APPENDIX B

Sets and Functions

For our purposes, a **set** is any collection of objects; for example,

The set $\mathbb{Z}$ of integers.
The set of right triangles with area 24.
The set of positive irrational numbers.

The objects in a set are called **elements** or **members** of the set. If B is a set, the statement "b is an element of B" is abbreviated as "$b \in B$." Similarly, "$b \notin B$" means "b is not an element of B." For example, if $\mathbb{Z}$ is the set of integers,* then

$$2 \in \mathbb{Z} \qquad \text{and} \qquad \pi \notin \mathbb{Z}.$$

There are several methods of describing sets. A set may be defined by **verbal description** as in the examples above. A small finite set can be described by **listing** all its elements. Such a list is customarily placed between curly brackets; for instance,

$$\{3, 7, -4, 9\} \qquad \text{or} \qquad \{a, b, c, r, s, t\}.$$

Listing notation is sometimes used for infinite sets as well. For example, $\{2, 4, 6, 8, \ldots\}$ indicates the set of positive even integers. Strictly speaking, this notation is ambiguous in the infinite case since it relies on everyone's seeing the same pattern and understanding that it is to continue forever. But when the context is clear, no confusion will result.

Finally, a set can be described in terms of properties that are satisfied by its elements, and by these elements only. This is usually done with **set-builder notation.** For example,

$$\{x \mid x \text{ is an integer and } x > 9\}$$

* Throughout this book boldface capital $\mathbb{Z}$ always denotes the set of integers.

denotes the set of all elements x *such that* x is an integer greater than 9. In general, the vertical line is shorthand for "such that" and "$\{y \mid P\}$" is read "the set of all elements y such that P." Thus each of the following is the set of even integers:

$\{x \mid x \text{ is an even integer}\}$.
$\{t \mid t \in \mathbb{Z} \text{ and } t \text{ is even}\}$.
$\{r \mid r \in \mathbb{Z} \text{ and } r \text{ is a multiple of } 2\}$.
$\{y \mid y \in \mathbb{Z} \text{ and } y = 2k \text{ for some integer } k\}$.

The Empty Set

Some special cases of set-builder notation lead to an unusual set. For instance, the set

$$\{x \mid x \text{ is an integer and } 0 < x < 1\}$$

has no elements since there is no integer between 0 and 1. The set with no elements is called the **empty set** or **null set** and is denoted $\varnothing$. For every element c,

$$c \in \varnothing \text{ is false} \qquad \text{and} \qquad c \notin \varnothing \text{ is true.}$$

The empty set is a very convenient concept to have around, but some care must be taken when dealing with theorems that are true only for **nonempty sets** (that is, sets that have at least one element).

Subsets

A set B is said to be a **subset** of a set C (written $B \subseteq C$) provided that every element of B is also an element of C. In other words, $B \subseteq C$ exactly when this statement is true:

$$x \in B \Rightarrow x \in C.$$

For example, the set of even integers is a subset of the set $\mathbb{Z}$ of all integers, and the set of rational numbers is a subset of the set of real numbers.

The definition of "$B \subseteq C$" allows the possibility that $B = C$ (since it is certainly true in this case that every element of B is also an element of C). In other words,

$$\boldsymbol{B \subseteq B} \textbf{ for every set } \boldsymbol{B}.$$

If B is a subset of C and $B \neq C$ we say that B is a **proper subset** of C and write $B \subsetneqq C$.

The subset relation is easily seen to be *transitive,* that is,

$$\textbf{If } \boldsymbol{B \subseteq C} \textbf{ and } \boldsymbol{C \subseteq D}\textbf{, then } \boldsymbol{B \subseteq D}.$$

Two sets B and C are **equal** when they have exactly the same elements. In this case every element of B is an element of C *and* every element of C is an element of B. Thus,

$$B = C \qquad \textbf{if and only if} \qquad B \subseteq C \textbf{ and } C \subseteq B.$$

This fact is the most commonly used method of proving that two sets are equal: Prove that each is a subset of the other.

Basic logic leads to a surprising fact about the empty set. Since the statement $x \in \varnothing$ is always false, the implication

$$x \in \varnothing \Rightarrow x \in C$$

is always true (see Appendix A). But this is precisely the definition of "$\varnothing$ is a subset of C." So

the empty set $\varnothing$ is a subset of every set.

Operations on Sets

We now review the standard ways of constructing new sets from given ones. If B and C are sets, then the **relative complement** of C in B is denoted $B - C$ and consists of the elements of B that are not in C. Thus

$$B - C = \{x \mid x \in B \textbf{ and } x \notin C\}.$$

For example, if E is the set of even integers, then $\mathbb{Z} - E$ is the set of odd integers.

The **intersection** of sets B and C consists of all the elements that are in *both* B and C and is denoted $B \cap C$. Thus

$$B \cap C = \{x \mid x \in B \textbf{ and } x \in C\}.$$

For example, if $B = \{-2, 1, \sqrt{2}, 5, \pi\}$ and C is the set of positive rational numbers, then $B \cap C = \{1, 5\}$ since 1 and 5 are the only elements in both sets. If B is the set of positive integers and C the set of negative integers, then $B \cap C = \varnothing$ since there are no elements in both sets. When B and C are sets such that $B \cap C = \varnothing$, we say that B and C are **disjoint.**

The **union** of sets B and C consists of all elements that are in at least one of B or C and is denoted $B \cup C$. Thus,

$$B \cup C = \{x \mid x \in B \textbf{ or } x \in C\}.$$

For example, the union of $B = \{1, 3, 5, 7\}$ and $C = \{-1, 1, 4, 9\}$ is $B \cup C = \{-1, 1, 3, 4, 5, 7, 9\}$. If B is the set of rational numbers and C is the set of irrational numbers, then $B \cup C$ is the set of all real numbers.

You should verify that union and intersection have the following properties. For any sets B, C, and D:

$$B \cup B = B \qquad B \cap B = B$$
$$B \cup \varnothing = B \qquad B \cap \varnothing = \varnothing$$
$$B \cup C = C \cup B \qquad B \cap C = C \cap B$$
$$B \subseteq B \cup C \qquad B \cap C \subseteq B$$
$$B \subseteq C \quad \text{if and only if} \quad B \cup C = C$$
$$B \subseteq C \quad \text{if and only if} \quad B \cap C = B$$
$$B \cup (C \cup D) = (B \cup C) \cup D \qquad B \cap (C \cap D) = (B \cap C) \cap D$$
$$B \cap (C \cup D) = (B \cap C) \cup (B \cap D)$$
$$B \cup (C \cap D) = (B \cup C) \cap (B \cup D).$$

The concepts of union and intersection extend readily to large, possibly infinite, collections of sets. Suppose that I is some nonempty set (called an **index set**) and that for each $i \in I$, we are given a set A_i. Then the intersection of this family of sets (denoted $\bigcap_{i \in I} A_i$) is the set of elements that are in *all* the sets A_i, that is,

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for every } i \in I\}.$$

Similarly, the union of this family of sets (denoted $\bigcup_{i \in I} A_i$) is the set of elements that are in at least one of the sets A_i, that is,

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_j \text{ for some } j \in I\}.$$

The **Cartesian product** of sets B and C is denoted $B \times C$ and consists of all ordered pairs (x,y) with $x \in B$ and $y \in C$. Equality of ordered pairs is defined by this rule:

$$(x,y) = (u,v) \quad \text{if and only if} \quad x = u \text{ in } B \text{ and } y = v \text{ in } C.$$

For example, if $B = \{r, s, t\}$ and $C = \{5, 7\}$, then $B \times C$ is the set

$$\{(r,5), (r,7), (s,5), (s,7), (t,5), (t,7)\}.$$

The set $\mathbb{R}$ of real numbers is sometimes identified with the number line. When this is done, the Cartesian product $\mathbb{R} \times \mathbb{R}$ is just the ordinary coordinate plane, the set of all points with coordinates (x,y) where $x, y \in \mathbb{R}$.

The Cartesian product of any finite number of sets $B_1, B_2, \ldots, B_n$ is defined in a similar fashion. $B_1 \times B_2 \times \cdots \times B_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$ where $x_i \in B_i$ for each $i = 1, 2, \ldots, n$. For example, if $B = \{0, 1\}$, $\mathbb{Z}$ is the set of integers, and $\mathbb{R}$ the set of real numbers, then $B \times \mathbb{Z} \times \mathbb{R}$ is the set of all ordered triples of the form $(0,k,r)$ and $(1,k,r)$ with $k \in \mathbb{Z}$ and $r \in \mathbb{R}$. The product $B \times \mathbb{Z} \times \mathbb{R}$ is an infinite set; among its elements are $(0,-5,3)$, $(1,24,\pi)$, and $(1,1,-\sqrt{3})$.

FUNCTIONS

A **function** (or **map** or **mapping**) f from a set B to a set C (denoted $f\colon B \to C$) is a rule that assigns to each element b of B exactly one element c of C; c is called the **image** of b or the **value** of the function f at b and is usually denoted $f(b)$. The set B is called the **domain** and the set C the **range** of the function f.

Your previous mathematics courses dealt with a wide variety of functions. For instance, if $\mathbb{R}$ is the set of real numbers, then each of the following rules defines a function from $\mathbb{R}$ to $\mathbb{R}$:

$$f(x) = \cos x, \qquad g(x) = x^2 + 1, \qquad h(x) = x^3 - 5x + 2.$$

The rule of a function need not be given by an algebraic formula. For instance, consider the function $f\colon \mathbb{Z} \to \{0, 1\}$, whose rule is

$$f(x) = 0 \text{ if } x \text{ is even and } f(x) = 1 \text{ if } x \text{ is odd.}$$

If B is a set, then the function from B to B defined by the rule "map every element to itself" is called the **identity map** on B and is denoted ι_B. Thus $\iota_B\colon B \to B$ is defined by

$$\iota_B(x) = x \text{ for every } x \in B.$$

Composition of Functions

Let f and g be functions such that the range of f is the same as the domain of g, say $f\colon B \to C$ and $g\colon C \to D$. Then the **composite** of f and g is the function $h\colon B \to D$ whose rule is

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

In other words, the composite function is obtained by first applying f and then applying g:

$$\begin{array}{ccccc} B & \xrightarrow{f} & C & \xrightarrow{g} & D \\ x & \dashrightarrow & f(x) & \dashrightarrow & g(f(x)). \end{array}$$

Instead of h, the usual notation for the composite function of f and g is $g \circ f$ (note the order). Thus $(g \circ f)(x) = g(f(x))$.

EXAMPLE Let E be the set of even integers and $\mathbb{N}$ the set of nonnegative integers. Let $f\colon E \to \mathbb{Z}$ be defined by $f(x) = x/2$ (since x is even, $x/2$ *is* an integer). Let $g\colon \mathbb{Z} \to \mathbb{N}$ be given by $g(n) = n^2$. Then the composite function $g \circ f\colon E \to \mathbb{N}$ has this rule:

$$(g \circ f)(x) = g(f(x)) = g(x/2) = (x/2)^2 = x^2/4.$$

The composite function in the opposite order, $f \circ g$ (first apply g, then f), is *not defined* since the range of g is not the same as the domain of f. For instance, $g(3) = 9$, but the domain of f is the set of even integers; even though the rule of f makes sense for odd integers, $f(g(3)) = f(9) = 9/2$, which is not in $\mathbb{Z}$.

EXAMPLE Let $f:\mathbb{Z} \to \mathbb{Z}$ and $g:\mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = x - 1$ and $g(x) = x^2$. Then the composite function $f \circ g$ is given by the rule

$$(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 - 1.$$

In this case the composite function in the opposite order $g \circ f$ is also defined; its rule is

$$(g \circ f)(x) = g(f(x)) = g(x - 1) = (x - 1)^2 = x^2 - 2x + 1.$$

Thus we have, for instance,

$$(f \circ g)(3) = 9 - 1 = 8 \quad \text{but} \quad (g \circ f)(3) = 9 - 6 + 1 = 4.$$

So even though both are defined, $f \circ g$ *is not the same function as* $g \circ f$.

Two functions $h:B \to C$ and $k:B \to C$ are said to be **equal** provided that $h(b) = k(b)$ for every $b \in B$.

EXAMPLE Let $f:B \to C$ be any function and $\iota_C:C \to C$ the identity map on C. Then $\iota_C \circ f:B \to C$, and for every $b \in B$

$$(\iota_C \circ f)(b) = \iota_C(f(b)) = f(b).$$

Therefore $\iota_C \circ f = f$. Similarly, if ι_B is the identity map on B, then $f \circ \iota_B:B \to C$, and for every $b \in B$

$$(f \circ \iota_B)(b) = f(\iota_B(b)) = f(b).$$

Consequently,

$$\textbf{If } f:B \longrightarrow C, \textbf{ then } \quad \iota_C \circ f = f \quad \textbf{and} \quad f \circ \iota_B = f.$$

If $f:B \to C$, $g:C \to D$, and $h:D \to E$ are functions, then each of the composite functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ is a map from B to E. We claim that

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

The proof of this statement is simply an exercise in using the definition of composite function. For each $b \in B$

$$[(f \circ g) \circ h](b) = (f \circ g)(h(b)) = f[g(h(b))]$$

and

$$[f \circ (g \circ h)](b) = f[(g \circ h)(b)] = f[g(h(b))].$$

Since the right sides of the two equalities are identical, the composite functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have the same effect on each $b \in B$, which proves the claim.

Binary Operations

Informally we can think of a binary operation on the integers, for example, as a rule for producing a new integer from two given ones. Ordinary addition and multiplication are operations in this sense: Given a and b we get $a + b$ and ab. Producing a new integer from a pair of given ones also suggests the idea of a function. Addition of integers may be thought of as the function f from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ whose rule is

$$f(a,b) = a + b.$$

Similarly, multiplication can be thought of as the function $g: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $g(a,b) = ab$.

With the preceding examples in mind we make this formal definition. A **binary operation** on a nonempty set B (usually called simply an **operation** on B) is a function $f: B \times B \to B$. The familiar examples suggest a new notation for the general case. We use some symbol, say $*$, to denote the operation and write $a * b$ instead of $f(a,b)$.

EXAMPLE As we saw above, ordinary addition and multiplication are operations on $\mathbb{Z}$. Another operation on $\mathbb{Z}$ is defined by the function $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ whose rule is $f(a,b) = ab - 1$. If we denote this operation by $*$, then $3 * 5 = 15 - 1 = 14$, and, similarly,

$$12 * 4 = 47 \qquad -7 * 4 = -29 \qquad 0 * 8 = -1.$$

Note that $a * b = ab - 1 = ba - 1 = b * a$, so that the order of the elements doesn't matter when applying $*$, as is the case with ordinary addition and multiplication (the technical term for this property is *commutativity*). On the other hand,

$$(1 * 2) * 3 = 1 * 3 = 2 \qquad \text{but} \qquad 1 * (2 * 3) = 1 * 5 = 4,$$

so that $(a * b) * c \neq a * (b * c)$ in general. Thus $*$ is not *associative* as are addition and multiplication (meaning that $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ always).

EXAMPLE Let S be a nonempty set. If $f: S \to S$ and $g: S \to S$ are functions, then their composite $f \circ g$ is also a function from S to S. So if B is the set of all functions from S to S, then composition of functions is an operation on the set B. In other words, the map that sends (f,g) to $f \circ g$ is a function from $B \times B$ to B. The discussion of composite functions above shows that the operation $\circ$ on B is associative (that is, $(f \circ g) \circ h = f \circ (g \circ h)$ always) but not commutative ($f \circ g$ need not equal $g \circ f$).

Let $*$ be an operation on a set B and $C \subseteq B$. The subset C is said to be **closed** under the operation $*$ provided that

$$\text{Whenever } a, b \in C, \text{ then } a * b \in C.$$

Consider, for example, the operation of ordinary multiplication on the set B of positive real numbers. Let C be the subset of positive integers. Then C is closed under the operation since ab is a positive integer whenever a and b are. But when the operation on B is ordinary division, then C is not closed: If a and b are integers, $a \div b$ need not be an integer (for instance, $3 \div 7 = 3/7 \notin C$).

If $*$ is an operation on a set B, then B (considered as a subset of itself) is closed under $*$ by the definition of an operation. Nevertheless many texts, including this one, routinely list the **closure** of B under $*$ as one of the properties of the operation. Although this isn't logically necessary, it calls your attention to the importance of closure and reminds you that closure cannot be taken for granted for subsets other than B.

Injective and Surjective Functions

A function $f: B \to C$ is said to be **injective** (or **one-to-one**) provided f maps distinct elements of B to distinct elements of C, or in functional notation: If $a \neq b$ in B, then $f(a) \neq f(b)$ in C. This rather awkward statement is equivalent to its contrapositive, so that we have this useful description:

$f: B \longrightarrow C$ is injective provided that whenever $f(a) = f(b)$ in C, then $a = b$ in B.

EXAMPLE Let $\mathbb{R}$ be the set of real numbers. In order to show that the function $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x + 3$ is injective, we assume that $f(a) = f(b)$, that is,

$$2a + 3 = 2b + 3.$$

Subtracting 3 from each side shows that $2a = 2b$; dividing both sides by 2 we conclude that $a = b$. Therefore, f is injective.

EXAMPLE The map $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^2$ is *not* injective because we have $f(-3) = 9 = f(3)$, but $-3 \neq 3$. Alternatively, the distinct elements 3 and -3 have the same image.

A function $f{:}B \to C$ is said to be **surjective** (or **onto**) provided that every element of C is the image under f of at least one element of B, that is,

If $c \in C$, then there exists $b \in B$ such that $f(b) = c$.

EXAMPLE Let $\mathbb{N}$ be the set of nonnegative integers and $f{:}\mathbb{Z} \to \mathbb{N}$ the function given by $f(x) = |x|$. Then f is surjective since every element of $\mathbb{N}$ is the image under f of at least one element of $\mathbb{Z}$ (namely itself). Note, however, that f is not injective since, for example, $f(1) = f(-1)$.

EXAMPLE Let E be the set of even integers and consider the map $g{:}\mathbb{Z} \to E$ given by $g(x) = 4x$. We claim that the element 2 in E is *not* the image under g of any element of $\mathbb{Z}$. If $2 = g(b)$ for some $b \in \mathbb{Z}$, then $2 = 4b$, so that $1 = 2b$. This is impossible since 1 is not an integer multiple of 2. Therefore, g is *not* surjective. Note, however, that g *is* injective since $4a = 4b$ (that is, $g(a) = g(b)$) implies that $a = b$.

EXAMPLE Let $\mathbb{R}$ be the set of real numbers and $f{:}\mathbb{R} \to \mathbb{R}$ the function given by $f(x) = 2x + 3$. To prove that f is surjective, let $c \in \mathbb{R}$; we must find $b \in \mathbb{R}$ such that $f(b) = c$. In other words, we must find a number b such that $2b + 3 = c$. To do so, we solve this last equation for b and find $b = \dfrac{c-3}{2}$. Then $f(b) = 2\left(\dfrac{c-3}{2}\right) + 3 = c - 3 + 3 = c$. Therefore, f is surjective. The map f is also injective (see the Example on page 511).

The preceding examples demonstrate that *injectivity and surjectivity are independent concepts.* One does not imply the other, and a particular map might have one, both, or neither of these properties.

If $f{:}B \to C$ is a function, then the **image of f** is this subset of C:

$$\operatorname{Im} f = \{c \mid c = f(b) \text{ for some } b \in B\} = \{f(b) \mid b \in B\}.$$

For example, if $f{:}\mathbb{Z} \to \mathbb{Z}$ is given by $f(x) = 2x$, then $\operatorname{Im} f$ is the set of even integers since $\operatorname{Im} f = \{f(x) \mid x \in \mathbb{Z}\} = \{2x \mid x \in \mathbb{Z}\}$. Similarly, if $g{:}\mathbb{Z} \to \mathbb{Z}$ is given by $g(x) = |x|$, then $\operatorname{Im} g$ is the set of nonnegative integers. A map $f{:}B \to C$ is surjective exactly when every element of C is the image of an element of B. Thus

$$\boldsymbol{f{:}B \to C \text{ is surjective if and only if } \operatorname{Im} f = C.}$$

If $f{:}B \to C$ is a function and S is a subset of B, then the **image of the subset** S is the set

$$f(S) = \{c \mid c = f(b) \text{ for some } b \in S\} = \{f(b) \mid b \in S\}.$$

If $f: \mathbb{Z} \to \mathbb{Z}$ is given by $f(x) = 2x$, for example, and S is the set of odd integers, then $f(S) = \{2x \mid x \text{ is odd}\}$ is the set of even integers that are not multiples of 4. If the subset S is the entire set B, then $f(B)$ is precisely $\operatorname{Im} f$.

Bijective Functions

A function $f: B \to C$ is **bijective** (or a **bijection** or **one-to-one correspondence**) provided that f is both injective and surjective.

EXAMPLE The Examples on pages 511 and 512 show that the map $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x + 3$ is bijective.

EXAMPLE The map f from the set $\{1, 2, 3, 4, 5\}$ to the set $\{v, w, x, y, z\}$ given by

$$f(1) = v \qquad f(2) = w \qquad f(3) = x \qquad f(4) = y \qquad f(5) = z$$

is easily seen to be bijective.

The last example illustrates the fact that for any *finite* sets B and C, there is a bijection from B to C if and only if B and C have the same number of elements. In particular, if B is finite and $C \subsetneqq B$, then there cannot be a bijection from B to C. But the situation is quite different with infinite sets.

EXAMPLE Let E be the set of even integers and consider the map $f: \mathbb{Z} \to E$ given by $f(x) = 2x$. By definition every even integer is 2 times some integer, so f is surjective. Furthermore, $2a = 2b$ implies that $a = b$, so f is injective. Therefore, f is a bijection. In this case, a bit more is true. Define a map $g: E \to \mathbb{Z}$ by $g(u) = u/2$; this makes sense since $u/2$ is an integer when u is even. Consider the composite function $g \circ f: \mathbb{Z} \to \mathbb{Z}$:

$$(g \circ f) = g(f(x)) = g(2x) = 2x/2 = x.$$

Thus $(g \circ f)(x) = x = \iota_{\mathbb{Z}}(x)$ for every x, and the composite map $g \circ f$ is just the identity map $\iota_{\mathbb{Z}}$ on $\mathbb{Z}$. Now look at the other composite, $f \circ g: E \to E$:

$$(f \circ g)(u) = f(g(u)) = f(u/2) = 2(u/2) = u.$$

Therefore, the composite map $f \circ g$ is the identity map ι_E.

The preceding example illustrates a property that all bijective functions have, as we now prove.

THEOREM B.1 *A function $f: B \to C$ is bijective if and only if there exists a function $g: C \to B$ such that*

$$g \circ f = \iota_B \quad \text{and} \quad f \circ g = \iota_C.$$

Proof Assume first that f is bijective. Define $g: C \to B$ as follows. If $c \in C$, then there exists $b \in B$ such that $f(b) = c$ because f is surjective. Furthermore, since f is also injective, there is only one element b such that $f(b) = c$ (for if $f(b') = c$, then $f(b) = f(b')$ implies $b = b'$). So we can define a function $g: C \to B$ by this rule:

$$g(c) = b, \text{ where } b \text{ is the unique element of } B \text{ such that } f(b) = c.$$

Then $g(c) = b$ exactly when $f(b) = c$. Thus for any $c \in C$

$$(f \circ g)(c) = f(g(c)) = f(b) = c,$$

from which we conclude that $f \circ g = \iota_C$. Similarly, for each $u \in B$, $f(u)$ is an element of C, say $f(u) = v$, and, hence, by the definition of g, we have $g(v) = u$. Therefore,

$$(g \circ f)(u) = g(f(u)) = g(v) = u$$

and $g \circ f = \iota_B$. This proves the first half of our biconditional theorem.

To prove the other half, we assume that a map $g: C \to B$ with the stated properties is given. We must show that f is bijective. Suppose $f(a) = f(b)$. Then

$$\begin{aligned} g(f(a)) &= g(f(b)) \\ (g \circ f)(a) &= (g \circ f)(b) \\ \iota_B(a) &= \iota_B(b) \\ a &= b. \end{aligned}$$

Therefore, $f(a) = f(b)$ implies $a = b$, and f is injective. To show that f is surjective, let c be any element of C. Then $g(c) \in B$ and $f(g(c)) = (f \circ g)(c) = \iota_C(c) = c$. So we have found an element of B that f maps onto c (namely $g(c)$); hence, f is surjective. Therefore, f is bijective, and the theorem is proved. ◆

If $f: B \to C$ is a bijection, then the map g in Theorem B.1 is called the **inverse** of f and is sometimes denoted by f^{-1}. Reversing the roles of f and g in Theorem B.1 shows that the inverse map g of a bijection f is itself a bijection.

◆ EXERCISES

NOTE: *$\mathbb{Z}$ is the set of integers, $\mathbb{Q}$ the set of rational numbers, and $\mathbb{R}$ the set of real numbers.*

A. **1.** Describe each set by listing:

(a) The integers strictly between -3 and 9.

(b) The negative integers greater than -10.

(c) The positive integers whose square roots are less than or equal to 4.

2. Describe each set in set-builder notation:

(a) All positive real numbers.

(b) All negative irrational numbers.

(c) All points in the coordinate plane with rational first coordinate.

(d) All negative even integers greater than -50.

3. Which of the following sets are nonempty?

(a) $\{r \in \mathbb{Q} \mid r^2 = 2\}$

(b) $\{r \in \mathbb{R} \mid r^2 + 5r - 7 = 0\}$

(c) $\{t \in \mathbb{Z} \mid 6t^2 - t - 1 = 0\}$

4. Is B a subset of C when

(a) $B = \mathbb{Z}$ and $C = \mathbb{Q}$?

(b) $B =$ all solutions of $x^2 + 2x - 5 = 0$ and $C = \mathbb{Z}$?

(c) $B = \{a, b, 7, 9, 11, -6\}$ and $C = \mathbb{Q}$?

5. If $A \subseteq B$ and $B \subseteq C$, prove that $A \subseteq C$.

6. In each part find $B - C$, $B \cap C$, and $B \cup C$:

(a) $B = \mathbb{Z}, C = \mathbb{Q}$. **(b)** $B = \mathbb{R}, C = \mathbb{Q}$.

(c) $B = \{a, b, c, 1, 2, 3, 4, 5\}$, $C = \{a, c, e, 2, 4, 6, 8\}$.

7. List the elements of $B \times C$ when $B = \{a, b, c\}$ and $C = \{0, 1, c\}$.

8. List the elements of $A \times B \times C$ when $A = \{0, 1\}$ and B, C are as in Exercise 7.

9. Let $A = \{1, 2, 3, 4\}$. Exhibit functions f and g from A to A such that $f \circ g \neq g \circ f$.

10. Do Exercise 9 when $A = \mathbb{Z}$.

11. Is the subset B closed under the given operation?

(a) $B =$ even integers; operation: multiplication in $\mathbb{Z}$.

(b) $B =$ odd integers; operation: addition in $\mathbb{Z}$.

(c) $B =$ nonzero rational numbers; operation: division in the set of nonzero real numbers.

(d) $B =$ odd integers; operation $*$ on $\mathbb{Z}$, where $a * b$ is defined to be the number $ab - (a + b) + 2$.

12. Find the image of the function f when

(a) $f: \mathbb{R} \to \mathbb{R}; f(x) = x^2$. **(b)** $f: \mathbb{Z} \to \mathbb{Q}; f(x) = x - 1$.

(c) $f: \mathbb{R} \to \mathbb{R}; f(x) = -x^2 + 1$.

13. Let $B = \{1, 2, 3, 4\}$ and $C = \{a, b, c\}$.

(a) List four different surjective functions from B to C.

(b) List four different injective functions from C to B.

(c) List all bijective functions from C to C.

14. (a) Give an example of a function f that is injective but not surjective.

(b) Give an example of a function g that is surjective but not injective.

15. Let B and C be nonempty sets. Prove that the function

$$f: B \times C \longrightarrow C \times B$$

given by $f(x,y) = (y,x)$ is a bijection.

B. 16. List all the subsets of $\{1, 2\}$. Do the same for $\{1, 2, 3\}$ and $\{1, 2, 3, 4\}$. Make a conjecture as to the number of subsets of an n-element set. [Don't forget the empty set.]

17. Verify each of the properties of sets listed on page 507.

18. If $a, b \in \mathbb{R}$ with $a < b$, then the set $\{r \in \mathbb{R} \mid a \leq r < b\}$ is denoted $[a,b)$. Let N denote the nonnegative integers and P the positive integers. Find these unions and intersections:

(a) $\bigcup_{n \in N} [n, n+1)$ (b) $\bigcap_{n \in P} \left[-\frac{1}{n}, 0\right)$

(c) $\bigcup_{n \in P} \left[\frac{1}{n}, 2 + \frac{1}{n}\right)$ (d) $\bigcap_{n \in P} \left[\frac{1}{n}, 2 + \frac{1}{n}\right)$

19. Prove that for any sets A, B, C:

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

20. Let A, B be subsets of U. Prove **De Morgan's laws:**

(a) $U - (A \cap B) = (U - A) \cup (U - B)$

(b) $U - (A \cup B) = (U - A) \cap (U - B)$

21. Prove that for any sets A, B, C:

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

22. If C is a finite set, then $|C|$ denotes the number of elements in C. If A and B are finite sets, is it true that $|A \cup B| = |A| + |B|$?

23. Let $\mathbb{R}^{**}$ denote the positive real numbers. Does the following rule define a function from $\mathbb{R}^{**}$ to $\mathbb{R}$: assign to each positive real number c the real number whose square is c?

24. Determine whether the given operation on $\mathbb{R}$ is commutative (that is, $a * b = b * a$ for all a, b) or associative (that is, $a * (b * c) = (a * b) * c$ for all a, b, c).

(a) $a * b = 2^{ab}$ **(b)** $a * b = ab^2$

(c) $a * b = 0$ **(d)** $a * b = (a + b)/2$

(e) $a * b = 1$ **(f)** $a * b = b$

(g) $a * b = a^2 + b^2$

25. Prove that the given function is injective.

(a) $f: \mathbb{Z} \to \mathbb{Z}; f(x) = 2x$ **(b)** $f: \mathbb{R} \to \mathbb{R}; f(x) = x^3$

(c) $f: \mathbb{Z} \to \mathbb{Q}; f(x) = x/7$ **(d)** $f: \mathbb{R} \to \mathbb{R}; f(x) = -3x + 5$

26. Prove that the given function is surjective.

(a) $f: \mathbb{R} \to \mathbb{R}; f(x) = x^3$

(b) $f: \mathbb{Z} \to \mathbb{Z}; f(x) = x - 4$

(c) $f: \mathbb{R} \to \mathbb{R}; f(x) = -3x + 5$

(d) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}; f(a,b) = a/b$ when $b \neq 0$ and 0 when $b = 0$.

27. Let $f: B \to C$ and $g: C \to D$ be functions. Prove:

(a) If f and g are injective, then $g \circ f: B \to D$ is injective.

(b) If f and g are surjective, then $g \circ f$ is surjective.

28. **(a)** Let $f: B \to C$ and $g: C \to D$ be functions such that $g \circ f$ is injective. Prove that f is injective.

(b) Give an example of the situation in part (a) in which g is not injective.

29. **(a)** Let $f: B \to C$ and $g: C \to D$ be functions such that $g \circ f$ is surjective. Prove that g is surjective.

(b) Give an example of the situation in part (a) in which f is not surjective.

30. Let $g: B \times C \to C$ (with $B \neq \varnothing$) be the function given by $g(x,y) = y$.

(a) Prove that g is surjective.

(b) Under what conditions, if any, is g injective?

31. If $f: B \to C$ is a function, then f can be considered as a map from B to $\operatorname{Im} f$ since $f(b) \in \operatorname{Im} f$ for every $b \in B$. Show that the map $f: B \to \operatorname{Im} f$ is surjective.

32. Let B be a finite set and $f: B \to B$ is a function. Prove that f is injective if and only if f is surjective.

33. Let $f: B \to C$ be a function and let S, T be subsets of B.

(a) Prove that $f(S \cup T) = f(S) \cup f(T)$.

(b) Prove that $f(S \cap T) \subseteq f(S) \cap f(T)$.

(c) Give an example where $f(S \cap T) \neq f(S) \cap f(T)$.

34. Prove that $f: B \to C$ is injective if and only if $f(S \cap T) = f(S) \cap f(T)$ for every pair of subsets S, T of B.

35. Let $f: B \to C$ and $g: C \to D$ be bijective functions. Then the composite function $g \circ f: B \to D$ is bijective by Exercise 27. Prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.