mathbf{R} \times \mathbf{R} \rightarrow \mathbf{R} \times \mathbf{R}$ as follows:
- $$H(x, y) = (x + 1, 2 - y) \text{ for all } (x, y) \in \mathbf{R} \times \mathbf{R}.$$
- Is H one-to-one? Prove or give a counterexample.
 - Is H onto? Prove or give a counterexample.
- 30.** Define $J: \mathbf{Q} \times \mathbf{Q} \rightarrow \mathbf{R}$ by the rule $J(r, s) = r + \sqrt{2}s$ for all $(r, s) \in \mathbf{Q} \times \mathbf{Q}$.
- Is J one-to-one? Prove or give a counterexample.
 - Is J onto? Prove or give a counterexample.
- *31.** Define $F: \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ and $G: \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ as follows: For all $(n, m) \in \mathbf{Z}^+ \times \mathbf{Z}^+$,
- $$F(n, m) = 3^n 5^m \quad \text{and} \quad G(n, m) = 3^n 6^m.$$
- H a.** Is F one-to-one? Prove or give a counterexample.
- H b.** Is G one-to-one? Prove or give a counterexample.
- 32. a.** Is $\log_8 27 = \log_2 3$? Why or why not?
- 32. b.** Is $\log_{16} 9 = \log_4 3$? Why or why not?
- The properties of logarithm established in 33–35 are used in Sections 11.4 and 11.5.
- 33.** Prove that for all positive real numbers b, x , and y with $b \neq 1$,
- $$\log_b \left(\frac{x}{y} \right) = \log_b x - \log_b y.$$
- 34.** Prove that for all positive real numbers b, x , and y with $b \neq 1$,
- $$\log_b(xy) = \log_b x + \log_b y.$$
- H 35.** Prove that for all real numbers a, b , and x with b and x positive and $b \neq 1$,
- $$\log_b(x^a) = a \log_b x.$$
- Exercises 36 and 37 use the following definition: If $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ are functions, then the function $(f + g): \mathbf{R} \rightarrow \mathbf{R}$ is defined by the formula $(f + g)(x) = f(x) + g(x)$ for all real numbers x .
- 36.** If $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ are both one-to-one, is $f + g$ also one-to-one? Justify your answer.
- 37.** If $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ are both onto, is $f + g$ also onto? Justify your answer.
- Exercises 38 and 39 use the following definition: If $f: \mathbf{R} \rightarrow \mathbf{R}$ is a function and c is a nonzero real number, the function $(c \cdot f): \mathbf{R} \rightarrow \mathbf{R}$ is defined by the formula $(c \cdot f)(x) = c \cdot f(x)$ for all real numbers x .
- 38.** Let $f: \mathbf{R} \rightarrow \mathbf{R}$ be a function and c a nonzero real number. If f is one-to-one, is $c \cdot f$ also one-to-one? Justify your answer.
- 39.** Let $f: \mathbf{R} \rightarrow \mathbf{R}$ be a function and c a nonzero real number. If f is onto, is $c \cdot f$ also onto? Justify your answer.
- H 40.** Suppose $F: X \rightarrow Y$ is one-to-one.
- Prove that for all subsets $A \subseteq X$, $F^{-1}(F(A)) = A$.
 - Prove that for all subsets A_1 and A_2 in X ,
- $$F(A_1 \cap A_2) = F(A_1) \cap F(A_2).$$

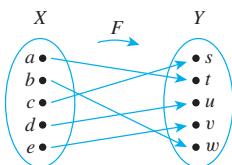
41. Suppose $F:X \rightarrow Y$ is onto. Prove that for all subsets $B \subseteq Y$, $F(F^{-1}(B)) = B$.

Let $X = \{a, b, c, d, e\}$ and $Y = \{s, t, u, v, w\}$. In each of 42 and 43 a one-to-one correspondence $F: X \rightarrow Y$ is defined by an arrow diagram. In each case draw an arrow diagram for F^{-1} .

42.



43.



In 44–55 indicate which of the functions in the referenced exercise are one-to-one correspondences. For each function that is a one-to-one correspondence, find the inverse function.

44. Exercise 10a 45. Exercise 10b
 46. Exercise 11a 47. Exercise 11b
 48. Exercise 12a 49. Exercise 12b

50. Exercise 21 51. Exercise 22

52. Exercise 15 with the co-domain taken to be the set of all real numbers not equal to 1.

H 53. Exercise 16 with the co-domain taken to be the set of all real numbers.

54. Exercise 17 with the co-domain taken to be the set of all real numbers not equal to 3.

55. Exercise 18 with the co-domain taken to be the set of all real numbers not equal to 1.

56. In Example 7.2.8 a one-to-one correspondence was defined from the power set of $\{a, b\}$ to the set of all strings of 0's and 1's that have length 2. Thus the elements of these two sets can be matched up exactly, and so the two sets have the same number of elements.

- Let $X = \{x_1, x_2, \dots, x_n\}$ be a set with n elements. Use Example 7.2.8 as a model to define a one-to-one correspondence from $\mathcal{P}(X)$, the set of all subsets of X , to the set of all strings of 0's and 1's that have length n .
- Use the one-to-one correspondence of part (a) to deduce that a set with n elements has 2^n subsets. (This provides an alternative proof of Theorem 6.3.1.)

H 57. Write a computer algorithm to check whether a function from one finite set to another is one-to-one. Assume the existence of an independent algorithm to compute values of the function.

H 58. Write a computer algorithm to check whether a function from one finite set to another is onto. Assume the existence of an independent algorithm to compute values of the function.

Answers for Test Yourself

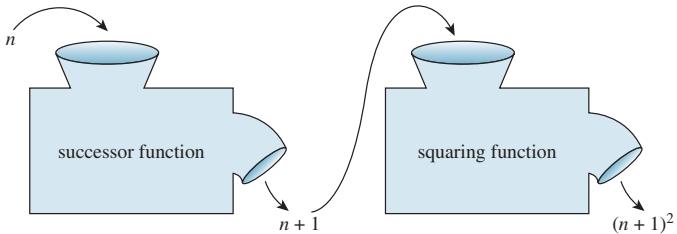
- for all x_1 and x_2 in X , if $F(x_1) = F(x_2)$ then $x_1 = x_2$
- there exist elements x_1 and x_2 in X such that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$
- for all y in Y , there exists at least one element x in X such that $f(x) = y$
- there exists an element y in Y such that for all elements x in X , $f(x) \neq y$
- logically equivalent ways of expressing what it means for a function H to be one-to-one (The second is the contrapositive of the first.)
- x_1 and x_2 are any [particular but arbitrarily chosen] elements in X with the property that $F(x_1) = F(x_2)$; $x_1 = x_2$
- y is any [particular but arbitrarily chosen] element in Y ; there exists at least one element x in X such that $F(x) = y$
- show that there are concrete elements x_1 and x_2 in X with the property that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$
- show that there is a concrete element y in Y with the property that $F(x) \neq y$ for any element x in X
- function from X to Y ; both one-to-one and onto
- the unique element x in X such that $F(x) = y$ (in other words, $F^{-1}(y)$ is the unique preimage of y in X)

7.3 Composition of Functions

It is no paradox to say that in our most theoretical moods we may be nearest to our most practical applications. — Alfred North Whitehead

Consider two functions, the successor function and the squaring function, defined from \mathbf{Z} (the set of integers) to \mathbf{Z} , and imagine that each is represented by a machine. If the two machines are hooked up so that the output from the successor function is used as input

to the squaring function, then they work together to operate as one larger machine. In this larger machine, an integer n is first increased by 1 to obtain $n + 1$; then the quantity $n + 1$ is squared to obtain $(n + 1)^2$. This is illustrated in the following drawing.



Combining functions in this way is called *composing* them; the resulting function is called the *composition* of the two functions. Note that the composition can be formed only if the output of the first function is acceptable input to the second function. That is, the range of the first function must be contained in the domain of the second function.

• Definition

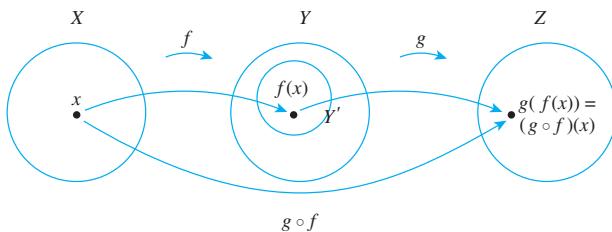
Note We put the f first when we say “the composition of f and g ” because an element x is acted upon first by f and then by g .

Let $f: X \rightarrow Y'$ and $g: Y \rightarrow Z$ be functions with the property that the range of f is a subset of the domain of g . Define a new function $g \circ f: X \rightarrow Z$ as follows:

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X,$$

where $g \circ f$ is read “ g circle f ” and $g(f(x))$ is read “ g of f of x .” The function $g \circ f$ is called the **composition of f and g** .

This definition is shown schematically below.



Example 7.3.1 Composition of Functions Defined by Formulas

Let $f: \mathbf{Z} \rightarrow \mathbf{Z}$ be the successor function and let $g: \mathbf{Z} \rightarrow \mathbf{Z}$ be the squaring function. Then $f(n) = n + 1$ for all $n \in \mathbf{Z}$ and $g(n) = n^2$ for all $n \in \mathbf{Z}$.



Caution! Be careful not to confuse $g \circ f$ and $g(f(x))$: $g \circ f$ is the name of the function whereas $g(f(x))$ is the value of the function at x .

- Find the compositions $g \circ f$ and $f \circ g$.

- Is $g \circ f = f \circ g$? Explain.

Solution

- The functions $g \circ f$ and $f \circ g$ are defined as follows:

$$(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2 \quad \text{for all } n \in \mathbf{Z},$$

and

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1 \quad \text{for all } n \in \mathbf{Z}.$$

- b. Two functions from one set to another are equal if, and only if, they always take the same values. In this case,

$$(g \circ f)(1) = (1 + 1)^2 = 4, \text{ whereas } (f \circ g)(1) = 1^2 + 1 = 2.$$

Thus the two functions $g \circ f$ and $f \circ g$ are not equal:

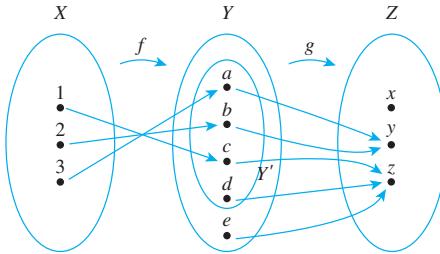
$$g \circ f \neq f \circ g.$$

■

Example 7.3.1 illustrates the important fact that composition of functions is not a commutative operation: *For general functions F and G , $F \circ G$ need not necessarily equal $G \circ F$* (although the two *may* be equal).

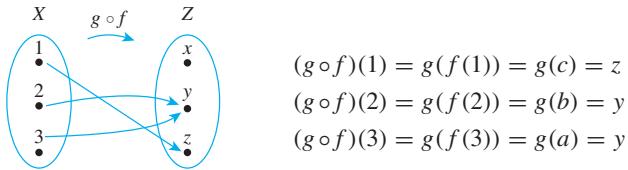
Example 7.3.2 Composition of Functions Defined on Finite Sets

Let $X = \{1, 2, 3\}$, $Y' = \{a, b, c, d\}$, $Y = \{a, b, c, d, e\}$, and $Z = \{x, y, z\}$. Define functions $f: X \rightarrow Y'$ and $g: Y \rightarrow Z$ by the arrow diagrams below.



Draw the arrow diagram for $g \circ f$. What is the range of $g \circ f$?

Solution To find the arrow diagram for $g \circ f$, just trace the arrows all the way across from X to Z through Y . The result is shown below.



The range of $g \circ f$ is $\{y, z\}$.

■

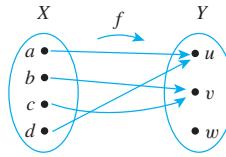
Recall that the identity function on a set X , I_X , is the function from X to X defined by the formula

$$I_X(x) = x \quad \text{for all } x \in X.$$

That is, the identity function on X sends each element of X to itself. What happens when an identity function is composed with another function?

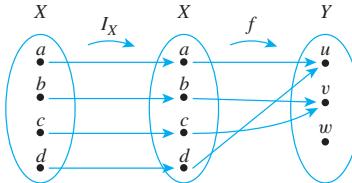
Example 7.3.3 Composition with the Identity Function

Let $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$, and suppose $f: X \rightarrow Y$ is given by the arrow diagram shown on the next page.



Find $f \circ I_X$ and $I_Y \circ f$.

Solution The values of $f \circ I_X$ are obtained by tracing through the arrow diagram shown below.



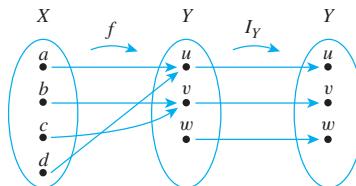
$$\begin{aligned}(f \circ I_X)(a) &= f(I_X(a)) = f(a) = u \\ (f \circ I_X)(b) &= f(I_X(b)) = f(b) = v \\ (f \circ I_X)(c) &= f(I_X(c)) = f(c) = v \\ (f \circ I_X)(d) &= f(I_X(d)) = f(d) = u\end{aligned}$$

Note that for all elements x in X ,

$$(f \circ I_X)(x) = f(x).$$

By definition of equality of functions, this means that $f \circ I_X = f$.

Similarly, the equality $I_Y \circ f = f$ can be verified by tracing through the arrow diagram below for each x in X and noting that in each case, $(I_Y \circ f)(x) = f(x)$.



■

More generally, the composition of any function with an identity function equals the function.

Theorem 7.3.1 Composition with an Identity Function

If f is a function from a set X to a set Y , and I_X is the identity function on X , and I_Y is the identity function on Y , then

$$(a) \quad f \circ I_X = f \quad \text{and} \quad (b) \quad I_Y \circ f = f.$$

Proof:

Part (a): Suppose f is a function from a set X to a set Y and I_X is the identity function on X . Then, for all x in X ,

$$(f \circ I_X)(x) = f(I_X(x)) = f(x).$$

Hence, by definition of equality of functions, $f \circ I_X = f$, as was to be shown.

Part (b): This is exercise 13 at the end of this section.

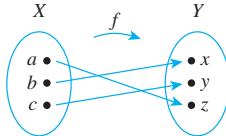
Now let f be a function from a set X to a set Y , and suppose f has an inverse function f^{-1} . Recall that f^{-1} is the function from Y to X with the property that

$$f^{-1}(y) = x \Leftrightarrow f(x) = y.$$

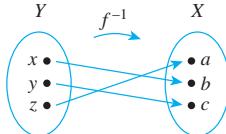
What happens when f is composed with f^{-1} ? Or when f^{-1} is composed with f ?

Example 7.3.4 Composing a Function with Its Inverse

Let $X = \{a, b, c\}$ and $Y = \{x, y, z\}$. Define $f: X \rightarrow Y$ by the following arrow diagram.



Then f is one-to-one and onto. Thus f^{-1} exists and is found by tracing the arrows backwards, as shown below.



Now $f^{-1} \circ f$ is found by following the arrows from X to Y by f and back to X by f^{-1} . If you do this, you will see that

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a$$

$$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b$$

and $(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c$.

Thus the composition of f and f^{-1} sends each element to itself. So by definition of the identity function,

$$f^{-1} \circ f = I_X.$$

In a similar way, you can see that

$$f \circ f^{-1} = I_Y.$$

■

More generally, the composition of any function with its inverse (if it has one) is an identity function. Intuitively, the function sends an element in its domain to an element in its co-domain and the inverse function sends it back again, so the composition of the two sends each element to itself. This reasoning is formalized in Theorem 7.3.2.

Theorem 7.3.2 Composition of a Function with Its Inverse

If $f: X \rightarrow Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \rightarrow X$, then

$$(a) f^{-1} \circ f = I_X \quad \text{and} \quad (b) f \circ f^{-1} = I_Y.$$

Proof:

Part (a): Suppose $f: X \rightarrow Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \rightarrow X$. [To show that $f^{-1} \circ f = I_X$, we must show that for all $x \in X$, $(f^{-1} \circ f)(x) = x$.] Let x be any element in X . Then

$$(f^{-1} \circ f)(x) = f^{-1}(f(x))$$

by definition of composition of functions. Now the inverse function f^{-1} satisfies the condition

$$f^{-1}(b) = a \Leftrightarrow f(a) = b \quad \text{for all } a \in X \text{ and } b \in Y. \quad 7.3.1$$

Let

$$x' = f^{-1}(f(x)). \quad 7.3.2$$

Apply property (7.3.1) with x' playing the role of a and $f(x)$ playing the role of b . Then

$$f(x') = f(x).$$

But since f is one-to-one, this implies that $x' = x$. Substituting x for x' in equation (7.3.2) gives

$$x = f^{-1}(f(x)).$$

Then by definition of composition of functions,

$$(f^{-1} \circ f)(x) = x,$$

as was to be shown.

Part (b): This is exercise 14 at the end of this section.

Composition of One-to-One Functions

The composition of functions interacts in interesting ways with the properties of being one-to-one and onto. What happens, for instance, when two one-to-one functions are composed? Must their composition be one-to-one? For example, let $X = \{a, b, c\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3, 4, 5\}$, and define one-to-one functions $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ as shown in the arrow diagrams of Figure 7.3.1.

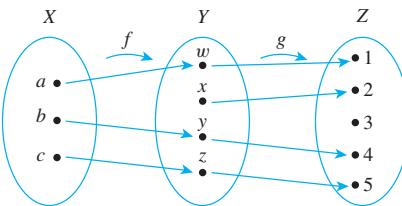


Figure 7.3.1

Then $g \circ f$ is the function with the arrow diagram shown in Figure 7.3.2.

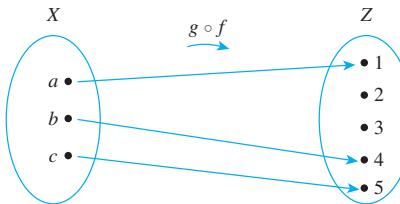


Figure 7.3.2

From the diagram it is clear that for these particular functions, the composition is one-to-one. This result is no accident. It turns out that the compositions of two one-to-one functions is always one-to-one.

Theorem 7.3.3

If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.

By the method of direct proof, the proof of Theorem 7.3.3 has the following starting point and conclusion to be shown.

Starting Point: Suppose f is a one-to-one function from X to Y and g is a one-to-one function from Y to Z .

To Show: $g \circ f$ is a one-to-one function from X to Z .

The conclusion to be shown says that a certain function is one-to-one. How do you show that? The crucial step is to realize that if you substitute $g \circ f$ into the definition of one-to-one, you see that

$$g \circ f \text{ is one-to-one} \Leftrightarrow \forall x_1, x_2 \in X, \text{ if } (g \circ f)(x_1) = (g \circ f)(x_2) \text{ then } x_1 = x_2.$$

By the method of direct proof, then, to show $g \circ f$ is one-to-one, you

suppose x_1 and x_2 are elements of X such that $(g \circ f)(x_1) = (g \circ f)(x_2)$,

and you

show that $x_1 = x_2$.

Now the heart of the proof begins. To show that $x_1 = x_2$, you work forward from the supposition that $(g \circ f)(x_1) = (g \circ f)(x_2)$, using the fact that f and g are both one-to-one. By definition of composition,

$$(g \circ f)(x_1) = g(f(x_1)) \quad \text{and} \quad (g \circ f)(x_2) = g(f(x_2)).$$

Since the left-hand sides of the equations are equal, so are the right-hand sides. Thus

$$g(f(x_1)) = g(f(x_2)).$$

Now just stare at the above equation for a moment. It says that

$$g(\text{something}) = g(\text{something else}).$$

Because g is a one-to-one function, any time g of one thing equals g of another thing, those two things are equal. Hence

$$f(x_1) = f(x_2).$$

But f is also a one-to-one function. Any time f of one thing equals f of another thing, those two things are equal. Therefore,

$$x_1 = x_2.$$

This is what was to be shown!

This discussion is summarized in the following formal proof.

Proof of Theorem 7.3.3:

Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both one-to-one functions. [We must show that $g \circ f$ is one-to-one.] Suppose x_1 and x_2 are elements of X such that

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

[We must show that $x_1 = x_2$.] By definition of composition of functions,

$$g(f(x_1)) = g(f(x_2)).$$

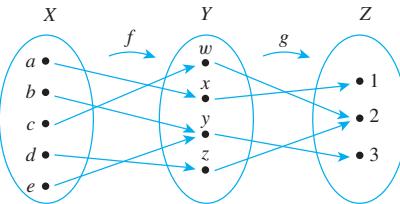
Since g is one-to-one, $f(x_1) = f(x_2)$.

And since f is one-to-one, $x_1 = x_2$.

[This is what was to be shown.] Hence $g \circ f$ is one-to-one.

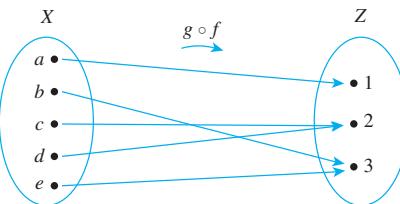
Composition of Onto Functions

Now consider what happens when two onto functions are composed. For example, let $X = \{a, b, c, d, e\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3\}$. Define onto functions f and g by the following arrow diagrams.



Then $g \circ f$ is the function with the arrow diagram shown below.

It is clear from the diagram that $g \circ f$ is onto.



It turns out that the composition of any two onto functions (that can be composed) is onto.

Theorem 7.3.4

If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both onto functions, then $g \circ f$ is onto.

A direct proof of Theorem 7.3.4 has the following starting point and conclusion to be shown:

Starting Point: Suppose f is an onto function from X to Y , and g is an onto function from Y to Z .

To Show: $g \circ f$ is an onto function from X to Z .

The conclusion to be shown says that a certain function is onto. How do you show that? The crucial step is to realize that if you substitute $g \circ f$ into the definition of onto, you see that

$g \circ f: X \rightarrow Z$ is onto \Leftrightarrow given any element z of Z , it is possible to find an element x of X such that $(g \circ f)(x) = z$.



Caution! To show that a function is onto, you *must* start with an arbitrary element of the co-domain and deduce that it is the image of some element in the domain.

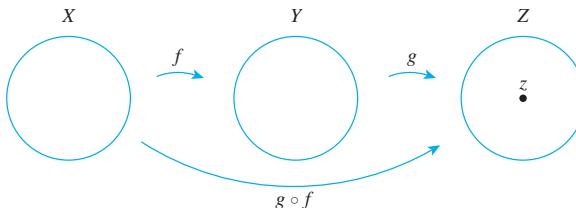
Since this statement is universal, to prove it you

suppose z is a [particular but arbitrarily chosen] element of Z

and **show** that there is an element x in X such that $(g \circ f)(x) = z$.

Hence you must start the proof by supposing you are given a particular but arbitrarily chosen element in Z . Let us call it z . Your job is to find an element x in X such that $(g \circ f)(x) = z$.

To find x , reason from the supposition that z is in Z , using the fact that both g and f are onto. Imagine arrow diagrams for the functions f and g .

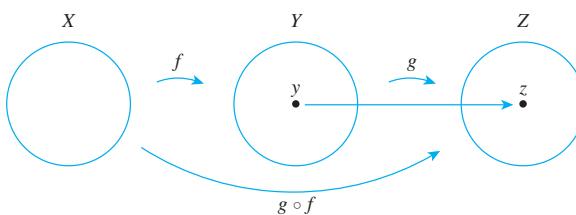


You have a particular element z in Z , and you need to find an element x in X such that when x is sent over to Z by $g \circ f$, its image will be z . Since g is onto, z is at the tip of some arrow coming from Y . That is, there is an element y in Y such that

$$g(y) = z.$$

7.3.3

This means that the arrow diagrams can be drawn as follows:

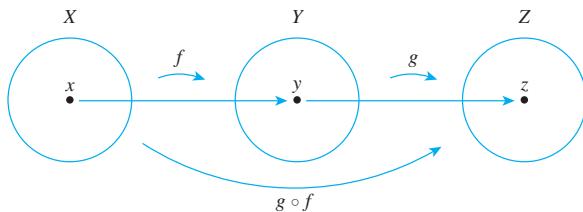


But f also is onto, so every element in Y is at the tip of an arrow coming from X . In particular, y is at the tip of some arrow. That is, there is an element x in X such that

$$f(x) = y.$$

7.3.4

The diagram, therefore, can be drawn as shown below.



Now just substitute equation (7.3.4) into equation (7.3.3) to obtain

$$g(f(x)) = z.$$

But by definition of $g \circ f$,

$$g(f(x)) = (g \circ f)(x).$$

Hence

$$(g \circ f)(x) = z.$$

Thus x is an element of X that is sent by $g \circ f$ to z , and so x is the element you were supposed to find.

This discussion is summarized in the following formal proof.

Proof of Theorem 7.3.4:

Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both onto functions. [We must show that $g \circ f$ is onto.] Let z be a [particular but arbitrarily chosen] element of Z . [We must show the existence of an element x in X such that $(g \circ f)(x) = z$.] Since g is onto, there is an element y in Y such that $g(y) = z$. And since f is onto, there is an element x in X such that $f(x) = y$. Hence there exists an element x in X such that

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

[as was to be shown]. It follows that $g \circ f$ is onto.

Example 7.3.5 An Incorrect “Proof” That a Function Is Onto

To prove that a composition of onto functions is onto, a student wrote,

“Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both onto. Then

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y (*)$$

and

$$\forall z \in Z, \exists y \in Y \text{ such that } f(y) = z.$$

So

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

and thus $g \circ f$ is onto.”

Explain the mistakes in this “proof.”

Solution To show that $g \circ f$ is onto, you must be able to meet the following challenge: If someone gives you an element z in Z (over which you have no control), you must be able to explain how to find an element x in X such that $(g \circ f)(x) = z$. Thus a proof that $g \circ f$ is onto must start with the assumption that you have been given a particular but arbitrarily chosen element of Z . This proof does not do that.

Moreover, note that statement (*) simply asserts that f is onto. An informal version of (*) is the following: Given any element in the co-domain of f , there is an element in the domain of f that is sent by f to the given element. Use of the symbols x and y to denote these elements is arbitrary. Any other two symbols could equally well have been used. Thus, if we replace the x and y in (*) by u and v , we obtain a logically equivalent statement, and the “proof” becomes the following:

“Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both onto. Then

$$\forall v \in Y, \exists u \in X \text{ such that } f(u) = v$$

and

$$\forall z \in Z, \exists y \in Y \text{ such that } f(y) = z.$$

So (??!)

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

and thus $g \circ f$ is onto.”

From this logically equivalent version of the “proof,” you can see that the statements leading up to the word *So* do not provide a rationale for the statement that follows it. The original reason for writing *So* was based on a misinterpretation of the meaning of the notation. ■

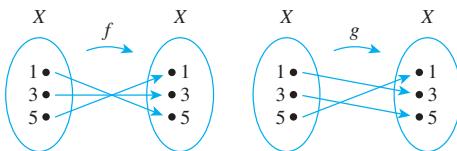
Test Yourself

- If f is a function from X to Y' , g is a function from Y to Z , and $Y' \subseteq Y$, then $g \circ f$ is a function from to , and $(g \circ f)(x) = \underline{\hspace{2cm}}$ for all x in X .
- If f is a function from X to Y and I_x and I_y are the identity functions from X to X and Y to Y , respectively, then $f \circ I_x = \underline{\hspace{2cm}}$ and $I_y \circ f = \underline{\hspace{2cm}}$.
- If f is a one-to-one correspondence from X to Y , then $f^{-1} \circ f = \underline{\hspace{2cm}}$ and $f \circ f^{-1} = \underline{\hspace{2cm}}$.
- If f is a one-to-one function from X to Y and g is a one-to-one function from Y to Z , you prove that $g \circ f$ is one-to-one by supposing that and then showing that .
- If f is an onto function from X to Y and g is an onto function from Y to Z , you prove that $g \circ f$ is onto by supposing that and then showing that .

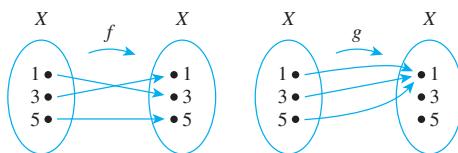
Exercise Set 7.3

In each of 1 and 2, functions f and g are defined by arrow diagrams. Find $G \circ F$ and $F \circ g$ and determine whether $G \circ F$ equals $F \circ g$.

1.



2.



In 3 and 4, functions F and G are defined by formulas. Find $G \circ F$ and $F \circ G$ and determine whether $G \circ F$ equals $F \circ G$.

$$3. F(x) = x^3 \text{ and } G(x) = x - 1, \text{ for all real numbers } x.$$

$$4. F(x) = x^5 \text{ and } G(x) = x^{1/5} \text{ for all real numbers } x.$$

5. Define $f: \mathbf{R} \rightarrow \mathbf{R}$ by the rule $f(x) = -x$ for all real numbers x . Find $(f \circ f)(x)$.
6. Define $F: \mathbf{Z} \rightarrow \mathbf{Z}$ and $G: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules $F(a) = 7a$ and $G(a) = a \bmod 5$ for all integers a . Find $(G \circ F)(0)$, $(G \circ F)(1)$, $(G \circ F)(2)$, $(G \circ F)(3)$, and $(G \circ F)(4)$.
7. Define $H: \mathbf{Z} \rightarrow \mathbf{Z}$ and $K: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules $H(a) = 6a$ and $K(a) = a \bmod 4$ for all integers a . Find $(K \circ H)(0)$, $(K \circ H)(1)$, $(K \circ H)(2)$, and $(K \circ H)(3)$.
8. Define $L: \mathbf{Z} \rightarrow \mathbf{Z}$ and $M: \mathbf{Z} \rightarrow \mathbf{Z}$ by the rules $L(a) = a^2$ and $M(a) = a \bmod 5$ for all integers a .
- Find $(L \circ M)(12)$, $(M \circ L)(12)$, $(L \circ M)(9)$, and $(M \circ L)(9)$.
 - Is $L \circ M = M \circ L$?

The functions of each pair in 9–11 are inverse to each other. For each pair, check that both compositions give the identity function.

9. $F: \mathbf{R} \rightarrow \mathbf{R}$ and $F^{-1}: \mathbf{R} \rightarrow \mathbf{R}$ are defined by

$$F(x) = 3x + 2 \quad \text{and} \quad F^{-1}(y) = \frac{y - 2}{3},$$

for all $y \in \mathbf{R}$.

10. $G: \mathbf{R}^+ \rightarrow \mathbf{R}^+$ and $G^{-1}: \mathbf{R}^+ \rightarrow \mathbf{R}^+$ are defined by

$$G(x) = x^2 \quad \text{and} \quad G^{-1}(x) = \sqrt{x},$$

for all $x \in \mathbf{R}^+$.

11. H and H^{-1} are both defined from $\mathbf{R} - \{1\}$ to $\mathbf{R} - \{1\}$ by the formula

$$H(x) = H^{-1}(x) = \frac{x + 1}{x - 1}, \quad \text{for all } x \in \mathbf{R} - \{1\}.$$

12. Explain how it follows from the definition of logarithm that
- $\log_b(b^x) = x$, for all real numbers x .
 - $b^{\log_b x} = x$, for all positive real numbers x .

- H 13.** Prove Theorem 7.3.1(b): If f is any function from a set X to a set Y , then $I_Y \circ f = f$, where I_Y is the identity function on Y .

14. Prove Theorem 7.3.2(b): If $f: X \rightarrow Y$ is a one-to-one and onto function with inverse function $f^{-1}: Y \rightarrow X$, then $f \circ f^{-1} = I_Y$, where I_Y is the identity function on Y .

15. Suppose Y and Z are sets and $g: Y \rightarrow Z$ is a one-to-one function. This means that if g takes the same value on any two elements of Y , then those elements are equal. Thus, for example, if a and b are elements of Y and $g(a) = g(b)$, then it can be inferred that $a = b$. What can be inferred in the following situations?

- s_k and s_m are elements of Y and $g(s_k) = g(s_m)$.
- $z/2$ and $t/2$ are elements of Y and $g(z/2) = g(t/2)$.
- $f(x_1)$ and $f(x_2)$ are elements of Y and $g(f(x_1)) = g(f(x_2))$.

16. If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions and $g \circ f$ is one-to-one, must g be one-to-one? Prove or give a counterexample.

17. If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions and $g \circ f$ is onto, must f be onto? Prove or give a counterexample.

- H 18.** If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions and $g \circ f$ is one-to-one, must f be one-to-one? Prove or give a counterexample.

- H 19.** If $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions and $g \circ f$ is onto, must g be onto? Prove or give a counterexample.

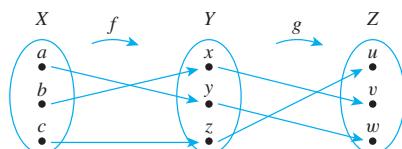
20. Let $f: W \rightarrow X$, $g: X \rightarrow Y$, and $h: Y \rightarrow Z$ be functions. Must $h \circ (g \circ f) = (h \circ g) \circ f$? Prove or give a counterexample.

21. True or False? Given any set X and given any functions $f: X \rightarrow X$, $g: X \rightarrow X$, and $h: X \rightarrow X$, if h is one-to-one and $h \circ f = h \circ g$, then $f = g$. Justify your answer.

22. True or False? Given any set X and given any functions $f: X \rightarrow X$, $g: X \rightarrow X$, and $h: X \rightarrow X$, if h is one-to-one and $f \circ h = g \circ h$, then $f = g$. Justify your answer.

In 23 and 24 find $g \circ f$, $(g \circ f)^{-1}$, g^{-1} , f^{-1} , and $f^{-1} \circ g^{-1}$, and state how $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are related.

23. Let $X = \{a, c, b\}$, $Y = \{x, y, z\}$, and $Z = \{u, v, w\}$. Define $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ by the arrow diagrams below.



24. Define $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ by the formulas

$$f(x) = x + 3 \quad \text{and} \quad g(x) = -x \quad \text{for all } x \in \mathbf{R}.$$

25. Prove or give a counterexample: If $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are functions such that $g \circ f = I_X$ and $f \circ g = I_Y$, then f and g are both one-to-one and onto and $g = f^{-1}$.

- H 26.** Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are both one-to-one and onto. Prove that $(g \circ f)^{-1}$ exists and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

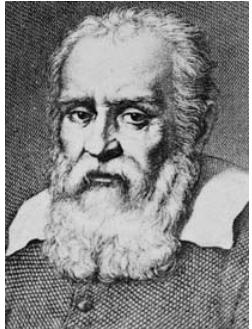
27. Let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$. Is the following property true or false? For all subsets C in Z , $(g \circ f)^{-1}(C) = (f^{-1}(g^{-1}(C)))$. Justify your answer.

Answers for Test Yourself

1. X ; Z ; $g(f(x))$ 2. f ; f 3. I_X ; I_Y 4. x_1 and x_2 are any [particular but arbitrarily chosen] elements in X with the property that $(g \circ f)(x_1) = (g \circ f)(x_2)$; $x_1 = x_2$ 5. z is any [particular but arbitrarily chosen] element in Z ; there exists at least one element x in X such that $(g \circ f)(x) = z$

7.4 Cardinality with Applications to Computability

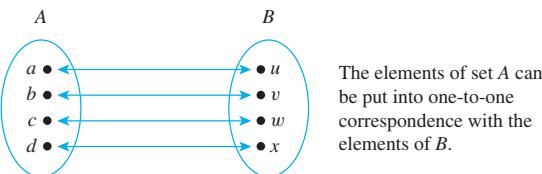
There are as many squares as there are numbers because they are just as numerous as their roots. —Galileo Galilei, 1632



Galileo Galilei
(1564–1642)

istockphoto.com/Steven Wynn

Historically, the term *cardinal number* was introduced to describe the size of a set (“This set has *eight* elements”) as distinguished from an *ordinal number* that refers to the order of an element in a sequence (“This is the *eighth* element in the row”). The definition of cardinal number derives from the primitive technique of representing numbers by fingers or tally marks. Small children, when asked how old they are, will often answer by holding up a certain number of fingers, each finger being paired with a year of their life. As was discussed in Section 7.2, a pairing of the elements of two sets is called a one-to-one correspondence. We say that two finite sets whose elements can be paired by a one-to-one correspondence have the *same size*. This is illustrated by the following diagram.



Now a **finite set** is one that has no elements at all or that can be put into one-to-one correspondence with a set of the form $\{1, 2, \dots, n\}$ for some positive integer n . By contrast, an **infinite set** is a nonempty set that cannot be put into one-to-one correspondence with $\{1, 2, \dots, n\}$ for any positive integer n . Suppose that, as suggested by the quote from Galileo at the beginning of this section, we extend the concept of size to infinite sets by saying that one infinite set has the same size as another if, and only if, the first set can be put into one-to-one correspondence with the second. What consequences follow from such a definition? Do all infinite sets have the same size, or are some infinite sets larger than others? These are the questions we address in this section. The answers are sometimes surprising and have the interesting consequence that there are functions defined on the set of integers whose values cannot be computed on a computer.

• Definition

Let A and B be any sets. **A has the same cardinality as B** if, and only if, there is a one-to-one correspondence from A to B . In other words, A has the same cardinality as B if, and only if, there is a function f from A to B that is one-to-one and onto.

The following theorem gives some basic properties of cardinality, most of which follow from statements proved earlier about one-to-one and onto functions.

Theorem 7.4.1 Properties of Cardinality

For all sets A , B , and C :

- Reflexive property of cardinality:** A has the same cardinality as A .
- Symmetric property of cardinality:** If A has the same cardinality as B , then B has the same cardinality as A .
- Transitive property of cardinality:** If A has the same cardinality as B and B has the same cardinality as C , then A has the same cardinality as C .

Proof:

Part (a), Reflexivity: Suppose A is any set. [To show that A has the same cardinality as A , we must show there is a one-to-one correspondence from A to A .] Consider the identity function I_A from A to A . This function is one-to-one because if x_1 and x_2 are any elements in A with $I_A(x_1) = I_A(x_2)$, then, by definition of I_A , $x_1 = x_2$. The identity function is also onto because if y is any element of A , then $y = I_A(y)$ by definition of I_A . Hence I_A is a one-to-one correspondence from A to A . [So there exists a one-to-one correspondence from A to A , as was to be shown.]

Part (b), Symmetry: Suppose A and B are any sets and A has the same cardinality as B . [We must show that B has the same cardinality as A .] Since A has the same cardinality as B , there is a function f from A to B that is one-to-one and onto. But then, by Theorems 7.2.2 and 7.2.3, there is a function f^{-1} from B to A that is also one-to-one and onto. Hence B has the same cardinality as A [as was to be shown].

Part (c), Transitivity: Suppose A , B , and C are any sets and A has the same cardinality as B and B has the same cardinality as C . [We must show that A has the same cardinality as C .] Since A has the same cardinality as B , there is a function f from A to B that is one-to-one and onto, and since B has the same cardinality as C , there is a function g from B to C that is one-to-one and onto. But then, by Theorems 7.3.3 and 7.3.4, $g \circ f$ is a function from A to C that is one-to-one and onto. Hence A has the same cardinality as C [as was to be shown].

Note that Theorem 7.4.1(b) makes it possible to say simply that two sets have the same cardinality instead of always having to say that one set has the same cardinality as another. That is, the following definition can be made.

• **Definition**

A and B have the same cardinality if, and only if, A has the same cardinality as B or B has the same cardinality as A .

The following example illustrates a very important property of infinite sets—namely, that an infinite set can have the same cardinality as a proper subset of itself. This property is sometimes taken as the definition of infinite set. The example shows that even though it may seem reasonable to say that there are twice as many integers as there are even integers, the elements of the two sets can be matched up exactly, and so, according to the definition, the two sets have the same cardinality.

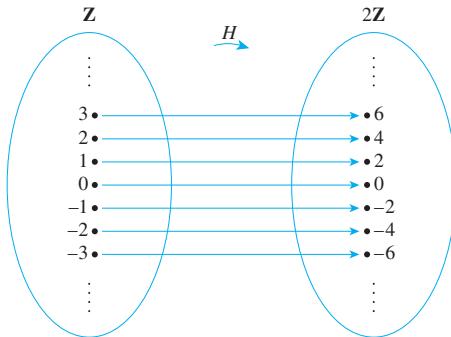
Example 7.4.1 An Infinite Set and a Proper Subset Can Have the Same Cardinality

Let $2\mathbf{Z}$ be the set of all even integers. Prove that $2\mathbf{Z}$ and \mathbf{Z} have the same cardinality.

Solution Consider the function H from \mathbf{Z} to $2\mathbf{Z}$ defined as follows:

$$H(n) = 2n \quad \text{for all } n \in \mathbf{Z}.$$

A (partial) arrow diagram for H is shown below.



To show that H is one-to-one, suppose $H(n_1) = H(n_2)$ for some integers n_1 and n_2 . Then $2n_1 = 2n_2$ by definition of H , and dividing both sides by 2 gives $n_1 = n_2$. Hence H is one-to-one.

To show that H is onto, suppose m is any element of $2\mathbb{Z}$. Then m is an even integer, and so $m = 2k$ for some integer k . It follows that $H(k) = 2k = m$. Thus there exists k in \mathbb{Z} with $H(k) = m$, and hence H is onto.

Therefore, by definition of cardinality, \mathbb{Z} and $2\mathbb{Z}$ have the same cardinality. ■

Note So there are “as many” even integers as there are integers!

In Section 9.4 we will show that a function from one finite set to another set of the same size is one-to-one if, and only if, it is onto. This result does not hold for infinite sets. Although it is true that for two infinite sets to have the same cardinality there must exist a function from one to the other that is both one-to-one and onto, it is also always the case that:

If A and B are infinite sets with the same cardinality, then there exist functions from A to B that are one-to-one but not onto and functions from A to B that are onto but not one-to-one.

For instance, since the function H in Example 7.4.1 is one-to-one and onto, \mathbb{Z} and $2\mathbb{Z}$ have the same cardinality. But the “inclusion function” I from $2\mathbb{Z}$ to \mathbb{Z} , given by $I(n) = n$ for all even integers n , is one-to-one but not onto. And the function J from \mathbb{Z} to $2\mathbb{Z}$ defined by $J(n) = 2\lfloor n/2 \rfloor$, for all integers n , is onto but not one-to-one. (See exercise 6 at the end of this section.)

Countable Sets

The set \mathbb{Z}^+ of counting numbers $\{1, 2, 3, 4, \dots\}$ is, in a sense, the most basic of all infinite sets. A set A having the same cardinality as this set is called *countably infinite*. The reason is that the one-to-one correspondence between the two sets can be used to “count” the elements of A : If F is a one-to-one and onto function from \mathbb{Z}^+ to A , then $F(1)$ can be designated as the first element of A , $F(2)$ as the second element of A , $F(3)$ as the third element of A , and so forth. This is illustrated graphically in Figure 7.4.1 on the next page. Because F is one-to-one, no element is ever counted twice, and because it is onto, every element of A is counted eventually.

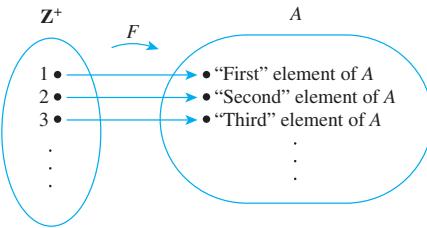


Figure 7.4.1 “Counting” a Countably Infinite Set

• **Definition**

A set is called **countably infinite** if, and only if, it has the same cardinality as the set of positive integers \mathbf{Z}^+ . A set is called **countable** if, and only if, it is finite or countably infinite. A set that is not countable is called **uncountable**.

Example 7.4.2 Countability of \mathbf{Z} , the Set of All Integers

Show that the set \mathbf{Z} of all integers is countable.

Solution The set \mathbf{Z} of all integers is certainly not finite, so if it is countable, it must be because it is countably infinite. To show that \mathbf{Z} is countably infinite, find a function from the positive integers \mathbf{Z}^+ to \mathbf{Z} that is one-to-one and onto. Looked at in one light, this contradicts common sense; judging from the diagram below, there appear to be more than twice as many integers as there are positive integers.



But you were alerted that results in this section might be surprising. Try to think of a way to “count” the set of all integers anyway.

The trick is to start in the middle and work outward systematically. Let the first integer be 0, the second 1, the third -1 , the fourth 2, the fifth -2 , and so forth as shown in Figure 7.4.2, starting at 0 and swinging outward in back-and-forth arcs from positive to negative integers and back again, picking up one additional integer at each swing.

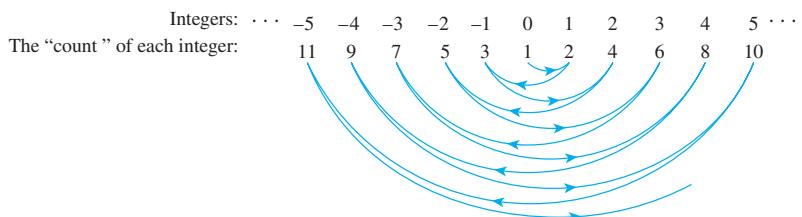


Figure 7.4.2 “Counting” the Set of All Integers

It is clear from the diagram that no integer is counted twice (so the function is one-to-one) and every integer is counted eventually (so the function is onto). Consequently, this diagram defines a function from \mathbf{Z}^+ to \mathbf{Z} that is one-to-one and onto. Even though in one sense there seem to be more integers than positive integers, the elements of the two sets

can be paired up one for one. It follows by definition of cardinality that \mathbf{Z}^+ has the same cardinality as \mathbf{Z} . Thus \mathbf{Z} is countably infinite and hence countable.

The diagrammatic description of the previous function is acceptable as given. You can check, however, that the function can also be described by the explicit formula

$$F(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even positive integer} \\ -\frac{n-1}{2} & \text{if } n \text{ is an odd positive integer.} \end{cases}$$

■

Example 7.4.3 Countability of $2\mathbf{Z}$, the Set of All Even Integers

Show that the set $2\mathbf{Z}$ of all even integers is countable.

Solution Example 7.4.2 showed that \mathbf{Z}^+ has the same cardinality as \mathbf{Z} , and Example 7.4.1 showed that \mathbf{Z} has the same cardinality as $2\mathbf{Z}$. Thus, by the transitive property of cardinality, \mathbf{Z}^+ has the same cardinality as $2\mathbf{Z}$. It follows by definition of countably infinite that $2\mathbf{Z}$ is countably infinite and hence countable. ■

The Search for Larger Infinities: The Cantor Diagonalization Process

Every infinite set we have discussed so far has been countably infinite. Do any larger infinities exist? Are there uncountable sets? Here is one candidate.

Imagine the number line as shown below.



As noted in Section 1.2, the integers are spread along the number line at discrete intervals. The rational numbers, on the other hand, are *dense*: Between any two rational numbers, no matter how close, lies another rational number (the average of the two numbers, for instance; see exercise 17). This suggests the conjecture that the infinity of the set of rational numbers is larger than the infinity of the set of integers.

Amazingly, this conjecture is false. Despite the fact that the rational numbers are crowded onto the number line whereas the integers are quite separated, the set of all rational numbers can be put into one-to-one correspondence with the set of integers. The next example gives part of a proof of this fact. It shows that the set of all positive rational numbers can be put into one-to-one correspondence with the set of all positive integers. In exercise 16 at the end of this section you are asked to use this result, together with a technique similar to that of Example 7.4.2, to show that the set of *all* rational numbers is countable.

Example 7.4.4 The Set of All Positive Rational Numbers Is Countable

Show that the set \mathbf{Q}^+ of all positive rational numbers is countable.

Solution Display the elements of the set \mathbf{Q}^+ of positive rational numbers in a grid as shown in Figure 7.4.3 on the next page.

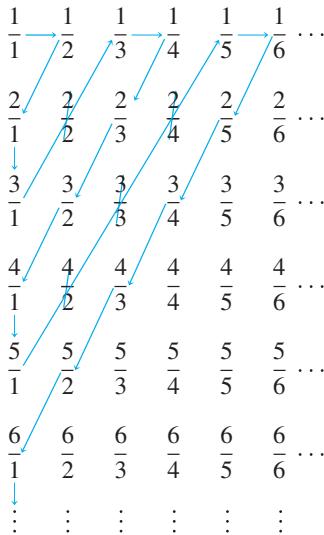


Figure 7.4.3

Define a function F from \mathbf{Z}^+ to \mathbf{Q}^+ by starting to count at $\frac{1}{1}$ and following the arrows as indicated, skipping over any number that has already been counted.

To be specific: Set $F(1) = \frac{1}{1}$, $F(2) = \frac{1}{2}$, $F(3) = \frac{2}{1}$ and $F(4) = \frac{3}{1}$. Then skip $\frac{2}{2}$ since $\frac{2}{2} = \frac{1}{1}$, which was counted first. After that, set $F(5) = \frac{1}{3}$, $F(6) = \frac{1}{4}$, $F(7) = \frac{2}{3}$, $F(8) = \frac{3}{2}$, $F(9) = \frac{4}{1}$, and $F(10) = \frac{5}{1}$. Then skip $\frac{4}{2}$, $\frac{3}{3}$, and $\frac{2}{4}$ (since $\frac{4}{2} = \frac{2}{1}$, $\frac{3}{3} = \frac{1}{1}$, and $\frac{2}{4} = \frac{1}{2}$) and set $F(11) = \frac{1}{5}$. Continue in this way, defining $F(n)$ for each positive integer n .

Note that every positive rational number appears somewhere in the grid, and the counting procedure is set up so that every point in the grid is reached eventually. Thus the function F is onto. Also, skipping numbers that have already been counted ensures that no number is counted twice. Thus F is one-to-one. Consequently, F is a function from \mathbf{Z}^+ to \mathbf{Q}^+ that is one-to-one and onto, and so \mathbf{Q}^+ is countably infinite and hence countable. ■

In 1874 the German mathematician Georg Cantor achieved success in the search for a larger infinity by showing that the set of all real numbers is uncountable. His method of proof was somewhat complicated, however. We give a proof of the uncountability of the set of all real numbers between 0 and 1 using a simpler technique introduced by Cantor in 1891 and now called the **Cantor diagonalization process**. Over the intervening years, this technique and variations on it have been used to establish a number of important results in logic and the theory of computation.

Before stating and proving Cantor's theorem, we note that every real number, which is a measure of location on a number line, can be represented by a decimal expansion of the form

$$a_0.a_1a_2a_3\dots,$$

where a_0 is an integer (positive, negative, or zero) and for each $i \geq 1$, a_i is an integer from 0 through 9.

This way of thinking about numbers was developed over several centuries by mathematicians in the Chinese, Hindu, and Islamic worlds, culminating in the work of Ghiyāth al-Dīn Jamshīd al-Kashi in 1427. In Europe it was first clearly formulated and successfully promoted by the Flemish mathematician Simon Stevin in 1585. We illustrate the concept with an example.



al-Kashi
(1380–1429)



Bettmann/CORBIS

Simon Stevin
(1548–1620)

Consider the point P in Figure 7.4.4. Figure 7.4.4(a) shows P located between 1 and 2. When the interval from 1 to 2 is divided into ten equal subintervals (see Figure 7.4.4(b)) P is seen to lie between 1.6 and 1.7. If the interval from 1.6 to 1.7 is itself divided into ten equal subintervals (see Figure 7.4.4(c)), the P is seen to lie between 1.62 and 1.63 but closer to 1.62 than to 1.63. So the first three digits of the decimal expansion for P are 1.62.

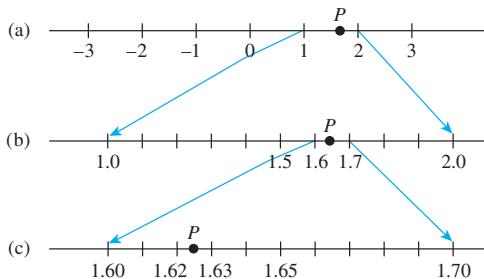


Figure 7.4.4

Assuming that any interval of real numbers, no matter how small, can be divided into ten equal subintervals, the process of obtaining additional digits in the decimal expansion for P can, in theory, be repeated indefinitely. If at any stage P is seen to be a subdivision point, then all further digits in the expansion may be taken to be 0. If not, then the process gives an expansion with an infinite number of digits.

The resulting decimal representation for P is unique except for numbers that end in infinitely repeating 9's or infinitely repeating 0's. For example (see exercise 25 at the end of this section),

$$0.199999\dots = 0.200000\dots$$

Let us agree to express any such decimal in the form that ends in all 0's so that we will have a unique representation for every real number.

Theorem 7.4.2 (Cantor)

The set of all real numbers between 0 and 1 is uncountable.

Proof (by contradiction):

Suppose the set of all real numbers between 0 and 1 is countable. Then the decimal representations of these numbers can be written in a list as follows:

$$\begin{aligned} & 0.a_{11}a_{12}a_{13}\dots a_{1n}\dots \\ & 0.a_{21}a_{22}a_{23}\dots a_{2n}\dots \\ & 0.a_{31}a_{32}a_{33}\dots a_{3n}\dots \\ & \vdots \\ & 0.a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots \\ & \vdots \end{aligned}$$

[We will derive a contradiction by showing that there is a number between 0 and 1 that does not appear on this list.]

For each pair of positive integers i and j , the j th decimal digit of the i th number on the list is a_{ij} . In particular, the first decimal digit of the first number on the list is

a_{11} , the second decimal digit of the second number on the list is a_{22} , and so forth. As an example, suppose the list of real numbers between 0 and 1 starts out as follows:

0.	②	0	1	4	8	8	0	2	...
0.	1	①	6	6	6	0	2	1	...
0.	0	3	③	5	3	3	2	0	...
0.	9	6	7	⑦	6	8	0	9	...
0.	0	0	0	3	①	0	0	2	...
							⋮		

The diagonal elements are circled: a_{11} is 2, a_{22} is 1, a_{33} is 3, a_{44} is 7, a_{55} is 1, and so forth.

Construct a new decimal number $d = 0.d_1d_2d_3 \dots d_n \dots$ as follows:

$$d_n = \begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1 \end{cases}.$$

In the previous example,

- d_1 is 1 because $a_{11} = 2 \neq 1$,
- d_2 is 2 because $a_{22} = 1$,
- d_3 is 1 because $a_{33} = 3 \neq 1$,
- d_4 is 1 because $a_{44} = 7 \neq 1$,
- d_5 is 2 because $a_{55} = 1$,

and so forth. Hence d would equal 0.12112

The crucial observation is that for each integer n , d differs in the n th decimal position from the n th number on the list. But this implies that d is not on the list! In other words, d is a real number between 0 and 1 that is not on the list of all real numbers between 0 and 1. This contradiction shows the falseness of the supposition that the set of all numbers between 0 and 1 is countable. Hence the set of all real numbers between 0 and 1 is uncountable.

Along with demonstrating the existence of an uncountable set, Cantor developed a whole arithmetic theory of infinite sets of various sizes. One of the most basic theorems of the theory states that any subset of a countable set is countable.

Theorem 7.4.3

Any subset of any countable set is countable.

Proof:

Let A be a particular but arbitrarily chosen countable set and let B be any subset of A . [We must show that B is countable.] Either B is finite or it is infinite. If B is finite, then B is countable by definition of countable, and we are done. So suppose B is infinite. Since A is countable, the distinct elements of A can be represented as a sequence

$$a_1, a_2, a_3, \dots$$

Define a function $g: \mathbf{Z}^+ \rightarrow B$ inductively as follows:

continued on page 436

Note If $g(k-1) = a_i$, then $g(k)$ could also be defined by applying the well-ordering principle for the integers to the set $\{n \in \mathbb{Z} \mid n > i \text{ and } a_i \in B\}$.

1. Search sequentially through elements of a_1, a_2, a_3, \dots until an element of B is found. [This must happen eventually since $B \subseteq A$ and $B \neq \emptyset$.] Call that element $g(1)$.
2. For each integer $k \geq 2$, suppose $g(k-1)$ has been defined. Then $g(k-1) = a_i$ for some a_i in $\{a_1, a_2, a_3, \dots\}$. Starting with a_{i+1} , search sequentially through $a_{i+1}, a_{i+2}, a_{i+3}, \dots$ trying to find an element of B . One must be found eventually because B is infinite, and $\{g(1), g(2), \dots, g(k-1)\}$ is a finite set. When an element of B is found, define it to be $g(k)$.

By (1) and (2) above, the function g is defined for each positive integer.

Since the elements of a_1, a_2, a_3, \dots are all distinct, g is one-to-one. Furthermore, the searches for elements of B are sequential: Each picks up where the previous one left off. Thus every element of A is reached during some search. But all the elements of B are located somewhere in the sequence a_1, a_2, a_3, \dots , and so every element of B is eventually found and made the image of some integer. Hence g is onto. These remarks show that g is a one-to-one correspondence from \mathbb{Z}^+ to B . So B is countably infinite and thus countable.

An immediate consequence of Theorem 7.4.3 is the following corollary.

Corollary 7.4.4

Any set with an uncountable subset is uncountable.

Proof:

Consider the following equivalent phrasing of Theorem 7.4.3: For all sets S and for all subsets A of S , if S is countable, then A is countable. The contrapositive of this statement is logically equivalent to it and states: For all sets S and for all subsets A of S , if A is uncountable then S is uncountable. But this is an equivalent phrasing for the corollary. So the corollary is proved.

Corollary 7.4.4 implies that the set of all real numbers is uncountable because the subset of numbers between 0 and 1 is uncountable. In fact, as Example 7.4.5 shows, the set of all real numbers has the same cardinality as the set of all real numbers between 0 and 1! This fact is further explored in exercises 13 and 14 at the end of this section.

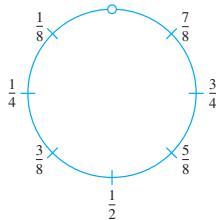
Example 7.4.5 The Cardinality of the Set of All Real Numbers

Show that the set of all real numbers has the same cardinality as the set of real numbers between 0 and 1.

Solution Let S be the open interval of real numbers between 0 and 1:

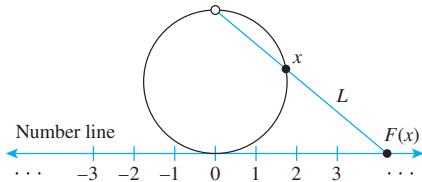
$$S = \{x \in \mathbf{R} \mid 0 < x < 1\}.$$

Imagine picking up S and bending it into a circle as shown below. Since S does not include either endpoint 0 or 1, the top-most point of the circle is omitted from the drawing.



Define a function $F: S \rightarrow \mathbf{R}$ as follows:

Draw a number line and place the interval, S , somewhat enlarged and bent into a circle, tangent to the line above the point 0. This is shown below.



For each point x on the circle representing S , draw a straight line L through the top-most point of the circle and x . Let $F(x)$ be the point of intersection of L and the number line. ($F(x)$) is called the *projection* of x onto the number line.)

It is clear from the geometry of the situation that distinct points on the circle go to distinct points on the number line, so F is one-to-one. In addition, given any point y on the number line, a line can be drawn through y and the top-most point of the circle. This line must intersect the circle at some point x , and, by definition, $y = F(x)$. Thus F is onto. Hence F is a one-to-one correspondence from S to \mathbf{R} , and so S and \mathbf{R} have the same cardinality. ■

You know that every positive integer is a real number, so putting Example 7.4.5 together with Cantor's theorem (Theorem 7.4.2) shows that the infinity of the set of all real numbers is "greater" than the infinity of the set of all positive integers. In exercise 35, you are asked to show that any set and its power set have different cardinalities. Because there is a one-to-one function from any set to its power set (the function that takes each element a to the singleton set $\{a\}$), this implies that the cardinality of any set is "less than" the cardinality of its power set. As a result, you can create an infinite sequence of larger and larger infinities! For example, you could begin with \mathbf{Z} , the set of all integers, and take \mathbf{Z} , $\mathcal{P}(\mathbf{Z})$, $\mathcal{P}(\mathcal{P}(\mathbf{Z}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{Z})))$, and so forth.

Application: Cardinality and Computability

Knowledge of the countability and uncountability of certain sets can be used to answer a question of computability. We begin by showing that a certain set is countable.

Example 7.4.6 Countability of the Set of Computer Programs in a Computer Language

Show that the set of all computer programs in a given computer language is countable.

Solution This result is a consequence of the fact that any computer program in any language can be regarded as a finite string of symbols in the (finite) alphabet of the language.

Given any computer language, let P be the set of all computer programs in the language. Either P is finite or P is infinite. If P is finite, then P is countable and we are done. If P is infinite, set up a binary code to translate the symbols of the alphabet of the language into strings of 0's and 1's. (For instance, either the seven-bit American Standard Code for Information Interchange, known as ASCII, or the eight-bit Extended Binary-Coded Decimal Interchange Code, known as EBCDIC, might be used.)

For each program in P , use the code to translate all the symbols in the program into 0's and 1's. Order these strings by length, putting shorter before longer, and order all

strings of a given length by regarding each string as a binary number and writing the numbers in ascending order.

Define a function $F: \mathbf{Z}^+ \rightarrow P$ by specifying that

$F(n) =$ the n th program in the list for each $n \in \mathbf{Z}^+$.

By construction, F is one-to-one and onto, and so P is countably infinite and hence countable. As a simple example, suppose the following are all the programs in P that translate into bit strings of length less than or equal to 5:

10111, 11, 0010, 1011, 01, 00100, 1010, 00010.

Ordering these by length gives

length 2: 11, 01

length 4: 0010, 1011, 1010

length 5: 10111, 00100, 00010

And ordering those of each given length by the size of the binary number they represent gives

$$\begin{aligned} 01 &= F(1) \\ 11 &= F(2) \\ 0010 &= F(3) \\ 1010 &= F(4) \\ 1011 &= F(5) \\ 00010 &= F(6) \\ 00100 &= F(7) \\ 10111 &= F(8) \end{aligned}$$

Note that when viewed purely as numbers, ignoring leading zeros, $0010 = 00010$. This shows the necessity of first ordering the strings by length before arranging them in ascending numeric order. ■

The final example of this section shows that a certain set is uncountable and hence that there must exist a noncomputable function.

Example 7.4.7 The Cardinality of a Set of Functions and Computability

- Let T be the set of all functions from the positive integers to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.
- Derive the consequence that there are noncomputable functions. Specifically, show that for any computer language there must be a function F from \mathbf{Z}^+ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with the property that no computer program can be written in the language to take arbitrary values as input and output the corresponding function values.

Solution

- Let S be the set of all real numbers between 0 and 1. As noted before, any number in S can be represented in the form

$$0.a_1a_2a_3\dots a_n\dots,$$

where each a_i is an integer from 0 to 9. This representation is unique if decimals that end in all 9's are omitted.

Define a function F from S to a subset of T (the set of all functions from \mathbf{Z}^+ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) as follows:

$$F(0.a_1a_2a_3\dots a_n\dots) = \text{the function that sends each positive integer } n \text{ to } a_n.$$

Choose the co-domain of F to be exactly that subset of T that makes F onto. That is, define the co-domain of F to equal the image of F . Note that F is one-to-one because if $F(x_1) = F(x_2)$, then each decimal digit of x_1 equals the corresponding decimal digit of x_2 , and so $x_1 = x_2$. Thus F is a one-to-one correspondence from S to a subset of T . But S is uncountable by Theorem 7.4.2. Hence T has an uncountable subset, and so, by Corollary 7.4.4, T is uncountable.

- b. Part (a) shows that the set T of all functions from \mathbf{Z}^+ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is uncountable. But Example 7.4.6 shows that given any computer language, the set of all programs in that language is countable. Consequently, in any computer language there are not enough programs to compute values of every function in T . There must exist functions that are not computable! ■

Test Yourself

1. A set is finite if, and only if, _____.
2. To prove that a set A has the same cardinality as a set B you must _____.
3. The reflexive property of cardinality says that given any set A , _____.
4. The symmetric property of cardinality says that given any sets A and B , _____.
5. The transitive property of cardinality says that given any sets A , B , and C , _____.
6. A set is called countably infinite if, and only if, _____.
7. A set is called countable if, and only if, _____.
8. In each of the following, fill in the blank with the word *countable* or the word *uncountable*.
 - (a) The set of all integers is _____.
 - (b) The set of all rational numbers is _____.
 - (c) The set of all real numbers between 0 and 1 is _____.
 - (d) The set of all real numbers is _____.
9. The Cantor diagonalization process is used to prove that _____.

Exercise Set 7.4

1. When asked what it means to say that set A has the same cardinality as set B , a student replies, “ A and B are one-to-one and onto.” What *should* the student have replied? Why?
 2. Show that “there are as many squares as there are numbers” by exhibiting a one-to-one correspondence from the positive integers, \mathbf{Z}^+ , to the set S of all squares of positive integers:

$$S = \{n \in \mathbf{Z}^+ \mid n = k^2, \text{ for some positive integer } k\}.$$
 3. Let $3\mathbf{Z} = \{n \in \mathbf{Z} \mid n = 3k, \text{ for some integer } k\}$. Prove that \mathbf{Z} and $3\mathbf{Z}$ have the same cardinality.
 4. Let \mathbf{O} be the set of all odd integers. Prove that \mathbf{O} has the same cardinality as $2\mathbf{Z}$, the set of all even integers.
 5. Let $25\mathbf{Z}$ be the set of all integers that are multiples of 25. Prove that $25\mathbf{Z}$ has the same cardinality as $2\mathbf{Z}$, the set of all even integers.
- H 6.** Use the functions I and J defined in the paragraph following Example 7.4.1 to show that even though there is a one-to-one correspondence, H , from $2\mathbf{Z}$ to \mathbf{Z} , there is also a function from $2\mathbf{Z}$ to \mathbf{Z} that is one-to-one but not onto and a function from \mathbf{Z} to $2\mathbf{Z}$ that is onto but not one-to-one. In other words, show that I is one-to-one but not onto, and show that J is onto but not one-to-one.
7. a. Check that the formula for F given at the end of Example 7.4.2 produces the correct values for $n = 1, 2, 3$, and 4.
b. Use the floor function to write a formula for F as a single algebraic expression for all positive integers n .
 8. Use the result of exercise 3 to prove that $3\mathbf{Z}$ is countable.
 9. Show that the set of all nonnegative integers is countable by exhibiting a one-to-one correspondence between \mathbf{Z}^+ and \mathbf{Z}^{nonneg} .

In 10–14, S denotes the set of real numbers strictly between 0 and 1. That is, $S = \{x \in \mathbf{R} \mid 0 < x < 1\}$.

- 10.** Let $U = \{x \in \mathbf{R} \mid 0 < x < 2\}$. Prove that S and U have the same cardinality.

- H 11.** Let $V = \{x \in \mathbf{R} \mid 2 < x < 5\}$. Prove that S and V have the same cardinality.

- 12.** Let a and b be real numbers with $a < b$, and suppose that $W = \{x \in \mathbf{R} \mid a < x < b\}$. Prove that S and W have the same cardinality.

- 13.** Draw the graph of the function f defined by the following formula:

For all real numbers x with $0 < x < 1$,

$$f(x) = \tan\left(\pi x - \frac{\pi}{2}\right).$$

Use the graph to explain why S and \mathbf{R} have the same cardinality.

- * 14.** Define a function g from the set of real numbers to S by the following formula:

For all real numbers x ,

$$g(x) = \frac{1}{2} \cdot \left(\frac{x}{1 + |x|} \right) + \frac{1}{2}.$$

Prove that g is a one-to-one correspondence. (It is possible to prove this statement either with calculus or without it.) What conclusion can you draw from this fact?

- 15.** Show that the set of all bit strings (strings of 0's and 1's) is countable.

- 16.** Show that \mathbf{Q} , the set of all rational numbers, is countable.

- 17.** Show that the set \mathbf{Q} of all rational numbers is dense along the number line by showing that given any two rational numbers r_1 and r_2 with $r_1 < r_2$, there exists a rational number x such that $r_1 < x < r_2$.

- H 18.** Must the average of two irrational numbers always be irrational? Prove or give a counterexample.

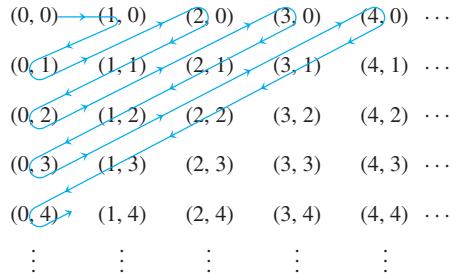
- H* 19.** Show that the set of all irrational numbers is dense along the number line by showing that given any two real numbers, there is an irrational number in between.

- 20.** Give two examples of functions from \mathbf{Z} to \mathbf{Z} that are one-to-one but not onto.

- 21.** Give two examples of functions from \mathbf{Z} to \mathbf{Z} that are onto but not one-to-one.

- H 22.** Define a function $g: \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ by the formula $g(m, n) = 2^m 3^n$ for all $(m, n) \in \mathbf{Z}^+ \times \mathbf{Z}^+$. Show that g is one-to-one and use this result to prove that $\mathbf{Z}^+ \times \mathbf{Z}^+$ is countable.

- 23. a.** Explain how to use the following diagram to show that $\mathbf{Z}^{nonneg} \times \mathbf{Z}^{nonneg}$ and \mathbf{Z}^{nonneg} have the same cardinality.



- H* b.** Define a function $H: \mathbf{Z}^{nonneg} \times \mathbf{Z}^{nonneg} \rightarrow \mathbf{Z}^{nonneg}$ by the formula

$$H(m, n) = n + \frac{(m+n)(m+n+1)}{2}$$

for all nonnegative integers m and n . Interpret the action of H geometrically using the diagram of part (a).

- * 24.** Prove that the function H defined analytically in exercise 23b is a one-to-one correspondence.

- H 25.** Prove that $0.1999\dots = 0.2$.

- 26.** Prove that any infinite set contains a countably infinite subset.

- 27.** If A is any countably infinite set, B is any set, and $g: A \rightarrow B$ is onto, then B is countable.

- 28.** Prove that a disjoint union of any finite set and any countably infinite set is countably infinite.

- H 29.** Prove that a union of any two countably infinite sets is countably infinite.

- H 30.** Use the result of exercise 29 to prove that the set of all irrational numbers is uncountable.

- H 31.** Use the results of exercises 28 and 29 to prove that a union of any two countable sets is countable.

- H 32.** Prove that $\mathbf{Z} \times \mathbf{Z}$, the Cartesian product of the set of integers with itself, is countably infinite.

- 33.** Use the results of exercises 27, 31, and 32 to prove the following: If R is the set of all solutions to all equations of the form $x^2 + bx + c = 0$, where b and c are integers, then R is countable.

- H 34.** Let $\mathcal{P}(S)$ be the set of all subsets of set S , and let T be the set of all functions from S to $\{0, 1\}$. Show that $\mathcal{P}(S)$ and T have the same cardinality.

- H 35.** Let S be a set and let $\mathcal{P}(S)$ be the set of all subsets of S . Show that S is “smaller than” $\mathcal{P}(S)$ in the sense that there is a one-to-one function from S to $\mathcal{P}(S)$ but there is no onto function from $\mathcal{P}(S)$ to S .

- *36.** The Schroeder–Bernstein theorem states the following: If A and B are any sets with the property that there is a one-to-one function from A to B and a one-to-one function from B to A , then A and B have the same cardinality. Use this theorem to prove that there are as many functions from \mathbf{Z}^+ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ as there are functions from \mathbf{Z}^+ to $\{0, 1\}$.
- H 37.** Prove that if A and B are any countably infinite sets, then $A \times B$ is countably infinite.
- *38.** Suppose A_1, A_2, A_3, \dots is an infinite sequence of countable sets. Recall that

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ for some positive integer } i\}.$$

Prove that $\bigcup_{i=1}^{\infty} A_i$ is countable. (In other words, prove that a countably infinite union of countable sets is countable.)

Answers for Test Yourself

1. it is the empty set or there is a one-to-one correspondence from $\{1, 2, \dots, n\}$ to it, where n is a positive integer
2. show that there exists a function from A to B that is one-to-one and onto (*Or:* show that there exists a one-to-one correspondence from A to B)
3. A has the same cardinality as A .
4. if A has the same cardinality as B , then B has the same cardinality as A
5. if A has the same cardinality as B and B has the same cardinality as C , then A has the same cardinality as C
6. it has the same cardinality as the set of all positive integers
7. it is finite or countably infinite
8. countable; countable; uncountable; uncountable
9. the set of all real numbers between 0 and 1 is uncountable