APPLIED MODERN ALGEBRA

LARRY L. DORNHOFF

Associate Professor of Mathematics,
University of Illinois, Urbana-Champaign

FRANZ E. HOHN

Late Professor of Mathematics,
University of Illinois, Urbana-Champaign

Macmillan Publishing Co., Inc.
866 Third Avenue, New York, New York 10022
Collier Macmillan Canada, Ltd.

Library of Congress Cataloging in Publication Data

Dornhoff, Larry.
Applied modern algebra.

Bibliography: p.
Includes index.
1. Algebra, Abstract. I. Hohn, Franz Edward, 1915–1977, joint author. II. Title.
QA162.D67 512'.02 76-30825
ISBN 0-02-329980-0

Printing: 1 2 3 4 5 6 7 8 Year: 8 9 0 1 2 3 4

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 9

CHAPTER 1
Sets and Functions

1.1 Sets

The concept of a **set** as an arbitrary collection of objects of interest is probably the most basic concept of modern mathematics. There are no constraints on what objects one may include in a set except that we do not consider it possible for a set to be one of its own objects. A set could consist of precisely these three objects: the real number π, the Taj Mahal, and the ball Hank Aaron hit when he broke the home-run record. Useful sets are, by contrast, ordinarily defined by obviously useful properties. Some examples are the set of positive integers, the set of teams in the National Football League, the set of FORTRAN instructions for a given computer, a complete collection of Zeppelin airmail stamps, and so on.

In this book we shall make use of the following infinite sets (among others):

$\mathbb{R}$: the set of real numbers.
$[a, b]$: the set of real numbers x such that $a \leqslant x \leqslant b$.
$\mathbb{Q}$: the set of rational numbers.
$\mathbb{Z}$: the set of integers (positive, negative, or zero).
$\mathbb{N}$: the set of nonnegative integers.
$\mathbb{P}$: the set of positive integers.
$k\mathbb{Z}$: the set of all integral multiples of the positive integer k.
$k\mathbb{N}$: the set of nonnegative integer multiples of the positive integer k.

We shall also make use of the following finite sets (among others):

$\mathbb{Z}_n$: the set of integers from 0 to $n-1$ inclusive.
$\mathbb{P}_n$: the set of positive integers from 1 to n inclusive.
$\mathbb{B}$: the set consisting of the integers 0 and 1.

In computer science applications, a finite set is often called an **alphabet**, and its elements are called **letters**.

The objects in a set are often called its **elements** or its **members**. If x is an element of the set S, we write $x \in S$, which is read "x belongs to S" or "x belonging to S" as the context requires, as in the phrases "if $x \in S$" and "for all $x \in S$," respectively. If x is not an element of the set S, we write $x \notin S$. Thus $2 \in \mathbb{Z}$ but $\frac{1}{2} \notin \mathbb{Z}$, Chicago Bears $\in$ NFL, J. William Fulbright $\notin$ United States Senate.

Two sets are **equal** if they contain precisely the same elements. Thus the set of all real numbers whose remainders on division by 2 are 0 is equal to the set of all integers of the form $2n$ where $n \in \mathbb{Z}$.

1.2 The Indexing of Sets

It is often useful to name the elements of a set S in some appropriate manner with the aid of another set I, called an **indexing set**. The elements of the indexing set are commonly used as subscripts; each element of S is assigned a subscript name and each element of I is used exactly once as such a name. In the case of a finite set S consisting of n elements, the elements are numbered in some convenient (perhaps random) order, the ith element being denoted by s_i. Then $S = \{s_1, s_2, \ldots, s_n\}$ and $\mathbb{P}_n$ is the indexing set.

Infinite sets may be indexed in a similar way. For example, a **complete polygon** with n distinct vertices consists of n vertices (points in the plane), each pair of vertices joined by a straight line segment (edge). The number E_n of edges of such a polygon is given by the formula $E_n = n(n-1)/2$. The infinite set of numbers $\{E_1, E_2, \ldots, E_n, \ldots\}$ has the indexing set $\mathbb{P}$. Any infinite set whose elements can be indexed by $\mathbb{P}$ is called **enumerable** or **denumerable** or **countably infinite**.

One might think offhand that every finite set can be effectively indexed, but this is not the case. For example, the set of all cloudy days at the site of Tombstone, Arizona, from January 1, A.D. 1700, through December 31, 1974, is a well-defined, reasonably small finite set although, for lack of the proper records, it is not possible to index it. On the other hand, many nondenumerable infinite sets can be indexed. The most familiar example is the indexing of the points P_x of a line by their coordinates x. Here the indexing set is $\mathbb{R}$.

Ordinarily, there is a natural choice for the indexing set and often for the manner of indexing as well. However, many of the finite sets we use in this book have no natural ordering and may be indexed in random order.

1.3 Sets Derived from Other Sets

If U is a set and P is a property (P may in fact be a combination of several properties) which elements x of U may or may not possess, we can define a new set with the "set-builder" notation

$$\{x \in U | P(x)\}.$$

This denotes "the set of all elements x that belong to U and have property P." For example,

$$\{x \in \mathbb{Z} | x > 0\} = \mathbb{P}$$

and

$$\left\{r \in \mathbb{R} \middle| \frac{r}{2} \in \mathbb{Z}\right\} = \{z \in \mathbb{Z} | z = 2n, \quad n \in \mathbb{Z}\}.$$

A **subset** of a set U is a set S all of whose elements belong to U. The set-builder notation is the basic tool for describing subsets. In a discussion dealing exclusively with subsets of a fixed set U, U is often called the **universal set** or the **universe of discourse**. If S is a subset of U, we say that S is **included** (or **contained**) in U and write $S \subseteq U$. We also say that U **includes** or **contains** S and write $U \supseteq S$. If $U \supseteq S$, then U is called a **superset** of S. The set of *all* subsets of U is called the **power set** of U and is denoted by $\mathcal{P}(U)$.

If the property P is so restrictive that no elements of U have that property, we say that $\{x \in U | P(x)\}$ defines the **empty set** or **null set** $\varnothing$. It is proper to refer to *the* empty set here because all empty sets, regardless of the properties that define them, contain exactly the same elements, namely none, and hence are equal. If S is a subset of U and $S \neq U$, we write $S \subset U$ and say that S is a **proper subset** of U.

It is often useful to denote the elements of a set A that are not in a set B by $A - B$, the **set-theoretic difference** of A and B, in that order.

From two sets S and T, not necessarily distinct, new sets may be derived in a variety of useful ways. Many such sets are based on the concept of an **ordered pair** of elements (s, t), where $s \in S$ and is listed first and $t \in T$ and is listed second. Two ordered pairs (s_1, t_1) and (s_2, t_2) are defined to be **equal** if and only if $s_1 = s_2$ and $t_1 = t_2$. For example, if $S = T = \mathbb{Z}$, then $(2, -3) \neq (-3, 2)$.

We may now define the **Cartesian product** of S and T, denoted by $S \times T$, to be the set of all ordered pairs (s, t) such that $s \in S$ and $t \in T$. That is,

$$S \times T = \{(s, t) | s \in S, t \in T\}.$$

For example, if $S = T = \mathbb{R}$, then the Cartesian product is

$$\mathbb{R} \times \mathbb{R} = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\},$$

which is denoted by $\mathbb{R}^2$ and which is interpreted as the set of points of the familiar Cartesian coordinate plane. This plane and its generalization, the Cartesian product of arbitrary sets S and T, are named after the French philosopher and mathematician René Descartes (1596–1650), who invented analytic geometry.

An indexed set $\{a_1, a_2, \ldots, a_n\}$ is called an **ordered n-tuple** and is written $(a_1, a_2, \ldots, a_n)$ if it matters which element is listed first, which is listed second, and so on; that is, if $(a_1, a_2, \ldots, a_n) \neq (b_1, b_2, \ldots, b_n)$ unless $a_i = b_i$, $i = 1, 2, \ldots, n$. We can now define the **Cartesian product** of n sets $S_1, S_2, \ldots, S_n$ as a set of ordered n-tuples thus:

$$S_1 \times S_2 \times \cdots \times S_n = \{(s_1, s_2, \ldots, s_n) | s_i \in S_i, \quad i = 1, 2, \ldots, n\}.$$

If $S_1 = S_2 = \cdots = S_n = S$, this product is denoted by S^n. For example,

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) | x \in \mathbb{R}, \quad y \in \mathbb{R}, \quad z \in \mathbb{R}\}$$

is a set-theoretic description of coordinatized 3-space. A subset of this space (recall that $\mathbb{B} = \{0, 1\}$) is the set of vertices of a unit cube defined by

$$\mathbb{B}^3 = \mathbb{B} \times \mathbb{B} \times \mathbb{B} = \{(b_1, b_2, b_3) | b_i \in \mathbb{B}, \quad i = 1, 2, 3\}.$$

Other examples of Cartesian products will appear naturally in what follows.

1.4 The Order of a Set

The **order** or **cardinality** of a finite set S is the number of elements in S and is denoted by $|S|$. For example, the order of the set $\{1, 3, 5, \dots, 2n-1\}$ is n. If a set can be indexed by the set $\mathbb{P}_n$, then its order is n.

It is important, when determining the order of a set, to observe precisely what the elements of the set are. Thus $|\{(1, 1), (2, 3), (3, 2)\}| = 3$ because this is a set of three ordered pairs. We shall have frequent occasion to employ sets whose elements are themselves sets or ordered sets.

Here are some more examples:

$$|\text{set of columns on an IBM card}| = 80,$$

$$|\text{Los Angeles Dodgers traveling squad}| = 25,$$

$$|\{x \in \mathbb{Z} | 0 < x < 100, x = 3n - 2, n \in \mathbb{P}\}| = 33.$$

A set of order 1 is called a **singleton** and a set of order 0 is the empty set.

If $|S| = m$ and $|T| = n$, then in forming an element (s, t) of $S \times T$, we have m choices for s and n choices for t, so $|S \times T| = mn$. This proves that for finite sets S and T,

$$|S \times T| = |S| \cdot |T|. \tag{1.4.1}$$

In the application of algebra to discrete systems, one has frequent occasion to determine the order of a finite set, so counting problems will often be treated in this book, in both text and exercises. In some cases, even though the order of S cannot be precisely determined, one can determine a number μ_S such that $|S| \leq \mu_S$. Such a number is called an **upper bound** for the order of S.

1.5 Functions

If S and T are sets, a **function** f from S to T, denoted by the symbolism $f: S \to T$, may be defined as a rule assigning to each $s \in S$ a unique element $f(s) \in T$. Although for each $s \in S$ there must be exactly one $f(s)$, it is not required that each $t \in T$ be $f(s)$ for some s. Nor is it required that $f(s_1) \neq f(s_2)$ whenever $s_1 \neq s_2$.

Most mathematics through calculus deals with functions from $\mathbb{R}$ to $\mathbb{R}$. Some examples are: if $f(x) = x^2 - 3x + 2$, then $f(3) = 2$ and $f(1.5) = -0.25$; if $g(x) = \sin x$, then $-1 \leq g(x) \leq 1$ for all $x \in \mathbb{R}$; if $h(x) = e^x$, then $0 < h(x)$ for all

$x \in \mathbb{R}$. In this book we shall encounter functions $f: S \to T$ for many different sets S and T.

Given a function $f: S \to T$, S is called the **domain** of f and T is called the **codomain** of f. The element $f(s)$ of T is called the **image** of s by f and s is a **counterimage** or **pre-image** (there may be others) of $f(s)$. A function $f: S \to T$ is also called a **mapping** of S into T and f is said to **map** s onto its image $f(s)$. The **range** or **image** of a function $f: S \to T$ is the subset $f(S)$ of T defined by

$$f(S) = \{t \in T | t = f(s) \text{ for some } s \in S\}.$$

If S_0 is a subset of S, we define $f(S_0) \subseteq f(S)$ by

$$f(S_0) = \{f(s) \in T | s \in S_0\}.$$

Here are some more examples of functions:

1. $f_1: \mathbb{R} \to \mathbb{R}$, defined by $f_1(x) = x^2 + 4x + 1$. Is every $y \in \mathbb{R}$ the image by f_1 of at least one $x \in \mathbb{R}$? If not, precisely which $y \in \mathbb{R}$ are images and which are not?

2. $f_2: \mathbb{Z} \to \mathbb{Q}$, defined by $f_2(n) = 1/(n + \frac{1}{2})$. Precisely which integers have integers as images by f_2?

3. f_3: {nonbigamous married American men} → {women} defined by f_3(man) = man's wife. Explain why the conditions "nonbigamous" and "American" are included here.

The third example illustrates the fact that there is no restriction on the nature of the sets S and T appearing in the definition of a function. In the following pages we often make use of functions in which S or T or both are not sets of numbers.

The functions

4. $f_4: \mathbb{Z} \to \{0, 1\}$ defined by $f_4(2n) = 0$, $f_4(2n-1) = 1$, $n \in \mathbb{Z}$,

5. $f_5: \mathbb{Z} \to \{0, 1, 2\}$ defined by $f_5(2n) = 0$, $f_5(2n-1) = 1$, $n \in \mathbb{Z}$,

are distinct functions even though their rules of assignment are the same. This illustrates the fact that a function involves three things: the *domain S*, the *codomain T*, and the *rule* that assigns to each $s \in S$ a unique $t \in T$.

Distinct rules at times effect the same mapping of S into T. We therefore make the following definition: The functions $f: S \to T$ and $g: S \to T$ are **equal**, written $f = g$, if and only if $f(s) = g(s)$ for all s in S. For example, f_1 defined above is equal to f_6, where

6. $f_6: \mathbb{R} \to \mathbb{R}$ is defined by $f_6(x) = (x+2)^2 - 3$.

The ordered pairs $(s, f(s))$ determined by a function $f: S \to T$ constitute a special kind of subset of $S \times T$: Each $s \in S$ appears in exactly one pair (s, t) of the subset and a given pair (s, t) of $S \times T$ belongs to the subset if and only if $t = f(s)$. As a consequence, a function $f: S \to T$ may alternatively be *defined* as any subset of $S \times T$ such that each $s \in S$ appears as the first element of precisely one pair of the subset. Then, given such a subset, the rule of assignment is simply this: "$f(s)$ is the element t of T associated with s in the pair (s, t) of the subset."

To illustrate, if $S=\{0, 1, 2, 3, 4, 5, 6\}$ and $T=\{0, 1, 2\}$, the subset

$$\{(0, 0), (1, 1), (2, 2), (3, 0), (4, 1), (5, 2), (6, 0)\}$$

defines a function $f\colon S\to T$. This function may also be described by the rule: "If $s=3q+r$, $0\leqslant r\leqslant 2$, then $f(s)=r$."

As we have pointed out before, one often has to answer the question "How many?" Thus if $|S|=m$, $|T|'=n$, how many functions f are there from S to T? For each of the m elements $s\in S$, we may choose any one of the n elements of T as $f(s)$, independently of the choices made for the other elements of S. Hence there are altogether $n\cdot n\cdot \cdots \cdot n=n^m$ functions from S to T. Because of this result, the set of all functions from S to T is often denoted by T^S, and we have proved the following theorem.

Theorem 1.5.1. *For finite sets S and T,*

$$|T^S|=|T|^{|S|}.$$

The basic counting principle used here is that if one of two independent tasks can be performed in p ways and the other in q ways, then the pair of tasks can be performed in pq ways.

1.6 Exercises

1. If $S=\{n\in\mathbb{Z}|1\leqslant n\leqslant 3\}$ and $T=\{n\in\mathbb{Z}|2\leqslant n\leqslant 5\}$, diagram $S\times T$ as a subset of the Cartesian plane.

2. For S and T as in Exercise 1, give a subset of $S\times T$ that does not represent a function.

3. Determine two sets such that the rectangle of Figure 1.6.1(a), including its boundaries, represents their Cartesian product. Then do the same for the rectangle of Figure 1.6.1(b), including only the two boldface boundaries.

4. If $S=\{3, 7, 21\}$, $T=\{11, 111, 10101\}$, under what conditions, if any, is $S=T$? Is indexing involved?

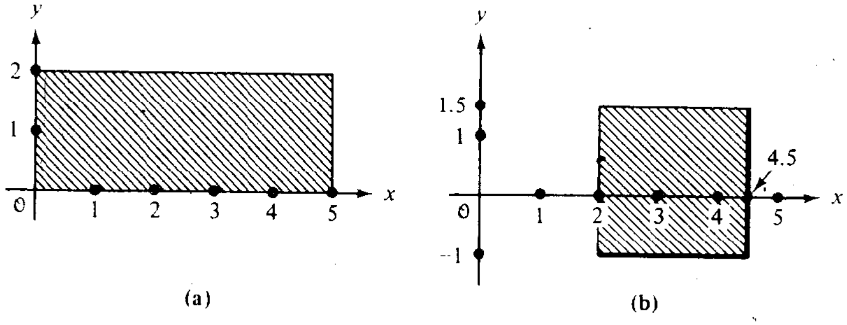


FIGURE 1.6.1. *Cartesian Products*

5. How would you index the seats in a largc rcctangular concert hall divided by a central aisle so that the index would readily identify the location of the seat? What is the indexing set in this case?

6. If $S=\{s_1, s_2, s_3\}$ and $T=\{t_1, t_2, t_3\}$, tabulate all the functions from S to T. Invent a way to index these functions such that the index identifies the function completely (that is, the index reveals the image of every $s \in S$).

7. Invent a function whose domain is a set of pairs of people and whose codomain is most appropriately $\mathbb{N}$.

8. Given $f: \mathbb{R}-\{0\} \rightarrow \mathbb{R}$ where $f(x)=\frac{1}{2}(x+2/x)$, what is the range of f? For what values of x is $f(x)=x$? (For any $f: A \rightarrow B$, the elements x such that $x \in A$, $x \in B$, and $f(x)=x$ are called the **fixed points** of f.)

***9.** The function $f: S \rightarrow S$, where $f(s)=s$ for all $s \in S$, is called the **identity function** on S. Describe the corresponding subset of $S \times S$. Show that for all functions $g: S \rightarrow S$, and for all $s \in S$, $f(g(s))=g(f(s))=g(s)$.

10. Let $A=\varnothing$, $B=\{\varnothing\}$, $C=\mathscr{P}(\varnothing)$, and $D=\mathscr{P}(\{\varnothing\})$. Are any of these sets equal? What are $|A|$, $|B|$, and $|C|$?

11. No two of $R \times S \times T$, $(R \times S) \times T$, and $R \times (S \times T)$ are equal. Explain.

***12.** Let U be a set with n elements. Determine, for each $k \in \mathbb{N}$ such that $0 \leqslant k \leqslant n$, the number of subsets S of U such that $|S|=k$. Then find the total number of subsets of U, including the empty set $\varnothing$ and the set U itself.

13. Let A be a finite set (alphabet) of m elements. Find the number of ordered n-tuples (code words) in the Cartesian product $A^n = A \times A \times \cdots \times A$. Use this result to show that the 26 letters of the English alphabet can be encoded using code words of length $\leqslant 4$ formed from the alphabet $\{\cdot, -\}$. Then look up Morse Code and the International Code in an encyclopedia to see the encodings that are actually used.

14. Consider a standard 8 × 8 chess board, regarded as a set of vertices in nine horizontal rows and nine vertical columns, joined by lines forming the edges of the 64 small squares. Let P denote the set of paths along the *lines* of the chess board from one vertex (the "lower left" vertex) to the diagonally opposite ("upper right") vertex. A path proceeds one step at a time, either one square to the right (H) or one square upward (V), and consists of eight horizontal moves H and eight vertical moves V. Determine $|P|$.

15. An ordered set of three positive integers (a, b, c) is a **Pythagorean triad** if and only if $a^2+b^2=c^2$. The most familiar such triad is $(3, 4, 5)$.

(a) A **primitive Pythagorean triad** is an ordered triple $(2mn, m^2-n^2, m^2+n^2)$, $m \in \mathbb{P}$, $n \in \mathbb{P}$, $0<n<m$. Show that any such triple is a Pythagorean triad.

(b) It is shown in number theory that any Pythagorean triad has form (ra_0, rb_0, rc_0) or (rb_0, ra_0, rc_0), where $r \in \mathbb{P}$ and (a_0, b_0, c_0) is a primitive Pythagorean triad. Write a program, in whatever computer language is available to you, that will produce all Pythagorean triads (a, b, c) with $c \leqslant 150$.

1.7 More Notation

In the following sections, we shall often have occasion to deal with **equivalent statements**, that is, statements which are both true or both false. We use the abbreviation "iff" for "if and only if." Then the theorem that statements P and Q are equivalent may be written "P iff Q." Proof of such a theorem always involves two parts: proof that P implies Q (written "$P \Rightarrow Q$") and proof that $Q \Rightarrow P$. This is reflected in the notation "$P \Leftrightarrow Q$," which means the same as "P iff Q." Informally, proof that $P \Rightarrow Q$ is called the "only if" part of the proof of "$P \Leftrightarrow Q$," and proof that $Q \Rightarrow P$ is called the "if" part.

A statement "P iff Q" may also be read "Q is a ***necessary and sufficient condition*** (abbreviated n.a.s.c. or n.s.c.) for P." Proof that $P \Rightarrow Q$ is proof of the necessity of the condition; in other words, for P to be true it is necessary that Q be true. Proof that $Q \Rightarrow P$ is proof of the sufficiency of the condition; that is, in order to conclude that P is true, it is sufficient to know that Q is true.

It is not uncommon that one of the two parts of an if-and-only-if theorem is obvious. In such a case, a simple remark may dispense with this half of the argument. The reader is warned against the common error of assuming that half of the proof may *always* be ignored. To the contrary, in many cases both parts of the proof require substantial arguments.

Many theorems apply to all the elements of a certain set. We use "$\forall$" to mean "for all." Thus "$\forall\, x \in X$" is read "for all x belonging to X" or "for each x belonging to X."

Some theorems, called **existence theorems**, assert the existence of certain objects. We use "$\exists$" to mean "there exists" and "$\exists!$" to mean "there exists a unique." The symbol "$\ni$" is used to mean "such that." Thus

$$\text{“}\exists!\, x \in \mathbb{R} \ni x^3 - 1 = 0\text{”}$$

means "there exists a unique real number x such that $x^3 - 1 = 0$."

1.8 One-to-One and Onto

A function $f\colon S \to T$ is said to be **one-to-one** (abbreviated one-one) iff for each $t \in T$ there exists at most one $s \in S$ such that $f(s) = t$; in other words, iff a given element of T has at most one counterimage in S. Equivalent definitions are that $f\colon S \to T$ is one-one iff $f(s_1) = f(s_2)$ implies that $s_1 = s_2$, or iff $s_1 \neq s_2$ implies that $f(s_1) \neq f(s_2)$.

For example, let $S = T = \mathbb{R}$ and consider $f\colon S \to T$ defined by $f(s) = t = as + b$, $a \neq 0$, a and b fixed real numbers. For each t, the unique s whose image is t is given by $s = (t - b)/a$. Also, if $as_1 + b = as_2 + b$, then $s_1 = s_2$ since $a \neq 0$. This example also illustrates the next definition.

A function $f\colon S \to T$ is **onto** iff for each $t \in T$ there exists at least one $s \in S$ such that $f(s) = t$; that is, f is onto iff every element of T has at least one counterimage in S. An equivalent definition is that $f\colon S \to T$ is onto iff the range of f is T, that is, if $f(S) = T$. We also say that f **maps** S **onto** T when the range of f is T. When the range of f is a proper subset of T, we say that f **maps** S **strictly into** T. If we do not require f to be onto or if we do not know whether or not it is onto, we say that f **maps** S **into** T. Thus "into" means "onto or strictly into."

A function $f: S \to T$ that is one-one is called an **injection**. A function $f: S \to T$ that is onto is called a **surjection**. A function $f: S \to T$ that is both one-one and onto is called a **bijection** or a **one-one correspondence**. In this case, each s has precisely one image t; because f is onto and one-one, each t has one and only one counterimage s; hence the name "correspondence."

In each of the following examples, the reader should verify that the function has the stated characteristics:

1. $f_1: \mathbb{R}^2 \to \mathbb{R}^2$, defined by $f_1((x, y)) = (x+y, x-y)$, is both one-one and onto, so it is a bijection.
2. $f_2: \mathbb{Z} \to \mathbb{Z}$, defined by $f_2(z) = z^2$, is neither one-one nor onto.
3. $f_3: \mathbb{P} \to \mathbb{P}$, defined by $f_3(n) = n^2$, is one-one but not onto (recall that $\mathbb{P} = \{\text{positive integers}\}$), so it is an injection.
4. $f_4: \mathbb{N} \to \{0, 1\}$, defined by $f_4(n) = 0$ when n is even, $f_4(n) = 1$ when n is odd, is onto but not one-one, o it is a surjection.

The several possibilities, for finite sets S and T, are illustrated in Figure 1.8.1.

If one considers functions $f: S \to T$, where S and T are finite, a variety of counting questions may be asked. For example, if $|S| = m$, $|T| = n$, how many one-one functions are there from S to T? For a one-one function to exist, we must have $n \geqslant m$ since $s_1 \neq s_2$ implies that $f(s_1) \neq f(s_2)$. If $n = m$, each $t \in T$ must be the image of precisely one $s \in S$. If $S = \{s_1, s_2, \ldots, s_m\}$, then there are $m = |T|$ choices for $f(s_1)$, $m-1 = |T - \{f(s_1)\}|$ choices for $f(s_2)$, $m-2 = |T - \{f(s_1), f(s_2)\}|$ choices for $f(s_3), \ldots$, so the number of one-one functions is, in this case, just $m! = m(m-1)(m-2)\cdots 1$. If $n > m$, we may select any m distinct elements from T, in any order, as images for the elements of S. Thus there are $n(n-1)\cdots(n-m+1) = n!/(n-m)!$ one-one functions in this case.

1.9 Composition and Inversion of Functions

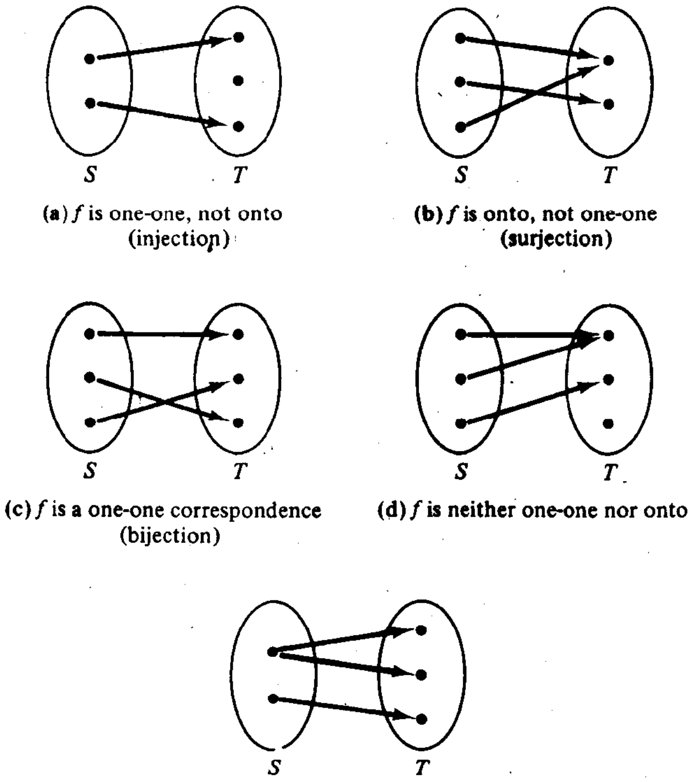
Let S, T, and U be sets and let $f: S \to T$ and $g: T \to U$ be functions. (Note that the codomain of f is the domain of g.) We define the **composite function** $g \circ f: S \to U$ (the **composite of** f **and** g, in that order) thus:

$$\forall s \in S, \qquad (g \circ f)(s) = g(f(s)).$$

Since this rule assigns to each $s \in S$ a unique $u \in U$, $g \circ f$ is indeed a function from S to U.

For example, if $S = T = U = \mathbf{R}$, $f(x) = x^2$, and $g(x) = x + 1$, then

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



(a) f is one-one, not onto (injection)

(b) f is onto, not one-one (surjection)

(c) f is a one-one correspondence (bijection)

(d) f is neither one-one nor onto

(e) Not a function

FIGURE 1.8.1. *Functions and a Nonfunction*

In general, $f \circ g$ need not be defined just because $g \circ f$ is. In this example, both are defined because S and U are the same set. We have, in fact,

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

which illustrates the fact that we need not have $f \circ g = g \circ f$, even though both are defined. Although the composition of functions is therefore not a commutative operation, we have the following theorem.

Theorem 1.9.1. *The composition of functions is associative.*

Proof. Let S, T, U, and V be sets and let $f: S \to T$, $g: T \to U$, and $h: U \to V$ be functions. Then the theorem says that

$$h \circ (g \circ f) = (h \circ g) \circ f. \tag{1.9.1}$$

Figure 1.9.1 shows what is happening: If $s \in S$, $f(s) = t$, $g(t) = u$, and $h(u) = v$, then $g \circ f$ maps s onto u via t and $h \circ g$ maps t onto v via u.

The proof follows from the definition of the operation of composition.