1

Functions on Sets

We take as a working definition that *mathematics is the study of functions on sets*. In this chapter we take up the primitive notions of sets, functions from one set to another, and injective, surjective, and bijective functions. Sets are classified as finite and infinite, countable and uncountable. All areas of mathematics use these fundamental concepts. This is the core of mathematics.

1.1 Sets

Suppose X is a collection (*set*) of objects (*points*) generically denoted by x. A *subset* S of X is a collection consisting of some of the objects of X, in symbols, $S \subset X$. For any two subsets S and T of X, their *intersection* $S \cap T$ is the set of all objects x in both S and T. Of course it is quite possible that S and T share no common points, in which case we say their intersection is the *empty set* $\emptyset$, and we write $S \cap T = \emptyset$.

The *union* $S \cup T$ is the set of all objects x in either S or T.[1] Two subsets S and T are *equal*, in symbols, $S = T$, if[2] they consist of exactly the same objects.

Subsets $A, B, C, \ldots$ of X under "cap" and "cup" enjoy an arithmetic of sorts:

Theorem A. (Boolean algebra)

$$\begin{array}{ll} A \cap B = B \cap A & A \cup B = B \cup A \\ A \cap (B \cap C) = (A \cap B) \cap C & A \cup (B \cup C) = (A \cup B) \cup C \\ A \cap A = A & A \cup A = A \\ A \cap X = A & A \cup \emptyset = A \\ A \cap \emptyset = \emptyset & A \cup X = X \end{array}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \quad (1.1)$$

[1]The word "or" is used in mathematics in the inclusive sense—either one or the other or both.

[2]We continue the age-old practice when defining terms of using "if" when we really should use "exactly when" or "if and only if." See [Euclid].

Proof. Such set-theoretic formulas are proved by tedious "point-chasing" arguments. For instance, let us prove the first of the distributive laws,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Let x be a point of the left-hand side, in symbols, $x \in A \cup (B \cap C)$. Then (Case 1) $x \in A$ or (Case 2) $x \in B \cap C$, that is, $x \in B$ and $x \in C$. If (Case 1) $x \in A$, then certainly $x \in A \cup B$ and $x \in A \cup C$, and hence $x \in (A \cup B) \cap (A \cup C)$. On the other hand, if (Case 2) $x \in B$ and $x \in C$, then certainly $x \in (A \cup B)$ and $(A \cup C)$, again giving $x \in (A \cup B) \cap (A \cup C)$.

Conversely, suppose x is an arbitrary point of the right side, that is, $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. But this means $x \in A$ or B and $x \in A$ or C. If (Case 1) $x \in A$, then certainly $x \in A \cup (B \cap C)$. On the other hand, if (Case 2) x is not in A, in symbols, $x \notin A$, then nevertheless $x \in B$ and C, again giving that $x \in A \cup (B \cap C)$. Obtain practice with this boring but important proof method by completing exercise 1.1.

Some of the tedium can be avoided by observing the *duality* of cup and cap—the identities of theorem A remain unchanged when one interchanges cap with cup and $\emptyset$ with X. Exercise 1.3 exploits this duality insight when coupled with the following theorem B.

Theorem B. (the De Morgan laws)

$$(A \cap B)' = A' \cup B' \qquad \text{and} \qquad (A \cup B)' = A' \cap B', \tag{1.2}$$

where the prime denotes the operation of *complementation*: the set S' is the set of all points of X not in S.

Proof. Exercise 1.2.

1.2 Functions

Definition. Let X and Y be two sets. A *function* (*mapping*) from X to Y, in symbols

$$f : X \longrightarrow Y, \tag{1.3}$$

is a rule that assigns to each point x in X exactly one point y in Y, that is, $f(x) = y$. The set X is called the *domain* of the function f.

Warning. The function f is the rule, not its *graph,* the set G of all ordered pairs $(x, f(x))$ with $x \in X$.

Example 1. Suppose X is the set of people on Earth and Y the set of real numbers $\mathbf{R}$ (to be defined carefully in Chapter 2). Let f be the rule that assigns to each person their height in meters.

Example 2. Let $X = Y = \mathbf{N}$ be the set of all *natural numbers* $\mathbf{N} = \{1, 2, 3, \ldots\}$. Consider the rule f that assigns to each $x \in X$ the number of distinct divisors of x.

Example 3. A function may be given as a table:

x	a	b	c	d	e
$f(x)$	3	4	1	1	2

In this example, $X = \{a, b, c, d, e\}$ and Y is some set containing the symbols 1, 2, 3, 4. The rule assigns a to 3, b to 4, c to 1, and so on. Note that the function repeats in value; the value 1 is taken on twice—the function is not injective (one-to-one).

Definition. A function $f : X \longrightarrow Y$ is *injective* if no value y is taken on more than once, that is, for all $x_1, x_2 \in X$,

$$f(x_1) = f(x_2) \quad \text{implies} \quad x_1 = x_2. \tag{1.4}$$

For example, the rule of example 1 assigning people to their height is injective, since with unlimited precision it is certain that no two people are exactly the same height.

Example 4. The function $f : \mathbf{R} \longrightarrow \mathbf{R}$ given by the rule $f(x) = x^2$ is two-to-one, since $f(x) = f(-x)$, and is hence not injective. Horizontal lines cut its graph more than once.

Definition. The *range* $f(X)$ of a function $f : X \longrightarrow Y$ is the subset of Y of all values taken on by f as x runs through all of X. That is, $y \in f(X)$ if and only if $y = f(x)$ for some $x \in X$. See figure 1.1.

In Example 4, the range of $f(x) = x^2$ is the set of all nonnegative real numbers. The range in example 3 is $f(X) = \{1, 2, 3, 4\}$.

Definition. A function $f : X \longrightarrow Y$ is *surjective* (*onto*) if the range of f is all of Y, that is, $f(X) = Y$; every object in Y occurs at least once among the values of f on X.

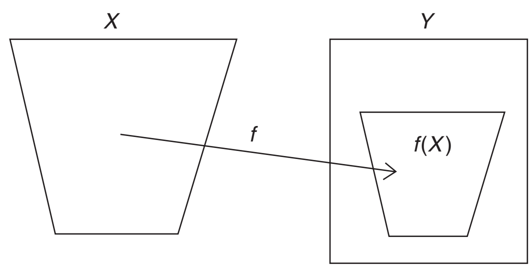


Figure 1.1 The range of the function f is the subset of Y consisting of the values of f.

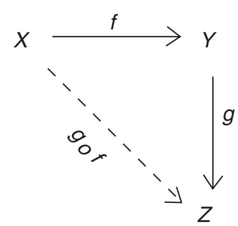


Figure 1.2 The composition $g \circ f$ is the function obtained by operating by g on the result of operating by f.

Definition. A function $f : X \longrightarrow Y$ that is both injective and surjective is called *bijective* (*one-to-one, onto*). Looking backward through such a bijective function yields (exercise 1.9) the bijective *inverse* function

$$f^{-1} : Y \longrightarrow X. \tag{1.5}$$

One last notion.

Definition. Suppose $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$. Then the function

$$h : X \longrightarrow Z$$

given by the rule $h(x) = g(f(x))$ is called the *composition* of f followed by g. We write $h = g \circ f$. See figure 1.2. Note that composition is associative (Exercise 1.13).

Theorem C. The composition of injective functions is injective. The composition of surjective functions is surjective. The composition of bijective functions is bijective.

Proof. Exercise 1.14.

With these simple notions and classifications in our toolkit, we are ready to attack some significant issues.

1.3 Cardinality

When do two sets X and Y contain exactly the "same number" of points? The answer is clear if both sets are finite—you merely count the number of points in each set and compare the count. But what if the sets are infinite? For that matter, what does it mean that X is an infinite set? What is the concept of infinity?

Definition. The sets X and Y are said to be of the *same cardinality* if there exists a bijective function from X onto Y. We indicate that X and Y have the same cardinality with the notation

$$|X| = |Y|. \tag{1.6}$$

Example 5. The rule

$$f(x) = \frac{e^x}{1+e^x} \tag{1.7}$$

maps the entire real line $\mathbf{R}$ bijectively onto the interval $(0, 1)$, and so

$$|\mathbf{R}| = |(0, 1)|. \tag{1.8}$$

(Exercise 1.10.) So even though the interval $(0, 1)$ is finite in length and a (very) proper subset of $\mathbf{R}$, it nevertheless contains exactly the "same number" of elements as its superset $\mathbf{R}$. This is the defining property of infinity.

Definition. The set X is said to be *infinite* if there exists an injective function $f : X \longrightarrow X$ onto a proper subset of itself, where $f(X) \neq X$. The set X is *finite* if it is not infinite, that is, no injective, nonsurjective function exists.

Corollary. (the pigeonhole principle) Every injective function f from a finite set X to itself is surjective.

Remark. We write $|X| \leq |Y|$ when there exists an injective map from X into Y. It is surprisingly difficult to prove that (exercise 1.40)

$$|X| \leq |Y| \quad \text{and} \quad |Y| \leq |X| \quad \text{implies} \quad |X| = |Y|. \tag{1.9}$$

This result is known as the Schröder-Bernstein theorem.

Definition. The (ring of) *integers* is the set

$$\mathbf{Z} = \{\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}, \tag{1.10}$$

the smallest subset of $\mathbf{R}$ closed under addition that contains both 1 and -1. (More about this definition in chapter 2.)

Theorem D. The integers have smaller cardinality than the reals, in symbols, $|\mathbf{Z}| < |\mathbf{R}|$. That is, there is an (obvious) injection from $\mathbf{Z}$ into $\mathbf{R}$, but no injection from $\mathbf{R}$ into $\mathbf{Z}$. Thus there are at least two distinct infinite cardinalities.

Proof. Exercise 1.31.

Any set with the same cardinality as $\mathbf{Z}$ is said to be a *countably infinite* set. All other infinite sets are said to be *uncountably infinite.*

Question. Do there exist sets X with

$$|\mathbf{Z}| < |X| < |\mathbf{R}|? \tag{1.11}$$

Exercises

1.1 Practice point chasing by proving the first five identities for cap in theorem A.

1.2 Prove the De Morgan laws (1.2).

1.3 Deduce the first five identities for cap (union) in theorem A by taking the complement of the first five identities for cup (intersection) and applying the De Morgan laws (theorem B).

For example, since we have $A' \cup B' = B' \cup A'$, taking complements gives $(A' \cap B')' = A'' \cup B'' = A \cup B = (B' \cup A')' = B'' \cap A'' = B \cap A$.

1.4 The set $A \setminus B$ is the set of all points in A that do not lie in B. Prove (by chasing points) or disprove (by example) that $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$.

1.5 Is $(A \setminus B) \cup (B \setminus A) = A \cup B$?

1.6 Prove or disprove (by example):

a. $A \cap B = A \cap C$ implies $B = C$.

b. $A \cup B = A \cup C$ implies $B = C$.

1.7 What is the graphical interpretation of the statement
"$f : \mathbf{R} \longrightarrow \mathbf{R}$ is injective"?

1.8 What is the graphical interpretation of the statement
"$f : \mathbf{R} \longrightarrow \mathbf{R}$ is surjective"?

1.9 Prove carefully that given a bijective function $f : X \longrightarrow Y$, there exists exactly one bijective function $g : Y \longrightarrow X$ prescribed by $g(f(x)) = x$. Thus *a bijective function possesses a bijective inverse function.*

1.10 Argue that the function of (1.7) is a bijective map of $\mathbf{R}$ onto $(0, 1)$.

1.11 Give an example of a function $f : \mathbf{R} \longrightarrow \mathbf{R}$ that is not injective, that in fact takes on each of its values infinitely often.
Suggestion: Examine $f(x) = \sin x$. What is its range?

1.12 Give an example of a function $f : \mathbf{R} \longrightarrow \mathbf{R}$ that is surjective, and in fact takes on every real value infinitely often.

1.13 Prove that composition is associative, that is, if $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$, and $h : Z \longrightarrow W$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

1.14 Prove theorem C.

1.15 Calculate the number N of possible functions $f : X \longrightarrow Y$ from a set X of cardinality m into a set Y of cardinality n.
Answer: $N = n^m$.

1.16 Calculate the number N of bijective functions f from a set X of cardinality n onto itself.
Answer: $N = n!$.

1.17 Calculate the number N of injective functions from a set X of cardinality m into a set Y of cardinality n.
Answer: $N = 0$ when $m > n$. Otherwise, $N = n!/(n - m)!$.

1.18 Count the number of surjective functions from a set of five elements onto a set of two elements.

1.19* Calculate the number N of surjective functions from a set X of cardinality m onto a set Y of cardinality n.
Answer: $N = 0$ when $m < n$. Otherwise,

$$N = n^m - \binom{n}{n-1}(n-1)^m + \binom{n}{n-2}(n-2)^m - \cdots.$$

1.20 Composition is rarely commutative. For example, $\sin x^2 \neq (\sin x)^2$. Give an example of two functions f, g from a finite set X to itself where $f \circ g \neq g \circ f$.

1.21 Prove $|\mathbf{Z}| = |\mathbf{N}|$.

1.22* Deduce from the pigeonhole principle that a surjective function f from a finite set X onto itself is injective.

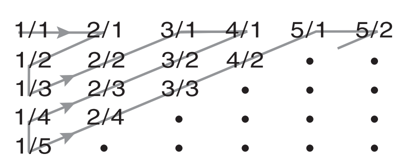
Outline: Consider the composition of the set-valued injection g given by $g(x) = f^{-1}(\{x\})$ followed by an injection h that selects one element from each preimage $g(x)$.

1.23 Seven people enter an elevator and each in turn presses one of the five floor buttons. What is the probability that all buttons will have been pushed?

1.24 **(Lord Russell's paradox)** Allowing sets of unlimited size leads to disaster. Let Ω be the set of all sets that do not contain themselves as elements. Answer this question: Does Ω contain itself as an element?

1.25* Prove that the set of *rational numbers* $\mathbf{Q}$, the set of all fractions $q = a/b$, where $a, b \in \mathbf{Z}$, $b \neq 0$, is countably infinite. That is, show $|\mathbf{Z}| = |\mathbf{Q}|$.

Cantor's Diagonalization: List all positive fractions (with repeats) in an array:



Count the entries starting in the upper left hand corner using the above serpentine pattern:

1.26 Prove that if $g \circ f$ is injective, then so is f.

1.27 Prove that if $g \circ f$ is surjective, then so is g.

1.28 Suppose $f : X \longrightarrow Y$. For any subset S of Y, the symbol $f^{-1}(S)$ denotes the *preimage of S under* f, that is, the subset of X consisting of all x

mapped by f into S. Show that for any two subsets S, T of Y,

$$f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$$
$$f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T).$$

1.29 In contrast to exercise 1.28, are the following statements always true?

$$f(S \cap T) = f(S) \cap f(T),$$
$$f(S \cup T) = f(S) \cup f(T).$$

1.30 Show that for any set X, no matter how large in cardinality, there exists a set Y of even larger cardinality, that is, there exists an injection from X into Y but no injection from Y into X. Thus there is a never-ending hierarchy of infinities.

Outline: Let $Y = \mathcal{P}(X)$ be the *power set* of X, the set of all subsets of X. There is clearly the injection from X into Y given by mapping each x to the singleton $\{x\}$. Assume however that there exists a bijection g from X onto Y. Let X_0 be the subset of X consisting of all points $x \in X$ not belonging to their image under g. Find the preimage x_0 of X_0 under g. Neither $x_0 \in X_0$ nor $x \notin X_0$ can obtain.

1.31 Show that $|\mathbf{Z}| < |\mathbf{R}|$.

Outline: It is enough to show that the reals in $(0, 1)$ are not countable. With some care, such reals have unique decimal expansions, not all of which can be enumerated, since one may construct a decimal expansion that differs in the first place from the first, differs in the second place from the second, and so on.

1.32 Let Y be the power set of X. In your opinion, does there exist a function $g : Y \longrightarrow X$ with the property that $g(y) \in y$ for all $y \in Y$? That is, can you select an element from each subset of a family of subsets?

1.33 Given two sets X and Y, then $X \times Y$ denotes the *cartesian product* of X with Y, the set of all ordered pairs $X \times Y = \{(x, y);\ x \in X,\ y \in Y\}$. For example, $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ is the familiar Euclidean plane. Sketch the subset of $\mathbf{R}^2$ that is the cartesian product $(0, 1) \times \mathbf{R}$.

1.34 Show that the operations of addition and multiplication in $\mathbf{R}$ are functions of the type $f : \mathbf{R} \times \mathbf{R} \longrightarrow \mathbf{R}$.

1.35 Let T denote the unit circle given by $x^2 + y^2 = 1$ in $\mathbf{R}^2$ and let I be the set of all reals $0 < x < 1$ in $\mathbf{R}$. Sketch the cartesian product $T \times I$ in $\mathbf{R}^3$.

1.36 Prove that the collection G of all bijective functions from a set X onto itself forms a *group*, that is,

Axiom I: For all $f, g, h \in G, \quad f \circ (g \circ h) = (f \circ g) \circ h$.
Axiom II: There is an element $e \in G$ with the property $e \circ f = f \circ e = f$ for all $f \in G$.
Axiom III: For each $f \in G$ there exists an element $g \in G$ for which $f \circ g = g \circ f = e$.

This group G is called the *symmetric group on the symbols of* X. See [Artin].

1.37 More concretely than in exercise 1.36, let us consider the symmetric group S_4 on four letters, that is, the twenty-four *permutations* of the digits 1, 2, 3, 4. Each of these permutations can be written in a clever shorthand as a product of disjoint *cycles*. For example, the bijective map (permutation) f that maps according to the rule

x	1	2	3	4
$f(x)$	2	1	4	3

can be simply written as (12)(34), which compactly indicates that $1 \mapsto 2 \mapsto 1$ and $3 \mapsto 4 \mapsto 3$. Fixed digits are not mentioned. For example, the permutation

x	1	2	3	4
$f(x)$	2	4	3	1

is given by (124). The identity permutation $f(i) = i$ is written simply as (1).
Write down all twenty-four elements of the group S_4 in cycle notation. Find pairs of permutations that do not commute. Find permutations that are self-inverse.

1.38 Construct the 6×6 multiplication (composition) table for the symmetric group S_3 on the three digits 1, 2, 3.

1.39 Prove that every subset of a finite set is finite.

1.40* Prove the **Schröder-Bernstein theorem:** $|X| \leq |Y|$ and $|Y| \leq |X|$ implies $|X| = |Y|$.

Outline: [Halmos] Suppose both $f : X \to Y$ and $g : Y \to X$ are injective. A point w in either X or Y is said to be a *descendant* of a point z in either X or Y if w is the eventual image of z under alternating applications of f and g; we also say then that z is an *ancestor* of w. Some points may be orphans. Partition X into three disjoint subsets: the set X_X of descendants of orphans in X, the set X_Y of descendants of orphans in Y, and the set X_∞ of points with infinitely many ancestors. Likewise, partition $Y = Y_X \cup Y_Y \cup Y_\infty$. Then $f : X_X \to Y_X$, $g : Y_Y \to X_Y$, and $f : X_\infty \to Y_\infty$ are all bijective. Piece together f, g^{-1}, and f on X_X, X_Y, and X_∞ respectively to obtain a bijection from X onto Y.

1.41* Prove that $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})|$, where $\mathcal{P}(\mathbf{N})$ is the power set of $\mathbf{N}$.

Outline: Note that a subset S of $\mathbf{N}$ can be uniquely specified by a sequence of zeros and ones by placing a 1 in the nth place of the sequence when $n \in S$, 0 if not. Such a sequence of zeros and ones represents a real number in the interval $[0, 1]$ written base 2. Thus there exists a surjection from the power set of $\mathbf{N}$ onto $[0, 1]$.