# PART I: Elementary Theory of Sets

# Chapter 1

## Sets and Basic Operations on Sets

### 1.1 INTRODUCTION

The concept of a *set* appears in all branches of mathematics. This concept formalizes the idea of grouping objects together and viewing them as a single entity. This chapter introduces this notion of a set and its members. We also investigate three basic operations on sets, that is, the operations union, intersection, and complement.

Although logic is formally treated in Chapter 10, we indicate here the close relationship between set theory and logic by showing how Venn diagrams, pictures of sets, can be used to determine the validity of certain arguments. The relation between set theory and logic will be further explored when we discuss Boolean algebra in Chapter 11.

### 1.2 SETS AND ELEMENTS

A *set* may be viewed as any well-defined collection of objects; the objects are called the *elements* or *members* of the set.

Although we shall study sets as abstract entities, we now list ten examples of sets:

(1) The numbers 1, 3, 7, and 10.
(2) The solutions of the equation $x^2 - 3x - 2 = 0$.
(3) The vowels of the English alphabet: a, e, i, o, u.
(4) The people living on the earth.
(5) The students Tom, Dick, and Harry.
(6) The students absent from school.
(7) The countries England, France, and Denmark.
(8) The capital cities of Europe.
(9) The even integers: 2, 4, 6, ....
(10) The rivers in the United States.

Observe that the sets in the odd-numbered examples are *defined*, that is, specified or presented, by actually listing its members; and the sets in the even-numbered examples are defined by stating properties or rules which decide whether or not a particular object is a member of the set.

**Notation**

A set will usually be denoted by a capital letter, such as,

$$A, B, X, Y, \ldots,$$

whereas lower-case letters, $a, b, c, x, y, z, \ldots$ will usually be used to denote elements of sets.

There are essentially two ways to specify a particular set, as indicated above. One way, if possible, is to list its elements. For example,

$$A = \{\text{a}, \text{e}, \text{i}, \text{o}, \text{u}\}$$

means that $A$ is the set whose elements are the letters a, e, i, o, u. Note that the elements are separated by commas and enclosed in braces { }. This is sometimes called the *tabular form* of a set.

The second way is to state those properties which characterize the elements in the set, that is, properties held by the members of the set but not by nonmembers. Consider, for example, the expression

$$B = \{x : x \text{ is an even integer}, x > 0\}$$

which reads:

"$B$ is the set of $x$ such that $x$ is an even integer and $x > 0$"

It denotes the set $B$ whose elements are the positive even integers. A letter, usually $x$, is used to denote a typical member of the set; the colon is read as "such that" and the comma as "and". This is sometimes called the *set-builder form* or *property method* of specifying a set.

Two sets $A$ and $B$ are *equal*, written $A = B$, if they both have the same elements, that is, if every element which belongs to $A$ also belongs to $B$, and vice versa. The negation of $A = B$ is written $A \neq B$.

The statement "$p$ is an element of $A$" or, equivalently, the statement "$p$ belongs to $A$" is written

$$p \in A$$

We also write

$$a, b \in A$$

to state that both $a$ and $b$ belong to $A$. The statement that $p$ is not an element of $A$, that is, the negation of $p \in A$, is written

$$p \notin A$$

**Remark**: It is common practice in mathematics to put a vertical line "|" or slanted line "/" through a symbol to indicate the opposite or negative meaning of the symbol.

**EXAMPLE 1.1**

(*a*) The set $A$ above can also be written as

$$A = \{x : x \text{ is a letter in the English alphabet}, x \text{ is a vowel}\}$$

Observe that $b \notin A$, $e \in A$, and $p \notin$ A.

(*b*) We cannot list all the elements of the above set $B$, although we frequently specify the set by writing

$$B = \{2, 4, 6, \dots\}$$

where we assume everyone knows what we mean. Observe that $8 \in B$, but $9 \notin B$.

(*c*) Let $E = \{x : x^2 - 3x + 2 = 0\}$. In other words, $E$ consists of those numbers which are solutions of the equation $x^2 - 3x + 2 = 0$, sometimes called the *solution set* of the given equation. Since the solutions are 1 and 2, we could also write $E = \{1, 2\}$.

(*d*) Let $E = \{x : x^2 - 3x + 2 = 0\}$, $F = \{2, 1\}$, and $G = \{1, 2, 2, 1, 6/3\}$. Then $E = F = G$ since each consists precisely of the elements 1 and 2. Observe that a set does not depend on the way in which its elements are displayed. A set remains the same even if its elements are repeated or rearranged.

Some sets of numbers will occur very often in the text, and so we use special symbols for them. Unless otherwise specified, we will let:

$\mathbf{N}$ = the set of nonnegative integers: $0, 1, 2, \dots$

$\mathbf{P}$ = the set of positive integers: $1, 2, 3, \dots$

$\mathbf{Z}$ = the set of integers: $\dots, -2, -1, 0, 1, 2, \dots$

$\mathbf{Q}$ = the set of rational numbers

$\mathbf{R}$ = the set of real numbers

$\mathbf{C}$ = the set of complex numbers

Even if we can list the elements of a set, it may not be practical to do so. For example, we would not list the members of the set of people born in the world during the year 1976 although theoretically it is possible to compile such a list. That is, we describe a set by listing its elements only if the set contains a few elements; otherwise we describe a set by the property which characterizes its elements.

## 1.3 UNIVERSAL SET, EMPTY SET

All sets under investigation in any application of set theory are assumed to be contained in some large fixed set called the *universal set* or *universe*. For example, in plane geometry, the universal set consists of all the points in the plane, and in human population studies the universal set consists of all the people in the world. We will denote the universal set by

$$\mathbf{U}$$

unless otherwise specified.

Given a universal set $\mathbf{U}$ and a property $P$, there may be no element in $\mathbf{U}$ which has the property $P$. For example, the set

$$S = \{x : x \text{ is a positive integer, } x^2 = 3\}$$

has no elements since no positive integer has the required property. This set with no elements is called the *empty set* or *null set*, and is denoted by

$$\varnothing$$

(based on the Greek letter phi). There is only one empty set: If $S$ and $T$ are both empty, then $S = T$ since they have exactly the same elements, namely, none.

## 1.4 SUBSETS

Suppose every element in a set $A$ is also an element of a set $B$; then $A$ is called a *subset* of $B$. We also say that $A$ is *contained* in $B$ or $B$ *contains* $A$. This relationship is written

$$A \subseteq B \quad \text{or} \quad B \supseteq A$$

If $A$ is not a subset of $B$, that is, if at least one element of $A$ does not belong to $B$, we write $A \not\subseteq B$ or $B \not\supseteq A$.

**EXAMPLE 1.2**

(*a*) Consider the sets

$$A = \{1, 3, 5, 8, 9\}, \qquad B = \{1, 2, 3, 5, 7\}, \qquad C = \{1, 5\}$$

Then $C \subseteq A$ and $C \subseteq B$ since 1 and 5, the elements of $C$, are also elements of $A$ and $B$. But $B \not\subseteq A$ since some of its elements, e.g., 2 and 7, do not belong to $A$. Furthermore, since the elements in the sets $A, B, C$ must also belong to the universal set $\mathbf{U}$, it is clear that $\mathbf{U}$ must at least contain the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(*b*) Let $\mathbf{P}, \mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ be defined as in Section 1.2. Then:

$$\mathbf{P} \subseteq \mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

(*c*) The set $E = \{2, 4, 6\}$ is a subset of the set $F = \{6, 2, 4\}$, since each number 2, 4, and 6 belonging to $E$ also belongs to $F$. In fact, $E = F$. Similarly, it can be shown that every set is a subset of itself.

The following properties of sets should be noted:

(i) Every set $A$ is a subset of the universal set $\mathbf{U}$ since, by definition, all the elements of $A$ belong to $\mathbf{U}$. Also the empty set $\varnothing$ is a subset of $A$.

(ii) Every set $A$ is a subset of itself since, trivially, the elements of $A$ belong to $A$.

(iii) If every element of $A$ belongs to a set $B$, and every element of $B$ belongs to a set $C$, then clearly every element of $A$ belongs to $C$. In other words, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(iv) If $A \subseteq B$ and $B \subseteq A$, then $A$ and $B$ have the same elements, i.e., $A = B$. Conversely, if $A = B$ then $A \subseteq B$ and $B \subseteq A$ since every set is a subset of itself.

We state these results formally.

**Theorem 1.1:** (i) For any set $A$, we have $\varnothing \subseteq A \subseteq \mathbf{U}$.
(ii) For any set $A$, we have $A \subseteq A$.
(iii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
(iv) $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

**Proper Subset**

If $A \subseteq B$, then it is still possible that $A = B$. When $A \subseteq B$ but $A \neq B$, we say that $A$ is a *proper subset* of $B$. We will write $A \subset B$ when $A$ is a proper subset of $B$. For example, suppose

$$A = \{1, 3\}, \qquad B = \{1, 2, 3\}, \qquad C = \{1, 3, 2\}$$

Then $A$ and $B$ are both subsets of $C$; but $A$ is a proper subset of $C$, whereas $B$ is not a proper subset of $C$.

**Disjoint Sets**

Two sets $A$ and $B$ are disjoint if they have no elements in common. For example, suppose

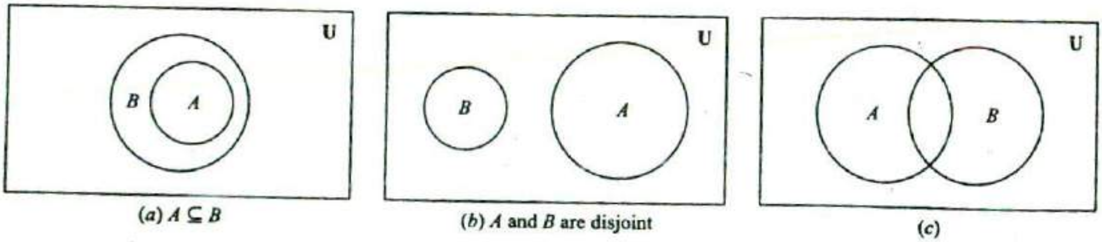
$$A = \{1, 2\}, \qquad B = \{2, 4, 6\}, \qquad C = \{4, 5, 6, 7\}$$

Note that $A$ and $B$ are not disjoint since they both contain the element 2. Similarly, $B$ and $C$ are not disjoint since they both contain the element 4, among others. On the other hand, $A$ and $C$ are disjoint since they have no element in common. We note that if two sets $A$ and $B$ are disjoint sets then neither is a subset of the other (unless one is the empty set).

## 1.5 VENN DIAGRAMS

A Venn diagram is a pictorial representation of sets where sets are represented by enclosed areas in the plane. The universal set $\mathbf{U}$ is represented by the points in a rectangle, and the other sets are represented by disks lying within the rectangle. If $A \subseteq B$, then the disk representing $A$ will be entirely within the disk representing $B$, as in Fig. 1-1($a$). If $A$ and $B$ are disjoint, i.e., have no elements in common, then the disk representing $A$ will be separated from the disk representing $B$, as in Fig. 1-1($b$).

On the other hand, if $A$ and $B$ are two arbitrary sets, it is possible that some elements are in $A$ but not $B$, some elements are in $B$ but not $A$, some are in both $A$ and $B$, and some are in neither $A$ nor $B$; hence, in general, we represent $A$ and $B$ as in Fig. 1-1($c$).



($a$) $A \subseteq B$ ($b$) $A$ and $B$ are disjoint ($c$)

Fig. 1-1

## 1.6 SET OPERATIONS

The reader has learned to add, subtract, and multiply in the ordinary arithmetic of numbers; that is, to each pair of numbers $a$ and $b$, we assign a number $a+b$ called the *sum* of $a$ and $b$, a number $a-b$ called the *difference* of $a$ and $b$, and a number $ab$ called the *product* of $a$ and $b$. These assignments are called the operations of addition, subtraction, and multiplication of numbers. This section defines a number of set operations, including the basic operations of union, intersection, and difference of sets, where new sets will be assigned to pairs of sets $A$ and $B$. We will see that set operations have many properties similar to the above operations on numbers.

### Union and Intersection

The *union* of two sets $A$ and $B$, denoted by $A \cup B$, is the set of all elements which belong to $A$ or $B$; that is,

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

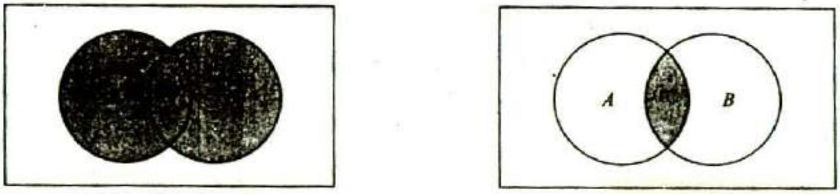
Here "or" is used in the sense of and/or. Figure 1-2($a$) is a Venn diagram in which $A \cup B$ is shaded.

The *intersection* of two sets $A$ and $B$, denoted by $A \cap B$, is the set of all elements which belong to both $A$ and $B$; that is,

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

Figure 1-2($b$) is a Venn diagram in which $A \cap B$ is shaded.

Recall that sets $A$ and $B$ are said to be disjoint if they have no elements in common. Accordingly, using the above notation, $A$ and $B$ are disjoint if $A \cap B = \varnothing$, the empty set.



**($a$) $A \cup B$ is shaded** **($b$) $A \cap B$ is shaded**

**Fig. 1-2**

**EXAMPLE 1.3**

($a$) Let $A = \{1,2,3,4\}$, $B = \{3,4,5,6,7\}$, $C = \{2,3,8,9\}$. Then

$$\begin{aligned} A \cup B &= \{1,2,3,4,5,6,7\}, & A \cap B &= \{3,4\} \\ A \cup C &= \{1,2,3,4,8,9\}, & A \cap C &= \{2,3\} \\ B \cup C &= \{2,3,4,5,6,7,8,9\}, & B \cap C &= \{3\} \end{aligned}$$

($b$) Let $\mathbf{U}$ denote the set of students at a university, and let $M$ and $F$ denote, respectively, the set of male and female students at the university. Then

$$M \cup F = \mathbf{U}$$

since each student in $\mathbf{U}$ is either in $M$ or in $F$. On the other hand,

$$M \cap F = \varnothing$$

since no student belongs to both $M$ and $F$.

The following properties of the union and intersection of sets should be noted:

(i) Every element $x$ in $A \cap B$ belongs to both $A$ and $B$; hence $x$ belongs to $A$ and $x$ belongs to $B$. Thus $A \cap B$ is a subset of $A$ and of $B$, that is,

$$A \cap B \subseteq A \quad \text{and} \quad A \cap B \subseteq B$$

(ii) An element $x$ belongs to the union $A \cup B$ if $x$ belongs to $A$ or $x$ belongs to $B$; hence every element in $A$ belongs to $A \cup B$, and also every element in $B$ belongs to $A \cup B$. That is,

$$A \subseteq A \cup B \quad \text{and} \quad B \subseteq A \cup B$$

We state the above results formally.

**Theorem 1.2:** For any sets $A$ and $B$, we have

$$A \cap B \subseteq A \subseteq A \cup B \quad \text{and} \quad A \cap B \subseteq B \subseteq A \cup B$$

The operation of set inclusion is also closely related to the operations of union and intersection, as shown by the following theorem, proved in Problem 1.13.

**Theorem 1.3:** The following are equivalent:

$$A \subseteq B, \qquad A \cap B = A, \qquad A \cup B = B$$

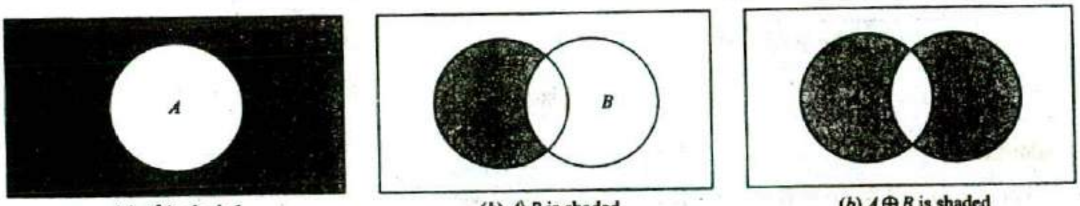
Other conditions equivalent to $A \subseteq B$ are given in Problem 1.51.

### Complement

Recall that all sets under consideration at a particular time are subsets of a fixed universal set **U**. The *absolute complement*, or, simply, *complement* of a set $A$, denoted by $A^c$, is the set of elements which belong to **U** but which do not belong to $A$; that is,

$$A^c = \{x : x \in \mathbf{U}, x \notin A\}$$

Some texts denote the complement of $A$ by $A'$ or $\bar{A}$. Figure 1-3($a$) is a Venn diagram in which $A^c$ is shaded.



($a$) $A^c$ is shaded ($b$) $A \backslash B$ is shaded ($b$) $A \oplus B$ is shaded

Fig. 1-3

**EXAMPLE 1.4**

($a$) Let $\mathbf{U} = \{a, b, c, \ldots, y, z\}$, the English alphabet, be the universal set, and let

$$A = \{\mathrm{a, b, c, d, e}\}, \qquad B = \{\mathrm{e, f, g}\}, \qquad V = \{\mathrm{a, e, i, o, u}\}$$

Then

$$A^c = \{\mathrm{f, g, h}, \ldots, \mathrm{y, z}\} \quad \text{and} \quad B^c = \{\mathrm{a, b, c, d, h, i}, \ldots, \mathrm{y, z}\}$$

Since $V$ consists of the vowels in **U**, $V^c$ consists of the nonvowels, called consonants.

($b$) Suppose the set **R** of real numbers is the universal set. Recall that **Q** denotes the set of rational numbers. Hence $\mathbf{Q}^c$ will denote the set of irrational numbers.

(c) Let U be the set of students at a university, and suppose $M$ and $F$ denote, respectively, the male and female students in U. Then

$$M^c = F \quad \text{and} \quad F^c = M$$

**Difference and Symmetric Difference**

Let $A$ and $B$ be sets. The *relative complement* of $B$ with respect to $A$ or, simply, the *difference* of $A$ and $B$, denoted by $A\backslash B$, is the set of elements which belong to $A$ but which do not belong to $B$; that is,

$$A\backslash B = \{x : x \in A, x \notin B\}$$

The set $A\backslash B$ is read "$A$ minus $B$". Many texts denote $A\backslash B$ by $A - B$ or $A \sim B$. Figure 1-3(b) is a Venn diagram in which $A\backslash B$ is shaded.

The *symmetric difference* of the sets $A$ and $B$, denoted by $A \oplus B$, consists of those elements which belong to $A$ or $B$ but not to both $A$ and $B$. That is,

$$A \oplus B = (A \cup B)\backslash(A \cap B) \quad \text{or} \quad A \oplus B = (A\backslash B) \cup (B\backslash A)$$

Figure 1-3(c) is a Venn diagram in which $A \oplus B$ is shaded. The fact that

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

is proved in Problem 1.18.

**EXAMPLE 1.5** Consider the sets

$$A = \{1, 2, 3, 4\}, \qquad B = \{3, 4, 5, 6, 7\}, \qquad C = \{6, 7, 8, 9\}$$

Then

$$A\backslash B = \{1, 2\}, \qquad B\backslash C = \{3, 4, 5\}, \qquad B\backslash A = \{5, 6, 7\}, \qquad C\backslash B = \{8, 9\}$$

Also,

$$A \oplus B = \{1, 2, 5, 6, 7\} \quad \text{and} \quad B \oplus C = \{3, 4, 5, 8, 9\}$$

Note that $A$ and $C$ are disjoint. This means

$$A\backslash C = A, \qquad C\backslash A = C, \qquad A \oplus C = A \cup C$$

## 1.7 ALGEBRA OF SETS, DUALITY

Sets under the above operations of union, intersection, and complement satisfy various laws (identities) which are listed in Table 1-1. In fact, we formally state:

**Theorem 1.4:** Sets satisfy the laws in Table 1-1.

Each of the laws in Table 1-1 follows from an equivalent logical law. Consider, for example, the proof of DeMorgan's law:

$$(A \cup B)^c = \{x : x \notin (A \text{ or } B)\} = \{x : x \notin A \text{ and } x \notin B\} = A^c \cap B^c$$

Here we use the equivalent (DeMorgan's) logical law:

$$\neg (p \vee q) \equiv \neg p \wedge \neg q$$

Here $\neg$ means "not", $\vee$ means "or", and $\wedge$ means "and". Sometimes Venn diagrams are used to illustrate the laws in Table 1-1 (cf. Problem 1.16).

**Table 1-1 Laws of the Algebra of Sets**

| | |
|---|---|
| **Idempotent laws** | |
| (1*a*) $A \cup A = A$ | (1*b*) $A \cap A = A$ |
| **Associative laws** | |
| (2*a*) $(A \cup B) \cup C = A \cup (B \cup C)$ | (2*b*) $(A \cap B) \cap C = A \cap (B \cap C)$ |
| **Commutative laws** | |
| (3*a*) $A \cup B = B \cup A$ | (3*b*) $A \cap B = B \cap A$ |
| **Distributive laws** | |
| (4*a*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ | (4*b*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ |
| **Identity laws** | |
| (5*a*) $A \cup \varnothing = A$ | (5*b*) $A \cap \mathbf{U} = A$ |
| (6*a*) $A \cup \mathbf{U} = \mathbf{U}$ | (6*b*) $A \cap \varnothing = \varnothing$ |
| **Involution law** | |
| (7) $(A^c)^c = A$ | |
| **Complement laws** | |
| (8*a*) $A \cup A^c = \mathbf{U}$ | (8*b*) $A \cap A^c = \varnothing$ |
| (9*a*) $\mathbf{U}^c = \varnothing$ | (9*b*) $\varnothing^c = \mathbf{U}$ |
| **DeMorgan's laws** | |
| (10*a*) $(A \cup B)^c = A^c \cap B^c$ | (10*b*) $(A \cap B)^c = A^c \cup B^c$ |

### Duality

The identities in Table 1-1 are arranged in pairs, as, for example, (2*a*) and (2*b*). We now consider the principle behind this arrangement. Let $E$ be an equation of set algebra. The *dual* $E^*$ of $E$ is the equation obtained by replacing each occurrence of $\cup, \cap, \mathbf{U}, \varnothing$ in $E$ by $\cap, \cup, \varnothing, \mathbf{U}$, respectively. For example, the dual of

$$(\mathbf{U} \cap A) \cup (B \cap A) = A \quad \text{is} \quad (\varnothing \cup A) \cap (B \cup A) = A$$

Observe that the pairs of laws in Table 1-1 are duals of each other. It is a fact of set algebra, called the *principle of duality*, that, if any equation $E$ is an identity, then its dual $E^*$ is also an identity.

## 1.8 FINITE SETS, COUNTING PRINCIPLES

A set is said to be *finite* if it contains exactly $m$ distinct elements where $m$ denotes some nonnegative integer. Otherwise a set is said to be infinite. For example, the empty set $\varnothing$ and the set of letters of the English alphabet are finite sets, whereas the set of even positive integers $\{2, 4, 6, \ldots\}$ is infinite. [Infinite sets will be studied in detail in Chapter 6.]

The notation $n(A)$ or $|A|$ will denote the number of elements in a finite set $A$.

First we begin with a special case.

**Lemma 1.5**: Suppose $A$ and $B$ are finite disjoint sets. Then $A \cup B$ is finite and

$$n(A \cup B) = n(A) + n(B)$$

*Proof.* In counting the elements of $A \cup B$, first count those that are in $A$. There are $n(A)$ of these. The only other elements of $A \cup B$ are those that are in $B$ but not in $A$. Since $A$ and $B$ are disjoint, no element of $B$ is in $A$, so there are $n(B)$ elements that are in $B$ but not in $A$. Therefore, $n(A \cup B) = n(A) + n(B)$, as claimed.

**Remark:** A set $C$ is called the *disjoint union* of $A$ and $B$ if

$$C = A \cup B \qquad \text{and} \qquad A \cap B = \varnothing$$

Lemma 1.5 tells us that, in such a case, $n(C) = n(A) + n(B)$.

### Special Cases of Disjoint Unions

There are two special cases of disjoint unions which occur frequently.

(1) Given any set $A$, then the universal set $U$ is the disjoint union of $A$ and its complement $A^c$. Thus, by Lemma 1.5,

$$n(U) = n(A) + n(A^c)$$

Accordingly, bringing $n(A)$ to the other side, we obtain the following useful result.

**Theorem 1.6**: Let $A$ be any set in a finite universal set $U$. Then

$$\boxed{n(A^c) = n(U) - n(A)}$$

For example, if there are 20 male students in a class of 35 students, then there are $35 - 20 = 15$ female students.

(2) Given any sets $A$ and $B$, we show (Problem 1.37) that $A$ is the disjoint union of $A \backslash B$ and $A \cap B$. This is pictured in Fig. 1-4. Thus Lemma 1.5 gives us the following useful result.

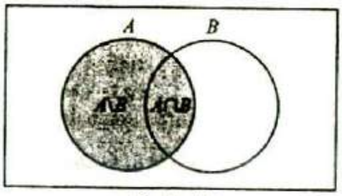
**Theorem 1.7**: Suppose $A$ and $B$ are finite sets. Then

$$\boxed{n(A \backslash B) = n(A) - n(A \cap B)}$$

For example, suppose an archery class $A$ contains 35 students, and 15 of them are also in a bowling class $B$. Then

$$n(A \backslash B) = n(A) - n(A \cap B) = 35 - 15 = 20$$

That is, there are 20 students in the class $A$ who are not in class $B$.



*A* is shaded

Fig. 1-4

### Inclusion-Exclusion Principle

There is also a formula for $n(A \cup B)$ even when they are not disjoint, called the *inclusion-exclusion principle*. Namely:

**Theorem 1.8**: Suppose $A$ and $B$ are finite sets. Then $A \cap B$ and $A \cup B$ are finite, and

$$\boxed{n(A \cup B) = n(A) + n(B) - n(A \cap B)}$$

That is, we find the number of elements in $A$ or $B$ (or both) by first adding $n(A)$ and $n(B)$ (inclusion) and then subtracting $n(A \cap B)$ (exclusion) since the elements in $A \cap B$ were counted twice.

We can apply this result to get a similar result for three sets.

**Corollary 1.9**: Suppose $A, B, C$ are finite sets. Then $A \cup B \cup C$ is finite and

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Mathematical induction (Section 1.11) may be used to further generalize this result to any finite number of finite sets.

**EXAMPLE 1.6** Consider the following data among 110 students in a college dormitory:

30 students are on a list A (taking Accounting),
35 students are on a list B (taking Biology),
20 students are on both lists.

Find the number of students: (*a*) on list or $B$, (*b*) on exactly one of the two lists, (*c*) on neither list.

(*a*) We seek $n(A \cup B)$. By Theorem 1.8,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) = 30 + 35 - 20 = 45$$

In other words, we combine the two lists and then cross out the 20 student names which appear twice.

(*b*) List $A$ contains 30 names and 20 of them are on list $B$; hence $30 - 20 = 10$ names are only on list $A$. That is,

$$n(A \backslash B) = n(A) - n(A \cup B) = 30 - 20 = 10$$

Similarly, list $B$ contains 35 names and 20 of them are on list A; hence $35 - 20 = 15$ names are only on list B. That is,

$$n(B \backslash A) = n(B) - n(A \cup B) = 35 - 20 = 15$$

Thus there are $10 + 15 = 25$ students on exactly one of the two lists.

(*c*) The students on neither the $A$ list nor the $B$ list form the set $A^c \cap B^c$. By DeMorgan's law, $A^c \cap B^c = (A \cup B)^c$. Hence

$$n(A^c \cap B^c) = n((A \cup B)^c) = n(U) - n(A \cup B) = 110 - 45 = 65$$

**EXAMPLE 1.7** Consider the following data for 120 mathematics students:

65 study French,
45 study German,
42 study Russian,
20 study French and German,
25 study French and Russian,
15 study German and Russian,
8 study all three languages

Let $F$, $G$, and $R$ denote the sets of students studying French, German, and Russian, respectively.

(*a*) Find the number of students studying at least one of the three languages, i.e. find $n(F \cup G \cup R)$.

(*b*) Fill in the correct number of students in each of the eight regions of the Venn diagram of Fig. 1-5(*a*).

(*c*) Find the number $k$ of students studying: (1) exactly one language, (2) exactly two languages.

(*a*) By Corollary 1.9,

$$\begin{aligned} n(F \cup G \cup R) &= n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) - n(F \cap G \cap R) \\ &= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100 \end{aligned}$$

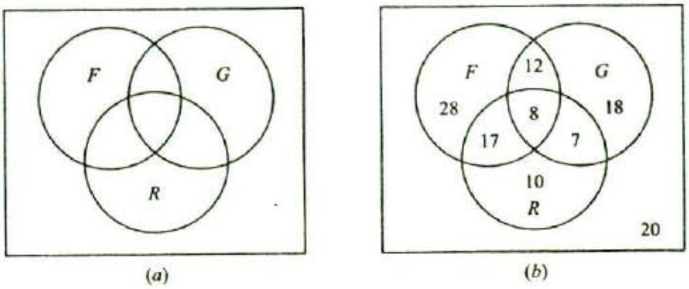


Fig. 1-5

(b) Using 8 study all three languages and 100 study at least one language, the remaining seven regions of the required Venn diagram Fig. 1-5(b) are obtained as follows:

$15 - 8 = 7$ study German and Russian but not French,
$25 - 8 = 17$ study French and Russian but not German,
$20 - 8 = 12$ study French and German but not Russian,
$42 - 17 - 8 - 7 = 10$ study only Russian,
$45 - 12 - 8 - 7 = 18$ study only German,
$65 - 12 - 8 - 17 = 28$ study only French,
$120 - 100 = 20$ do not study any of the languages.

(c) Use the Venn diagram of Fig. 1-5(b) to obtain:

(1) $k = 28 + 18 + 10 = 56$, (2) $k = 12 + 17 + 7 = 36$

## 1.9 CLASSES OF SETS, POWER SETS

Given a set $S$, we may wish to talk about some of its subsets. Thus we would be considering a "set of sets". Whenever such a situation arises, to avoid confusion, we will speak of a *class* of sets or a *collection* of sets. If we wish to consider some of the sets in a given class of sets, then we will use the term *subclass* or *subcollection*.

**EXAMPLE 1.8** Suppose $S = \{1, 2, 3, 4\}$. Let $\mathscr{A}$ be the class of subsets of $S$ which contain exactly three elements of $S$. Then

$$\mathscr{A} = [\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}]$$

The elements of $\mathscr{A}$ are the sets $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$, and $\{2,3,4\}$.

Let $\mathscr{B}$ be the class of subsets of $S$ which contain 2 and two other elements of $S$. Then

$$\mathscr{B} = [\{1,2,3\}, \{1,2,4\}, \{2,3,4\}]$$

The elements of $\mathscr{B}$ are $\{1,2,3\}$; $\{1,2,4\}$, and $\{2,3,4\}$. Thus $\mathscr{B}$ is a subclass of $\mathscr{A}$. (To avoid confusion, we will usually enclose the sets of a class in brackets instead of braces.)

### Power Sets

For a given set $S$, we may speak about the class of all subsets of $S$. This class is called the *power set* of $S$, and it will be denoted by $\mathscr{P}(S)$. If $S$ is finite, then so is $\mathscr{P}(S)$. In fact, the number of elements in $\mathscr{P}(S)$ is 2 raised to the power of $n(S)$; that is,

$$n(\mathscr{P}(S)) = 2^{n(S)}$$

(This is the reason $\mathscr{P}(S)$ is called the power set of $S$; it is also sometimes denoted by $2^S$.)

**EXAMPLE 1.9** Suppose $S = \{1, 2, 3\}$. Then

$$\mathcal{P}(S) = [\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, S]$$

Note that the empty set $\varnothing$ belongs to $\mathcal{P}(S)$ since $\varnothing$ is a subset of $S$. Similarly $S$ belongs to $\mathcal{P}(S)$. As expected from the above remark, $\mathcal{P}(S)$ has $2^3 = 8$ elements.

## 1.10 ARGUMENTS AND VENN DIAGRAMS

Many verbal statements are essentially statements about sets and they can therefore be described by Venn diagrams. Hence Venn diagrams can sometimes be used to determine whether or not an argument is valid. This is illustrated in the following example.

**EXAMPLE 1.10** Show that the following argument (adapted from a book on logic by Lewis Carroll, the author of *Alice in Wonderland*) is valid:

$S_1$: My saucepans are the only things I have that are made of tin.
$S_2$: I find all your presents very useful.
$S_3$: None of my saucepans is of the slightest use.

---

$S$: Your presents to me are not made of tin.

(The statements $S_1$, $S_2$, and $S_3$ above the horizontal line denote the assumptions, and the statement $S$ below the line denotes the conclusion. The argument is valid if the conclusion $S$ follows logically from the assumptions $S_1$, $S_2$, and $S_3$.)

By $S_1$ the tin objects are contained in the set of saucepans and by $S_3$ the set of saucepans and the set of useful things are disjoint: hence draw the Venn diagram of Fig. 1-6.

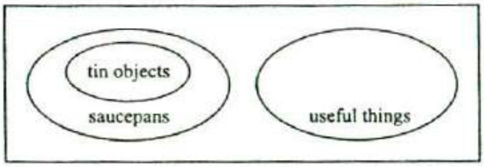


Fig. 1-6

By $S_2$ the set of "your presents" is a subset of the set of useful things; hence draw Fig. 1-7.

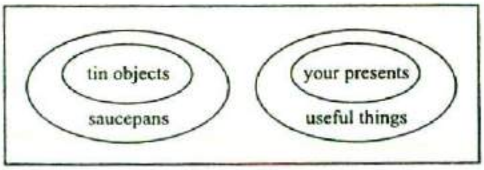


Fig. 1-7

The conclusion is clearly valid by the Venn diagram in Fig. 1-7 because the set of "your presents" is disjoint from the set of tin objects.

## 1.11 MATHEMATICAL INDUCTION

Consider the set $\mathbf{P} = \{1, 2, \ldots\}$ of positive integers (or counting numbers). We say that an assertion $A(n)$ is defined on $\mathbf{P}$ if $A(n)$ is true or false for each $n \in \mathbf{P}$. An essential property of $\mathbf{P}$, which is used in many proofs, follows.

**Principle of Mathematical Induction I**: Let $A(n)$ be an assertion defined on $\mathbf{P}$, that is, $A(n)$ is true or false for each integer $n \geq 1$. Suppose $A(n)$ has the following two properties:

(1) $A(1)$ is true.
(2) $A(n+1)$ is true whenever $A(n)$ is true.

Then $A(n)$ is true for every $n \geq 1$.

We shall not prove this principle. In fact, this principle is usually given as one of the axioms when $\mathbf{P}$ is developed axiomatically.

**EXAMPLE 1.11** Let $A(n)$ be the assertion that the sum of the first $n$ odd integers is $n^2$; that is,

$$A(n): \quad 1 + 3 + 5 + \cdots + (2n-1) = n^2$$

[The $n$th odd integer is $2n - 1$ and the next odd integer is $2n + 1$.] Observe that $A(n)$ is true for $n = 1$, that is,

$$A(1): \quad 1 = 1^2$$

Assuming $A(n)$ is true, we add $2n + 1$ to both sides of $A(n)$, obtaining:

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1) = n^2 + (2n+1) = (n+1)^2$$

However, this is $A(n+1)$. That is, $A(n+1)$ is true whenever $A(n)$ is true. By the principle of mathematical induction, $A(n)$ is true for all $n \geq 1$.

There is another form of the principle of mathematical induction which is sometimes more convenient to use. Although it appears different, it is really equivalent to the above principle of induction.

**Principle of Mathematical Induction II**: Let $A(n)$ be an assertion defined on the set $\mathbf{P}$ of positive integers which satisfies the following two conditions:

(1) $A(1)$ is true.
(2) $A(n)$ is true whenever $A(k)$ is true for $1 \leq k < n$.

Then $A(n)$ is true for every $n \geq 1$.

The above two principles may also be stated in terms of subsets of $\mathbf{P}$ rather than in terms of assertions defined on $\mathbf{P}$. (See Problem 1.40.) Although the languages are different, they are logically equivalent.

**Remark**: Sometimes one wants to prove that an assertion $A$ is true for a set of integers of the form

$$\{a, a+1, a+2, \ldots\}$$

where $a$ is any integer, possibly 0. This can be done by simply replacing 1 by the integer $a$ in either of the above principles of mathematical induction.

## 1.12 AXIOMATIC DEVELOPMENT OF SET THEORY

Any axiomatic development of a branch of mathematics begins with the following:

(1) undefined terms,
(2) undefined relations,
(3) axioms relating the undefined terms and undefined relations.

Then, one develops theorems based upon the axioms and definitions.

Consider, for example, the axiomatic development of plane Euclidean geometry. It begins with the following:

(1) "points" and "lines" are undefined terms;
(2) "point on a line" or, equivalently, "line contains a point" is an undefined relation.

Two of the many axioms of Euclidean geometry follow:

**Axiom 1**: Two distinct points are on one and only one line.

**Axiom 2**: Two distinct lines cannot contain more than one point in common.

The axiomatic development of set theory begins with the following:

(1) "element" and "set" are undefined terms;
(2) "element belongs to a set" is the undefined relation.

Two of the axioms (called principles) of set theory follow:

**Principle of Extension**: Two sets $A$ and $B$ are equal if and only if they have the same elements, that is, if every element in $A$ belongs to $B$ and every element in $B$ belongs to $A$.

**Principle of Abstraction**: Given any set $\mathbf{U}$ and any property $P$, there is a set $A$ such that the elements of $A$ are exactly those elements in $\mathbf{U}$ which have the property $P$; that is,

$$A = \{x : x \in \mathbf{U}, P(x) \text{ is true}\}$$

There are other axioms which are not listed. As our treatment of set theory is mainly intuitive, especially Part I, we will refrain from any further discussion of the axiomatic development of set theory.

## Solved Problems

### SETS AND SUBSETS

**1.1.** Which of these sets are equal: $\{r, t, s\}$, $\{s, t, r, s\}$, $\{t, s, t, r\}$, $\{s, r, s, t\}$?

They are all equal. Order and repetition do not change a set.

**1.2.** List the elements of the following sets where $\mathbf{P} = \{1, 2, 3, \ldots\}$.

(*a*) $A = \{x : x \in \mathbf{P},\ 3 < x < 12\}$
(*b*) $B = \{x : x \in \mathbf{P},\ x \text{ is even},\ x < 15\}$
(*c*) $C = \{x : x \in \mathbf{P},\ 4 + x = 3\}$
(*d*) $D = \{x : x \in \mathbf{P},\ x \text{ is a multiple of } 5\}$.

(*a*) A consists of the positive integers between 3 and 12; hence

$$A = \{4, 5, 6, 7, 8, 9, 10, 11\}$$

(*b*) $B$ consists of the even positive integers less than 15; hence

$$B = \{2, 4, 6, 8, 10, 12, 14\}$$

(*c*) There are no positive integers which satisfy the condition $4 + x = 3$; hence $C$ contains no elements. In other words, $C = \varnothing$, the empty set.

(*d*) $D$ is infinite, so we cannot list all its elements. However, sometimes we write

$$D = \{5, 10, 15, \ldots, 5n, \ldots\} \qquad \text{or simply} \qquad D = \{5, 10, 15, \ldots\}$$

where we assume everyone understands that we mean the multiples of 5.

**1.3.** Consider the following sets:

$$\varnothing, \quad A = \{1\}, \quad B = \{1, 3\}, \quad C = \{1, 5, 9\}, \quad D = \{1, 2, 3, 4, 5\},$$
$$E = \{1, 3, 5, 7, 9\}, \quad \mathbf{U} = \{1, 2, \ldots, 8, 9\}$$

Insert the correct symbol $\subseteq$ or $\nsubseteq$ between each pair of sets:

(*a*) $\varnothing, A$ (*c*) $B, C$ (*e*) $C, D$ (*g*) $D, E$
(*b*) $A, B$ (*d*) $B, E$ (*f*) $C, E$ (*h*) $D, \mathbf{U}$

(*a*) $\varnothing \subseteq A$ because $\varnothing$ is a subset of every set.
(*b*) $A \subseteq B$ because 1 is the only element of $A$ and it belongs to $B$.
(*c*) $B \nsubseteq C$ because $3 \in B$ but $3 \notin C$.
(*d*) $B \subseteq E$ because the elements of $B$ also belong to $E$.
(*e*) $C \nsubseteq D$ because $9 \in C$ but $9 \notin D$.
(*f*) $C \subseteq E$ because the elements of $C$ also belong to $E$.
(*g*) $D \nsubseteq E$ because $2 \in D$ but $2 \notin E$.
(*h*) $D \subseteq U$ because the elements of $D$ also belong to $\mathbf{U}$.

**1.4.** Show that $A = \{2, 3, 4, 5\}$ is not a subset of $B = \{x : x \in P,\ x \text{ is even}\}$.

It is necessary to show that at least one element in $A$ does not belong to $B$. Now $3 \in A$ and, since $B$ consists of even numbers, $3 \notin B$; hence $A$ is not a subset of $B$.

**1.5.** Show that $A = \{2, 3, 4, 5\}$ is a proper subset of $C = \{1, 2, 3, \ldots, 8, 9\}$.

Each element of $A$ belongs to $C$ so $A \subseteq C$. On the other hand, $1 \in C$ but $1 \in A$. Hence $A \neq C$. Therefore $A$ is a proper subset of $C$.

**1.6.** Determine whether or not each set is the null set:

(*a*) $X = \{x : x^2 = 9,\ 2x = 4\}$, (*b*) $Y = \{x : x \neq x\}$, (*c*) $Z = \{x : x + 8 = 8\}$.

(*a*) No number satisfies both $x^2 = 9$ and $2x = 4$; hence $X$ is the empty set; i.e., $X = \varnothing$.

(*b*) We interpret "=" to mean "is identical with" and so $Y$ is empty. In fact, some texts define the empty set as follows:

$$\varnothing \equiv \{x : x \neq x\}$$

(*c*) The number zero satisfies $x + 8 = 8$ and zero is the only solution; hence $Z = \{0\}$. Thus $Z$ is not the empty set since it contains 0. That is, $Z \neq \varnothing$.

## SET OPERATIONS

Problems 1-7 to 1-10 refer to the universal set $\mathbf{U} = \{1, 2, \ldots, 9\}$ and the sets:

$$A = \{1,2,3,4,5\} \qquad C = \{5,6,7,8,9\} \qquad E = \{2,4,6,8\}$$
$$B = \{4,5,6,7\} \qquad D = \{1,3,5,7,9\} \qquad F = \{1,5,9\}$$

**1.7.** Find:

(*a*) $A \cup B$ and $A \cap B$, (*c*) $A \cup C$ and $A \cap C$, (*e*) $E \cup E$ and $E \cap E$
(*b*) $B \cup D$ and $B \cap D$, (*d*) $D \cup E$ and $D \cap E$, (*f*) $D \cup F$ and $D \cap F$

Recall that the union $X \cup Y$ consists of those elements in either $X$ or $Y$ (or both), and that the intersection $X \cap Y$ consists of those elements in both X and Y.

(*a*) $A \cup B = \{1,2,3,4,5,6,7\}$, $A \cap B = \{4,5\}$
(*b*) $B \cup D = \{1,3,4,5,6,7,9\}$, $B \cap D = \{5,7\}$
(*c*) $A \cup C = \{1,2,3,4,5,6,7,8,9\} = \mathbf{U}$, $A \cap C = \varnothing$
(*d*) $D \cup E = \{1,2,3,4,5,6,7,8,9\} = \mathbf{U}$, $D \cap E = \varnothing$
(*e*) $E \cup E = \{2,4,6,8\} = E$, $E \cap E = \{2,4,6,8\} = E$
(*f*) $D \cup F = \{1,3,5,7,9\} = D$, $D \cap F = \{1,5,9\} = F$

Observe that $F \subseteq D$; so by Theorem 1.3 we must have $D \cup F = D$ and $D \cap F = F$.

**1.8.** Find: (*a*) $A^c$, $B^c$, $D^c$, $E^c$; (*b*) $\mathbf{U}^c$, $\varnothing^c$.

(*a*) The complement $X^c$ consists of those elements in the universal set U which do not belong to $X$. Thus:

$$A^c = \{6,7,8,9\}, \qquad B^c = \{1,2,3,8,9\}, \qquad D^c = \{2,4,6,8\} = E, \qquad E^c = \{1,3,5,7,9\} = D$$

(*Note*: Since $D^c = E$, we must have $E^c = D$.)

(*b*) Here $\mathbf{U}^c = \varnothing$, and $\varnothing^c = \mathbf{U}$, and this is always true.

**1.9.** Find: (*a*) $A\backslash B$, $B\backslash A$, $D\backslash E$, $F\backslash D$; (*b*) $A \oplus B$, $C \oplus D$, $E \oplus F$.

(*a*) The difference $X\backslash Y$ consist of the elements in $X$ which do not belong to $Y$. Thus:

$$A\backslash B = \{1,2,3\}, \qquad B\backslash A = \{6,7\}, \qquad D\backslash E = \{1,3,5,7,9\} = D, \qquad F\backslash D = \varnothing.$$

(*Note*: Since $D$ and $E$ are disjoint, we must have $D\backslash E = D$; and since $F \subseteq D$, we must have $F\backslash D = \varnothing$.)

(*b*) The symmetric difference $X \oplus Y$ consists of the elements in $X$ or in $Y$ but not in both $X$ and $Y$. Thus:

$$A \oplus B = \{1,2,3,6,7\}, \qquad C \oplus D = \{1,3,8,9\}, \qquad E \oplus F = \{2,4,6,8,1,5,9\} = E \cup F$$

(*Note*: Since $E$ and $F$ are disjoint, we must have $E \oplus F = E \cup F$.)

**1.10.** Find: (*a*) $A \cap (B \cup E)$, (*b*) $(A\backslash B)^c$, (*c*) $(A \cap D)\backslash B$, (*d*) $(B \cap F) \cup (C \cap E)$.

(*a*) First compute $B \cup E = \{2,4,5,6,7,8\}$. Then $A \cap (B \cup E) = \{2,4,5\}$.
(*b*) $A\backslash E = \{1,3,5\}$. Then $(A\backslash E)^c = \{2,4,6,7,8,9)$.
(*c*) $A \cap D = \{1,3,5\}$. Now $(A \cap D)\backslash B = \{1,3\}$.
(*d*) $B \cap F = \{5\}$ and $C \cap E = \{6,8)$. So $(B \cap F) \cup (C \cap E) = \{5,6,8)$.

**1.11.** Show that we can have $A \cap B = A \cap C$ without $B = C$.

Let $A = \{1,2\}$, $B = \{2,3\}$, and $C = \{2,4\}$. Then $A \cap B = (2\}$ and $A \cap C = \{2)$. Thus $A \cap B = A \cap C$ but $B \neq C$.

**1.12.** Prove: $B \backslash A = B \cap A$. Thus the set operation of difference can be written in terms of the operations of intersection and complementation.

$$B\backslash A = \{x : x \in B,\ x \notin A) = \{x : x \in B,\ x \in A^c) = B \cap A^c$$

**1.13.** Prove Theorem 1.3: The following are equivalent: $A \subseteq B$, $A \cap B = A$, and $A \cup B = B$.

Suppose $A \subseteq B$. Let $x \in A$. Then $x \in B$, hence $x \in A \cap B$ and so $A \subseteq A \cap B$. By Theorem 1.2, $(A \cap B) \subseteq A$. Therefore $A \cap B = A$. On the other hand, suppose $A \cap B = A$. Let $x \in A$. Then $x \in A \cap B$, hence $x \in B$. Therefore, $A \subseteq B$. Both results show that $A \subseteq B$ is equivalent to $A \cap B = A$.

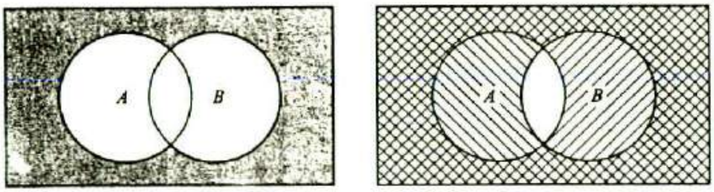
Suppose again that $A \subseteq B$. Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in A$, then $x \in B$ because $A \subseteq B$. In either case, $x \in B$. Therefore $A \cup B \subseteq B$. By Theorem 1.2, $B \subseteq A \cup B$. Therefore $A \cup B = B$. Now suppose $A \cup B = B$. Let $x \in A$. Then $x \in A \cup B$ by definition of union of sets. Hence $x \in B = A \cup B$. Therefore $A \subseteq B$. Both results show that $A \subseteq B$ is equivalent to $A \cup B = B$.

Thus $A \subseteq B$, $A \cap B = A$ and $A \cup B = B$ are equivalent.

## VENN DIAGRAMS, ALGEBRA OF SETS, DUALITY

**1.14.** Illustrate DeMorgan's law $(A \cup B)^c = A^c \cap B^c$ (proved in Section 1.7) using Venn diagrams.

Shade the area outside $A \cup B$ in a Venn diagram of sets $A$ and $B$. This is shown in Fig. 1-8(*a*); hence the shaded area represents $(A \cup B)^c$. Now shade the area outside $A$ in a Venn diagram of $A$ and $B$ with strokes in one direction (///), and then shade the area outside $B$ with strokes in another direction (\\\). This is shown in Fig. 1-8(*b*). Thus the cross-hatched area (area where both lines are present) represents the intersection of $A^c$ and $B^c$, that is, $A^c \cap B^c$. Both $(A \cup B)^c$ and $A^c \cap B^c$ are represented by the same area; hence the Venn diagrams indicate $(A \cup B)^c = A^c \cap B^c$. (We emphasize that a Venn diagram is not a formal proof but it can indicate relationships between sets.)



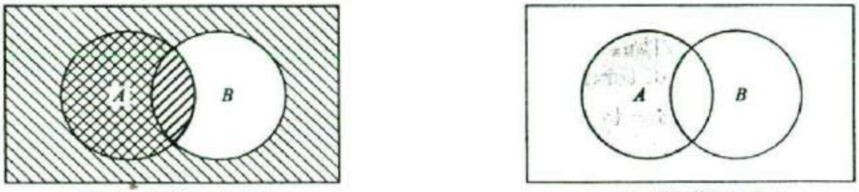
(*a*) Shaded area: $(A \cup B)^c$ (*b*) Cross-hatched area: $A^c \cap B^c$

**Fig. 1-8**

**1.15.** Consider the Venn diagram of two arbitrary sets $A$ and $B$ as pictured in Fig. 1-1(*c*). Shade the sets: (*a*) $A \cap B^c$, (*b*) $(B \backslash A)^c$.

(*a*) First shade the area represented by $A$ with strokes in one direction (///), and then shade the area represented by $B^c$ (the area outside $B$), with strokes in another direction (\\\). This is shown in Fig. 1-9(*a*). The cross-hatched area is the intersection of these two sets and represents $A \cap B^c$; and this is shown in Fig. 1-9(*b*). Observe that $A \cap B^c = A \backslash B$. In fact, $A \backslash B$ is sometimes defined to be $A \cap B^c$.

(*b*) First shade the area represented by $B \backslash A$ (the area of $B$ which does not lie in $A$) as in Fig. 1-10(*a*). Then the area outside this shaded region, which is shown in Fig. 1-10(*b*), represents $(B \backslash A)^c$.



(*a*) $A$ and $B^c$ are shaded (*b*) $A \cap B^c$ is shaded

**Fig. 1-9**

(*a*) $B \backslash A$ is shaded (*b*) $(B \backslash A)^c$ is shaded

**Fig. 1-10**

**1.16.** Prove Theorem 1.4: Distributive law (4*b*)

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

**Illustrate the law using Venn diagrams.**

By definition of union and intersection,

$$\begin{aligned} A \cap (B \cup C) &= \{x : x \in A,\ X \in B \cup C\} \\ &= \{x : x \in A,\ x \in B \text{ or } x \in A,\ x \in C) = (A \cap B) \cup (A \cap C) \end{aligned}$$

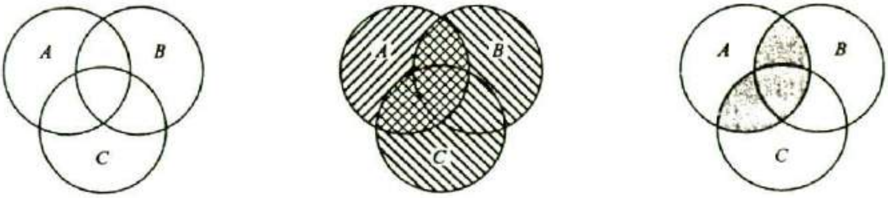
Here we use the analogous logical law

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

where $\wedge$ denotes "and" and $\vee$ denotes "or".

**Venn Diagram**

Draw three intersecting circles labeled $A, B, C$, as in Fig. 1-11(*a*). Now, as in Fig. 1-11(*b*) shade $A$ with strokes in one direction (///) and shade $B \cup C$ with strokes in another direction (\\\\\\). Then the cross-hatched area is $A \cap (B \cup C)$, as shaded in Fig. 1-11(*c*). Next shade $A \cap B$ and then $A \cap C$, as in Fig. 1-11(*d*). The total area shaded is $(A \cap B) \cup (A \cap C)$, as shaded in Fig. 1-11(*e*). As expected by the distributive law, $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ are both represented by the same set of points.



(*a*)		(*b*) $A$ and $B \cup C$ are shaded		(*c*) $A \cap (B \cup C)$ is shaded

(*d*) $A \cap B$ and $A \cap C$ are shaded		(*e*) $(A \cap B) \cup (A \cap C)$ is shaded

**Fig. 1-11**

**1.17.** Prove the commutative laws: (*a*) $A \cup B = B \cup A$, (*b*) $A \cap B = B \cap A$.

(*a*) $A \cup B = \{x : x \in A \text{ or } x \in B\} = \{x : x \in B \text{ or } x \in A\} = B \cup A$.

(*b*) $A \cap B = \{x : x \in A \text{ and } x \in B\} = \{x : x \in B \text{ and } x \in A\} = B \cap A$.

**1.18.** Prove: $(A \cup B)\backslash(A \cap B) = (A\backslash B) \cup (B\backslash A)$. (Thus either one may be used to define the symmetric difference $A \oplus B$.)

Using $X\backslash Y = X \cap Y^c$ and the laws in Table 1-1, including DeMorgan's laws, we obtain

$$\begin{aligned}(A \cup B)\backslash(A \cap B) &= (A \cup B) \cap (A \cap B)^c = (A \cup B) \cap (A^c \cup B^c)\\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c)\\ &= \varnothing \cup (A \cap B^c) \cup (B \cap A^c) \cup \varnothing\\ &= (A \cap B^c) \cup (B \cap A^c) = (A\backslash B) \cup (B\backslash A)\end{aligned}$$

**1.19.** Prove the following identity: $(A \cup B) \cap (A \cup B^c) = A$.

| **Statement** | **Reason** |
|---|---|
| 1. $(A \cup B) \cap (A \cup B^c) = A \cup (B \cap B^c)$ | Distributive law |
| 2. $B \cap B^c = \varnothing$ | Complement law |
| 3. $(A \cup B) \cap (A \cup B^c) = A \cup \varnothing$ | Substitution |
| 4. $A \cup \varnothing = A$ | Identity law |
| 5. $(A \cup B) \cap (A \cup B^c) = A$ | Substitution |

**1.20.** Write the dual of each set equation:

(*a*) $(\mathbf{U} \cap A) \cup (B \cap A) = A$ (*c*) $(A \cap \mathbf{U}) \cap (\varnothing \cup A^c) = \varnothing$

(*b*) $(A \cup B \cup C)^c = (A \cup C)^c \cap (A \cup B)^c$ (*d*) $(A \cap \mathbf{U})^c \cap A = \varnothing$

Interchange $\cup$ and $\cap$ and also $\mathbf{U}$ and $\varnothing$ in each set equation:

(*a*) $(\varnothing \cup A) \cap (B \cup A) = A$ (*c*) $(A \cup \varnothing) \cup (\mathbf{U} \cap A^c) = \mathbf{U}$

(*b*) $(A \cap B \cap C)^c = (A \cap C)^c \cup (A \cap B)^c$ (*d*) $(A \cup \varnothing)^c \cup A = \mathbf{U}$

## FINITE SETS AND THE COUNTING PRINCIPLE

**1.21.** Determine which of the following sets are finite.

(*a*) $A =$ {seasons in the year},

(*b*) $B =$ {states in the United States of America},

(*c*) $C =$ {positive integers less than 1},

(*d*) $D =$ {odd integers},

(*e*) $E =$ {positive integral divisors of 12},

(*f*) $F =$ {cats living in the United States}.

(*a*) $A$ is finite since there are four seasons in the year, i.e., $n(A) = 4$.

(*b*) $B$ is finite because there are 50 states in the United States, i.e., $n(B) = 50$.

(*c*) There are no positive integers less than 1; hence $C$ is empty. Thus $C$ is finite and $n(C) = \varnothing$.

(*d*) $D$ is infinite.

(*e*) The positive integer divisors of 12 are 1, 2, 3, 4, 6, 12. Hence $E$ is finite and $n(E) = 6$.

(*f*) Although it may be difficult to find the number of cats living in the United States, there is still a finite number of them at any point in time. Hence $F$ is finite.

**1.22.** Suppose 50 science students are polled tò see whether or not they have studied French (F) or German (G) yielding the following data:

25 studied French, 20 studied German, 5 studied both.

Find the number of the students who: (*a*) studied only French, (*b*) did not study German, (*c*) studied French or German, (*d*) studied neither language.

(*a*) Here 25 studied French, and 5 of them also studied German; hence $25 - 5 = 20$ students only studied French. That is, by Theorem 1.7,

$$n(F \backslash G) = n(F) - N(F \cap G) = 25 - 5 = 20.$$

(*b*) There are 50 students of whom 20 studied German; hence $50 - 20 = 30$ did not study German. That is, by Theorem 1.6,

$$n(G^c) = n(\mathbf{U}) - n(G) = 50 - 20 = 30$$

(*c*) By the inclusion-exclusion principle, Theorem 1.8,

$$n(F \cup G) = n(F) + n(G) - n(F \cap G) = 25 + 20 - 5 = 40$$

That is, 40 students studied French or German.

(*d*) The set $F^c \cap G^c$ consists of the students who studied neither language. By DeMorgan's law, $F^c \cap G^c = (F \cup G)^c$. By (*c*), 40 studied at least one of the languages; hence

$$n(F^c \cap G^c) = n(\mathbf{U}) - n(F \cup G) = 50 - 40 = 10$$

That is, 10 students studied neither language.

**1.23.** Suppose $n(\mathbf{U}) = 70$, $n(A) = 30$, $n(B) = 45$, $n(A \cap B) = 10$. Find:
(*a*) $n(A \cup B)$, (*b*) $n(A^c)$ and $n(B^c)$, (*c*) $n(A^c \cap B^c)$, (*d*) $n(A \oplus B)$.

(*a*) By Theorem 1.9, $n(A \cup B) = n(A) + n(B) - n(A \cap B) = 30 + 45 - 10 = 65$.

(*b*) Here

$$n(A^c) = n(\mathbf{U}) - n(A) = 70 - 30 = 40 \quad \text{and} \quad n(B^c) = n(\mathbf{U}) - n(B) = 70 - 45 = 25$$

(*c*) Using DeMorgan's law,

$$n(A^c \cap B^c) = n((A \cup B)^c) = n(\mathbf{U}) - n(A \cup B) = 70 - 65 = 5$$

(*d*) First find

$$n(A \backslash B) = n(A) - n(A \cap B) = 30 - 10 = 20$$
$$n(B \backslash A) = n(B) - n(A \cap B) = 45 - 10 = 25$$

Then

$$n(A \oplus B) = n(A \backslash B) + n(B \backslash A) = 20 + 25 = 45$$

**1.24.** A small college requires its students to take at least one mathematics course and at least one science course. A survey of 140 of its sophomore students shows that:

60 completed their mathematics requirement (M),
45 completed their science requirement (S),
20 completed both requirements (M and S).

Use a Venn diagram to find the number of the students who had completed:

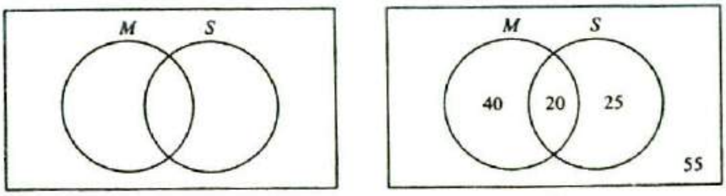
(*a*) exactly one of the two requirements,
(*b*) at least one of the requirements,
(*c*) neither requirement.

Translating the above data into set notation yields:

$$n(M) = 60, \quad n(S) = 45, \quad n(M \cap S) = 20, \quad \text{and} \quad n(\mathbf{U}) = 140$$

Draw a Venn diagram of sets $M$ and $S$ with four regions as in Fig. 1-12(*a*). Then, as in Fig. 1-12(*b*), assign numbers to the four regions as follows::

20 completed both $M$ and $S$, i.e. $n(M \cap S) = 20$,
$60 - 20 = 40$ completed $M$ but not $S$, i.e. $n(M \backslash S) = 40$,
$45 - 20 = 25$ completed $S$ but not $M$, i.e. $n(S \backslash M) = 25$,
$140 - 20 - 40 - 25 = 55$ completed neither $M$ nor $S$.



(*a*) (*b*)

Fig. 1-12

By the Venn diagram:

(*a*) $40 + 25 = 65$ completed exactly one of the requirements,

(*b*) $20 + 40 + 25 = 85$ completed $M$ or $S$. Alternately, we can find $n(M \cup S)$ without the Venn diagram by using Theorem 1.7. That is,

$$n(M \cup S) = n(M) + n(S) - n(M \cap S) = 60 + 45 - 20 = 85$$

(*c*) 55 completed neither requirement.

**1.25.** In a survey of 60 people, it was found that:

25 read *Newsweek* magazine
26 read *Time*
26 read *Fortune*

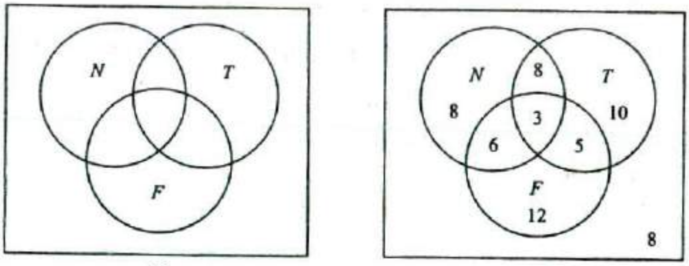
9 read both *Newsweek* and *Fortune*
11 read both *Newsweek* and *Time*
8 read both *Time* and *Fortune*

3 read all three magazines

(*a*) Find the number of people who read at least one of the three magazines.

(*b*) Fill in the correct number of people in each of the eight regions of the Venn diagram in Fig. 1-13(*a*) where $N$, $T$, and $F$ denote the set of people who read *Newsweek*, *Time*, and *Fortune*, respectively.

(*c*) Find the number of people who read exactly one magazine.



(*a*) (*b*)

Fig. 1-13

(*a*) We want $n(N \cup T \cup F)$. By Corollary 1.9,

$$n(N \cup T \cup F) - n(N) + N(T) + n(F) - n(N \cap F) - n(N \cap T) - n(T \cap F) + n(N \cap T \cap F)$$
$$= 25 + 26 + 26 - 11 - 9 - 8 + 3 = 52$$

(*b*) The required Venn diagram in Fig 1-13(*b*) is obtained as follows:

3 read all three magazines
$11 - 3 = 8$ read *Newsweek* and *Time* but not all three magazines
$9 - 3 = 6$ read *Newsweek* and *Fortune* but not all three magazines
$8 - 3 = 5$ read *Time* and *Fortune* but not all three magazines
$25 - 8 - 6 - 3 = 8$ read only *Newsweek*
$26 - 8 - 5 - 3 = 10$ read only *Time*
$26 - 6 - 5 - 3 = 12$ read only *Fortune*
$60 - 52 = 8$ read no magazine at all

(*c*) $8 + 10 + 12 = 30$ read only one magazine.

**1.26.** Prove Theorem 1.8: If $A$ and $B$ are finite sets, then $A \cup B$ and $A \cap B$ are finite and $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

If $A$ and $B$ are finite, then clearly $A \cap B$ and $A \cup B$ are finite.

Suppose we count the elements of $A$ and then count the elements of $B$. Then every element in $A \cap B$ would be counted twice, once in $A$ and once in $B$. Hence

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

Alternatively (Problems 1.37 and 1.50),

(i) $A$ is the disjoint union of $A \backslash B$ and $A \cap B$,

(ii) $B$ is the disjoint union of $B \backslash A$ and $A \cap B$,

(iii) $A \cup B$ is the disjoint union of $A \backslash B$, $A \cap B$, and $B \backslash A$.

Therefore, by Lemma 1.5 and Theorem 1.7,

$$\begin{aligned} n(A \cup B) &= n(A \backslash B) + n(A \cap B) + n(B \backslash A) \\ &= n(A) - n(A \cap B) + n(A \cap B) + n(B \backslash A) - n(A \cap B) \\ &= n(A) + n(B) - n(A \cap B) \end{aligned}$$

## CLASSES OF SETS

**1.27.** Find the elements of the set $A = [\{1,2,3\}, \{4,5\}, \{6,7,8\}]$, and determine whether each of the following is true or false:

(*a*) $1 \in A$ (*c*) $\{6,7,8\} \in A$ (*e*) $\varnothing \in A$

(*b*) $\{1,2,3\} \subseteq A$ (*d*) $\{\{4,5\}\} \subseteq A$ (*f*) $\varnothing \subseteq A$

$A$ is a collection (class) of sets; its elements are the sets $\{1,2,3\}$, $\{4,5\}$, and $\{6,7,8\}$.

(*a*) *False*. 1 is not one of the elements of $A$.

(*b*) *False*. $\{1,2,3\}$ is not a subset of $A$; it is one of the elements of $A$.

(*c*) *True*. $\{6,7,8\}$ is one of the elements of $A$.

(*d*) *True*. $\{\{4,5\}\}$, the set consisting of the element $\{4,5\}$ is a subset of $A$.

(*e*) *False*. The empty set $\varnothing$ is not an element of $A$, i.e., it is not one of the three elements of $A$.

(*f*) *True*. The empty set $\varnothing$ is a subset of every set; even a collection of sets.

**1.28.** Consider that class $A$ of sets in Problem 1.27. Find the subclass $B$ of $A$ where $B$ consists of the sets in $A$ with exactly: (*a*) three elements, (*b*) four elements.

(*a*) There are two sets in $A$ with three elements, $\{1,2,3\}$ and $\{6,7,8\}$. Hence $B = [\{1,2,3\}, \{6,7,8\}]$.

(*b*) There are no sets in $A$ with four elements; hence $B$ is empty, that is, $B = \varnothing$.

**1.29.** Determine the power set $\mathscr{P}(A)$ of $A = \{a,b,c,d\}$.

The elements of $\mathscr{P}(A)$ are the subsets of $A$. Hence

$$\begin{aligned} \mathscr{P}(A) = [&A, \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b\}, \{a,c\}, \\ &\{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}, \{a\}, \{b\}, \{c\}, \{d\}, \varnothing] \end{aligned}$$

As expected, $\mathscr{P}(A)$ has $2^4 = 16$ elements.

**1.30.** Find the number of elements in the power set of each of the following sets:

| | | | |
|---|---|---|---|
| (*a*) | {days of the week}, | (*c*) | {seasons of the year}, |
| (*b*) | {positive divisors of 12}, | (*d*) | {letters in the word "yes"}. |

Recall that $\mathscr{P}(A)$ contains $2^{|A|}$ elements. Hence:

(*a*) $2^7 = 128$.

(*b*) $2^6 = 64$ since there are six divisors, 1, 2, 3, 4, 6, 12, of 12.

(*c*) $2^4 = 16$ since there are four seasons.

(*d*) $2^3 = 8$.

## ARGUMENTS AND VENN DIAGRAMS

**1.31.** Determine the validity of the following argument:

$S_1$: All my friends are musicians

$S_2$: John is my friend.

$S_3$: None of my neighbors are musicians.

---

$S$: John is not my neighbor.

The premises $S_1$ and $S_3$ lead to the Venn diagram in Fig. 1-14. By $S_2$, John belongs to the set of friends which is disjoint from the set of neighbors. Thus $S$ is a valid conclusion and so the argument is valid.

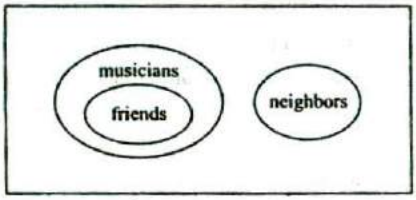


**Fig. 1-14**

**1.32.** Consider the following assumptions:

$S_1$: Poets are happy people.

$S_2$: Every doctor is wealthy.

$S_3$: No happy person is wealthy.

Determine the validity of each of the following conclusions:

(*a*) No poet is wealthy. (*b*) Doctors are happy people.

(*c*) No person can be both a poet and a doctor.

The three premises lead to the Venn diagram in Fig. 1-15. From the diagram it follows that (*a*) and (*c*) are valid conclusions whereas (*b*) is not valid.

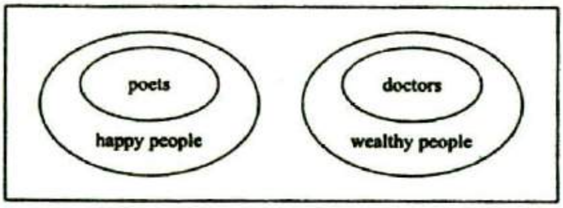


Fig. 1-15

**1.33.** Determine the validity of the following argument:

$S_1$: Babies are illogical.
$S_2$: Nobody is despised who can manage a crocodile.
$S_3$: Illogical people are despised.

$S$: Babies cannot manage crocodiles.

(The above argument is adapted from Lewis Carroll, *Symbolic Logic*; he is the author of *Alice in Wonderland*.)

The three premises lead to the Venn diagram in Fig. 1-16. Since the set of babies and the set of people who can manage crocodiles are disjoint, "Babies cannot manage crocodiles" is a valid conclusion.

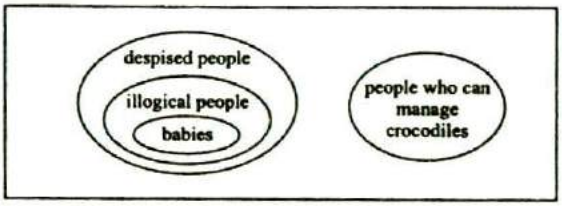


Fig. 1-16

## MATHEMATICAL INDUCTION

**1.34.** Prove the assertion $A(n)$ that the sum of the first $n$ positive integers is $\frac{1}{2}n(n+1)$; that is,

$$A(n)\colon\ 1+2+3+\cdots+n=\tfrac{1}{2}n(n+1)$$

The assertion holds for $n=1$ since

$$A(1)\colon\ 1=\tfrac{1}{2}(1)(1+1)$$

Assuming $A(n)$ is true, we add $n+1$ to both sides of $A(n)$, obtaining

$$\begin{aligned}1+2+3+\cdots+n+(n+1)&=\tfrac{1}{2}n(n+1)+(n+1)\\&=\tfrac{1}{2}[n(n+1)+2(n+1)]\\&=\tfrac{1}{2}[(n+1)(n+2)]\end{aligned}$$

which is $A(n+1)$. That is, $A(n+1)$ is true whenever $A(n)$ is true. By the principle of induction, $A(n)$ is true for all $n\geq 1$.

**1.35.** Prove the following assertion (for $n \geq 0$):

$$A(n): \quad 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

$A(0)$ is true since $1 = 2^1 - 1$. Assuming $A(n)$ is true, we add $2^{n+1}$ to both sides of $A(n)$, obtaining

$$\begin{aligned} 1 + 2 + 2^2 + 2^3 + \cdots + 2^n + 2^{n+1} &= 2^{n+1} - 1 + 2^{n+1} \\ &= 2(2^{n+1}) - 1 \\ &= 2^{n+2} - 1 \end{aligned}$$

which is $A(n+1)$. Thus $A(n+1)$ is true whenever $A(n)$ is true. By the principle of induction, $A(n)$ is true for all $n \geq 0$.

**1.36.** Prove: (*a*) $n^2 \geq 2n + 1$ for $n \geq 3$, (*b*) $n! \geq 2^n$ for $n \geq 4$.

(*a*) Since $3^2 = 9$ and $2(3) + 1 = 7$, the formula is true for $n = 3$. Using $n^2 \geq 2n + 1$ in the second step and $2n \geq 1$ in the fourth step, we have

$$(n+1)^2 = n^2 + 2n + 1 \geq (2n+1) + 2n + 1 = 2n + 2 + 2n \geq 2n + 2 + 1 = 2(n+1) + 1$$

Thus the formula is true for $n + 1$. By induction, the formula is true for all $n \geq 3$.

(*b*) Since $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ and $2^4 = 16$, the formula is true for $n = 4$. Assuming $n! \geq 2^n$ we have

$$(n+1)! = n!(n+1) \geq 2^n(n+1) \geq 2^n(2) = 2^{n+1}$$

Thus the formula is true for $n + 1$. By induction, the formula is true for all $n \geq 4$.

## MISCELLANEOUS PROBLEMS

**1.37.** Show that $A$ is the disjoint union of $A \backslash B$ and $A \cap B$; that is, show that:

(*a*) $A = (A \backslash B) \cup (A \cap B)$, (*b*) $(A \backslash B) \cap (A \cap B) = \varnothing$.

(*a*) By Problem 1.12, $A \backslash B = A \cap B^c$. Using the distributive law and the complement law, we get

$$(A \backslash B) \cup (A \cap B) = (A \cap B^c) \cup (A \cap B) = A \cap (B^c \cup B) = A \cap U = A$$

(*b*) Also,

$$(A \backslash B) \cap (A \cap B) = (A \cap B^c) \cap (A \cap B) = A \cap (B^c \cap B) = A \cap \varnothing = \varnothing.$$

**1.38.** Prove Corollary 1.9. Suppose $A$, $B$, $C$ are finite sets. Then $A \cup B \cup C$ is finite and

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Clearly $A \cup B \cup C$ is finite when $A$, $B$, $C$ are finite. Using

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \quad \text{and} \quad (A \cap B) \cap (B \cap C) = A \cap B \cap C$$

and using Theorem 1.8 repeatedly, we have

$$\begin{aligned} n(A \cup B \cup C) &= n(A \cup B) + n(C) - n[(A \cap C) \cup (B \cap C)] \\ &= [n(A) + n(B) - n(A \cap B)] + n(C) - [n(A \cap C) + n(B \cap C) - n(A \cap B \cap C)] \\ &= n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C) \end{aligned}$$

as required.

**1.39.** A set $A$ of real numbers is said to be *bounded from above* if there exists a number $M$ such that $x \leq M$ for every $x$ in $A$. (Such a number $M$ is called an *upper bound* of $M$.)

(*a*) Suppose $A$ and $B$ are sets which are bounded from above with respective upper bounds $M_1$ and $M_2$. What can be said about the union and intersection of $A$ and $B$?

(*b*) Suppose $C$ and $D$ are sets of real numbers which are unbounded. What can be said about the union and intersection of $C$ and $D$?

(*a*) Both the union and intersection are bounded from above. In fact, the larger of $M_1$ and $M_2$ is always an upper bound for $A \cup B$, and the smaller of $M_1$ and $M_2$ is always an upper bound for $A \cap B$.

(*b*) The union of $C$ and $D$ must be unbounded, but the intersection could be either bounded or unbounded.

**1.40.** Restate the Principle of Mathematical Induction I and II in terms of sets, rather than assertions.

(*a*) *Principle of Mathematical Induction I*: Let $S$ be a subset of $\mathbf{P} = \{1, 2, \ldots\}$ with two properties:

$$(1)\quad 1 \in S. \qquad (2)\quad \text{If } n \in S, \text{ then } n+1 \in S.$$

Then $S = \mathbf{P}$.

(*b*) *Principle of Mathematical Induction II*: Let $S$ be a subset of $\mathbf{P} = \{1, 2, \ldots\}$ with two properties:

$$(1)\quad 1 \in S. \qquad (2)\quad \text{If } \{1, 2, \ldots, n-1\} \subseteq S, \text{ then } n \in S.$$

Then $S = \mathbf{P}$.

## Supplementary Problems

### SETS AND SUBSETS

**1.41.** Which of the following sets are equal?

$$A = \{x : x^2 - 4x + 3 = 0\} \qquad C = \{x : x \in \mathbf{P}, x < 3\} \qquad E = \{1, 2\} \qquad G = \{3, 1\}$$
$$B = \{x : x^2 - 3x + 2 = 0\} \qquad D = \{x : x \in \mathbf{P}, x \text{ is odd}, x < 5\} \qquad F = \{1, 2, 1\} \qquad H = \{1, 1, 3\}$$

**1.42.** List the elements of the following sets if the universal set is $\mathbf{U} = \{\mathrm{a, b, c}, \ldots, \mathrm{y, z}\}$. Furthermore, identify which of the sets, if any, are equal.

$A = \{x : x \text{ is a vowel}\}$

$B = \{x : x \text{ is a letter in the word "little"}\}$

$C = \{x : x \text{ precedes f in the alphabet}\}$

$D = \{x : x \text{ is a letter in the word "title"}\}$

**1.43.** Let

$$A = \{1, 2, \ldots, 8, 9\}, \quad B = \{2, 4, 6, 8\}, \quad C = \{1, 3, 5, 7, 9\}, \quad D = \{3, 4, 5\}, \quad E = \{3, 5\}$$

Which of the above sets can equal a set $X$ under each of the following conditions?

(*a*) $X$ and $B$ are disjoint.

(*b*) $X \subseteq D$ but $X \not\subseteq B$.

(*c*) $X \subseteq A$ but $X \not\subseteq C$.

(*d*) $X \subseteq C$ but $X \not\subseteq A$.

**1.44.** Consider the following sets:

$$\varnothing, \quad A = \{a\}, \quad B = \{c, d\}, \quad C = \{a, b, c, d\}, \quad D = \{a, b\}, \quad E = \{a, b, c, d, e\}.$$

Insert the correct symbol, $\subseteq$ or $\not\subseteq$, between each pair of sets:

(*a*) $\varnothing, A$ (*c*) $A, B$ (*e*) $B, C$ (*g*) $C, D$
(*b*) $D, E$ (*d*) $D, A$ (*f*) $D, C$ (*h*) $B, D$

## SET OPERATIONS

**1.45.** Let $\mathbf{U} = \{1, 2, 3, \ldots, 8, 9\}$ be the universal set and let:

$$A = \{1, 2, 5, 6\}, \qquad B = \{2, 5, 7\}, \qquad C = \{1, 3, 5, 7, 9\}$$

Find: (*a*) $A \cap B$ and $A \cap C$, (*b*) $A \cup B$ and $A \cup C$, (*c*) $A^c$ and $C^c$.

**1.46.** For the sets in Problem 1.45, find: (*a*) $A \backslash B$ and $A \backslash C$, (*b*) $A \oplus B$ and $A \oplus C$.

**1.47.** For the sets in Problem 1.45, find: (*a*) $(A \cup C) \backslash B$, (*b*) $(A \cup B)^c$, (*c*) $(B \oplus C) \backslash A$.

**1.48.** Let $A = \{a, b, c, d, e\}$, $B = \{a, b, d, f, g\}$, $C = \{b, c, e, g, h\}$, $D = \{d, e, f, g, h\}$. Find:

(*a*) $A \cup B$ (*c*) $B \cap C$ (*e*) $C \backslash D$ (*g*) $A \oplus B$
(*b*) $C \cap D$ (*d*) $A \cap D$ (*f*) $D \backslash A$ (*h*) $A \oplus C$

**1.49.** For the sets in Problem 1.48, find:

(*a*) $A \cap (B \cup D)$ (*c*) $(A \cup D) \backslash C$ (*e*) $(C \backslash A) \backslash D$ (*g*) $(A \cap D) \backslash (B \cup C)$
(*b*) $B \backslash (C \cup D)$ (*d*) $B \cap C \cap D$ (*f*) $(A \oplus D) \backslash B$ (*h*) $(A \backslash C) \cap (B \cap D)$

**1.50.** Let $A$ and $B$ be any sets. Prove $A \cup B$ is the disjoint union of $A \backslash B$, $A \cap B$, and $B \backslash A$.

**1.51.** Prove the following:

(*a*) $A \subseteq B$ if and only if $A \cap B^c = \varnothing$ (*c*) $A \subseteq B$ if and only if $B^c \subseteq A^c$
(*b*) $A \subseteq B$ if and only if $A^c \cup B = U$ (*d*) $A \subseteq B$ if and only if $A \backslash B = \varnothing$
(Compare with Theorem 1.3.)

**1.52.** Prove the absorption laws: (*a*) $A \cup (A \cap B) = A$, (*b*) $A \cap (A \cup B) = A$.

**1.53.** The formula $A \backslash B = A \cap B^c$ defines the difference operation in terms of the operations of intersection and complement. Find a formula that defines the union $A \cup B$ in terms of the operations of intersection and complement.

**1.54.** (*a*) Prove: $A \cap (B \backslash C) = (A \cap B) \backslash (A \cap C)$.
(*b*) Give an example to show that $A \cup (B \backslash C) \neq (A \cup B) \backslash (A \cup C)$.

**1.55.** Prove the following properties of the symmetric difference:

(*a*) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (Associative law)
(*b*) $A \oplus B = B \oplus A$ (Commutative law)
(*c*) If $A \oplus B = A \oplus C$, then $B = C$ (Cancellation law)
(*d*) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ (Distributive law)

## VENN DIAGRAMS, ALGEBRA OF SETS, DUALITY

**1.56.** The Venn diagram in Fig. 1-17 shows sets $A$, $B$, $C$. Shade the following sets:

(*a*) $A \backslash (B \cup C)$, (*b*) $A^c \cap (B \cap C)$, (*c*) $(A \cup C) \cap (B \cup C)$.

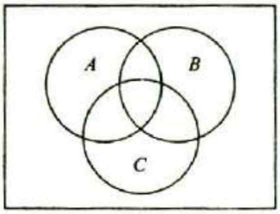


**Fig. 1-17**

**1.57.** Write the dual of each equation:

(*a*) $A = (B^c \cap A) \cup (A \cap B)$, (*b*) $(A \cap B) \cup (A \cap B^c) \cup (A^c \cap B) \cup (A^c \cap B^c) = U$

**1.58.** Use the laws in Table 1-1 to prove:

(*a*) $(A \cap B) \cup (A \cap B^c) = A$, (*b*) $A \cup B = (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B)$

## FINITE SETS AND THE COUNTING PRINCIPLE

**1.59.** Determine which of the following sets are finite:

(*a*) lines parallel to the $x$ axis,
(*b*) letters in the English alphabet,
(*c*) months in the year,
(*d*) animals living on the earth,
(*e*) circles through the origin $(0, 0)$,
(*f*) positive multiple of 5.

**1.60.** Given $n(U) = 20$, $n(A) = 12$, $n(B) = 9$, $n(A \cap B) = 4$. Find:

(*a*) $n(A \cup B)$, (*b*) $n(A^c)$, (*c*) $n(B^c)$, (*d*) $n(A \backslash B)$, (*e*) $n(\varnothing)$.

**1.61.** Among the 90 students in a dormitory, 35 own an automobile, 40 own a bicycle, and 10 have both an automobile and a bicycle. Find the number of the students who:

(*a*) do not have an automobile.
(*b*) have an automobile or a bicycle;
(*c*) have neither an automobile nor a bicycle;
(*d*) have an automobile or a bicycle, but not both.

**1.62.** Among 120 Freshmen at a college, 40 take mathematics, 50 take English, and 15 take both mathematics and English. Find the number of the Freshmen who:

(*a*) do not take mathematics;
(*b*) take mathematics or English;
(*c*) take mathematics, but not English;
(*d*) take English, but not mathematics;
(*e*) take exactly one of the two subjects;
(*f*) take neither mathematics nor English.

**1.63.** A survey on a sample of 25 new cars being sold at a local auto dealer was conducted to see which of three popular options, air-conditioning ($A$), radio ($R$), and power windows ($W$), were already installed. The survey found:

15 had air-conditioning
12 had radio
11 had power windows
5 had air-conditioning and power windows
9 had air-conditioning and radio
4 had radio and power windows
3 had all three options

Find the number of cars that had: (*a*) only power windows, (*b*) only air-conditioning, (*c*) only radio, (*d*) radio and power windows but not air-conditioning, (*e*) air-conditioning and radio, but not power windows, (*f*) only one of the options, (*g*) at least one option, (*h*) none of the options.

## CLASSES OF SETS, POWER SETS

**1.64.** Let $A = [\{a,b\}, \{c\}, \{d,e,f\}]$. List the elements of $A$ and determine whether each of the following statements is true or false:

(*a*) $a \in A$ (*c*) $c \in A$ (*e*) $\{d,e,f\} \subseteq A$ (*g*) $\varnothing \in A$
(*b*) $\{a\} \subseteq A$ (*d*) $\{c\} \in A$ (*f*) $\{\{a,b\}\} \subseteq A$ (*h*) $\varnothing \subseteq A$

**1.65.** Let $B = [\varnothing, \{1\}, \{2,3\}, \{3,4\}]$. List the elements of $B$ and determine whether each of the following statements is true or false:

(*a*) $1 \in B$ (*c*) $\{1\} \in B$ (*e*) $\{\{2,3\}\} \subseteq B$ (*g*) $\varnothing \subseteq A$
(*b*) $\{1\} \subseteq B$ (*d*) $\{2,3\} \subseteq B$ (*f*) $\varnothing \in A$ (*h*) $\{\varnothing\} \subseteq A$

**1.66.** Let $A = \{1,2,3,4,5\}$. (*a*) Find the power set $\mathscr{P}(A)$ of $A$. (*b*) Find the subcollection $\mathscr{B}$ of $\mathscr{P}(A)$ where each element of $\mathscr{B}$ consists of 1 and two other elements of $A$.

**1.67.** Find the power set $\mathscr{P}(A)$ of the set $A$ in Problem 1.64.

**1.68.** Suppose $A$ is a finite set and $n(A) = m$. Prove that $\mathscr{P}(A)$ has $2^m$ elements.

## ARGUMENTS AND VENN DIAGRAMS

**1.69.** Draw a Venn diagram for the following assumptions:

$S_1$: No practical car is expensive.
$S_2$: Cars with sunroofs are expensive.
$S_3$: All wagons are practical.

Use the Venn diagram to determine whether or not each of the following is a valid conclusion:

(*a*) No practical car has a sunroof. (*c*) No wagon has a sunroof.
(*b*) All practical cars are wagons. (*d*) Cars with sunroofs are not practical.

**1.70.** Draw a Venn diagram for the following assumptions:

$S_1$: I planted all my expensive trees last year.
$S_2$: All my fruit trees are in my orchard.
$S_3$: No tree in my orchard was planted last year.

Use the Venn diagram to determine whether or not each of the following is a valid conclusion:

(*a*) The fruit trees were planted last year. (*c*) No fruit tree is expensive.
(*b*) No expensive tree is in the orchard. (*d*) Only fruit trees are in the orchard.

**1.71.** Draw a Venn diagram for the following assumptions:

$S_1$: All poets are poor.
$S_2$: In order to be a teacher, one must graduate from college.
$S_3$: No college graduate is poor.

Use the Venn diagram to determine whether or not each of the following is a valid conclusion:

(*a*) Teachers are not poor.
(*b*) Poets are not teachers.
(*c*) College graduates do not become poets.
(*d*) Every poor person becomes a poet.

**1.72.** Draw a Venn diagram for the following assumptions:

$S_1$: All mathematicians are interesting people.
$S_2$: Only uninteresting people become insurance salespersons.
$S_3$: Every genius is a mathematician.

Use the Venn diagram to determine whether or not each of the following is a valid conclusion:

(*a*) No genius is an insurance salesperson.
(*b*) Insurance salespersons are not mathematicians.
(*c*) Every interesting person is a genius.

## MATHEMATICAL INDUCTION

**1.73.** Prove: $2 + 4 + 6 + \cdots + 2n = n(n+1)$.

**1.74.** Prove: $1 + 4 + 7 + \cdots + (3n-2) = 2n(3n-1)$.

**1.75.** Prove: $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{1}{2n+1}$.

**1.76.** Prove: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

**1.77.** Prove: Given $a^0 = 1$ and $a^n = a^{n-1}a$ for $n > 0$. Prove: (*a*) $a^m a^n = a^{m+n}$, (*b*) $(a^m)^n = a^{mn}$.

# Answers to Supplementary Problems

**1.41.** $B = C = E = F$; $A = D = G = H$

**1.42.** $A = \{a, e, i, o, u\}$; $B = D = \{l, i, t, e\}$; $C = \{a, b, c, d, e\}$

**1.43.** (*a*) $C$ and $E$; (*b*) $D$ and $E$; (*c*) $A$, $B$, $D$; (*d*) none

**1.44.** (*a*) $\subseteq$; (*b*) $\subseteq$; (*c*) $\not\subseteq$; (*d*) $\not\subseteq$; (*e*) $\subseteq$; (*f*) $\subseteq$; (*g*) $\not\subseteq$; (*h*) $\not\subseteq$

**1.45.** (*a*) $A \cap B = \{2, 5\}$, $A \cap C = \{1, 5\}$; (*b*) $A \cup B = \{1, 2, 5, 6, 7\}$, $A \cup C = \{1, 2, 3, 5, 6, 7, 9\}$;
(*c*) $A^c = \{3, 4, 7, 8, 9\}$, $C^c = \{2, 4, 6, 8\}$

**1.46.** (*a*) $A \backslash B = \{1, 6\}$, $A \backslash C = \{2, 6\}$; (*b*) $A \oplus B = \{1, 6, 7\}$, $A \oplus C = \{2, 3, 6, 7, 9\}$

**1.47.** (*a*) $\{1, 3, 6, 7, 9\}$. (*b*) $\{3, 4, 8, 9\}$. (*c*) $\{3, 9\}$

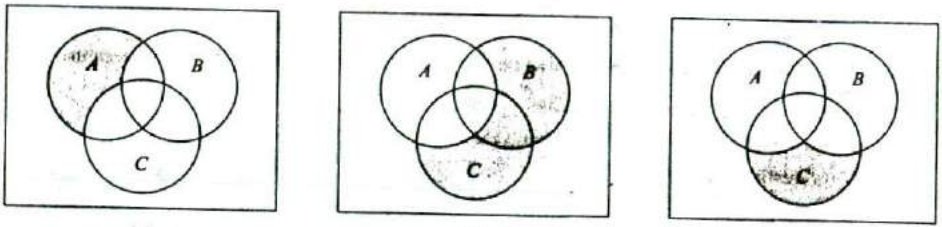
**1.48.** (*a*) $\{a, b, c, d, e, f, g\}$; (*b*) $\{e, g, h\}$; (*c*) $\{b, g\}$; (*d*) $\{d, e\}$; (*e*) $\{b, c\}$; (*f*) $\{f, g, h\}$; (*g*) $\{c, e, f, g\}$; (*h*) $\{a, d, g, h\}$

**1.49.** (*a*) $\{a, b, d, e\}$; (*b*) $\{a\}$; (*c*) $\{a, d, f\}$; (*d*) $\{g\}$; (*e*) $\varnothing$; (*f*) $\{c, h\}$; (*g*) $\varnothing$; (*h*) $\{a, d\}$

**1.53.** $A \cup B = (A^c \cap B^c)^c$

**1.54.** (*b*) $A = \{a\}$; $B = \{b\}$; $C = \{c\}$, $A \cup (B \backslash C) = \{a\}$, $(A \cup B) \backslash (A \cup C) = \{b\}$

**1.56.** See Fig. 1-18.



(*a*) (*b*) (*c*)

**Fig. 1-18**

**1.57.** (*a*) $A = (B^c \cup A) \cap (A \cup B)$
(*b*) $(A \cup B) \cap (A \cup B^c) \cap (A^c \cup B) \cap (A^c \cup B^c) = \varnothing$

**1.59.** (*b*), (*c*), and (*d*)

**1.60.** (*a*) 17; (*b*) 8; (*c*) 11; (*d*) 8; (*e*) 0

**1.61.** (*a*) 55; (*b*) 75; (*c*) 15, (*d*) 55

**1.62.** (*a*) 80; (*b*) 75; (*c*) 25; (*d*) 35; (*e*) 60; (*f*) 45

**1.63.** Use the data to first fill in the Venn diagram of $A$ (air-conditioning), $R$ (radio), $W$ (power windows) in Fig. 1-19. Then: (*a*) 5; (*b*) 4; (*c*) 2; (*d*) 4; (*e*) 6; (*f*) 11; (*g*) 23; (*h*) 2.

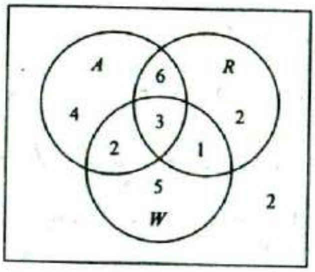


**Fig. 1-19**

**1.64.** Three elements: $\{a, b\}$, $\{c\}$, and $\{d, e, f\}$. (*a*) F; (*b*) F; (*c*) F; (*d*) T; (*e*) F; (*f*) T; (*g*) F; (*h*) T

**1.65.** Four elements: $\varnothing$, $\{1\}$, $\{2, 3\}$, and $\{3, 4\}$. (*a*) F; (*b*) F; (*c*) T; (*d*) F; (*e*) T; (*f*) T; (*g*) T; (*h*) T

**1.66.** (*a*) $\mathscr{P}(A)$ has $2^5 = 32$ elements as follows (where $135 = \{1, 3, 5\}$):

$[\varnothing, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, 24, 25, 34, 35, 45, 123, 124, 125, 134, 135, 145, 234, 235, 245, 345, 1234, 1235, 1245, 1345, 2345, A]$

(*b*) $\mathscr{B}$ has 6 elements: [123, 124, 125, 134, 135, 145].

**1.67.** $A$ has 3 elements, so $\mathscr{P}(A)$ has $2^3 = 8$ elements as follows (where $[ab, c] = [\{ab\}, \{c\}]$):

$$\{\varnothing,\ [ab],\ [c],\ [def],\ [ab, c],\ [ab, def], [c,\ def],\ A\}$$

Note that $\mathscr{P}(A)$ is a collection of collections of sets.

**1.68.** Let $X$ be an arbitrary element of $\mathscr{P}(A)$. For each $a \in A$, there are two possibilities, $a \in X$ or $a \not\subseteq X$. Since there are $m$ elements in $A$, there are $2 \cdot 2 \cdot \ldots \cdot 2$ ($m$ factors) $= 2^m$ different sets $X$. That is, $\mathscr{P}(A)$ has $2^m$ elements.

**1.69.** See Fig. 1-20. (*a*) Yes; (*b*) no; (*c*) yes; (*d*) yes

**1.70.** See Fig. 1-21. (*a*) No; (*b*) yes; (*c*) yes; (*d*) no

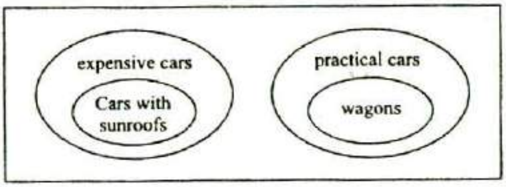


**Fig. 1-20**

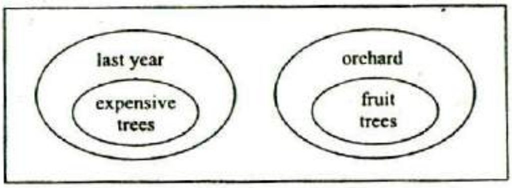


**Fig. 1-21**

**1.71.** See Fig. 1-22. (*a*) Yes; (*b*) yes; (*c*) yes; (*d*) no

**1.72.** See Fig. 1-23. (*a*) Yes; (*b*) yes; (*c*) no

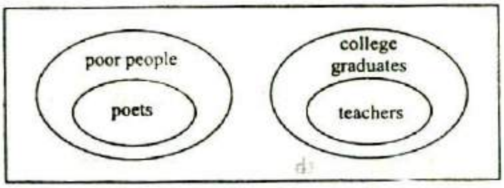


**Fig. 1-22**

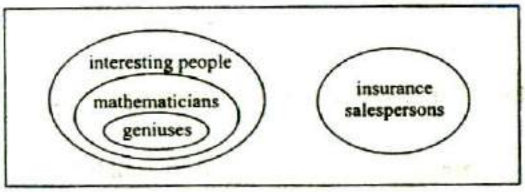


**Fig. 1-23**

# Chapter 2

# Sets and Elementary Properties of the Real Numbers

## 2.1 INTRODUCTION

This chapter investigates some sets and basic properties of the real numbers **R** and the integers

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

(The letter **Z** comes from the word *Zahlen* which means number in German.)

The following simple rules concerning the addition and multiplication of these numbers are assumed:

(*a*) Associative law for multiplication and addition:

$$(a+b)+c = a+(b+c) \qquad \text{and} \qquad (ab)c = a(bc)$$

(*b*) Commutative law for multiplication and addition:

$$a+b = b+a \qquad \text{and} \qquad ab = ba$$

(*c*) Distributive law:

$$a(b+c) = ab+ac$$

(*d*) Additive identity and multiplicative identity: There exists a zero element 0 and a unity element 1 such that, for any number $a$,

$$a+0 = 0+a = a \qquad \text{and} \qquad a \cdot 1 = 1 \cdot a = a$$

(*e*) Additive inverse (negative): For any number $a$, there exists its negative $-a$ such that

$$a+(-a) = (-a)+a = 0$$

(*f*) Multiplicative inverse: For any number $a \neq 0$, there exists an inverse $a^{-1}$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Subtraction and division (except by 0) are defined in **R** by

$$a - b \equiv a + (-b) \qquad \text{and} \qquad a \cdot b^{-1}$$

Observe that subtraction uses property (*e*) of negatives, and division uses property (*f*) of inverses.

**Warning**. The last property (*f*) holds for the real numbers **R** and the rational numbers **Q**, but does not hold for the integers **Z**. That is, one can add, subtract, multiply, and divide (except by 0) in **R** and **Q**, but only add, subtract, and multiply in **Z**.

## 2.2 REAL NUMBER SYSTEM R

The notation **R** will be used to denote the real numbers. These are the numbers one uses in basic arithmetic and algebra. **R** together with its properties is called the *real number system*.

The set **R** of real numbers includes the following sets of numbers:

$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} =$ set of *integers* (signed whole numbers)
$\mathbf{P} = \{1, 2, 3, \ldots\} =$ set of positive integers (counting numbers)
$\mathbf{N} = \{0, 1, 2, \ldots\} =$ set of nonnegative integers (natural numbers)
$\mathbf{Q} =$ set of *rational numbers*, i.e. numbers which are ratios of integers

Examples of rational numbers are 2/3 and $-3/4$. Those real numbers that are not rational, such as $\pi$ and $\sqrt{2}$, i.e., real numbers which cannot be represented as the ratio of integers, are called *irrational numbers*. The integer 0 is also a real number. Furthermore, for each positive real number, there is a corresponding negative real number.

**Real Line R, Decimal Expansion**

One of the most important properties of the real numbers is that they can be represented graphically by points on a straight line. Specifically, as pictured in Fig. 2-1, a point, called the *origin*, is chosen to represent 0, and another point, usually to the right of 0, is chosen to represent 1. The direction from 0 to 1 is the *positive direction* and is sometimes indicated by an arrowhead at the end of the line. The distance between 0 and 1 is the *unit length*. Now there is a natural way to pair off the points on the line and the real numbers, that is, where each point on the line corresponds to a unique real number and vice versa. The positive real numbers are those to the right of 0 (on the same side as 1) and the negative numbers are those to the left of 0. The points representing the rational numbers 5/4 and $-3/2$ are indicated in Fig. 2-1. We refer to such a line as the *real line* or the *real line* **R**.

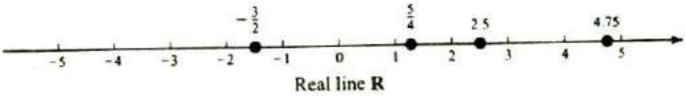


Fig. 2-1

Real numbers can also be represented by decimals. The decimal expansion of a rational number will either stop as in $\frac{3}{4} = 0.75$ or will have a pattern that repeats indefinitely, such as $\frac{17}{11} = 1.545454\ldots$. Even when the decimal expansion stops, it can be rewritten using repeated 9's, for example, $\frac{3}{4} = 0.74999\ldots$. The decimal expansion of an irrational number never stops nor does it have a repeating pattern. The points representing the decimal 2.5 and 4.75 are indicated in Fig. 2-1.

## 2.3 ORDER AND INEQUALITIES

Let $a$ and $b$ be real numbers. We say $a$ is *less* than $b$, written

$$a < b$$

if the difference $b - a$ is positive. Geometrically, $a < b$ if and only if the point $a$ lies to the left of the point $b$ on the real line **R**.

Observe that we define order in **R** in terms of the positive real numbers denoted by $\mathbf{R}^+$. All the usual properties of this order relation are a consequence of the following two properties of the positive real numbers $\mathbf{R}^+$:

[$\mathbf{P}_1$] If $a$ and $b$ are positive, then $a + b$ and $ab$ are positive.
[$\mathbf{P}_2$] For any real number $a$, either $a$ is positive, $a = 0$, or $-a$ is positive.

The following additional notation and terminology are used:

| | |
|---|---|
| $a > b$, means $b < a$; | read: *a is greater than b* |
| $a \leq b$, means $a < b$ or $a = b$; | read: *a is less than or equal to b* |
| $a \geq b$, means $b \leq a$; | read: *a is greater than or equal to b* |

Any statement of the form $a < b$, $a \leq b$, $a > b$, or $a \geq b$ is called an *inequality*; and any statement of the form $a < b$ or $a > b$ is sometimes called a *strict inequality*.

**EXAMPLE 2.1**

(*a*) $2 < 5$; $-6 < -3$; $4 \leq 4$; $5 > -8$; $6 \geq 0$; $-7 \leq 0$.

(*b*) Sorting the numbers 4, $-7$, 9, $-2$, 6, 0, $-11$, 13, $-1$, $-5$ in increasing order we obtain:

$$-11, -7, -5, -2, -1, 0\ 3, 4, 6, 9, 13$$

(*c*) A real number $a$ is positive iff $a > 0$, and $a$ is negative iff $a < 0$. (Recall that "iff" is short for "if and only if.")

(*d*) The statement $2 < x < 7$ means $2 < x$ and $x < 7$; hence $x$ will lie between 2 and 7 on the real line **R**.

Basic properties of the inequality relations follow.

**Proposition 2.1**: Let $a, b, c$ be real numbers. Then:

(i) $a \leq a$.
(ii) If $a \leq b$ and $b \leq a$, then $a = b$.
(iii) If $a \leq b$ and $b \leq c$, then $a \leq c$.

**Proposition 2.2 (Law of Trichotomy)**: For any real numbers $a$ and $b$, exactly one of the following holds:

$$a < b, \qquad a = b, \qquad \text{or} \qquad a > b$$

**Proposition 2.3**: Let $a, b, c$ be real numbers such that $a \leq b$. Then:

(i) $a + c \leq b + c$.
(ii) $ac \leq bc$ when $c > 0$; but $ac \geq bc$ when $c < 0$.

**Remark**: Observe that the above two properties $[\mathbf{P}_1]$ and $[\mathbf{P}_2]$ of the positive real numbers $\mathbf{R}^+$ are also true for the positive rational numbers $\mathbf{Q}^+$ viewed as a subset of the rational numbers **Q**, and the positive integers $\mathbf{P} = \mathbf{Z}^+$ viewed as a subset of the integers **Z**. Accordingly, Propositions 2.1, 2.2, and 2.3 also hold for the rational numbers **Q** and the integers **Z**.

## 2.4 ABSOLUTE VALUE, DISTANCE

The *absolute value* of a real number $a$, denoted by $|a|$, may be viewed as the distance between $a$ and the origin 0 on the real line **R**. Formally, $|a| = a$ or $-a$ according as $a$ is positive or negative, and $|0| = 0$. That is:

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{if } a < 0 \end{cases}$$

Accordingly, $|a|$ is always positive when $a \neq 0$. Intuitively, $|a|$ may be viewed as the magnitude of $a$ without regard to sign.

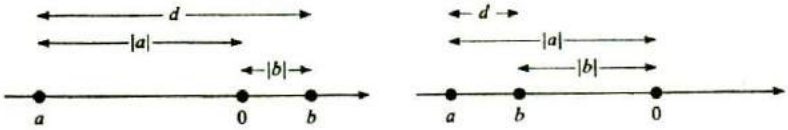
The distance $d$ between two points (real numbers) $a$ and $b$ is denoted by $d(a, b)$ and is obtained from the formula

$$d = d(a, b) = |a - b| = |b - a|$$

Alternatively:

$$d = \begin{cases} |a| + |b|, & \text{if } a \text{ and } b \text{ have different signs} \\ |a| - |b|, & \text{if } a \text{ and } b \text{ have the same sign and } |a| \geq |b| \end{cases}$$

These two cases are pictured in Fig. 2-2.



(*i*) $d = |a| + |b|$ (*ii*) $d = |a| - |b|$

**Fig. 2-2**

**EXAMPLE 2.2**

(*a*) $|-3| = 3$, $|7| = 7$, $|-13| = 13$, $|4.25| = 4.25$, $|-0.75| = 0.75$.

(*b*) $|2-7| = |-5| = 5$, $|7-2| = |5| = 5$, $|-3-8| = |-11| = 11$.

(*c*) Using Fig. 2-2,

$$d(-2,9) = 2+9 = 11, \qquad d(5,8) = 8-5 = 3, \qquad d(-4,-11) = 11-4 = 7$$

The following proposition gives some properties of the absolute value function. [Problems 2.14 and 2.15 prove (iii) and (iv).]

**Proposition 2.4:** Let $a$ and $b$ be any real numbers.

(i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$.
(ii) $-|a| \leq a \leq |a|$.
(iii) $|ab| = |a|\,|b|$.
(iv) $|a \pm b| \leq |a| + |b|$.
(v) $||a| - |b|| \leq |a \pm b|$.

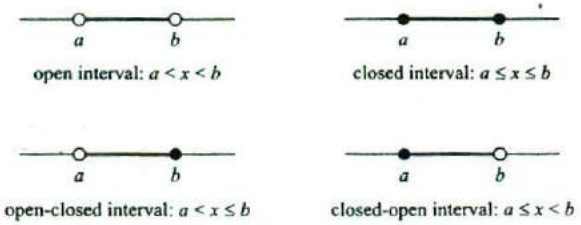
## 2.5 INTERVALS

Let $a$ and $b$ be distinct real numbers with, say, $a < b$. The *intervals* with *endpoints a* to $b$ are denoted and defined as follows:

$(a,b) = \{x : a \leq x \leq b\}$, open interval from $a$ to $b$
$[a,b] = \{x : a \leq x \leq b\}$, closed interval from $a$ to $b$
$(a,b] = \{x : a < x \leq b\}$, open-closed interval from $a$ to $b$
$[a,b) = \{x : a \leq x < b\}$, closed-open interval from $a$ to $b$

Observe that an interval is open if it does not include its endpoints and is closed if it does include its endpoints. Also, a parenthesis "(" or ")" is used to indicate that an endpoint does not belong to the interval, and a bracket "[" or "]" is used to indicate that an endpoint does belong to the interval.

Figure 2-3 shows how we picture each of the above four intervals on the real line **R**. Notice that in each case the endpoints $a$ and $b$ are circled, the line segment between $a$ and $b$ is thickened, and the circle about the endpoint is filled if the endpoint belongs to the interval.



open interval: $a < x < b$ closed interval: $a \le x \le b$

open-closed interval: $a < x \le b$ closed-open interval: $a \le x < b$

**Fig. 2-3**

**EXAMPLE 2.3**

(*a*) Find the interval satisfying each inequality, i.e., rewrite the inequality in terms of $x$ alone:

$$(1)\ 2 \le x - 5 \le 8, \quad (2)\ -1 \le x + 3 \le 4, \quad (3)\ -6 \le 3x \le 12, \quad (4)\ -6 \le -2x \le 4$$

(1) Add 5 to each side to obtain $7 \le x \le 13$.

(2) Add $-3$ to each side to obtain $-4 \le x \le 1$.

(3) Divide each side by 3 (or: multiply by $\frac{1}{3}$) to obtain $-2 \le x \le 4$.

(4) Divide each side by $-2$ (or: multiply by $-\frac{1}{2}$) and reverse inequalities to obtain $-6 \le x \le 3$.

(*b*) The inequality $|x| < 5$ may be interpreted to mean that the distance between $x$ and the origin 0 is less than 5; hence $x$ must lie between $-5$ and 5 on the real line **R**. In other words,

$$|x| < 5 \qquad \text{and} \qquad -5 < x < 5,$$

have the same meaning and, similarly,

$$|x| \le 5 \qquad \text{and} \qquad -5 \le x \le 5$$

have the same meaning.

**Definition**: A set $A$ of real numbers is said to be *dense* in **R** if every open interval contains a point of $A$ or, equivalently, if there is a point of $A$ between any two points in **R**.

The following theorem applies.

**Theorem 2.5**: The rational numbers **Q** are dense in **R**.

The proof of the above theorem lies beyond the scope of this text. It is closely related to the fact that every real number may be expressed as an infinite decimal or, equivalently, that every real number is the limit of a sequence of rational numbers.

### Infinite Intervals

Let $a$ be any real number. Then the set of real numbers $x$ satisfying $x < a$, $x \le a$, $x > a$, or $x \ge a$, is called an *infinite* interval with endpoint $a$. The interval is said to be *closed* or *open* according as the endpoint $a$ does or does not belong to the interval. The four infinite intervals may also be denoted and defined as follows:

$$(-\infty, a) = \{x : x < a\} \qquad (a, \infty) = \{x : x > a\}$$
$$(-\infty, a] = \{x : x \le a\} \qquad [a, \infty) = \{x : x \ge a\}$$

Note that the infinity symbol $\infty$ means all the numbers in the positive direction of $a$, whereas the minus infinity symbol $-\infty$ means all the numbers in the negative direction of $a$. A parenthesis is used with $\infty$ and $-\infty$ since they do not represent numbers in the interval. These infinite intervals are pictured in Fig. 2-4.

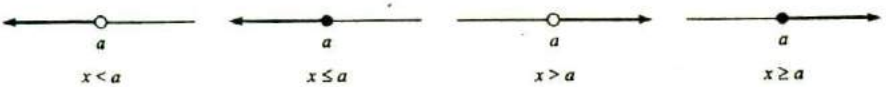


Fig. 2-4

## 2.6 BOUNDED SETS, COMPLETION PROPERTY

Let $A$ be a set of real numbers. Then $A$ is said to be:

(i) bounded, (ii) bounded from above, (iii) bounded from below

according as there exists a real number $M$ such that, for every $x \in A$:

$$\text{(i) } |x| \leq M, \quad \text{(ii) } x \leq M, \qquad \text{(iii) } M \leq x$$

The number $M$ is called a *bound* in (i), an *upper bound* in (ii), and a *lower bound* in (iii). Note that $A$ is bounded if and only if $A$ is a subset of some finite interval. Specifically, $M$ is a bound of $A$ if and only if $A$ is a subset of $[-M, M]$.

If $A$ is finite then $A$ is necessarily bounded. If $A$ is infinite, then $A$ may be bounded, bounded from above (below), or unbounded.

**EXAMPLE 2.4**

(*a*) $A = \{1, 1/2, 1/3, \ldots, 1/n, \ldots\}$ is bounded since $A$ is certainly a subset of the closed *unit* interval $I = [0, 1]$.

(*b*) $B = \{2, 4, 6, \ldots\}$ is unbounded, but it is bounded from below.

(*c*) $C = \{\ldots, -5, -3, -1\}$ is unbounded, but it is bounded from above.

(*d*) $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is unbounded. It has neither an upper bound nor a lower bound.

**Definition**: Let $A$ be a set of real numbers. A number $M$ is called the *least upper bound* or *supremum* of $A$, written

$$M = \sup(A)$$

if $M$ is an upper bound of $A$ but any number less than $M$ is not an upper bound of $A$, that is, for any positive number $\epsilon$, there exist $a \in A$ such that, $M - \epsilon < a$.

The following statement applies.

**Completion Property of R**: If a set $A$ of real numbers is bounded from above, then $\sup(A)$ exists.

The real numbers **R** are said to be *complete* since it satisfies the above property. We note that the rational numbers **Q** is not complete as seen by the following example.

**EXAMPLE 2.5** Let $A$ be the following subset of the rational numbers **Q**:

$$A = \{x \in \mathbf{Q} : x > 0, x^2 < 3\}$$

Observe that $A$ is bounded. However $\sup(A)$ does not exist. We cannot let $\sup(A) = \sqrt{3}$ since $\sqrt{3}$ is not a rational number.

The next two theorems (see Problems 6.17 and 6.49) follow from the completion property of **R**.

**Nested Interval Theorem:** The intersection $S = \cap_n I_n$ of a nested sequence of closed intervals is not empty. [A sequence $\{I_n\}$ of intervals is nested if $I_1 \supseteq I_2, \ldots$.]

**Heine-Borel Theorem:** Let $\mathscr{C}$ be a collection of open intervals which contain a closed interval $A = [a, b]$. Then a finite subcollection of $\mathscr{C}$ contains $A$.

## 2.7 INTEGERS Z (OPTIONAL MATERIAL)

The notation **Z** is used to denote the integers, the "signed whole numbers"; that is,

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

As noted above, **Z** satisfies all the properties in Section 2.1 except ($f$). Accordingly, one can always add, subtract, and multiply integers obtaining integers. However, the quotient of two integers need not be an integer, hence the question of divisibility plays an important role in **Z**.

One fundamental property of the integers **Z** is mathematical induction, which was discussed in Section 1.11. We give an equivalent statement below.

### Well-Ordering Principle

A property of the positive integers **P** which is equivalent to the principle of induction, although apparently very dissimilar, is the well-ordering principle (proved in Problem 2.32). Namely:

**Theorem 2.6 (Well-Ordering Principle):** Let $S$ be a nonempty set of positive integers. Then $S$ contains a *least element*; that is, $S$ contains an element $a$ such that $a \leq s$ for every $s$ in $S$.

Generally speaking, an ordered set $S$ is said to be *well-ordered* if every subset of $S$ contains a first element. Thus Theorem 2.6 states that **P** is well-ordered.

A set $S$ of integers is said to be *bounded from below* if every element of $S$ is greater than some integer $m$ (which may be negative). (The number $m$ is called a *lower bound* of $S$.) A simple corollary of the above theorem follows:

**Corollary 2.7:** Let $S$ be a nonempty set of integers which is bounded from below. Then $S$ contains a least element.

### Division Algorithm

The following fundamental property of arithmetic (proved in Problems 2.36 and 2.37) is essentially a restatement of the result of long division.

**Theorem 2.8 (Division Algorithm):** Let $a$ and $b$ be integers with $b \neq 0$. Then there exists integers $q$ and $r$ such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|$$

Also, the integers $q$ and $r$ are unique.

The number $q$ in the above theorem is called the *quotient*, and $r$ is called the *remainder*. We stress the fact that $r$ must be nonnegative. The theorem also states that

$$a - bq = r$$

This equation will be used subsequently.

**EXAMPLE 2.6**

($a$) Let $a = 4461$ and $b = 16$. Dividing $a = 4461$ by $b = 16$ yields a quotient $q = 278$ and remainder $r = 13$. As expected, $a = bq + r$, that is,

$$4461 = 16(278) + 13$$

($b$) Let $a = -262$ and $b = 3$. Here $a$ is negative. First divide $|a| = 262$ by $b = 3$ to obtain a quotient $q' = 87$ and a remainder $r' = 1$; hence

$$262 = 3(87) + 1$$

We need $a = -262$, so we multiply by $-1$ obtaining

$$-262 = 3(-87) - 1$$

However, $-1$ is negative and hence cannot be $r$. We correct this by adding and subtracting $b = 3$ as follows:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Therefore, $q = -(q' + 1) = -88$ and $r = b - r' = 2$.

**Remark**: The result in Example 2.6(*b*) is true in general. That is, suppose $a$ is negative and suppose we want to find the quotient $q$ and remainder $r$ when $a$ is divided by $b$. First divide $|a|$ by $b$ to obtain a positive quotient $q'$ and remainder $r'$. If $r' \neq 0$, then set

$$q = -(q' + 1) \qquad \text{and} \qquad r = b - r'$$

but if $r' = 0$, then set $q = -q'$ and $r = r' = 0$.

### Divisibility

Let $a$ and $b$ be integers with $a \neq 0$. Suppose $ac = b$ for some integer $c$. We then say that a *divides b* or $b$ is *divisible* by $a$ and write

$$a|b$$

We may also say that $b$ is a *multiple* of $a$ or that $a$ is a *factor* or *divisor* of $b$. If $a$ does not divide $b$, we will write $a \nmid b$.

**EXAMPLE 2.7**

(*a*) $3|6$ since $3 \cdot 2 = 6$; and $-4|28$ since $(-4)(-7) = 28$.

(*b*) The divisors:

- (i) of 1 are $\pm 1$
- (ii) of 2 are $\pm 1, \pm 2$
- (iii) of 4 are $\pm 1, \pm 2, \pm 4$
- (iv) of 5 are $\pm 1, \pm 5$
- (v) of 7 are $\pm 1, \pm 7$,
- (vi) of 9 are $\pm 1, \pm 3, \pm 9$

(*c*) If $a \neq 0$, then $a|0$ since $a \cdot 0 = 0$.

(*d*) Every integer $a$ is divisible by $\pm 1$ and $\pm a$. These are sometimes called the *trivial divisors* of $a$.

Simple properties of divisibility follow.

- (i) If $a|b$ and $b|c$, then $a|c$.
- (ii) If $a|b$ then, for any integer $x$, $a|bx$.
- (iii) If $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.
- (iv) If $a|b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.
- (v) If $a|b$ and $b|a$, then $|a| = |b|$, i.e., $a = \pm b$.
- (vi) If $a|1$, then $a = \pm 1$.

Putting (ii) and (iii) together, we obtain the following important result.

**Proposition 2.9**: Suppose $a|b$ and $a|c$. Then, for any integers $x$ and $y$, $a|(bx + cy)$.

The expression $bx + cy$ will be called a *linear combination* of $b$ and $c$.

### Primes

A positive integer $p > 1$ is called a *prime number* or a *prime* if its only divisors are $\pm 1$ and $\pm p$, that is, if $p$ only has trivial divisors. If $n > 1$ is not prime, then $n$ is said to be *composite*. We note (Problem 2.31) that if $n > 1$ is composite then $n = ab$ where $1 < a, b < n$.

**EXAMPLE 2.8**

(*a*) The integers 2 and 7 are primes, whereas $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$ are composite.

(*b*) The primes less than 50 follow:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

(*c*) Although 21, 24, and 1729 are not primes, each can be written as a product of primes:

$$21 = 3 \cdot 7, \qquad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3, \qquad 1729 = 7 \cdot 13 \cdot 19$$

The Fundamental Theorem of Arithmetic states that every integer $n > 1$ can be written as a product of primes in essentially one way; it is a deep and somewhat difficult theorem to prove. However, using induction, it is easy at this point to prove that such a product exists. Namely:

**Theorem 2.10**: Every integer $n > 1$ can be written as a product of primes.

Note that a product may consist of a single factor so that a prime $p$ is itself a product of primes.

We prove Theorem 2.10 here, since its proof is relatively simple.

*Proof*: The proof is by induction. Let $n = 2$. Since 2 is prime, $n$ is a product of primes. Suppose $n > 2$, and the theorem holds for positive integers less than $n$. If $n$ is prime, then $n$ is a product of primes. If $n$ is composite, then $n = ab$ where $a, b < n$. By induction, $a$ and $b$ are products of primes; hence $n = ab$ is also a product of primes.

Euclid, who proved the Fundamental Theorem of Arithmetic, also asked whether or not there was a largest prime. He answered the question thus:

**Theorem 2.11**: There is no largest prime, that is, there exists an infinite number of primes.

*Proof*: Suppose there is a finite number of primes, say $p_1, p_2, \ldots, p_m$. Consider the integer

$$n = p_1 p_2 \cdots p_m + 1$$

Since $n$ is a product of primes (Theorem 2.10), it is divisible by one of the primes, say $p_k$. Note that $p_k$ also divides the product $p_1 p_2 \cdots p_m$. Therefore $p_k$ divides

$$n - p_1 p_2 \cdots p_m = 1$$

This is impossible, and so $n$ is divisible by some other prime. This contradicts the assumption that $p_1, p_2, \ldots, p_m$ are the only primes. Thus the number of primes is infinite, and the theorem is proved.

## 2.8 GREATEST COMMON DIVISOR, EUCLIDEAN ALGORITHM

Suppose $a$ and $b$ are integers, not both 0. An integer $d$ is called a *common divisor* of $a$ and $b$ if $d$ divides both $a$ and $b$, that is, if $d|a$ and $d|b$. Note that 1 is always a positive common divisor of $a$ and $b$, and that any common divisor of $a$ and $b$ cannot be greater than $|a|$ or $|b|$. Thus there exists a largest common divisor of $a$ and $b$; it is denoted by

$$\gcd\,(a, b)$$

and it is called the *greatest common divisor* of $a$ and $b$.

**EXAMPLE 2.9**

(*a*) The common divisors of 12 and 18 are $\pm 1, \pm 2, \pm 3, \pm 6$. Thus $\gcd\,(12, 18) = 6$. Similarly,

$$\gcd\,(12, -18) = 6, \qquad \gcd\,(12, -16) = 4, \qquad \gcd\,(29, 15) = 1, \qquad \gcd\,(14, 49) = 7$$

(*b*) For any integer $a$, we have $\gcd(1, a) = 1$.

(*c*) For any prime $p$, we have $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as $p|a$ or $p\nmid a$.

(*d*) Suppose $a$ is positive. Then $a|b$ if and only if $\gcd(a, b) = a$.

The following theorem (proved in Problem 2.43) gives an alternative characterization of the greatest common divisor.

**Theorem 2.12**: Let $d$ be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

**Corollary 2.13**: Suppose $d = \gcd(a, b)$. Then there exists integers $x$ and $y$ such that $d = ax + by$.

Another way to characterize the greatest common divisor, without using the inequality relation, follows:

**Theorem 2.14**: A positive integer $d = \gcd(a, b)$ if and only if $d$ has the following properties:
(1) $d$ divides both $a$ and $b$;
(2) if $c$ divides both $a$ and $b$, then $c|d$.

Simple properties of the greatest common divisor follow.

(*a*) $\gcd(a, b) = \gcd(b, a)$.
(*b*) If $x > 0$, then $\gcd(ax, bx) = x \cdot \gcd(a, b)$.
(*c*) If $d = \gcd(a, b)$, then $\gcd(a/d,\ b/d) = 1$.
(*d*) For any integer $x$, $\gcd(a, b) = \gcd(a, b + ax)$.

### Euclidean Algorithm

Let $a$ and $b$ be integers, and let $d = \gcd(a, b)$. One can always find $d$ by listing all the divisors of $a$ and then all the divisors of $b$ and then choosing the largest common divisor. This procedure does not find the integers $x$ and $y$ such that

$$d = ax + by$$

This subsection gives a very efficient algorithm for finding both $d = \gcd(a, b)$ and the above integers $x$ and $y$.

This algorithm, called the Euclidean algorithm, consists of repeatedly applying the division algorithm (long division). We illustrate the algorithm with an example.

**EXAMPLE 2.10** Let $a = 540$ and $b = 168$. We find $d = \gcd(a, b)$ by dividing $a$ by $b$ and then repeatedly dividing each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 2-5. The last nonzero remainder is 12. Thus

$$12 = \gcd(540, 168)$$

This follows from the fact that

$$\gcd(540, 168) = \gcd(168, 36) = \gcd(36, 24) = \gcd(24, 12) = 12$$

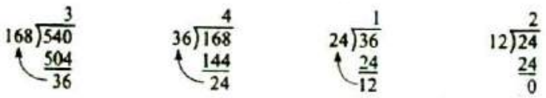


Fig. 2-5

Next we find $x$ and $y$ such that

$$12 = 540x + 168y$$

The first three quotients in Fig. 2-5 yield the equations:

$$\begin{array}{llll} (1) & 540 = 3(168) + 36 & \text{or} & 36 = 540 - 3(168) \\ (2) & 168 = 4(36) + 24 & \text{or} & 24 = 168 - 4(36) \\ (3) & 36 = 1(24) + 12 & \text{or} & 12 = 36 - 1(24) \end{array}$$

Equation (3) tells us that 12 is a linear combination of 36 and 24. We use (2) to replace 24 in (3) so we can write 12 as a linear combination of 168 and 36 as follows:

$$\begin{aligned} (4) \quad 12 &= 36 - 1[168 - 4(36)] = 36 - (168) + 4(36) \\ &= 5(36) - 1(168) \end{aligned}$$

We now use (1) in (4) so we can write 12 as a linear combination of 168 and 540 as follows:

$$\begin{aligned} 12 &= 5[540 - 3(168)] - 1(168) \\ &= 5(540) - 15(168) - 1(168) \\ &= 5(540) - 16(168) \end{aligned}$$

This is our desired linear combination. Thus $x = 5$ and $y = -16$.

### Least Common Multiple

Suppose $a$ and $b$ are nonzero integers. Note that $|ab|$ is a positive common multiple of $a$ and $b$. Thus there exists a smallest positive common multiple of $a$ and $b$; it is denoted by

$$\operatorname{lcm}(a, b)$$

and it is called the *least common multiple* of $a$ and $b$.

**EXAMPLE 2.11**

(*a*) $\operatorname{lcm}(2, 3) = 6$, $\operatorname{lcm}(4, 6) = 12$, $\operatorname{lcm}(9, 10) = 90$.

(*b*) For any positive integer $a$, we have $\operatorname{lcm}(1, a) = a$.

(*c*) For any prime $p$ and any positive integer $a$, $\operatorname{lcm}(p, a) = a$ or $\operatorname{lcm}(p, a) = ap$ according as $p|a$ or $p\nmid a$.

(*d*) Suppose $a$ and $b$ are positive integers. Then $a|b$ if and only if $\operatorname{lcm}(a, b) = b$.

The next theorem gives an important relationship between the greatest common divisor and the least common multiple.

**Theorem 2.15**: Suppose $a$ and $b$ are nonzero integers. Then

$$\operatorname{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)}$$

## 2.9 FUNDAMENTAL THEOREM OF ARITHMETIC

This section discusses the Fundamental Theorem of Arithmetic. First we need the notion of relatively prime integers.

Two integers $a$ and $b$ are said to be *relatively prime*, or *coprime*, if

$$\gcd(a, b) = 1$$

Accordingly, if $a$ and $b$ are relatively prime, then there exist integers $x$ and $y$ such that

$$ax + by = 1$$

Conversely, if $ax + by = 1$, then $a$ and $b$ are relatively prime.

**EXAMPLE 2.12**

(*a*) Observe that gcd $(12, 35) = 1$, gcd $(49, 18) = 1$, gcd $(21, 64) = 1$, gcd $(-28, 45) = 1$

(*b*) If $p$ and $q$ are distinct primes, then gcd $(p, q) = 1$.

(*c*) For any integer $a$, we have gcd $(a, a+1) = 1$. This follows from the fact that any common divisor of $a$ and $a+1$ must divide their difference $(a+1) - a = 1$.

The relation of being relatively prime is particularly important because of the following results. We will prove the second theorem here.

**Theorem 2.16**: Suppose gcd $(a, b) = 1$, and $a$ and $b$ both divide $c$. Then $ab$ divides $c$.

**Theorem 2.17**: Suppose $a|bc$, and gcd $(a, b) = 1$. Then $a|c$.

*Proof*: Since gcd $(a, b) = 1$, there exist $x$ and $y$ such that $ax + by = 1$. Multiplying by $c$ yields

$$acx + bcy = c$$

We have $a|acx$. Also, $a|bcy$ since, by hypothesis, $a|bc$. Hence $a$ divides the sum $acx + bcy = c$.

**Corollary 2.18**: Suppose a prime $p$ divides a product $ab$. Then

$$p|a \text{ or } p|b$$

This corollary dates back to Euclid. In fact, it is the basis of his proof of the fundamental theorem of arithmetic.

### Fundamental Theorem of Arithmetic

Theorem 2.10 asserts that every positive integer is a product of primes. Can different products of primes yield the same number? Clearly, we can rearrange the order of the prime factors, e.g.

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

The fundamental theorem of arithmetic (proved in Problem 2.49) says that this is the only way that two "different" products can give the same number. Namely:

**Theorem 2.19 (Fundamental Theorem of Arithmetic)**: Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

The primes in the factorization of $n$ need not be distinct. Frequently, it is useful to collect together all equal primes. Then $n$ can be expressed uniquely in the form

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the $m_i$ are positive and $p_1 < p_2 < \cdots < p_r$. This is called the *canonical factorization* of $n$.

**EXAMPLE 2.13** Let $a = 2^4 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$ and $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Find $d =$ gcd $(a, b)$ and $m =$ lcm $(a, b)$.

(*a*) First we find $d =$ gcd $(a, b)$. Those primes $p_i$ which appear in both $a$ and $b$, i.e., 2, 3, and 11, will also appear in $d$, and the exponent of $p_i$ in $d$ will be the smaller of its exponents in $a$ and $b$. Thus

$$d = \text{gcd } (a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(*b*) Next we find $m =$ lcm $(a, b)$. Those primes $p_i$ which appear in either $a$ and $b$, i.e., 2, 3, 5, 7, 11, 13 and 17 will also appear in $m$, and the exponent of $p_i$ in $m$ will be the larger of its exponents in $a$ and $b$. Thus

$$m = \text{lcm } (a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

## Solved Problems

### REAL NUMBER SYSTEM R, SETS OF NUMBERS

**2.1.** Assuming **R**, **Q**, **Q**′, **Z**, and **P** denote respectively, the real numbers, rational numbers, irrational numbers, integers, and positive integers, state whether each of the following is true or false:

(*a*) $-7 \in \mathbf{P}$ (*d*) $3\pi \in \mathbf{Q}$ (*g*) $\pi^2 \in \mathbf{R}$ (*j*) $-6 \in \mathbf{Q}$
(*b*) $\sqrt{2} \in \mathbf{Q}'$ (*e*) $\sqrt[3]{8} \in \mathbf{P}$ (*h*) $\sqrt{9/4} \in \mathbf{Q}'$ (*k*) $\sqrt{-4} \in \mathbf{R}$
(*c*) $4 \in \mathbf{Z}$ (*f*) $-2 \in \mathbf{Z}$ (*i*) $1/2 \in \mathbf{Z}$ (*l*) $6 \in \mathbf{R}$

(*a*) False. **P** only contains positive integers, $-7$ is negative.

(*b*) True. $\sqrt{2}$ cannot be expressed as the ratio of two integers; hence $\sqrt{2}$ is irrational.

(*c*) True. The integers **Z** contain all the "whole" numbers, so 4 is an integer.

(*d*) False. $\pi$ is not rational and neither is $3\pi$.

(*e*) True. $\sqrt[3]{8} = 2$ is a positive integer.

(*f*) True. **Z** contains both the positive and negative "whole" numbers.

(*g*) True. $\pi$ is real and so is $\pi^2$.

(*h*) False. $\sqrt{9/4} = 3/2$ is rational, not irrational.

(*i*) False. 1/2 is not an integer.

(*j*) True. The rational numbers include the integers.

(*k*) False. $\sqrt{-4} = 2i$ is not a real number.

(*l*) True. The real numbers include the integers.

**2.2.** Plot the numbers $\frac{5}{2}$, 3.8, $-4.5$, and $-3.3$ on the real line **R**.

The points corresponding to the numbers are shown in Fig. 2-6.

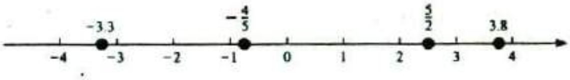


Fig. 2-6

**2.3.** Express each real number as an infinite decimal (that is, without ending in zeros): (*a*) 2/3, (*b*) 4/7, (*c*) 3/8.

(*a*) Dividing 2 by 3 yields $2/3 = 0.6666\ldots$.

(*b*) Dividing 4 by 7 yields the following where 571428 repeats:

$$4/7 = 0.571\,428\,571\,428\ldots$$

(*c*) Dividing 3 by 8 yields $3/8 = 0.375$, which is not an infinite decimal. However, for any nonzero digit $d$, one can show that $d = d'.999\ldots$ where $d' = d - 1$. Thus replace $5000\ldots$ by $4999\ldots$ to obtain the required infinite decimal

$$3/8 = 0.3749999\ldots$$

**2.4.** Consider (*a*) the rational numbers **Q** and (*b*) the irrational numbers **Q**′. Determine whether or not each is closed under the operations of addition and multiplication.

A set $S$ of real numbers is closed under addition and multiplication according as the sum and product of any numbers in $S$ still belongs to $S$.

(*a*) The sum and product of rational numbers are rational; hence **Q** is closed under addition and multiplication.

(*b*) The sum and product of irrational numbers, need not be irrational. For example, $\sqrt{2}+(-\sqrt{2})=0$ is not irrational, and $\sqrt{2}\sqrt{2}=2$ is not irrational. Thus **Q**′ is not closed under addition and not closed under multiplication.

**2.5.** Let (*a*) $E=\{2,4,6,\ldots\}$ and (*b*) $F=\{1,3,5,\ldots\}$. Determine whether or not each is closed under the operations of addition and multiplication.

(*a*) The sum and product of positive even integers are positive and even; hence $E$ is closed under addition and multiplication.

(*b*) The sum of two odd numbers is not odd, hence $F$ is not closed under addition. However, the product of two positive odd integers is positive and odd; hence $F$ is closed under multiplication.

## ORDER AND INEQUALITIES, ABSOLUTE VALUE

**2.6.** Insert the correct symbol, <, >, or =, between each pair of real numbers:

(*a*) 4 ____ −7 (*c*) $3^2$ ____ 9 (*e*) $3^2$ ____ 5.5

(*b*) −2 ____ −9 (*d*) −8 ____ $\pi$ (*f*) 6.25 ____ 8

For each pair of real numbers, say $a$ and $b$, determine their relative positions on the number line **R**; or, alternately, compute $b-a$, and write

$$a<b, \qquad a>b, \qquad \text{or} \qquad a=b$$

according as $b-a$ is positive, negative, or zero. Hence:

(*a*) $4>-7$, (*c*) $3^2=9$, (*e*) $3^2>5.5$,

(*b*) $-2>-9$, (*d*) $-8<\pi$, (*f*) $6.25<8$.

**2.7.** Rewrite the following geometric relationships between the given real numbers using the inequality notation: (*a*) $x$ lies to the right of 8; (*b*) $y$ lies to the left of −2; (*c*) $z$ lies between −3 and 7; (*d*) $t$ lies between 5 and 1.

Recall that $a<b$ means that $a$ lies to the left of $b$ on the real line **R**. Thus: (*a*) $x>8$ or $8<x$; (*b*) $y<-2$; (*c*) $-3<z$ and $z<7$ or, simply, $-3<z<7$; (*d*) $1<t<5$.

**2.8.** Sort the following numbers in increasing order (where $e=2.7814\ldots$):

$$5,\ -8,\ 2,\ -3,\ \pi,\ -2.8,\ 0,\ 9,\ e,\ -1.5,\ 3$$

The negative numbers will be on the left of 0, decreasing in magnitude (absolute value) from left to right, and the positive numbers will be on the right of 0 increasing in magnitude from left to right:

$$-8,\ -3,\ -2.8,\ -1.5,\ 0,\ 2,\ e,\ 3,\ \pi,\ 5,\ 9$$

**2.9.** Evaluate: (*a*) $|-4|$, $|6.2|$, $|0|$, $|-1.25|$

(*b*) $|2-5|$, $|-2+5|$, $|-2-5|$

(*c*) $|5-8|+|2-4|$, $|4-3|-|3-9|$

(*a*) The absolute value is the magnitude of the number without regard to sign. Hence:

$$|-4|=4, \qquad |6.2|=6.2, \qquad |0|=0, \qquad |-1.25|=1.25$$

(*b*) Evaluate inside the absolute value sign first:

$$|2-5|=|-3|=3, \qquad |-2+5|=|3|=3, \qquad |-2-5|=|-7|=7$$

(*c*) Evaluate inside the absolute value sign first:

$$|5-8|+|2-4|=|-3|+|-2|=3+2=5$$
$$|4-3|-|3-9|=|1|-|-6|=1-6=-5$$

**2.10.** Find the distance $d$ between each pair of integers:

(*a*) 3 and $-7$ (*c*) 1 and 9 (*e*) 4 and $-4$

(*b*) $-4$ and 2 (*d*) $-8$ and $-3$ (*f*) $-5$ and $-8$

The distance $d$ between $a$ and $b$ is given by $d=|a-b|=|b-a|$. Alternatively, as shown in Fig. 2-2, $d=|a|+|b|$ when $a$ and $b$ have different signs, and $d=|a|-|b|$ when $a$ and $b$ have the same sign and $|a|\geq|b|$. Thus:

(*a*) $d=3+7=10$ (*c*) $d=9-1=8$ (*e*) $d=4+4=8$

(*b*) $d=4+2=6$ (*d*) $d=8-3=5$ (*f*) $d=8-5=3$

**2.11.** Find all integers $n$ such that: (*a*) $1<2n-6<14$, (*b*) $2<8-3n<18$.

(*a*) Add 6 to the "three sides" to get $7<2n<20$. Then divide all sides by 2 (or multiply by 1/2) to get $3.5<n<10$. Hence

$$n=4,5,6,7,8,9$$

(*b*) Add $-8$ to the three sides to get $-6<-3n<10$. Divide by $-3$ (or multiply by $-1/3$) and, since $-3$ is negative, change the direction of the inequality to get

$$2>n>-3.3 \qquad \text{or} \qquad -3.3<n<2$$

Hence $n=-3,-2,-1,0,1$.

**2.12.** Prove Proposition 2.1(iii): If $a\leq b$ and $b\leq c$, then $a\leq c$.

The proposition is clearly true when $a=b$ or $b=c$. Thus we need only consider the case that $a<b$ and $b<c$. Hence $b-a$ and $c-b$ are positive. Therefore, by property $[\mathbf{P}_1]$ of the positive real numbers $\mathbf{R}^+$, the sum is also positive. That is,

$$(b-a)+(c-b)=c-a$$

is positive. Thus $a<c$ and hence $a\leq c$.

**2.13.** Prove Proposition 2.3: Let $a, b, c$ be real numbers such that $a \leq b$. Then:

(i) $a + c \leq b + c$, (ii) $ac \leq bc$ when $c > 0$; but $ac \geq bc$ when $c < 0$.

The proposition is certainly true when $a = b$. Hence we need only consider the case when $a < b$, that is, when $b - a$ is positive.

(i) The following difference is positive:

$$(b + c) - (a + c) = b - a$$

Hence $a + c < b + c$.

(ii) Suppose $c$ is positive. By property $[\mathbf{P}_1]$ of the positive real numbers $\mathbf{R}^+$, the following product is also positive:

$$c(b - a) = bc - ac$$

Thus $ac < bc$. Now suppose $c$ is negative. Then $-c$ is positive. Thus the following product is also positive:

$$(-c)(b - a) = ac - bc$$

Accordingly, $bc < ac$, whence $ac > bc$.

**2.14.** Prove Proposition 2.4(iii): $|ab| = |a||b|$.

The proof consists of a case-by-case analysis.

(*a*) Suppose $a = 0$ or $b = 0$.

Then $|a| = 0$ or $|b| = 0$, and so $|a||b| = 0$. Also $ab = 0$. Hence

$$|ab| = 0 = |a||b|$$

(*b*) Suppose $a > 0$ and $b > 0$.

Then $|a| = a$ and $|b| = b$. Hence

$$|ab| = ab = |a||b|$$

(*c*) Suppose $a > 0$ and $b < 0$.

Then $|a| = a$ and $|b| = -b$. Also $ab < 0$. Hence

$$|ab| = -(ab) = a(-b) = |a||b|$$

(*d*) Suppose $a < 0$ and $b > 0$.

Then $|a| = -a$ and $|b| = b$. Also $ab < 0$. Hence

$$|ab| = -(ab) = (-a)b = |a||b|$$

(*e*) Suppose $a < 0$ and $b < 0$.

Then $|a| = -a$ and $|b| = -b$. Also $ab > 0$. Hence

$$|ab| = ab = (-a)(-b) = |a||b|$$

**2.15.** Prove Proposition 2.4(iv): $|a \pm b| \leq |a| + |b|$.

Now $ab \leq |ab| = |a||b|$, and so $2ab \leq 2|a||b|$. Hence

$$(a + b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$$

But $\sqrt{(a + b)^2} = |a + b|$. Thus the square root of the above yields $|a + b| \leq |a| + |b|$.

Also,

$$|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$$

**2.16.** Plot and describe the absolute value function $f(x) = |x|$.

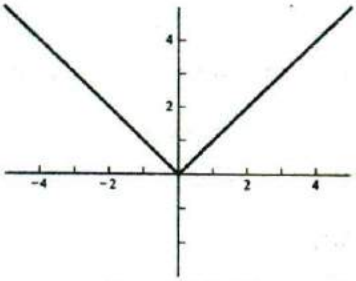
For nonnegative values of $x$ we have $f(x) = x$ and hence we obtain points of the form $(a, a)$, e.g.,

$$(0,0),\ (1,1),\ (2,2),\ldots$$

For negative values of $x$ we have $f(x) = -x$ and hence we obtain points of the form $(-a, a)$, e.g.,

$$(-1,1),\ (-2,2),\ (-3,3),\ldots$$

This yields the graph in Fig. 2-7. Observe that the graph of $f(x) = |x|$ lies entirely in the upper half-plane since $f(x) \geq 0$ for every $x \in \mathbf{R}$. Also, the graph consists of the line $y = x$ in the right half-plane and the line $y = -x$ in the left half-plane.



Graph of $f(x) = |x|$

**Fig. 2-7**

## INTERVALS

**2.17.** Rewrite each interval in set-builder form:

(*a*) $A = [-3, 5)$, (*b*) $B = (3, 8)$, (*c*) $C = [0, 4]$, (*d*) $D = (-7, -2]$.

Recall that a parenthesis means the endpoint does not belong to the interval, and that a bracket means that the endpoint does belong to the interval. Thus:

(*a*) $A = \{x : -3 \leq x < 5\}$ (*c*) $C = \{x : 0 \leq x \leq 4\}$

(*b*) $B = \{x : 3 < x < 8\}$ (*d*) $D = \{x : -7 < x \leq -2\}$

**2.18.** Describe and plot each interval:

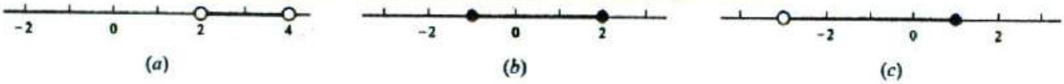
(*a*) $A = (2, 4)$, (*b*) $B = [-1, 2]$, (*c*) $C = (-3, 1]$.

(*a*) $A$ consists of all numbers between 2 and 4 without the endpoints 2 and 4. See Fig. 2-8(*a*).

(*b*) $B$ consists of all points between $-1$ and 2 including both endpoints $-1$ and 2. See Fig. 2-8(*b*).

(*c*) $C$ consists of all points between $-3$ and 1 including only the endpoint 1. See Fig. 2-8(*c*).

Note that a circle about an endpoint is filled or unfilled according as the endpoint does or does not belong to the interval.



(*a*) (*b*) (*c*)

**Fig. 2-8**

**2.19.** Find the interval satisfying each inequality, i.e., rewrite the inequality in terms of $x$ alone:

(*a*) $3 \leq x - 4 \leq 9$, (*b*) $-2 \leq x + 5 \leq 3$, (*c*) $-8 \leq 2x \leq 2$, (*d*) $-9 \leq -3x \leq 15$.

(*a*) Add 4 to each side to obtain $7 \leq x \leq 13$.

(*b*) Add $-5$ to each side to obtain $-7 \leq x \leq -2$.

(*c*) Divide each side 2 (or multiply by 1/2) to obtain $-4 \leq x \leq 1$.

(*d*) Divide each side $-3$ and reverse inequalities to obtain $3 \geq x \geq -5$ or, in the usual form, $-5 \leq x \leq 3$.

**2.20.** Rewrite without the absolute value sign: (*a*) $|x| < 3$, (*b*) $|x - 2| < 5$.

(*a*) Here $x$ lies between $-3$ and 3; hence $-3 < x < x$.

(*b*) Here $-5 < x - 2 < 5$ or $-3 < x < 7$.

**2.21.** Write each open interval in the form $|x - a| < r$: (*a*) $2 < x < 10$, (*b*) $-7 < x < 3$.

Here $a$ will be the "center" and $r$ will be the "radius" of the interval, i.e., $a$ is the midpoint and $r$ is half the length of the interval. Thus find the sum $s$ of the endpoints and divide by 2 to obtain $a$, and find the distance $d$ between the endpoints and divide by 2 to obtain $r$.

(*a*) $s = 12$ so $a = 6$; $d = 8$ so $r = 4$; hence $|x - 6| < 4$.

(*b*) $s = -4$ so $a = -2$; $d = 10$ so $r = 5$; hence $|x + 2| < 5$.

**2.22.** Under what condition will the intersection of two intervals be an interval?

The intersection of two intervals will always be an interval or a singleton set $\{a\}$ or the empty set $\varnothing$. In other words, if we view

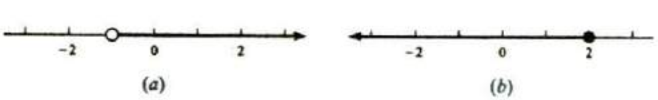
$$[a, a] = \{x : a \leq x \leq a\} = \{a\} \quad \text{and} \quad (a, a) = \{x : a < x < a\} = \varnothing$$

as intervals, then the intersection of any two intervals is always an interval.

**2.23.** Describe, plot, and write in interval notation each set: (*a*) $x > -1$, (*b*) $x \leq 2$.

(*a*) All numbers greater than $-1$, and hence all numbers to the right of $-1$ as pictured in Fig. 2-9(*a*). The interval notation is $(-1, \infty)$ where the infinity symbol $\infty$ means all the numbers in the positive direction of $-1$.

(*b*) All numbers less than or equal to 2, and hence 2 and all numbers to the left of 2 as pictured in Fig. 2-9(*b*). The interval notation is $(-\infty, 2])$ where the minus infinity symbol $-\infty$ means all the numbers in the negative direction of 2.



(*a*) (*b*)

**Fig. 2-9**

**2.24.** Are the integers **Z** dense in **R**?

A set $A$ is dense in **R** if every open interval contains an element of $A$. Thus **Z** is not dense in **R** since, for example, the open interval $(1/3, 1/2)$ does not contain an integer.

## BOUNDED AND UNBOUNDED SETS

**2.25.** State whether each set of real numbers is bounded or unbounded:

(*a*) $A = \{x : x < 5\}$ (*d*) $D = \{2, 4, 8, \ldots, 2^n, \ldots\}$

(*b*) $B = \{\ldots -10, -5, 0, 5, 10, \ldots\}$ (*e*) $E = \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, (\frac{1}{2})^n, \ldots\}$

(*c*) $C = \{2^{18}, 3^{-7}, 7, 0, 8^{35}\}$ (*f*) $F = \{1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{3}, \ldots\}$

(*a*) $A$ is unbounded. There are negative numbers whose absolute values are arbitrarily large.

(*b*) $B$ is unbounded.

(*c*) Although $C$ contains very large numbers, C is still bounded since $C$ is finite.

(*d*) $D$ is the set of powers of 2 and they are arbitrarily large. Thus $D$ is unbounded.

(*e*) $E$ is the set of positive powers of 1/2. Although $E$ is infinite, it is still bounded. In fact, $E$ is contained in the unit interval $I = [0, 1]$.

(*f*) Although $F$ is infinite it is still bounded. In fact, $F$ is contained in the interval $[-1, 1]$.

**2.26.** Which of the unbounded sets $A, B, D$ in Problem 2.25 are bounded from: (*a*) below, (*b*) above?

$A$ is bounded from above, $D$ is bounded from below, but $B$ has neither an upper nor a lower bound.

**2.27.** If two sets are bounded, what can be said about their union and intersection?

Both the union and intersection of bounded sets are bounded.

**2.28.** If two sets are unbounded, what can be said about their union and intersection?

The union of the sets must be unbounded, but the intersection could be either unbounded or bounded. For example, $A = (-\infty, 1]$ and $B = [-1, \infty)$ are unbounded, but $A \cap B = [-1, 1]$ is bounded. On the other hand, $C = [3, \infty)$ and $\mathbf{Z}$ are unbounded, and $C \cap \mathbf{Z} = \{3, 4, 5, \ldots\}$ is also unbounded.

## INTEGERS Z, MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

The reader is referred to Section 1.11 where the principle of mathematical induction is stated and discussed.

**2.29.** Suppose $a \neq 1$. Let $A$ be the assertion on the integers $n \geq 1$ defined by

$$A(n)\colon\ 1 + a + a^2 + a^3 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

Show that $A$ is true for all $n$.

$A(1)$ is true since

$$1 + a = \frac{a^2 - 1}{a - 1}$$

Assuming $A(n)$ is true, we add $a^{n+1}$ to both sides of $A(n)$, obtaining

$$\begin{aligned} 1+a+a^2+a^3+\cdots+a^n+a^{n+1} &= \frac{a^{n+1}-1}{a-1}+a^{n+1} \\ &= \frac{a^{n+1}-1+(a-1)a^{n+1}}{a-1} \\ &= \frac{a^{n+2}-1}{a-1} \end{aligned}$$

which is $A(n+1)$. Thus $A(n+1)$ is true whenever $A(n)$ is true. By the principle of induction, $A$ is true for all $n \in \mathbf{P}$.

**2.30.** Prove: If $n \in \mathbf{Z}$ and $n$ is a positive integer, then $n \geq 1$. (This is not true for the rational numbers $\mathbf{Q}$.) In other words, if $A(n)$ is the statement that $n \geq 1$, then $A(n)$ is true for every $n \in \mathbf{P}$.

**Method 1:** (Mathematical Induction)

$A(n)$ holds for $n = 1$ since $1 \geq 1$. Assuming $A(n)$ is true, that is, $n \geq 1$, add 1 to both sides to obtain

$$n+1 \geq 2 > 1$$

which is $A(n+1)$. That is, $A(n+1)$ is true whenever $A(n)$ is true. By the principle of mathematical induction, $A$ is true for every $n \in \mathbf{P}$.

**Method 2:** (Well-Ordering Principle)

Suppose there does exist a positive integer less than 1. By the well-ordering principle, there exists a least positive integer $a$ such that

$$0 < a < 1$$

Multiplying the inequality by the positive integer $a$ we obtain

$$0 < a^2 < a$$

Therefore, $a^2$ is a positive integer less than $a$ which is also less than 1. This contradicts $a$'s property of being the least positive integer less than 1. Thus there exists no positive integer less than 1.

**2.31.** Suppose $a$ and $b$ are positive integers. Prove: (*a*) If $b \neq 1$, then $a < ab$. (*b*) If $ab = 1$, then $a = 1$ and $b = 1$. (*c*) If $n$ is composite, then $n = ab$ where $1 < a, b < n$.

(*a*) By Problem 2.30, $b > 1$. Hence $b - 1 > 0$, that is, $b - 1$ is positive. By the property $[\mathbf{P}_1]$ of the positive integers $\mathbf{P}$, the following product is also positive:

$$a(b-1) = ab - a$$

Thus $a < ab$, as required.

(*b*) Suppose $b \neq 1$. By (*a*), $a < ab = 1$. This contradicts Problem 2.30; hence $b = 1$. It then follows that $a = 1$.

(*c*) If $n$ is not prime, then $n$ has a positive divisor $a$ such that $a \neq 1$ and $a \neq n$. Then $n = ab$ where $b \neq 1$ and $b \neq n$. Thus, by Problem 2.30 and by part (*a*), $1 < a, b < ab = n$.

**2.32.** Prove Theorem 2.6 (Well-Ordering Principle): Let $S$ be a nonempty set of positive integers. Then $S$ contains a least element.

Suppose $S$ has no least element. Let $M$ consist of those positive integers which are less than every element of $S$. Then $1 \in M$; otherwise, $1 \in S$ and 1 would be a least element of $S$. Suppose $k \in M$. Then $k$ is less than every element of $S$. Therefore $k + 1 \in M$; otherwise $k + 1$ would be a least element of $S$.

By the principle of mathematical induction, $M$ contains every positive integer. Thus $S$ is empty. This contradicts the hypothesis that $S$ is nonempty. Accordingly, the original assumption that $S$ has no least element cannot be true. Thus the theorem is true.

**2.33.** Prove the Principle of Mathematical Induction II: Let $A(n)$ be an assertion defined on the integers $n \geq 1$ such that:

(i) $A(1)$ is true.

(ii) $A(n)$ is true whenever $P(k)$ is true for all $1 \leq k < n$.

Then $A$ is true for all $n \geq 1$.

Let $S$ be the set of integers $n \geq 1$ for which $A$ is not true. Suppose $S$ is not empty. By the well-ordering principle, $S$ contains a least element $s_0$. By (i), $s_0 \neq 1$.

Since $s_0$ is the least element of $S$, $A$ is true for every integer $k$ where $1 \leq k < s_0$. By (ii), $A$ is true for $s_0$. This contradicts the fact that $s_0 \in S$. Hence $S$ is empty, and so $A$ is true for every integer $n \geq 1$.

## DIVISION ALGORITHM

**2.34.** For each pair of integers $a$ and $b$, find integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < |b|$:

(*a*) $a = 258$ and $b = 12$ (*c*) $a = -381$ and $b = 14$

(*b*) $a = 573$ and $b = -16$ (*d*) $a = -433$ and $b = -17$

(*a*) Here $a$ and $b$ are positive. Simply divide $a$ by $b$, that is, 258 by 12, to obtain the quotient $q = 21$ and the remainder $r = 6$.

(*b*) Here $a$ is positive, but $b$ is negative. Divide $a$ by $|b|$, that is, 573 by 16, to obtain a quotient $q' = 35$ and remainder $r' = 13$. Then

$$573 = (16)(35) + 13 = 573 = (-16)(-35) + 13$$

That is, $q = -q' = -35$ and $r = r' = 13$.

(*c*) Here $a$ is negative and $b$ is positive. Thus we have to make some adjustments to be sure that $0 \leq r < |b|$. Divide $|a| = 381$ by $b = 14$ to obtain the quotient $q' = 27$ and remainder $r' = 14$. Therefore,

$$381 = (14)(27) + 3 \qquad \text{and so} \qquad -381 = (14)(-27) - 3$$

We add and subtract $b = 14$ as follows:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Thus $q = -28$ and $r = 11$. Alternatively, $q = -(q' + 1) = -28$ and $r = b - r' = 11$.

(*d*) Divide $|a| = 433$ by $|b| = 17$ to obtain a quotient $q' = 25$ and $r' = 8$. Then

$$433 = (17)(25) + 8 \qquad \text{and so} \qquad -433 = (-17)(25) - 8$$

We add and subtract $|b| = 17$ as follows:

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9$$

Thus $q = 26$ and $r = 9$. Thus $q = q' + 1$ and $r = b - r'$.

**2.35.** Prove $\sqrt{2}$ is not rational, that is, $\sqrt{2} \neq a/b$ where $a$ and $b$ are integers.

Suppose $\sqrt{2}$ is rational and $\sqrt{2} = a/b$ where $a$ and $b$ are integers reduced to lowest terms, i.e. gcd $(a, b) = 1$. Squaring both sides yields

$$2 = \frac{a^2}{b^2} \qquad \text{or} \qquad a^2 = 2b^2$$

Then 2 divides $a^2$. Since 2 is a prime, $2|a$. Say $a = 2c$. Then

$$2b^2 = a^2 = 4c^2 \qquad \text{or} \qquad b^2 = 2c^2$$

Then 2 divides $b^2$. Since 2 is a prime, $2|b$. Thus 2 divides both $a$ and $b$. This contradicts the assumption that gcd $(a, b) = 1$. Therefore, $\sqrt{2}$ is not rational.

**2.36.** Prove Theorem 2.8 (Division Algorithm) for the case of positive integers. That is, assuming $a$ and $b$ are positive integers, prove that there exist nonnegative integers $q$ and $r$ such that

$$a = bq + r \qquad \text{and} \qquad 0 \le r < b \tag{$*$}$$

If $a < b$, choose $q = 0$ and $r = a$; and if $a = b$, choose $q = 1$ and $r = 0$. In either case, $q$ and $r$ satisfy $(*)$.

The proof is now by induction on $a$. If $a = 1$ then $a < b$ or $a = b$; hence the theorem holds when $a = 1$. Suppose $a > b$. Then $a - b$ is positive and $a - b < a$. By induction, the theorem holds for $a - b$. Thus there exist $q'$ and $r'$ such that

$$a - b = bq' + r' \qquad \text{and} \qquad 0 \le r' < b$$

Then

$$a = bq' + b + r' = b(q' + 1) + r'$$

Choose $q = q' + 1$ and $r = r'$. Then $q$ and $r$ are nonnegative integers and satisfy $(*)$.

**2.37.** Prove Theorem 2.8 (Division Algorithm): Let $a$ and $b$ be integers with $b \neq 0$. Then there exists integers $q$ and $r$ such that

$$a = bq + r \qquad \text{and} \qquad 0 \le r < |b|$$

Also, the integers $q$ and $r$ are unique.

Let $M$ be the set of nonnegative integers of the form $a - xb$ for some integer $x$. If $x = -|a|b$, then $a - xb$ is nonnegative (Problem 2.63); hence $M$ is nonempty. By the well-ordering principle, $M$ has a least element, say $r$. Since $r \in M$, we have

$$r \ge 0 \qquad \text{and} \qquad r = a - qb$$

for some integer $q$. We need only show that $r < |b|$.

Suppose $r \ge |b|$. Let $r' = r - |b|$. Then $r' \ge 0$ and also $r' < r$ because $b \neq 0$. Furthermore,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{if } b < 0 \\ a - (q-1)b, & \text{if } b > 0 \end{cases}$$

In either case, $r'$ belongs to $M$. This contradicts the fact that $r$ is the least element of $M$. Accordingly, $r < |b|$. Thus the existence of $q$ and $r$ is proved.

We now show that $q$ and $r$ are unique. Suppose there exist integers $q$ and $r$ and $q'$ and $r'$ such that

$$a = bq + r \qquad \text{and} \qquad a = bq' + r' \qquad \text{and} \qquad 0 \le r,\ r' < |b|$$

Then $bq + r = bq' + r'$; hence

$$b(q - q') = r' - r$$

Thus $b$ divides $r' - r$. But $|r' - r| < |b|$ since $0 \le r, r' < |b|$. Accordingly, $r' - r = 0$. This implies $q - q' = 0$ since $b \neq 0$. Consequently, $r' = r$ and $q' = q$; that is, $q$ and $r$ are uniquely determined by $a$ and $b$.

## DIVISIBILITY, PRIMES, GREATEST COMMON DIVISOR

**2.38.** Find all positive divisors of: (*a*) 18, (*b*) $256 = 2^8$, (*c*) $392 = 2^3 \cdot 7^2$.

(*a*) Since 18 is relatively small, we simply write down all positive integers ($\le 18$) which divide 18. These are

$$1, 2, 3, 6, 9, 18$$

(*b*) Since 2 is a prime, the positive divisors of $256 = 2^8$ are simply the lower powers of 2, that is,

$$2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8$$

In other words, the positive divisors of 256 are

$$1, 2, 4, 8, 16, 32, 64, 128, 256$$

(*c*) Since 2 and 7 are prime, the positive divisors of $392 = 2^3 \cdot 7^2$ are the products of lower powers of 2 times lower powers of 7, that is:

$$2^0 \cdot 7^0, 2^1 \cdot 7^0, 2^2 \cdot 7^0, 2^3 \cdot 7^0, 2^0 \cdot 7^1, 2^1 \cdot 7^1, 2^2 \cdot 7^1, 2^3 \cdot 7^1, 2^0 \cdot 7^2, 2^1 \cdot 7^2, 2^2 \cdot 7^2, 2^3 \cdot 7^2$$

In other words, the positive powers of 392 are:

$$1, 2, 4, 8, 7, 14, 28, 56, 49, 98, 196, 392$$

(We have used the usual convention that $n^0 = 1$ for any nonzero number $n$.)

**2.39.** List all primes between 50 and 100.

Simply list all numbers $p$ between 50 and 100 which cannot be written as a product of two positive integers, excluding 1 and $p$. This yields:

$$51, 53, 57, 59, 61, 67, 71, 73, 79, 83, 87, 89, 91, 93, 97$$

**2.40.** Let $a = 8316$ and $b = 10\,920$.

(*a*) Find $d = \gcd(a, b)$, the greatest common divisor of $a$ and $b$.

(*b*) Find integers $m$ and $n$ such that $d = ma + nb$.

(*c*) Find lcm $(a, b)$, the least common multiple of $a$ and $b$.

(*a*) Divide the smaller number $a = 8316$ into the larger number $b = 10\,920$, and then repeatedly divide each remainder into the divisor until obtaining a zero remainder. These steps are pictured in Fig. 2-10. The last nonzero remainder is 84. Thus

$$84 = \gcd(8316, 10\,920)$$

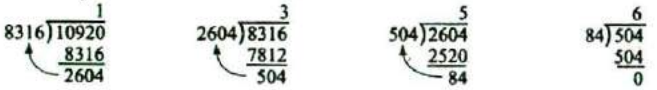


**Fig. 2-10**

(*b*) Now we find $m$ and $n$ such that

$$84 = 8316m + 10920n$$

The first three quotients in Fig. 2-10 yield the equations:

(*1*) $10\,920 = 1(8316) + 2604;$ or $2604 = 10\,920 - 1(8316)$

(*2*) $8316 = 3(2604) + 504;$ or $504 = 8316 - 3(2604)$

(*3*) $2064 = 5(504) + 84;$ or $84 = 2604 - 5(504)$

Equation (*3*) tells us that 84 is a linear combination of 2604 and 504. We use (*2*) to replace 504 in (*3*) so we can write 84 as a linear combination of 2604 and 8316 as follows:

$$(4) \quad 84 = 2604 - 5[8316 - 3(2604)] = 2604 - 5(8316) + 15(2604)$$
$$= 16(2604) - 5(8316)$$

We now use (*1*) to replace 2604 in (*4*) so we can write 84 as a linear combination of 8316 and 10 920 as follows:

$$\begin{aligned}84 &= 16[10\,920 - 1(8316)] - 5(8316)\\&= 16(10\,920) - 16(8316) - 5(8316)\\&= -21(8316) + 16(10\,920)\end{aligned}$$

This is our desired linear combination. Thus $m = -21$ and $n = 16$.

(*c*) By Theorem 2.15,

$$\text{lcm}\,(a, b) = \frac{|ab|}{\gcd\,(a, b)} = \frac{(8316)(10\,920)}{84} = 1\,081\,080$$

**2.41.** Suppose $a, b, c$ are integers. Prove:

(i) If $a|b$ and $b|c$, then $a|c$.
(ii) If $a|b$ then, for any integer $x, a|bx$.
(iii) If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$.
(iv) If $a|b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.
(v) If $a|b$ and $b|a$, then $|a| = |b|$, i.e., $a = \pm b$.
(vi) If $a|1$, then $a = \pm 1$.

(i) If $a|b$ and $b|c$, then there exist integers $x$ and $y$ such that $ax = b$ and $by = c$. Replacing $b$ by $ax$, we obtain $axy = c$. Hence $a|c$.

(ii) If $a|b$, then there exists an integer $c$ such that $ac = b$. Multiplying the equation by $x$, we obtain $acx = bx$. Hence $a|bx$.

(iii) If $a|b$ and $a|c$, then there exist integers $x$ and $y$ such that $ax = b$ and $ay = c$. Adding the equalities, we obtain

$$ax + ay = b + c \qquad \text{and so} \qquad a(x+y) = b + c$$

Hence $a|(b+c)$. Subtracting the equalities, we obtain

$$ax - ay = b - c \qquad \text{and so} \qquad a(x-y) = b - c$$

Hence $a|(b-c)$.

(iv) If $a|b$, then there exists $c$ such that $ac = b$. Then

$$|b| = |ac| = |a||c|$$

By Problem 2.31(*b*), either $|c| = 1$ or $|a| < |a||c| = |b|$. If $|c| = 1$, then $c = \pm 1$; whence $a = \pm b$, as required.

(v) If $a|b$, then $a = \pm b$ or $|a| < |b|$. If $|a| < |b|$, $b \nmid a$. Hence $a = \pm b$.

(vi) If $a|1$, then $a = \pm 1$ or $|a| < |1| = 1$. By Problem 2.30, $|a| \geq 1$. Therefore, $a = \pm 1$.

**2.42.** A nonempty subset $J$ of $\mathbf{Z}$ is called an *ideal* if $J$ has the following two properties:

(1) If $a, b \in J$, then $a + b \in J$.
(2) If $a \in J$ and $n \in \mathbf{Z}$, then $na \in J$.

Let $d$ be the least positive integer in an ideal $J \neq \{0\}$. Prove that $d$ divides every element of $J$.

Since $J \neq \{0\}$, there exists $a \in J$ with $a \neq 0$. Then $-a = (-1)a \in J$. Thus $J$ contains positive elements. By the well-ordering principle, $J$ contains a least positive integer, so $d$ exists. Now let $b \in J$. Dividing $b$ by $d$, the division algorithm tells us there exist $q$ and $r$ such that

$$b = qd + r \qquad \text{and} \qquad 0 \leq r < d$$

Now $b, d \in J$, and $J$ is an ideal; hence $b + (-q)d = r$ also belongs to $J$. By the minimality of $d$, we must have $r = 0$. Hence $d|b$, as required.

**2.43.** Prove Theorem 2.12: Let $d$ be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

Consider the set $J = \{ax + yb : x, y \in \mathbf{Z}\}$. Then

$$a = 1(a) + 0(b) \in J \qquad \text{and} \qquad b = 0(a) + 1(b) \in J$$

Also, suppose $s, t \in J$, say $s = x_1a + y_1b$ and $t = x_2a + y_2b$. Then, for any $n \in \mathbf{Z}$,

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \qquad \text{and} \qquad ns = (nx_1)a + (ny_1)b$$

also belong to $J$. Thus $J$ is an ideal. Let $d$ be the least positive element in $J$. We claim $d = \gcd(a, b)$.

By the preceding Problem 2.42, $d$ divides every element of $J$. Thus, in particular, $d$ divides $a$ and $b$. Now suppose $h$ divides both $a$ and $b$. Then $h$ divides $xa + yb$ for any $x$ and $y$; that is, $h$ divides every element of $J$. Thus $h$ divides $d$, and so $h < d$. Accordingly, $d = \gcd(a, b)$.

## FUNDAMENTAL THEOREM OF ARITHMETIC

**2.44.** Find the unique factorization of each number:

(*a*) 135, (*b*) 1330, (*c*) 3105, (*d*) 211.

(*a*) $135 = 5 \cdot 27 = 5 \cdot 3 \cdot 3 \cdot 3$ or $135 = 3^3 \cdot 5$.

(*b*) $1330 = 2 \cdot 665 = 2 \cdot 5 \cdot 133 = 2 \cdot 5 \cdot 7 \cdot 19$.

(*c*) $3105 = 5 \cdot 621 = 5 \cdot 3 \cdot 207 = 5 \cdot 3 \cdot 3 \cdot 69 = 5 \cdot 3 \cdot 3 \cdot 3 \cdot 23$ or $3105 = 3^3 \cdot 5 \cdot 23$.

(*d*) None of the primes 2, 3, 5, 7, 11 and 13 divides 211; hence 211 cannot be factored, that is, 211 is a prime.

**Remark**: We need only test those primes less than $\sqrt{211}$.

**2.45.** Let $a = 2^3 \cdot 3^5 \cdot 5^4 \cdot 11^6 \cdot 17^3$ and $b = 2^5 \cdot 5^3 \cdot 7^2 \cdot 114 \cdot 13^2$. Find $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$.

Those primes $p_i$ which appear in both $a$ and $b$ will also appear in $\gcd(a, b)$. Furthermore, the exponent of $p_i$ in $\gcd(a, b)$ will be the smaller of its exponents in $a$ and $b$. Hence

$$\gcd(a, b) = 2^3 \cdot 5^3 \cdot 11^4$$

Those primes $p_i$ which appear in either $a$ or $b$ will also appear in $\operatorname{lcm}(a, b)$. Also, the exponent of $p_i$ in $\operatorname{lcm}(a, b)$ will be the larger of its exponents in $a$ and $b$. Hence

$$\operatorname{lcm}(a, b) = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^2 \cdot 17^3$$

**2.46.** Prove Theorem 2.16: Suppose $\gcd(a, b) = 1$, and $a$ and $b$ divide $c$. Then $ab$ divides $c$.

Since $\gcd(a, b) = 1$, there exist $x$ and $y$ such that $ax + by = 1$. Since $a|c$ and $b|c$, there exist $m$ and $n$ such that $c = ma$ and $c = nb$. Multiplying $ax + by = 1$ by $c$ yields

$$acx + bcy = c \qquad \text{or} \qquad a(nb)x + b(ma)y = c \qquad \text{or} \qquad ab(nx + my) = c$$

Thus $ab$ divides $c$.

**2.47.** Prove Corollary 2.18: Suppose a prime $p$ divides a product $ab$. Then $p|a$ or $p|b$.

Suppose $p$ does not divide $a$. Then $\gcd(p, a) = 1$ since the only divisors of $p$ are $\pm 1$ and $\pm p$. Thus there exist integers $m$ and $n$ such that $1 = mp + nq$. Multiplying by $b$ yields $b = mpb + nab$. By hypothesis, $p|ab$, say $ab = cp$. Then

$$b = mpb + nab = mpb + ncp = p(mb + nc)$$

Hence $p|b$, as required.

**2.48.** Prove: (*a*) Suppose $p|q$ where $p$ and $q$ are primes. Then $p = q$.
(*b*) Suppose $p|q_1 q_2 \cdots q_r$ where $p$ and the $q$'s are primes. Then $p$ is equal to one of the $q$'s.

(*a*) The only divisors of $q$ are $\pm 1$ and $\pm q$. Since $p > 1$, $p = q$.

(*b*) If $r = 1$, then $p = q_1$ by (*a*). Suppose $r > 1$. By Problem 2.47 (Corollary 2.18), $p|q_1$ or $p|(q_2 \cdots q_r)$. If $p|q_1$, then $p = q_1$ by (*a*). If not, then $p|(q_2 \cdots q_r)$. We repeat the argument. That is, we get $p = q_2$ or $p|(q_3 \cdots q_r)$. Finally (or by induction) $p$ must equal one of the $q$'s.

**2.49.** Prove the Fundamental Theorem of Arithmetic (Theorem 2.19): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

We already proved Theorem 2.10 that such a product of primes exists. Hence we need only show that such a product is unique (except for order). Suppose

$$n = p_1 p_2 \cdots p_k \quad q_1 q_2 \cdots q_r$$

where the $p$'s and $q$'s are primes. Note that $p_1|(q_1 \cdots q_r)$. By the preceding Problem 2.48, $p_1$ equals one of the $q$'s. We arrange the $q$'s so that $p_1 = q_1$. Then

$$p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_r \qquad \text{and so} \qquad p_2 \cdots p_k = q_2 \cdots q_r$$

By the same argument, we can rearrange the remaining $q$s so that $p_2 = q_2$. And so on. Thus $n$ can be expressed uniquely as a product of primes (except for order).

## Supplementary Problems

### REAL NUMBER SYSTEM R, SETS OF NUMBERS

**2.50.** Assuming $\mathbf{R}, \mathbf{Q}, \mathbf{Q}', \mathbf{Z}$, and $\mathbf{P}$ denote respectively, the real numbers, rational numbers, irrational numbers, integers, and positive integers, state whether each of the following is true or false.

(*a*) $\pi \in \mathbf{Q}$
(*b*) $\sqrt{9} \in \mathbf{Q}$
(*c*) $-3 \in \mathbf{P}$
(*d*) $\sqrt[3]{5} \in \mathbf{Q}$
(*e*) $7 \in \mathbf{P}$
(*f*) $\sqrt{-3} \in \mathbf{R}$
(*g*) $-6 \in \mathbf{Q}'$
(*h*) $\sqrt{2} \in \mathbf{R}$
(*i*) $7 \in \mathbf{Q}$
(*j*) $\frac{2}{3} \in \mathbf{Q}'$

**2.51.** State whether each is: (*a*) always true, (*b*) sometimes true, (*c*) never true. Here $a \neq 0$, $b \neq 0$.

(1) $a \in \mathbf{Z}$, $b \in \mathbf{Q}$, and $a - b \in \mathbf{P}$.
(2) $a \in \mathbf{Q}$, $b \in \mathbf{Q}'$, and $ab \in \mathbf{Q}'$.
(3) $a \in \mathbf{Q}'$, $b \in \mathbf{Q}'$, and $ab \in \mathbf{Q}'$.
(4) $a \in \mathbf{P}$, $b \in \mathbf{Q}$, and $ab \in \mathbf{P}$.
(5) $a \in \mathbf{Z}$, $b \in \mathbf{Q}$, and $a/b \in \mathbf{P}$.
(6) $a \in \mathbf{Z}$, $b \in \mathbf{Q}'$ and $a/b \in \mathbf{Q}$.
(7) $a \in \mathbf{P}$, $b \in \mathbf{R}$, and $a + b \in \mathbf{P}$.
(8) $a \in \mathbf{Z}$, $b \in \mathbf{Q}$, and $ab \in \mathbf{Q}'$.

**2.52.** Express each real number as an infinite decimal (without ending in zeros): (*a*) 5/6, (*b*) 3/11, (*c*) 3/5.

**2.53.** Consider the sets

$$A = \{2, 4, 8, \ldots, 2^n, \ldots\}, \qquad B = \{3, 6, 9, \ldots, 3n, \ldots\}, \qquad C = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

Which of these sets are closed under the operations of:

(*a*) addition, (*b*) subtraction, (*c*) multiplication?

## ORDER AND INEQUALITIES, ABSOLUTE VALUE

**2.54.** Insert the correct symbol, $<$, $>$, or $=$, between each pair of integers:

(*a*) $2$ ____ $-6$ (*c*) $-7$ ____ $3$ (*e*) $2^3$ ____ $11$ (*g*) $-2$ ____ $-7$
(*b*) $-3$ ____ $-5$ (*d*) $-8$ ____ $-1$ (*f*) $2^3$ ____ $-9$ (*h*) $4$ ____ $-9$

**2.55.** Evaluate: (*a*) $|-6|$, $|5|$, $|0|$, (*b*) $|3-7|$, $|-3+7|$, $|-3-7|$.

**2.56.** Evaluate: (*a*) $|2-5|+|3+7|$, $|1-4|-|2-9|$;
(*b*) $|-4|+|2-3|$, $|-6-2|-|2-6|$.

**2.57.** Find the distance $d$ between each pair of real numbers:
(*a*) 2 and $-5$, (*b*) $-6$ and 3, (*c*) 2 and 8, (*d*) $-7$ and $-1$, (*e*) 3 and $-3$, (*f*) $-7$ and $-9$.

**2.58.** Find all integers $n$ such that: (*a*) $3 < 2n - 4 < 10$, (*b*) $1 < 6 - 3n < 13$.

**2.59.** Prove Proposition 2.1: (i), $a \leq a$, for any real number $a$.
(ii) If $a \leq b$ and $b \leq a$, then $a = b$

**2.60.** Prove Proposition 2.2: For any real numbers $a$ and $b$, exactly one of the following holds:

$$a < b, a = b, \text{ or } a > b.$$

**2.61.** Prove: (*a*) $2ab \leq a^2 + b^2$, (*b*) $ab + ac + bc \leq a^2 + b^2 + c^2$.

**2.62.** Prove Proposition 2.4: (i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$.
(ii) $-|a| \leq a \leq |a|$.
(v) $||a| - |b|| \leq |a \pm b|$.

**2.63.** Show that $a - xb \geq 0$ if $b \neq 0$, and $x = -|a|b$.

## INTERVALS

**2.64.** Rewrite each interval in set-builder form:
(*a*) $A = [-1, 6)$, (*b*) $B = (2, 5)$, (*c*) $C = [-3, 0]$, (*d*) $D = (1, 4]$.

**2.65.** Which of the sets in Problem 2.64 is: (*a*) an open interval, (*b*) a closed interval?

**2.66.** Find the interval satisfying each inequality, i.e., rewrite the inequality in terms of $x$ alone:
(*a*) $1 \leq x - 2 \leq 4$, (*b*) $-3 \leq x + 4 \leq 7$, (*c*) $-6 \leq 3x \leq 12$, (*d*) $-4 \leq -2x \leq 6$.

**2.67.** Find the interval satisfying each inequality:
(*a*) $3 \leq 2x - 5 \leq 7$, (*b*) $-8 \leq 4 - 3x \leq 7$.

**2.68.** Rewrite without the absolute value sign:

(*a*) $|x| < 2$, (*b*) $|x - 3| < 5$, (*c*) $|2x - 5| < 9$.

**2.69.** Write each open interval in the form $|x - a| < r$:

(*a*) $3 < x < 9$, (*b*) $-5 < x < 1$.

**2.70.** Rewrite each set using an infinite interval notation:

(*a*) $x > -4$, (*b*) $x \leq 5$, (*c*) $x \geq 2$, (*d*) $x < -3$.

**2.71.** Let $A = [-4, 2)$, $B = (-1, 6)$, $C = (-\infty, 1]$. Find, and write in interval notation:

(*a*) $A \cup B$, (*c*) $A \backslash B$, (*e*) $A \cup C$, (*g*) $A \backslash C$, (*i*) $B \cup C$, (*k*) $B \backslash C$,
(*b*) $A \cap B$, (*d*) $B \backslash A$, (*f*) $A \cap C$, (*h*) $C \backslash A$, (*j*) $B \cap C$, (*l*) $C \backslash B$.

## BOUNDED AND UNBOUNDED SETS

**2.72.** State whether each set is bounded, bounded below, bounded above, unbounded:

(*a*) $A = \{x : x = \frac{1}{n}, n \in \mathbf{P}\}$, (*c*) $C = \{x : x = \frac{1}{2^n}, n \in \mathbf{Z}\}$, (*e*) $E = \{x : x = 2^n, n \in \mathbf{Z}\}$,
(*b*) $B = \{x : x = 3^n, n \in \mathbf{P}\}$, (*d*) $D = \{x : x \in \mathbf{P}, x < 2567\}$, (*f*) $F = \{x : |x| < 6\}$.

**2.73.** Are the following statements: (1) always true, (2) sometimes true, (3) never true?

(*a*) If $A$ is finite, then $A$ is bounded. (*c*) If $A$ is a subset of $[-23, 79]$, then $A$ is finite.
(*b*) If $A$ is infinite, then $A$ is bounded. (*d*) If $A$ is a subset of $[-23, 79]$, then $A$ is unbounded.

## INTEGERS Z, MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

**2.74.** Prove the assertion $A$ that the sum of the first $n$ even positive integers is $n(n+1)$; that is,

$$A(n)\colon 2 + 4 + 6 + \cdots + 2n = n(n+1)$$

**2.75.** Prove: (*a*) $a^n a^m = a^{n+m}$, (*b*) $(a^n)^m = a^{nm}$, (*c*) $(ab)^n = a^n b^n$

**2.76.** Prove: $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \dfrac{1}{3 \cdot 4} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

**2.77.** Prove: $|\mathscr{P}(A)| = 2^n$ where $|A| = n$. [Here $\mathscr{P}(A)$ is the power set of the finite set $A$ with $n$ elements.]

## DIVISION ALGORITHM

**2.78.** For each pair of integers $a$ and $b$, find integers $q$ and $r$ such that $a = bq + r$ and $0 \leq r < |b|$:

(*a*) $a = 395$ and $b = 14$ (*c*) $a = -278$ and $b = 12$
(*b*) $a = 608$ and $b = -17$ (*d*) $a = -417$ and $b = -8$

**2.79.** Prove each of the following statements:

(*a*) The product of any three consecutive integers is divisible by 6.
(*b*) The product of any four consecutive integers is divisible by 24.

**2.80.** Show that each of the following numbers is not rational: (*a*) $\sqrt{3}$, (*b*) $\sqrt[3]{2}$.

**2.81.** Show that $\sqrt{p}$ is not rational, where $p$ is any prime number.

### DIVISIBILITY, GREATEST COMMON DIVISORS, PRIMES

**2.82.** Find all possible divisors of: (*a*) 24, (*b*) $19\,683 = 3^9$, (*c*) $432 = 2^4 \cdot 3^3$.

**2.83.** List all prime numbers between 100 and 150.

**2.84.** For each pair of integers $a$ and $b$, find $d = \gcd(a, b)$ and express $d$ as a linear combination of $a$ and $b$:

(*a*) $a = 48$, $b = 356$ (*c*) $a = 2310$, $b = 168$
(*b*) $a = 165$, $b = 1287$ (*d*) $a = 195$, $b = 968$

**2.85.** Prove: (*a*) If $a|b$, then $a| - b$, $-a|b$, and $-a| - b$.
(*b*) If $ac|bc$, then $b|c$.

**2.86.** Prove: (*a*) If $am + bn = 1$, then $\gcd(a, b) = 1$
(*b*) If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

**2.87.** Prove: (*a*) $\gcd(a, a + k)$ divides $k$.
(*b*) $\gcd(a, a + 2)$ equals 1 or 2.

**2.88.** Prove: If $n > 1$ is composite, then $n$ has a positive divisor $d$ such that $d \leq \sqrt{n}$.

### FUNDAMENTAL THEOREM OF ARITHMETIC

**2.89.** Express as a product of prime numbers:
(*a*) 2940, (*b*) 1485, (*c*) 8712, (*d*) 319410.

**2.90.** Suppose $a = 5880$ and $b = 8316$.

(*a*) Express $a$ and $b$ as products of primes.
(*b*) Find $\gcd(a, b)$ and $\text{lcm}(a, b)$.
(*c*) Verify that $\text{lcm}(a, b) = (|ab|)/\gcd(a, b)$.

**2.91.** Prove: If $a_1|n$ and $a_2|n, \ldots, a_k|n$, then $m|n$ where $m = \text{lcm}(a_1, \ldots a_k)$.

**2.92.** Let $n$ be a positive integer. Prove:

(*a*) 3 divides $n$ if and only if 3 divides the sum of the digits of $n$.
(*b*) 9 divides $n$ if and only if 9 divides the sum of the digits of $n$.
(*c*) 8 divides $n$ if and only if 8 divides the integer formed by the last three digits of $n$.

## Answers to Supplementary Problems

**2.50.** Only (*b*), (*e*), (*h*), (*i*) are true.

**2.51.** (1) *b*; (2) *a*; (3) *b*; (4) *b*; (5) *b*; (6) *c*; (7) *b*; (8) *c*

**2.52.** (*a*) $5/6 = 0.8333\ldots$, (*b*) $3/11 = 0.2727\ldots$, (*c*) $3/5 = 0.5999\ldots$

**2.53.** (*a*) $B$ and $C$; (*b*) $C$; (*c*) $A, B, C$

**2.54.** (*a*) $2 > -6$; (*b*) $-3 > -5$; (*c*) $-7 < 3$; (*d*) $-8 < -1$; (*e*) $2^3 < 11$; (*f*) $2^3 > -9$;
(*g*) $-2 > -7$; (*h*) $4 > -9$

**2.55.** (*a*) 6, 5, 0; (*b*) 4, 4, 10

**2.56.** (*a*) $3 + 10 = 13$, $3 - 7 = -4$; (*b*) $4 + 1 = 5$, $8 - 4 = 4$

**2.57.** (*a*) 7; (*b*) 9; (*c*) 6; (*d*) 6; (*e*) 6; (*f*) 3

**2.58.** (*a*) 4, 5, 6; (*b*) $-2, -1, 0, 1$

**2.64.** (*a*) $A = \{x : -1 \leq x < 6\}$ (*c*) $C = \{x : -3 \leq x \leq 0\}$
(*b*) $B = \{x : 2 < x < 5\}$ (*d*) $D = \{x : 1 < x \leq 4\}$

**2.65.** $B$ is open and $C$ is closed.

**2.66.** (*a*) $3 \leq x \leq 6$; (*b*) $-7 \leq x \leq 3$; (*c*) $-2 \leq x \leq 4$; (*d*) $-3 \leq x \leq 2$

**2.67.** (*a*) $4 \leq x \leq 6$; (*b*) $-1 \leq x \leq 4$

**2.68.** (*a*) $-2 < x < 2$; (*b*) $-2 < x < 8$; (*c*) $-2 < x < 7$

**2.69.** (*a*) $|x - 6| < 3$; (*b*) $|x + 2| < 3$

**2.70.** (*a*) $(-4, \infty)$; (*b*) $(-\infty, 5]$; (*c*) $[2, \infty)$; (*d*) $(-\infty, -3)$

**2.71.** (*a*) $[-4, 6)$, (*c*) $[-4, -1]$, (*e*) $(-\infty, 2)$, (*g*) $(1, 2)$, (*i*) $(-\infty, 6)$, (*k*) $(1, 6)$,
(*b*) $(-1, 2)$, (*d*) $[2, 6)$, (*f*) $[-4, -1]$, (*h*) $(-\infty, -4)$, (*j*) $(-1, 1]$, (*l*) $(-\infty, -1]$.

**2.72.** (*a*) bounded; (*b*) only bounded below; (*c*) bounded; (*d*) bounded; (*e*) unbounded; (*f*) bounded

**2.73.** (*a*) 1; (*b*) 2; (*c*) 1; (*d*) 3

**2.74–2.77.** *Hint*: Use mathematical induction or well-ordering principle.

**2.78.** (*a*) $q = 28$, $r = 3$ (*b*) $q = -15$, $r = 13$ (*c*) $q = -24$, $r = 10$ (*d*) $q = 53$, $r = 7$

**2.79.** (*a*) One is divisible by 2 and one is divisible by 3.
(*b*) One is divisible by 4, another is divisible by 2, and one is divisible by 3.

**2.82.** (*a*) 1, 2, 3, 4, 6, 12, 24; (*b*) $3^n$ for $n = 0$ to 9; (*c*) $2^r 3^s$ for $r = 0$ to 4 and $s = 0$ to 3.

**2.83.** 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

**2.84.** (*a*) $d = 4 = 5(356) - 37(48)$ (*c*) $d = 42 = 14(168) - 1(2310)$
(*b*) $d = 33 = 8(165) - 1(1287)$ (*d*) $d = 1 = 139(195) - 28(968)$

**2.89.** (*a*) $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; (*b*) $1485 = 3^3 \cdot 5 \cdot 11$; (*c*) $8712 = 2^3 \cdot 3^2 \cdot 11^2$; (*d*) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$

**2.90.** (*a*) $a = 2^4 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$; (*b*) $\gcd(a, b) = 2^2 \cdot 3 \cdot 7$, $\operatorname{lcm}(a, b) = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 = 1\,164\,240$

# Chapter 3

# Relations

## 3.1 INTRODUCTION

The reader is familiar with many relations which are used in mathematics and computer science, e.g., "less than", "is parallel to", "is a subset of", and so on. In a certain sense, these relations consider the existence or nonexistence of certain connections between pairs of objects taken in a definite order. Formally, we define a relation in terms of these "ordered pairs".

There are three kinds of relations which play a major role in our theory: (i) equivalence relations, (ii) order relations, (iii) functions. Equivalence relations are mainly covered in this chapter. Order relations are introduced here, but will also be discussed in Chapter 7. Functions are covered in the next chapter.

The connection between relations on finite sets and matrices are also included here for completeness. These sections, however, can be ignored at a first reading by those with no previous knowledge of matrix theory.

### Ordered Pairs

Relations, as noted above, will be defined in terms of ordered pairs $(a, b)$ of elements, where $a$ is designated as the first element and $b$ as the second element. Specifically:

$$\boxed{(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d}$$

In particular, $(a, b) \neq (b, a)$ unless $a = b$. This contrasts with sets studied in Chapter 1 where the order of elements is irrelevant, for example, $\{3, 5\} = \{5, 3\}$.

## 3.2 PRODUCT SETS

Let $A$ and $B$ be two sets. The *product set* or *cartesian product* of $A$ and $B$, written $A \times B$ and read "$A$ cross $B$", is the set of all ordered pairs $(a, b)$ such that $a \in A$ and $b \in B$. Namely:

$$A \times B = \{(a, b) : a \in A,\ b \in B\}$$

One usually writes $A^2$ instead of $A \times A$.

**EXAMPLE 3.1** Recall that $\mathbf{R}$ denotes the set of real numbers, so $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ is the set of ordered pairs of real numbers. The reader may be familiar with the geometrical representation of $\mathbf{R}^2$ as points in the plane as in Fig. 3-1. Here each point $P$ represents an ordered pair $(a, b)$ of real numbers and vice versa; the vertical line through $P$ meets the (horizontal) $x$-axis at $a$, and the horizontal line through $P$ meets the (vertical) $y$-axis at $b$. $\mathbf{R}^2$ is frequently called the *cartesian* plane.

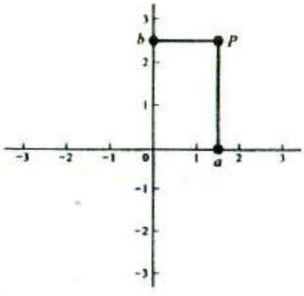


**Fig. 3-1**

**EXAMPLE 3.2** Let $A = \{1,2\}$ and $B = \{a,b,c\}$. Then

$$A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$$
$$B \times A = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$$

Also,

$$A \times A = \{(1,1)(1,2),(2,1),(2,2)\}$$

There are two things worth noting in Example 3.2. First of all, $A \times B \neq B \times A$. The cartesian product deals with ordered pairs, so naturally the order in which the sets are considered is important. Secondly,

$$n(A \times B) = 6 = 2 \cdot 3 = n(A) \cdot n(B)$$

[where $n(A)$ = number of elements in $A$]. In fact:

$$\boxed{n(A \times B) = n(A) \cdot n(B)}$$

for any finite sets $A$ and $B$. This follows from the observation that, for any ordered pair $(a,b)$ in $A \times B$, there are $n(A)$ possibilities for $a$, and for each of these there are $n(B)$ possibilities for $b$.

### Product of Three or More Sets

The idea of a product of sets can be extended to any finite number of sets. Specifically, for any sets $A_1, A_2, \ldots, A_m$, the set of all $m$-element lists $(a_1, a_2, \ldots, a_m)$, where each $a_i \in A_i$, is called the (*cartesian*) *product* of the sets $A_1, A_2, \ldots, A_m$; it is denoted by

$$A_1 \times A_2 \times \cdots \times A_m \quad \text{or equivalently} \quad \prod_{i=1}^{m} A_i$$

Just as we write $A^2$ instead of $A \times A$, so we write $A^n$ for $A \times A \times \cdots \times A$ where there are $n$ factors. For example, $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ denotes the usual three-dimensional space.

## 3.3 RELATIONS

We begin with a definition.

**Definition**: Let $A$ and $B$ be sets. A *binary relation* or, simply, a *relation* from $A$ to $B$ is a subset of $A \times B$.

Suppose $R$ is a relation from $A$ to $B$. Then $R$ is a set of ordered pairs where each first element comes from $A$ and each second element comes from $B$. That is, for each pair $a \in A$ and $b \in B$, exactly one of the following is true:

(i) $(a,b) \in R$; we then say "$a$ is *R-related* to $b$", written $a\,R\,b$.

(ii) $(a,b) \notin R$; we then say "$a$ is not *R-related* to $b$", written $a \not R\, b$.

The *domain* of a relation $R$ from $A$ to $B$ is the set of all first elements of the ordered pairs which belong to $R$, and so it is a subset of $A$; and the *range* of $R$ is the set of all second elements, and so it is a subset of $B$.

Sometimes $R$ is a relation from a set $A$ to itself, that is, $R$ is a subset of $A^2 = A \times A$. In such a case, we say that $R$ is a relation *on* $A$.

Although $n$-ary relations, which involve ordered $n$-tuples, are introduced in Section 3.11, the term relation shall mean binary relation unless otherwise stated or implied.

**EXAMPLE 3.3**

(*a*) Let $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$, and let $R = \{(1, y), (1, z), (3, y)\}$. Then $R$ is a relation from $A$ to $B$ since $R$ is a subset of $A \times B$. With respect to this relation,

$$1Ry,\ 1Rz,\ 3Ry, \qquad \text{but} \qquad 1 \not R\, x,\ 2 \not R\, x,\ 2 \not R\, y,\ 2 \not R\, z,\ 3 \not R\, x,\ 3 \not R\, z$$

The domain of $R$ is $\{1, 3\}$ and the range is $\{y, z\}$.

(*b*) Suppose we say that two countries are *adjacent* if they have some part of their boundaries in common. Then "is adjacent to" is a relation $R$ on the countries of the earth. Thus:

$$(\text{Italy, Switzerland}) \in R \qquad \text{but} \qquad (\text{Canada, Mexico}) \notin R$$

(*c*) Set inclusion $\subseteq$ is a relation on any collection of sets. For, given any pair of sets $A$ and $B$, either $A \subseteq B$ or $A \not\subseteq B$.

(*d*) A familiar relation on the set $\mathbf{Z}$ of integers is "$m$ divides $n$". A common notation for this relation is to write $m|n$ when $m$ divides $n$. Thus $6|30$ but $7 \nmid 25$.

(*e*) Consider the set $L$ of lines in the plane. Perpendicularity, written $\perp$, is a relation on $L$. That is, given any pair of lines $a$ and $b$, either $a \perp b$ or $a \not\perp b$. Similarly, "is parallel to", written $\|$, is a relation on $L$ since either $a \parallel b$ or $a \nparallel b$.

### Universal, Empty, Equality Relations

Let $A$ be any set. Then $A \times A$ and $\varnothing$ are subsets of $A \times A$ and hence are relations on $A$ called the *universal relation* and *empty relation*, respectively. Thus, for any relation $R$ on $A$, we have

$$\varnothing \subseteq R \subseteq A \times A$$

An important relation on the set $A$ is that of *equality*, that is, the relation

$$\{(a, a) : a \in A\}$$

which is usually denoted by "=". This relation is also called the *identity* or *diagonal relation* on $A$, and it may sometimes be denoted by $\Delta_A$ or simply $\Delta$.

### Inverse Relation

Let $R$ be any relation from a set $A$ to a set $B$. The *inverse* of $R$, denoted by $R^{-1}$, is the relation from $B$ to $A$ which consists of those ordered pairs which, when reversed, belong to $R$; that is,

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

For example:

$$\text{If} \quad R = \{(1, y),\ (1, z),\ (3, y)\}, \qquad \text{then} \qquad R^{-1} = \{(y, 1),\ (z, 1),\ (y, 3)\}.$$

[Here $R$ is the relation from $A = \{1, 2, 3\}$ to $B = \{x, y, z\}$ in Example 3.3(*a*).]

Clearly, if $R$ is any relation, then $(R^{-1})^{-1} = R$. Also, the domain of $R^{-1}$ is the range of $R$, and vice versa. Moreover, if $R$ is a relation on $A$, i.e., $R$ is a subset of $A \times A$, then $R^{-1}$ is also a relation on $A$.

## 3.4 PICTORIAL REPRESENTATIONS OF RELATIONS

This section discusses a number of ways of picturing and representing binary relations.

### Relations on R

Let $S$ be a relation on the set **R** of real numbers; that is, let $S$ be a subset of $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$. Since $\mathbf{R}^2$ can be represented by the set of points in the plane, we can picture $S$ by emphasizing those points in the plane which belong to $S$. This pictorial representation of $S$ is sometimes called the *graph* of $S$.

Frequently, the relation $S$ consists of all ordered pairs of real numbers which satisfy some given equation

$$E(x, y) = 0$$

We usually identify the relation with the equation, i.e., we speak of the relation $E(x, y) = 0$.

**EXAMPLE 3.4** Consider the relation $S$ defined by the equation

$$x^2 + y^2 = 25 \qquad \text{or equivalently} \qquad x^2 + y^2 - 25 = 0$$

That is, $S$ consists of all ordered pairs $(x_0, y_0)$ which satisfy the given equation. The graph of the equation is a circle having its center at the origin and radius 5, as shown in Fig. 3-2.

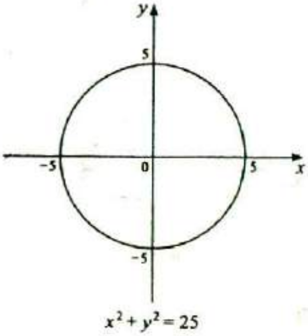


Fig. 3-2

### Representation of Relations on Finite Sets

Suppose $A$ and $B$ are finite sets. The following are two ways of picturing a relation $R$ from $A$ to $B$.

(i) Form a rectangular array whose rows are labeled by the elements of $A$ and whose columns are labeled by the elements of $B$. Put a 1 or 0 in each position of the array according as $a \in A$ is or is not related to $b \in B$. This array is called the *matrix* of the relation.

(ii) Write down the elements of $A$ and the elements of $B$ in two disjoint disks, and then draw an arrow from $a \in A$ to $b \in B$ whenever $a$ is related to $b$. This picture will be called the *arrow diagram* of the relation.

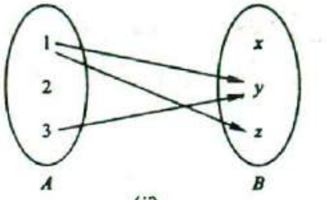
Consider, for example, the following relation $R$ from $A = \{1, 2, 3\}$ to $B = \{x, y, z\}$:

$$R = \{(1, y),\ (1, z), (3, y)\}$$

Figure 3-3 pictures this relation $R$ by the above two ways.

|  |  | B |  |  |
|---|---|---|---|---|
|  |  | x | y | z |
|  | 1 | 0 | 1 | 1 |
| A | 2 | 0 | 0 | 0 |
|  | 3 | 0 | 1 | 0 |

(i)



(ii)

$R = \{(1, y),\ (1, z),\ (3, y)\}$

Fig. 3-3

### Directed Graphs of Relations on Sets

There is another way of picturing a relation $R$ when $R$ is a relation from a finite set $A$ to itself. First we write down the elements of the set $A$, and then we draw an arrow from each element $x$ to each element $y$ whenever $x$ is related to $y$. This diagram is called the *directed graph* of the relation $R$. Figure 3-4, for example, shows the directed graph of the following relation $R$ on the set $A = \{1, 2, 3, 4\}$:

$$R = \{(1,2),\ (2,2),\ (2,4),\ (3,2),\ (3,4),\ (4,1),\ (4,3)\}$$

Observe that there is an arrow from 2 to itself, since 2 is related to 2 under $R$.

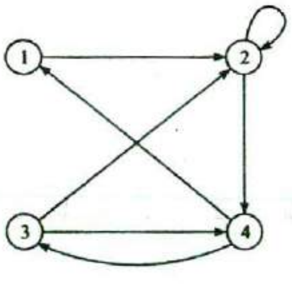


Fig. 3-4

## 3.5 COMPOSITION OF RELATIONS

Let $A$, $B$, $C$ be sets, and let $R$ be a relation from $A$ to $B$ and let $S$ be a relation from $B$ to $C$. Then $R$ and $S$ give rise to a relation from $A$ to $C$ denoted by $R \circ S$ and defined as follows:

$$\boxed{R \circ S = \{(a, c) : \text{there exists } b \in B \text{ for which } (a, b) \in R \text{ and } (b, c) \in S\}}$$

That is,

$$\boxed{a(R \circ S)c \text{ whenever there exists } b \in B \text{ such that } a\,R\,b \text{ and } b\,S\,c}$$

This relation $R \circ S$ is called the *composition* of $R$ and $S$; it is sometimes denoted by $RS$.

Our first theorem (proved in Problem 3.10) tells us that the composition of relations is associative. Namely:

**Theorem 3.1**: Let $A, B, C, D$ be sets. Suppose $R$ is a relation from $A$ to $B$, $S$ is a relation from $B$ to $C$, and $T$ is a relation from $C$ to $D$. Then

$$(R \circ S) \circ T = R \circ (S \circ T)$$

The arrow diagrams of relations give us a geometrical interpretation of the composition $R \circ S$ as seen in the following example.

**EXAMPLE 3.5** Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z)$ and let

$$R = \{(1, a),\ (2, d),\ (3, a),\ (3, b),\ (3, d)\} \qquad \text{and} \qquad S = \{(b, x),\ (b, z),\ (c, y),\ (d, z)\}$$

Consider the arrow diagrams of $R$ and $S$ as in Fig. 3-5. Observe there is an arrow from 2 to $d$ which is followed by an arrow from $d$ to $x$. We can view these two arrows as a "path" which "connects" the element $2 \in A$ to the element $z \in C$. Thus

$$2(R \circ S)z \qquad \text{since} \qquad 2Rd \text{ and } dSz$$

Similarly there are paths from 3 to $x$ and from 3 to $z$. Hence

$$3(R \circ S)x \qquad \text{and} \qquad 3(R \circ S)z$$

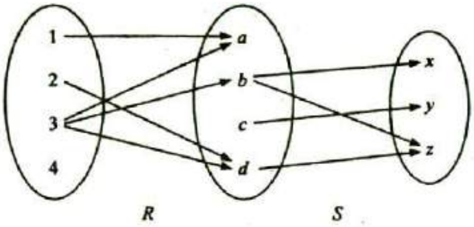


Fig. 3-5

No other element of $A$ is connected to an element of $C$. Accordingly,

$$R \circ S = \{(2, z),\ (3, x),\ (3, z)\}$$

Suppose $R$ is a relation on a set $A$, that is, $R$ is a relation from a set $A$ to itself. Then $R \circ R$, the composition of $R$ with itself, is always defined, and $R \circ R$ is sometimes denoted by $R^2$. Similarly, $R^3 = R^2 \circ R = R \circ R \circ R$, and so on. Thus $R^n$ is defined for all positive $n$.

**Warning**: Many texts denote the composition of relations $R$ and $S$ by $S \circ R$ rather than $R \circ S$. This is done in order to conform with the usual use of $g \circ f$ to denote the composition of $f$ and $g$ where $f$ and $g$ are functions. Thus the reader may have to adjust his notation when using this text as a supplement with another text. However, when a relation $R$ is composed with itself, then the meaning of $R \circ R$ is unambiguous.

### Composition of Relations and Matrices

There is a way of finding the composition $R \circ S$ of relations using matrices. Specifically, let $M_R$ and $M_S$ denote respectively the matrices of the relations $R$ and $S$ in Example 3.5. Then:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \qquad \text{and} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Multiplying $M_R$ and $M_S$ we obtain the matrix

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

The nonzero entries in this matrix tell us which elements are related by $R \circ S$. Thus $M = M_R M_S$ and $M_{R \circ S}$ have the same nonzero entries.

## 3.6 TYPES OF RELATIONS

Consider a given set $A$. This section discusses a number of important types of relations which are defined on $A$.

(1) **Reflexive Relations**: A relation $R$ on a set $A$ is *reflexive* if $a\,R\,a$ for every $a \in A$, that is, if $(a, a) \in R$ for every $a \in A$. Thus $R$ is not reflexive if there exists an $a \in A$ such that $(a, a) \notin R$.

(2) **Symmetric Relations**: A relation $R$ on a set $A$ is *symmetric* if whenever $a\,R\,b$ then $b\,R\,a$, that is, if whenever $(a, b) \in R$, then $(b, a) \in R$. Thus $R$ is not symmetric if there exists $a, b \in A$ such that $(a, b) \in R$ but $(b, a) \notin R$.

(3) **Antisymmetric Relations**: A relation $R$ on a set $A$ is *antisymmetric* if whenever $a\,R\,b$ and $b\,R\,a$ then $a = b$, that is, if whenever $(a, b)$ and $(b, a)$ belong to $R$ then $a = b$. Thus $R$ is not antisymmetric if there exist $a, b \in A$ such that $(a, b)$ and $(b, a)$ belong to $R$, but $a \neq b$.

(4) **Transitive Relations**: A relation $R$ on a set $A$ is *transitive* if whenever $a\,R\,b$ and $b\,R\,c$ then $a\,R\,c$, that is, if whenever $(a, b), (b, c) \in R$ then $(a, c) \in R$. Thus $R$ is not transitive if there exist $a, b, c \in A$ such that $(a, b), (b, c) \in R$, but $(a, c) \notin R$.

**EXAMPLE 3.6** Consider the following five relations on the set $A = \{1, 2, 3, 4\}$:

$$R_1 = \{(1,1),\ (1,2),\ (2,3),\ (1,3),\ (4,4)\}$$
$$R_2 = \{(1,1),\ (1,2),\ (2,1)\,(2,2),\ (3,3), (4,4)\}$$
$$R_3 = \{(1,3),\ (2,1)\}$$
$$R_4 = \varnothing,\ \text{the empty relation}$$
$$R_5 = A \times A,\ \text{the universal relation}$$

Determine which of the relations are: (*a*) reflexive, (*b*) symmetric, (*c*) antisymmetric, (*d*) transitive.

(*a*) Since $A$ contains the four elements 1, 2, 3, 4, a relation $R$ on $A$ is reflexive if it contains the four pairs $(1, 1)$, $(2, 2)$, $(3, 3)$, and $(4, 4)$. Thus only $R_2$ and the universal relation $R_5 = A \times A$ are reflexive. Note that $R_1$, $R_3$, and $R_4$ are not reflexive since, for example, $(2, 2)$ does not belong to any of them.

(*b*) $R_1$ is not symmetric since $(1, 2) \in R_1$ but $(2, 1) \notin R_1$. $R_3$ is not symmetric since $(1, 3) \in R_3$ but $(3, 1) \notin R_3$. The other relations are symmetric.

(*c*) $R_2$ is not antisymmetric since $(1, 2)$ and $(2, 1)$ belong to $R_2$, but $1 \neq 2$. Similarly, the universal relation $R_5$ is not antisymmetric. All the other relations are antisymmetric.

(*d*) The relation $R_3$ is not transitive since $(2, 1), (1, 3) \in R_3$ but $(2, 3) \notin R_3$. All the other relations are transitive.

**EXAMPLE 3.7** Consider the following five relations:

(1) Relation $\le$ (less than or equal) on the set $\mathbf{Z}$ of integers.
(2) Set inclusion $\subseteq$ on a collection $\mathscr{C}$ of sets.
(3) Relation $\perp$ (perpendicular) on the set $L$ of lines in the plane.
(4) Relation $\|$ (parallel) on the set $L$ of lines in the plane.
(5) Relation $|$ of divisibility on the set $\mathbf{P}$ of positive integers. (Recall that $x|y$ if there exists $z$ such that $xz = y$.)

Determine which of the relations are: (*a*) reflexive, (*b*) symmetric, (*c*) antisymmetric, (*d*) transitive.

(*a*) The relation (3) is not reflexive since no line is perpendicular to itself. Also, (4) is not reflexive since no line is parallel to itself. The other relations are reflexive; that is, $x \le x$ for every integer $x$ in $\mathbf{Z}$, $A \subseteq A$ for any set $A$ in $\mathscr{C}$, and $n|n$ for every positive integer $n$ in $\mathbf{P}$.

(*b*) The relation $\perp$ is symmetric since if line $a$ is perpendicular to line $b$ then $b$ is perpendicular to $a$. Also, $\|$ is symmetric since if line $a$ is parallel to line $b$ then $b$ is parallel to $a$. The other relations are not symmetric. For example, $3 \le 4$ but $4 \le 3$; $\{1,2\} \subseteq \{1,2,3\}$ but $\{1,2,3\} \not\subseteq \{1,2\}$; and $2|6$ but $6|2$.

(*c*) The relation $\le$ is antisymmetric since whenever $a \le b$ and $b \le a$ then $a = b$. Set inclusion $\subseteq$ is antisymmetric since whenever $A \subseteq B$ and $B \subseteq A$ then $A = B$. Also, divisibility on $\mathbf{P}$ is antisymmetric since whenever $m|n$ and $n|m$ then $m = n$. (Note that divisibility on $\mathbf{Z}$ is not antisymmetric since $3|-3$ and $-3|3$ but $3 \ne -3$.) The relation $\perp$ is not antisymmetric since we can have distinct lines $a$ and $b$ such that $a \perp b$ and $b \perp a$. Similarly, $\|$ is not antisymmetric.

(*d*) The relations $\le$, $\subseteq$ and $|$ are transitive. That is:

(i) If $a \le b$ and $b \le c$, then $a \le c$.
(ii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
(iii) If $a|b$ and $b|c$, then $a|c$.

On the other hand, the relation $\perp$ is not transitive. If $a \perp b$ and $b \perp c$, then it is not true that $a \perp c$. Since no line is parallel to itself, we can have $a \| b$ and $b \| a$, but $a \nparallel a$. Thus $\|$ is not transitive. (We note that the relation "is parallel or equal to" is a transitive relation on the set $L$ of lines in the plane.)

**Remark 1**: The properties of being symmetric and antisymmetric are not negatives of each other. For example, the relation $R = \{(1,3), (3,1), (2,3)\}$ is neither symmetric nor antisymmetric. On the other hand, the relation $R' = \{(1,1), (2,2)\}$ is both symmetric and antisymmetric.

**Remark 2**: The property of transitivity can also be expressed in terms of the composition of relations. Recall that, for a relation $R$ on a set $A$, we defined

$$R^2 = R \circ R \qquad \text{and, more generally,} \qquad R^n = R^{n-1} \circ R$$

Then one can show (Problem 3.66) that a relation $R$ is transitive if and only if $R^n \subseteq R$ for every $n \ge 1$.

## 3.7 CLOSURE PROPERTIES

Let $\mathscr{P}$ denote a property of relations on a set $A$ such as being symmetric or transitive. A relation on $A$ with property $\mathscr{P}$ will be called a *$\mathscr{P}$-relation*.

Now let $R$ be a given relation on $A$ with or without property $\mathscr{P}$. The *$\mathscr{P}$-closure* of $R$, written $\mathscr{P}(R)$, is a relation on $A$ containing $R$ such that

$$R \subseteq \mathscr{P}(R) \subseteq S$$

for any other $\mathscr{P}$-relation $S$ containing $R$. Clearly $R = \mathscr{P}(R)$ if $R$ itself has property $\mathscr{P}$.

The reflexive, symmetric, and transitive closures of a relation $R$ will be denoted respectively by:

$$\text{reflexive}(R), \qquad \text{symmetric}(R), \qquad \text{transitive}(R)$$

### Reflexive and Symmetric Closures

The next theorem tells us how to easily obtain the reflexive and symmetric closures of a relation. Here $\Delta_A = \{(a, a): a \in A\}$ is the *diagonal* or *equality* relation on $A$.

**Theorem 3.2**: Let $R$ be a relation on a set $A$. Then:

(i) $R \cup \Delta_A$ is the reflexive closure of $R$.

(ii) $R \cup R^{-1}$ is the symmetric closure of $R$.

In other words, reflexive($R$) is obtained by simply adding to $R$ those elements $(a, a)$ in the diagonal which do not already belong to $R$, and symmetric($R$) is obtained by adding to $R$ all pairs $(b, a)$ whenever $(a, b)$ belongs to $R$.

**EXAMPLE 3.8** Consider the following relation $R$ on the set $A = \{1, 2, 3, 4\}$:

$$R = \{(1,1),\ (1,3),\ (2,4),\ (3,1),\ (3,3),\ (4,3)\}$$

Then

$$\begin{aligned}\text{reflexive}(R) &= R \cup \{(2,2), (4,4)\}\\ &= \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3), (2,2), (4,4)\}\end{aligned}$$

and

$$\begin{aligned}\text{symmetric}(R) &= R \cup \{(4,2), (3,4)\}\\ &= \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3), (4,2), (3,4)\}\end{aligned}$$

### Transitive Closure

Let $R$ be a relation on a set $A$. Recall that $R^2 = R \circ R$ and $R^n = R^{n-1} \circ R$. We define

$$R^* = \bigcup_{i=1}^{\infty} R^i$$

The following theorem applies.

**Theorem 3.3**: $R^*$ is the transitive closure of a relation $R$.

Suppose $A$ is a finite set with $n$ elements. Using graph theory, one can easily show that

$$R^* = R \cup R^2 \cup \cdots \cup R^n$$

This gives us the following result.

**Theorem 3.4**: Let $R$ be a relation on a set $A$ with $n$ elements. Then

$$\text{transitive}(R) = R \cup R^2 \cup \cdots \cup R^n$$

Finding transitive($R$) can take a lot of time when $A$ has a large number of elements. Here we give a simple example where $A$ has only three elements.

**EXAMPLE 3.9** Consider the following relation $R$ on $A = \{1, 2, 3\}$:

$$R = \{(1,2),\ (2,3),\ (3,3)\}$$

Then

$$R^2 = R \circ R = \{(1,3),\ (2,3),\ (3,3)\} \qquad \text{and} \qquad R^3 = R^2 \circ R = \{(1,3),\ (2,3),\ (3,3)\}$$

Accordingly,

$$\text{transitive}(R) = R \cup R^2 \cup R^3 = \{(1,2),\ (2,3),\ (3,3),\ (1,3)\}$$

## 3.8 PARTITIONS

Let $S$ be a nonempty set. A *partition* of $S$ is a subdivision of $S$ into nonoverlapping, nonempty subsets. Precisely, a partition of $S$ is a collection $P = \{A_i\}$ of nonempty subsets of $S$ such that

(i) Each $a \in S$ belongs to one of the $A_i$.

(ii) The sets $\{A_i\}$ are mutually disjoint; that is,

$$\boxed{\text{If } A_i \neq A_j, \text{ then } A_i \cap A_j = \varnothing}$$

The subsets in a partition are called *cells*. Thus each $a \in S$ belongs to exactly one of the cells. Figure 3-6 is a Venn diagram of a partition of the rectangular set $S$ of points into five cells: $A_1$, $A_2$, $A_3$, $A_4$, $A_5$.

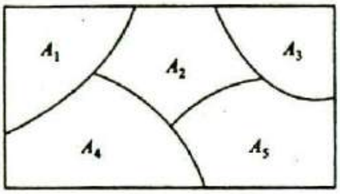


Fig. 3-6

**EXAMPLE 3.10** Consider the following collections of subsets of $S = \{1, 2, \ldots, 8, 9\}$:

(i) $P_1 = [\{1,3,5\}, \{2,6\}, \{4,8,9\}]$

(ii) $P_2 = [\{1,3,5\}, \{2,4,6,8\}, \{5,7,9\}]$

(iii) $P_3 = [\{1,3,5\}, \{2,4,6,8\}, \{7,9\}]$

Then $P_1$ is not a partition of $S$ since $7 \in S$ does not belong to any of the subsets. $P_2$ is not a partition of $S$ since $\{1,3,5\}$ and $\{5,7,9\}$ are not disjoint. On the other hand, $P_3$ is a partition of $S$.

**Remark**: Given a partition $P = \{A_i\}$ of a set $S$, any element $b \in A_i$ is called a *representative* of the cell $A_i$, and a subset $B$ of $S$ is called a *system* of representatives if $B$ contains exactly one element of each of the cells of $P$. Note $B = \{1, 2, 7\}$ is a system of representatives of the partition $P_3$ in Example 3.10.

## 3.9 EQUIVALENCE RELATIONS

Consider a nonempty set $S$. A relation $R$ on $S$ is an *equivalence relation* if $R$ is reflexive, symmetric, and transitive. That is, $R$ is an equivalence relation on $S$ if it has the following three properties:

(1) For every $a \in S$, $a R a$.
(2) If $a R b$, then $b R a$.
(3) If $a R b$ and $b R c$, then $a R c$.

The general idea behind an equivalence relation is that it is a classification of objects which are in some way "alike". In fact, the relation $=$ of equality on any set $S$ is an equivalence relation; that is,

(1) $a = a$ for every $a \in S$.
(2) If $a = b$, then $b = a$.
(3) If $a = b$ and $b = c$, then $a = c$.

For this reason, one frequently uses $\sim$ or $\equiv$ to denote an equivalence relation.

Examples of equivalence relations other than equality follow.

**EXAMPLE 3.11**

(*a*) Consider the set $L$ of lines and the set $T$ of triangles in the Euclidean plane. The relation "is parallel to or identical to" is an equivalence relation on $L$, and congruence and similarity are equivalence relations on $T$.

(*b*) The classification of animals by species, that is, the relation "is of the same species as," is an equivalence relation on the set of animals.

(*c*) The relation $\subseteq$ of set inclusion is not an equivalence relation. It is reflexive and transitive, but it is not symmetric since $A \subseteq B$ does not imply $B \subseteq A$.

(*d*) Let $m$ be a fixed positive integer. Two integers $a$ and $b$ are said to be *congruent modulo m*, written

$$a \equiv b \pmod{m}$$

if $m$ divides $a - b$. For example, for $m = 4$ we have $11 \equiv 3 \pmod{4}$ since 4 divides $11 - 3$, and $22 \equiv 6 \pmod{4}$ since 4 divides $22 - 6$. This relation of congruence modulo $m$ is an equivalence relation.

### Equivalence Relations and Partitions

Suppose $R$ is an equivalence relation on a set $S$. For each $a$ in $S$, let $[a]$ denote the set of elements of $S$ to which $a$ is related under $R$; that is,

$$[a] = \{x : (a, x) \in R\}$$

We call $[a]$ the *equivalence class* of $a$ in $S$ under $R$. The collection of all such equivalence classes is denoted by $S/R$, that is,

$$S/R = \{[a] : a \in S\}$$

It is called the *quotient* set of $S$ by $R$.

The fundamental property of an equivalence relation and its quotient set is contained in the following theorem (which is proved in Problem 3.28).

**Theorem 3.5**: Let $R$ be an equivalence relation on a set $S$. Then the quotient set $S/R$ is a partition of $S$. Specifically:

(i) For each $a$ in $S$, we have $a \in [a]$.
(ii) $[a] = [b]$ if and only if $(a, b) \in R$.
(iii) If $[a] \neq [b]$, then $[a]$ and $[b]$ are disjoint.

The converse of the above theorem (proved in Problem 3.29) is also true. That is,

**Theorem 3.6**: Suppose $P = \{A_i\}$ is a partition of a set $S$. Then there is an equivalence relation $\sim$ on $S$ such that the set $S/\sim$ of equivalence classes is the same as the partition $P = \{A_i\}$.

cifically, for $a, b \in S$, the equivalence $\sim$ in Theorem 3.6 is defined by $a \sim b$ if $a$ and $b$ belong to the e cell in $P$.

hus we see there is a one-to-one correspondence between the equivalence relations on a set $S$ and partitions of $S$. Accordingly, for a given equivalence relation $R$ on a set $S$, we can talk about a system of representatives of the quotient set $S/R$ which would contain exactly one representative from each uivalence class.

**EXAMPLE 3.12**

(*a*) Consider the following relation $R$ on $S = \{1, 2, 3, 4\}$:

$$R = \{(1,1),\ (2,2),\ (1,3),\ (3,1),\ (3,3),\ (4,4)\}$$

One can show that $R$ is reflexive, symmetric and transitive, that is, that $R$ is an equivalence relation. Under the relation $R$,

$$[1] = \{1,3\}, \qquad [2] = \{2\}, \qquad [3] = \{1,3\}, \qquad [4] = \{4\}$$

Observe that $[1] = [3]$ and that $S/R = \{[1], [2], [4]\}$ is a partition of $S$. One can choose either $\{1, 2, 4\}$ or $\{2, 3, 4\}$ as a system of representatives of the equivalence classes.

(*b*) Let $R_5$ be the relation on the set $\mathbf{Z}$ of integers defined by

$$x \equiv y \pmod 5$$

which reads "$x$ is congruent to $y$ modulo 5" and which means that the difference $x - y$ is divisible by 5. Then $R_5$ is an equivalence relation on $\mathbf{Z}$. There are exactly five equivalence classes in the quotient set $\mathbf{Z}/R_5$ as follows:

$$\begin{aligned}
A_0 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
A_1 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
A_2 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
A_3 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
A_4 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

Observe that any integer $x$, which can be uniquely expressed in the form $x = 5q + r$ where $0 \le r < 5$, is a member of the equivalence class $A_r$ where $r$ is the remainder. As expected, the equivalence classes are disjoint and

$$\mathbf{Z} = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4$$

This quotient set $\mathbf{Z}/R_5$ is usually denoted by

$$\mathbf{Z}/5\mathbf{Z} \text{ or simply } \mathbf{Z}_5$$

Usually one chooses $\{0, 1, 2, 3, 4\}$ or $\{-2, -1, 0, 1, 2\}$ as a system of representatives of the equivalence classes.

## 3.10 PARTIAL ORDERING RELATIONS

This section defines another important class of relations. A relation $R$ on a set $S$ is called a *partial ordering* of $S$ or a *partial order* on $S$ if it has the following three properties:

(1) For every $a \in S$, we have $a\,R\,a$.
(2) If $a\,R\,b$ and $b\,R\,a$, then $a = b$.
(3) If $a\,R\,b$ and $b\,R\,c$, then $a\,R\,c$.

That is, $R$ is a partial ordering of $S$ if $R$ is reflexive, antisymmetric, and transitive.

A set $S$ together with a partial ordering $R$ is called a *partially ordered set* or *poset*. Partially ordered sets will be studied in more detail in Chapter 7, so here we simply give some examples.

**EXAMPLE 3.13**

(*a*) The relation $\subseteq$ of set inclusion is a partial ordering of any collection of sets since set inclusion has the three desired properties. That is,

(1) $A \subseteq A$ for any set $A$.
(2) If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
(3) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(*b*) The relation $\leq$ on the set $R$ of real numbers is reflexive, antisymmetric, and transitive. Thus $\leq$ is a partial ordering.

(*c*) The relation "$a$ divides $b$" is a partial ordering of the set $p$ of positive integers. However, "$a$ divides $b$" is not a partial ordering of the set **Z** of integers since $a|b$ and $b|a$ does not imply $a = b$. For example, $3|-3$ and $-3|3$ but $3 \neq -3$.

### 3.11 *n*-ARY RELATIONS

All the relations discussed above were binary relations. By an *n-ary relation*, we mean a set of ordered $n$-tuples. For any set $S$, a subset of the product set $S^n$ is called an $n$-ary relation on $S$. In particular, a subset of $S^3$ is called a *ternary relation* on $S$.

**EXAMPLE 3.14**

(*a*) Let $L$ be a line in the plane. Then "betweenness" is a ternary relation $R$ on the points of $L$; that is, $(a, b, c) \in R$ if $b$ lies between $a$ and $c$ on $L$.

(*b*) The equation $x^2 + y^2 + z^2 = 1$ determines a ternary relation $T$ on the set $\mathbf{R}$ of real numbers. That is, a triple $(x, y, z)$ belongs to $T$ if $(x, y, z)$ satisfies the equation which means that $(x, y, z)$ is the coordinates of a point in $\mathbf{R}^3$ on the sphere $S$ with radius 1 and center at the origin $0 = (0, 0, 0)$.

## Solved Problems

### ORDERED PAIRS AND PRODUCT SETS

**3.1.** Let $A = \{1, 2\}$, $B = \{x, y, z\}$, $C = \{3, 4\}$. Find $A \times B \times C$.

$A \times B \times C$ consists of all ordered triplets $(a, b, c)$ where $a \in A$, $b \in B$, $c \in C$. These elements of $A \times B \times C$ can be systematically obtained by a so-called tree diagram (Fig. 3-7). The elements of $A \times B \times C$ are precisely the 12 ordered triplets to the right of the tree diagram.

Observe that $n(A) = 2$, $n(B) = 3$, and $n(C) = 2$ and, as expected,

$$n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$

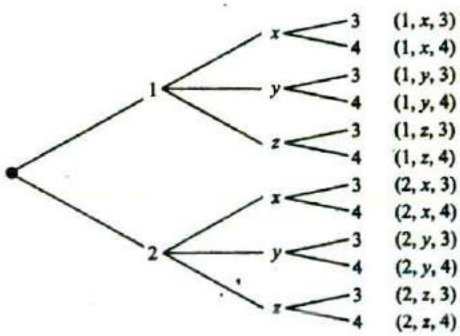


Fig. 3-7

**3.2.** Find $x$ and $y$ given $(2x,\ x+y) = (6,2)$.

Two ordered pairs are equal if and only if the corresponding components are equal. Hence we obtai the equations

$$2x = 6 \quad \text{and} \quad x + y = 2$$

from which we derive the answer $x = 3$ and $y = -1$.

**3.3.** Let $A = \{1,2\}$, $B = \{a,b,c\}$, $C = \{c,d\}$. Find $(A \times B) \cap (A \times C)$ and $A \times (B \cap C)$.

We have

$$A \times B = \{(1,a),\ (1,b),\ (1,c),\ (2,a),\ (2,b),(2,c)\}$$
$$A \times C = \{(1,c),\ (1,d),\ (2,c),\ (2,d)\}$$

Hence

$$(A \times B) \cap (A \times C) = \{(1,c),\ (2,c)\}$$

Since $B \cap C = \{c\}$,

$$A \times (B \cap C) = \{(1,c),\ (2,c)\}$$

Observe that $(A \times B) \cap (A \times C) = A \times (B \cap C)$. This is true for any sets $A$, $B$, and $C$ (see Problem 3.4).

**3.4.** Prove $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

$$\begin{aligned}(A \times B) \cap (A \times C) &= \{(x,y):\ (x,y) \in A \times B \text{ and } (x,y) \in A \times C\} \\ &= \{(x,y):\ x \in A, y \in B \text{ and } x \in A, y \in C\} \\ &= \{(x,y):\ x \in A, y \in B \cap C\} = A \times (B \cap C)\end{aligned}$$

## RELATIONS AND THEIR GRAPHS

**3.5.** Find the number of relations from $A = \{a,b,c\}$ to $B = \{1,2\}$.

There are $3 \cdot 2 = 6$ elements in $A \times B$, and hence there are $m = 2^6 = 64$ subsets of $A \times B$. Thus there are $m = 64$ relations from $A$ to $B$.

**3.6.** Given $A = \{1,2,3,4\}$ and $B = \{x,y,z\}$. Let $R$ be the following relation from $A$ to $B$:

$$R = \{(1,y),\ (1,z),\ (3,y),\ (4,x),\ (4,z)\}$$

(*a*) Determine the matrix of the relation.

(*b*) Draw the arrow diagram of $R$.

(*c*) Find the inverse relation $R^{-1}$ of $R$.

(*d*) Determine the domain and range of $R$.

(*a*) See Fig. 3-8(*a*). Observe that the rows of the matrix are labeled by the elements of $A$ and the columns by the elements of $B$. Also observe that the entry in the matrix corresponding to $a \in A$ and $b \in B$ is 1 if $a$ is related to $b$ and 0 otherwise.

(*b*) See Fig. 3-8(*b*). Observe that there is an arrow from $a \in A$ to $b \in B$ iff $a$ is related to $b$, i.e., iff $(a,b) \in R$.

(*c*) Reverse the ordered pairs of $R$ to obtain $R^{-1}$:

$$R^{-1} = \{(y,1),\ (z,1),\ (y,3),\ (x,4),\ (z,4)\}$$

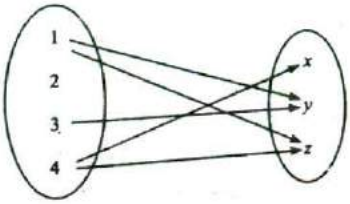
Observe that by reversing the arrows in Fig. 3-8(*b*) we obtain the arrow diagram of $R^{-1}$.

(*d*) The domain of $R$, $\mathrm{Dom}(R)$, consists of the first elements of the ordered pairs of $R$, and the range of $R$, $\mathrm{Ran}(R)$, consists of the second elements. Thus,

$$\mathrm{Dom}(R) = \{1, 3, 4\} \qquad \text{and} \qquad \mathrm{Ran}(R) = \{x, y, z\}$$

$$\begin{array}{c@{}c} & \begin{array}{ccc} x & y & x \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array}$$

(*a*)



(*b*)

Fig. 3-8

**3.7.** Let $A = \{1, 2, 3, 4, 6\}$, and let $R$ be the relation on $A$ defined by "$x$ divides $y$", written $x|y$.

(*a*) Write $R$ as a set of ordered pairs.

(*b*) Draw its directed graph.

(*c*) Find the inverse relation $R^{-1}$ of $R$. Can $R^{-1}$ be described in words?

(*a*) Find those numbers in $A$ divisible by 1, 2, 3, 4, and then 6. These are

$$1|1,\ 1|2,\ 1|3,\ 1|4,\ 1|6,\ 2|2,\ 2|4,\ 2|6,\ 3|3,\ 3|6,\ 4|4,\ 6|6$$

Hence

$$R = \{(1,1),\ (1,2),\ (1,3),\ (1,4),\ (1,6),\ (2,2),\ (2,4),\ (2,6),\ (3,3),\ (3,6),\ (4,4),\ (6,6)\}$$

(*b*) See Fig. 3-9.

(*c*) Reverse the ordered pairs of $R$ to obtain $R^{-1}$:

$$R^{-1} = \{(1,1),\ (2,1),\ (3,1),\ (4,1),\ (6,1),\ (2,2),\ (4,2),\ (6,2),\ (3,3),\ (6,3),\ (4,4),\ (6,6)\}$$

$R^{-1}$ can be described by the statement "$x$ is a multiple of $y$".

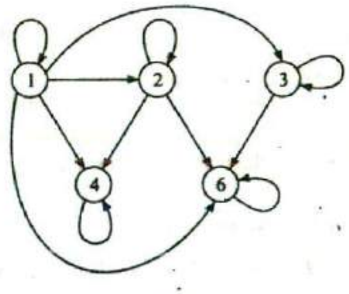


Fig. 3-9

**3.8.** Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{x, y, z\}$. Consider the following relation $R$ from $A$ to $B$ and relation $S$ from $B$ to $C$:

$$R = \{(1, b),\ (2, a),\ (2, c)\} \quad \text{and} \quad S = \{(a, y),\ (b, x),\ (c, y),\ (c, z)\}$$

(*a*) Find the composition relation $R \circ S$.

(*b*) Find the matrices $M_R$, $M_S$, and $M_{R \circ S}$ of the respective relations $R$, $S$, and $R \circ S$, and compare $M_{R \circ S}$ to the product $M_R M_S$.

(*a*) Draw the arrow diagram of the relations $R$ and $S$ as in Fig. 3-10. Observe that 1 in $A$ is "connected" to $x$ in $C$ by the path $1 \to b \to x$; hence $(1, x)$ belongs to $R \circ S$. Similarly, $(2, y)$ and $(2, z)$ belong to $R \circ S$. We have (as in Example 3.5)

$$R \circ S = \{(1, x),\ (2, y),\ (2, z)\}$$

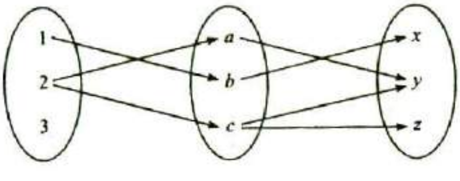


Fig. 3-10

(*b*) The matrices of $M_R$, $M_S$, and $M_{R \circ S}$ follow:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \qquad M_{R \circ S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Multiplying $M_R$ and $M_S$ we obtain

$$M_R M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Observe that $M_{R \circ S}$ and $M_R M_S$ have the same zero entries.

**3.9.** Let $R$ and $S$ be the following relations on $A = \{1, 2, 3\}$:

$$R = \{(1, 1),\ (1, 2),\ (2, 3),\ (3, 1),\ (3, )\}, \qquad S = \{(1, 2),\ (1, 3),\ (2, 1),\ (3, 3)\}$$

Find: (*a*) $R \cap S$, $R \cup S$, $R^c$; (*b*) $R \circ S$; (*c*) $S^2 = S \circ S$.

(*a*) Treat $R$ and $S$ simply as sets, and take the usual intersection and union. For $R^c$, use the fact that $A \times A$ is the universal relation on $A$.

$$R \cap S = \{(1, 2), (3, 3)\}, \quad R \cup S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$$
$$R^c = \{(1, 3), (2, 1), (2, 2), (3, 2)\}$$

(*b*) For each pair $(a, b) \in R$, find all pairs $(b, c) \in S$. Then $(a, c) \in R \circ S$. For example, $(1, 1) \in R$ and $(1, 2), (1, 3) \in S$; hence $(1, 2)$ and $(1, 3)$ belong to $R \circ S$. Thus,

$$R \circ S = \{(1, 2), (1, 3), (1, 1), (2, 3), (3, 2), (3, 3)\}$$

(*c*) Following the algorithm in (*b*), we get $S^2 = S \circ S = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 3)\}$.

**3.10.** Prove Theorem 3.1: Let $A, B, C, D$ be sets. Suppose $R$ is a relation from $A$ to $B$, $S$ is a relation from $B$ to $C$, and $T$ is a relation from $C$ to $D$. Then $(R \circ S) \circ T = R \circ (S \circ T)$.

We need to show that each ordered pair in $(R \circ S) \circ T$ belongs to $R \circ (S \circ T)$, i.e., that $(R \circ S) \circ T \subseteq R \circ (S \circ T)$, and vice versa.

Suppose $(a, d)$ belongs to $(R \circ S) \circ T$. Then there exists a $c$ in $C$ such that $(a, c) \in R \circ S$ and $(c, d) \in T$. Since $(a, c) \in R \circ S$, there exists a $b$ in $B$ such that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$ and $(c, d) \in T$, we have $(b, d) \in S \circ T$; and since $(a, b) \in R$ and $(b, d) \in S \circ T$, we have $(a, d) \in R \circ (S \circ T)$. Thus

$$(R \circ S) \circ T \subseteq R \circ (S \circ T)$$

Similarly, $R \circ (S \circ T) \subseteq (R \circ S) \circ T$. Both inclusion relations prove $(R \circ S) \circ T = R \circ (S \circ T)$

## TYPES OF RELATIONS AND CLOSURE PROPERTIES

**3.11.** Determine when a relation $R$ on a set $A$ is:

(*a*) not reflexive, (*b*) not symmetric, (*c*) not transitive, (*d*) not antisymmetric.

(*a*) There exists $a \in A$ such that $(a, a)$ does not belong to $R$.

(*b*) There exists $(a, b)$ in $R$ such that $(b, a)$ does not belong to $R$.

(*c*) There exists $(a, b)$ and $(b, c)$ in $R$ such that $(a, c)$ does not belong to $R$.

(*d*) There exists distinct elements $a, b \in A$ such that $(a, b)$ and $(b, a)$ belong to $R$.

**3.12.** Let $A = \{1, 2, 3, 4\}$. Consider the following relation $R$ on $A$:

$$R = \{(1,1), (2,2), (2,3), (3,2), (4,2), (4,4)\}$$

(*a*) Draw its directed graph.

(*b*) Is $R$ (i) reflexive? (ii) symmetric? (iii) transitive? (iv) antisymmetric?

(*c*) Find $R^2 = R \circ R$.

(*a*) See Fig. 3-11.

(*b*) (i) $R$ is not reflexive because $3 \in A$ but $3 \not{R} 3$, i.e., $(3, 3) \notin R$.

(ii) $R$ is not symmetric because $4R2$ but $2 \not{R} 4$, i.e., $(4, 2) \in R$ but $(2, 4) \notin R$.

(iii) $R$ is not transitive because $4R2$ and $2R3$ but $4 \not{R} 3$, i.e., $(4, 2) \in R$ and $(2, 3) \in R$ but $(4, 3) \notin R$.

(iv) $R$ is not antisymmetric because $2R3$ and $3R2$ but $2 \neq 3$.

(*c*) For each pair $(a, b) \in R$, find all $(b, c) \in R$. Since $(a, c) \in R^2$,

$$R^2 = \{(1,1), (2,2), (2,3), (3,2), (3,3), (4,2), (4,3), (4,4)\}$$

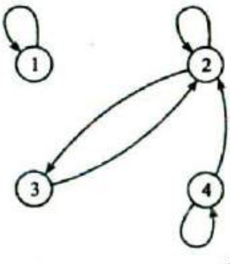


Fig. 3-11

**3.13.** Give examples of relations $R$ on $A = \{1, 2, 3\}$ having the stated property.

(*a*) $R$ is both symmetric and antisymmetric.

(*b*) $R$ is neither symmetric nor antisymmetric.

(*c*) $R$ is transitive but $R \cup R^{-1}$ is not transitive.

There are several possible examples for each answer. One possible set of examples follows:

(*a*) $R = \{(1, 1), (2, 2)\}$

(*b*) $R = \{(1, 2), (2, 1), (2, 3)\}$

(*c*) $R = \{(1, 2)\}$

**3.14.** Suppose $\mathscr{C}$ is a collection of relations $S$ on a set $A$ and let $T$ be the intersection of the relations $S$, that is, $T = \cap(S : S \in \mathscr{C})$. Prove:

(*a*) If every $S$ is symmetric, then $T$ is symmetric.

(*b*) If every $S$ is transitive, then $T$ is transitive.

(*a*) Suppose $(a, b) \in T$. Then $(a, b) \in S$ for every $S$. Since each $S$ is symmetric, $(b, a) \in S$ for every $S$. Hence $(b, a) \in T$ and $T$ is symmetric.

(*b*) Suppose $(a, b)$ and $(b, c)$ belong to $T$. Then $(a, b)$ and $(b, c)$ belong to $S$ for every $S$. Since each $S$ is transitive, $(a, c)$ belongs to $S$ for every $S$. Hence, $(a, c) \in T$ and $T$ is transitive.

**3.15.** Let $A = \{a, b, c\}$ and let $R$ be defined by

$$R = \{(a, a),\ (a, b),\ (b, c),\ (c, c)\}$$

Find: (*a*) reflexive($R$), (*b*) symmetric($R$), (*c*) transitive($R$).

(*a*) The reflexive closure of $R$ is obtained by adding all diagonal pairs of $A \times A$ to $R$ which are not currently in $R$. Hence

$$\text{reflexive}(R) = R \cup \{(b, b)\} = \{(a, a),\ (a, b),\ (b, c),\ (c, c),\ (b, b)\}$$

(*b*) The symmetric closure of $R$ is obtained by adding all pairs in $R^{-1}$ which are not currently in $R$. Hence

$$\begin{aligned}\text{symmetric}(R) &= R \cup \{(b, a),\ (c, b)\} \\ &= \{(a, a),\ (a, b),\ (b, a),\ (b, c),\ (c, b),\ (c, c)\}\end{aligned}$$

(*c*) Since $A$ has three elements, the transitive closure of $R$ is obtained by taking the union of $R$ with $R^2 = R \circ R$ and $R^3 = R \circ R \circ R$. We have:

$$R^2 = R \circ R = \{(a, a),\ (a, b),\ (a, c),\ (b, c),\ (c, c)\}$$
$$R^3 = R^2 \circ R = \{(a, a),\ (a, b),\ (a, c),\ (b, c),\ (c, c)\}$$

Hence transitive($R$) $= R \cup R^2 \cup R^3 = \{(a, a),\ (a, b),\ (a, c),\ (b, c),\ (c, c)\}$.

## PARTITIONS

**3.16.** Let $S = \{1, 2, 3, 4, 5, 6\}$. Determine which of the following are partitions of $S$:

(*a*) $P_1 = [\{1, 2, 3\},\ \{1, 4, 5, 6\}]$

(*b*) $P_2 = [\{1, 2\},\ \{3, 5, 6\}]$

(*c*) $P_3 = [\{1, 3, 5\},\ \{2, 4\},\ \{6\}]$

(*d*) $P_4 = [\{1, 3, 5\},\ \{2, 4, 6, 7\}]$

(*a*) No, since $1 \in S$ belongs to two cells.

(*b*) No, since $4 \in S$ does not belong to any cell.

(*c*) $P_3$ is a partition of $S$.

(*d*) No, since $\{2, 4, 6, 7\}$ is not a subset of $S$.

**3.17.** Find all partitions of $S = \{a, b, c, d\}$.

Note first that each partition of $S$ contains either 1, 2, 3, or 4 distinct cells. The partitions are as follows:

(1) $[S]$;

(2) $[\{a\}, \{b,c,d\}]$, $[\{b\}, \{a,c,d\}]$, $[\{c\}, \{a,b,d\}]$, $[\{d\}, \{a,b,c\}]$, $[\{a,b\}, \{c,d\}]$, $[\{a,c\}, \{b,d\}]$, $[\{a,d\}, \{b,c\}]$;

(3) $[\{a\}, \{b\}, \{c,d\}]$, $[\{a\}, \{c\}, \{b,d\}]$, $[\{a\}, \{d\}, \{b,c\}]$, $[\{b\}, \{c\}, \{a,d\}]$, $[\{b\}, \{d\}, \{a,c\}]$, $[\{c\}, \{d\}, \{a,b\}]$;

(4) $[\{a\}, \{b\}, \{c\}, \{d\}]$.

There are 15 different partitions of $S$.

**3.18.** Let $[A_1, A_2, \ldots, A_m]$ and $[B_1, B_2, \ldots, B_n]$ be partitions of $X$. Show that the collection of sets

$$P = [\{A_i \cap B_j\}] \backslash \varnothing$$

is also a partition (called the *cross partition*) of $X$. (Observe that we have deleted the empty set $\varnothing$.)

Let $x \in X$. Then $x$ belongs to $A_r$ for some $r$, and to $B_s$ for some $s$; hence $x$ belongs to $A_r \cap B_s$. Thus the union of the $A_i \cap B_j$ is equal to $X$. Now suppose $A_r \cap B_s$ and $A_{r'} \cap B_{s'}$ are not disjoint, say $y$ belongs to both sets. Then $y$ belongs to $A_r$ and $A_{r'}$; hence $A_r = A_{r'}$. Similarly $y$ belongs to $B_s$ and $B_{s'}$; hence $B_s = B_{s'}$. Accordingly, $A_r \cap B_s = A_{r'} \cap B_{s'}$. Thus the cells are mutually disjoint or equal. Accordingly, $P$ is a partition of $X$.

**3.19.** Let $X = \{1, 2, 3, \ldots, 8, 9\}$. Find the cross partition $P$ of the following partitions of $X$:

$$P_1 = [\{1,3,5,7,9\},\ \{2,4,6,8\}] \qquad \text{and} \qquad P_2 = [\{1,2,3,4\},\ \{5,7\},\ \{6,8,9\}]$$

Intersect each cell in $P_1$ with each cell in $P_2$ (omitting empty intersections) to obtain

$$P = [\{1,3\}, \{5,7\}, \{9\}, \{2,4\}, \{8\}]$$

**3.20.** Let $f(n,k)$ represent the number of partitions of a set $S$ with $n$ elements into $k$ cells (for $k = 1, 2, \ldots, n$). Find a recursion formula for $f(n,k)$.

Note first that $f(n,1) = 1$ and $f(n,n) = 1$ since there is only one way to partition $S$ with $n$ elements into either one cell or $n$ cells. Now suppose $n > 1$ and $1 < k < n$. Let $b$ be some distinguished element of $S$. If $\{b\}$ constitutes a cell, then $S\backslash\{b\}$ can be partitioned into $k-1$ cells in $f(n-1, k-1)$ ways. On the other hand, each partition of $S\backslash\{b\}$ into $k$ cells allows $b$ to be admitted into a cell in $k$ ways. We have thus shown that

$$f(n,k) = f(n-1, k-1) + kf(n-1, k)$$

which is the desired recursion formula.

**3.21.** Consider the recursion formula in Problem 3.20. (*a*) Find the solution for $n = 1, 2, \ldots, 6$ in a form similar to Pascal's triangle. (*b*) Find the number $m$ of partitions of a set with $m = 6$ elements.

(*a*) Use the recursion formula to obtain the triangle in Fig. 3-12, for example:

$$f(6,4) = f(5,3) + 4f(5,4) = 25 + 4(10) = 65$$

(*b*) Use row 6 in Fig. 3-12 to obtain $m = 1 + 31 + 90 + 65 + 15 + 1 = 203$.

| | | | | | |
|---|---|---|---|---|---|
| 1 | | | | | |
| 1 | 1 | | | | |
| 1 | 3 | 1 | | | |
| 1 | 7 | 6 | 1 | | |
| 1 | 15 | 25 | 10 | 1 | |
| 1 | 31 | 90 | 65 | 15 | 1 |

**Fig. 3-12**

## EQUIVALENCE RELATIONS AND PARTITIONS

**3.22.** Consider the set **Z** of integers and any integer $m > 1$. We say that $x$ is congruent to $y$ modulo $m$, written

$$x \equiv y \pmod{m}$$

if $x - y$ is divisible by $m$. Show that this defines an equivalence relation on **Z**.

We must show that the relation is reflexive, symmetric, and transitive.

(i) For any $x$ in **Z** we have $x \equiv x \pmod{m}$ because $x - x = 0$ is divisible by $m$. Hence the relation is reflexive.

(ii) Suppose $x \equiv y \pmod{m}$, so $x - y$ is divisible by $m$. Then $-(x - y) = y - x$ is also divisible by $m$, so $y \equiv x \pmod{m}$. Thus the relation is symmetric.

(iii) Now suppose $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$, so $x - y$ and $y - z$ are each divisible by $m$. Then the sum

$$(x - y) + (y - z) = x - z$$

is also divisible by $m$; hence $x \equiv z \pmod{m}$. Thus the relation is transitive.

Accordingly, the relation of congruence modulo $m$ on **Z** is an equivalence relation.

**3.23.** Let $R$ be the following equivalence relation on the set $A = \{1, 2, 3, 4, 5, 6\}$:

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

Find the partition of $A$ *induced* by $R$, i.e., find the equivalence classes of $R$.

Those elements related to 1 are 1 and 5, hence

$$[1] = \{1, 5\}$$

We pick an element which does not belong to [1], say 2. Those elements related to 2 are 2, 3, and 6, hence

$$[2] = \{2, 3, 6\}$$

The only element which does not belong to [1] or [2] is 4. The only element related to 4 is 4. Thus

$$[4] = \{4\}$$

Accordingly,

$$[\{1, 5\}, \{2, 3, 6\}, \{4\}]$$

is the partition of $A$ induced by $R$.

**3.24.** Let $A = \{1, 2, 3, \ldots, 14, 15\}$. Let $R$ be the equivalence relation on $A$ defined by congruence modulo 4.

(*a*) Find the equivalence classes determined by $R$.

(*b*) Find a system $B$ of equivalence class representatives which are multiples of 3.

(*a*) Recall (Problem 3.22) that $a \equiv b \pmod 4$ if 4 divides $a - b$ or, equivalently, if $a = b + 4k$ for some integer $k$. Accordingly:

(1) Add multiples of 4 to 1 to obtain $[1] = \{1, 5, 9, 13\}$.
(2) Add multiples of 4 to 2 to obtain $[2] = \{2, 6, 10, 14\}$.
(3) Add multiples of 4 to 3 to obtain $[3] = \{3, 7, 11, 15\}$.
(4) Add multiples of 4 to 4 to obtain $[4] = \{4, 8, 12\}$.

Then [1], [2], [3], [4] are all the equivalence classes since they include all the elements of $A$.

(*b*) Choose an element in each equivalence class which is a multiple of 3. Thus $B = \{9, 6, 3, 12\}$ or $B = \{9, 6, 15, 12\}$.

**3.25.** Consider the set of words $W =$ {sheet, last, sky, wash, wind, sit}. Find $W/R$ where $R$ is the equivalence relation defined by:

(*a*) "has the same number of letters", (*b*) "begins with the same letter".

(*a*) Those words with the same number of letters belong to the same cell; hence

$$W/R = [\{\text{sheet}\},\ \{\text{last, wash, wind}\},\ \{\text{sky, sit}\}]$$

(*b*) Those words beginning with the same letter belong to the same cell; hence

$$W/R = [\{\text{sheet, sky, sit}\},\ \{\text{last}\},\ \{\text{wash, wind}\}]$$

**3.26.** Let $A$ be a set of nonzero integers and let $\approx$ be the relation on $A \times A$ defined as follows:

$$(a, b) \approx (c, d) \qquad \text{whenever} \qquad ad = bc$$

Prove that $\approx$ is an equivalence relation.

We must show that $\approx$ is reflexive, symmetric, and transitive.

(i) *Reflexivity*: We have $(a, b) \approx (a, b)$ since $ab = ba$. Hence $\approx$ is reflexive.

(ii) *Symmetry*: Suppose $(a, b) \approx (c, d)$. Then $ad = bc$. Accordingly, $cb = da$ and hence $(c, d) = (a, b)$. Thus, $\approx$ is symmetric.

(iii) *Transitivity*: Suppose $(a, b) \approx (c, d)$ and $(c, d) \approx (e, f)$. Then $ad = bc$ and $cf = de$. Multiplying corresponding terms of the equations gives $(ad)(cf) = (bc)(de)$. Canceling $c \neq 0$ and $d \neq 0$ from both sides of the equation yields $af = be$, and hence $(a, b) \approx (e, f)$. Thus $\approx$ is transitive.

Accordingly, $\approx$ is an equivalence relation.

**3.27.** Let $A = \{1, 2, 3, \ldots, 14, 15\}$. Let $\approx$ be the equivalence relation on $A \times A$ defined by $(a, b) \approx (c, d)$ if $ad = bc$. (See Problem 3.26.) Find the equivalence class of $(3, 2)$.

We seek all $(m, n)$ such that $(3, 2) \approx (m, n)$, that is, such that $3n = 2m$ or $3/2 = m/n$. [In other words, if $(3, 2)$ is written as the fraction 3/2, then we seek all fractions $m/n$ which are equal to 3/2.] Thus:

$$[(3, 2)] = \{(3, 2),\ (6, 4),\ (9, 6),\ (12, 8),\ (15, 10)\}$$

**3.28.** Prove Theorem 3.5: Let $R$ be an equivalence relation on a set $S$. Then the quotient set $S/R$ is a partition of $S$. Specifically:

(i) For each $a \in S$, we have $a \in [a]$.

(ii) $[a] = [b]$ if and only if $(a, b) \in R$.

(iii) If $[a] \neq [b]$, then $[a]$ and $[b]$ are disjoint.

*Proof of* (i): Since $R$ is reflexive, $(a, a) \in R$ for every $a \in S$ and therefore $a \in [a]$.

*Proof of* (ii): Suppose $(a, b) \in R$. We want to show that $[a] = [b]$. Let $x \in [b]$; then $(b, x) \in R$. But by hypothesis $(a, b) \in R$ and so, by transitivity, $(a, x) \in R$. Accordingly $x \in [a]$. Thus $[b] \subseteq [a]$. To prove that $[a] \subseteq [b]$, we observe that $(a, b) \in R$ implies, by symmetry, that $(b, a) \in R$. Then, by a similar argument, we obtain $[a] \subseteq [b]$. Consequently, $[a] = [b]$.

On the other hand, if $[a] = [b]$, then, by (i), $b \in [b] = [a]$; hence $(a, b) \in R$.

*Proof of* (iii): We prove the equivalent contrapositive statement:

$$\text{If } [a] \cap [b] \neq \varnothing \qquad \text{then} \qquad [a] = [b]$$

If $[a] \cap [b] \neq \varnothing$, then there exists an element $x \in A$ with $x \in [a] \cap [b]$. Hence $(a, x) \in R$ and $(b, x) \in R$. By symmetry, $(x, b) \in R$ and by transitivity, $(a, b) \in R$. Consequently by (ii), $[a] = [b]$.

**3.29.** Prove Theorem 3.6: Suppose $P = \{A_i\}$ is a partition of a set $S$. Then there is an equivalence relation $\sim$ on $S$ such that $S/\sim$ is the same as the partition $P = \{A_i\}$.

For $a, b \in S$, define $a \sim b$ if $a$ and $b$ belong to the same cell $A_k$ in $P$. We need to show that $\sim$ is reflexive, symmetric, and transitive.

(i) Let $a \in S$. Since $P$ is a partition, there exists some $A_k$ in $P$ such that $a \in A_k$. Hence $a \sim a$. Thus $\sim$ is reflexive.

(ii) Symmetry follows from the fact that if $a, b \in A_k$, then $b, a \in A_k$.

(iii) Suppose $a \sim b$ and $b \sim c$. Then $a, b \in A_i$ and $b, c \in A_j$. Therefore $b \in A_i \cap B_j$. Since $P$ is a partition, $A_i = A_j$. Thus $a, c \in A_i$ and so $a \sim c$. Thus $\sim$ is transitive.

Accordingly, $\sim$ is an equivalence relation on $S$.

Furthermore,

$$[a] = \{x : a \sim x\} = \{x : x \text{ is in the same cell } A_k \text{ as } a\}$$

Thus the equivalence classes under $\sim$ are the same as the cells in the partition $P$.

## MISCELLANEOUS PROBLEMS

**3.30.** Consider the set $\mathbf{Z}$ of integers. Define $a \sim b$ if $b = a^r$ for some positive integer $r$. Show that $\sim$ is a partial ordering of $\mathbf{Z}$; that is, show that: (i) (Reflexive) $a \sim a$ for every $a \in \mathbf{Z}$. (ii) (Antisymmetric) If $a \sim b$ and $b \sim a$, then $a = b$. (iii) (Transitive) If $a \sim b$ and $b \sim c$, then $a \sim c$.

(i) Since $a = a^1$, we have $a \sim a$. Thus $\sim$ is reflexive.

(ii) Suppose $a \sim b$ and $b \sim a$, say $b = a^r$ and $a = b^s$. Then $a = (a^r)^s = a^{rs}$. There are four possibilities:

(1) $rs = 1$. Then $r = 1$ and $s = 1$ and so $a = b$.

(2) $a = 1$. Then $b = 1^r = 1 = a$.

(3) $b = 1$. Then $a = 1^s = 1 = b$.

(4) $a = -1$. Then $b = 1$ or $b = -1$. By (3), $b \neq 1$. Hence $b = -1 = a$.

In all cases $a = b$. Thus $\sim$ is antisymmetric.

(iii) Suppose $a \sim b$ and $b \sim c$, say $b = a^r$ and $c = b^s$. Then $c = (a^r)^s = a^{rs}$, and hence $a \sim c$. Thus $\sim$ is transitive.

Accordingly, $\sim$ is a partial ordering of $\mathbf{Z}$.

**3.31.** Let $A = \{1, 2, 3, \ldots, 14, 15\}$.

(*a*) Let $R$ be the ternary relation on $A$ defined by the equation $x^2 + 5y = z$. Write $R$ as a set of ordered triples.

(*b*) Let $S$ be the 4-ary relation on $A$ defined by

$$S = \{(x, y, z, t) : 4x + 3y + z^2 = t\}$$

Write $S$ as a set of 4-tuples.

(*a*) Since $x^2 > 15$ for $x > 3$, we need only find solutions for $y$ and $z$ when $x = 1, 2, 3$. This yields:

$$R = \{(1, 1, 6),\ (1, 2, 1),\ (2, 1, 9),\ (2, 2, 14),\ (3, 1, 14)\}$$

(*b*) Note we can only have $x = 1, 2, 3$. This yields:

$$S = \{(1, 1, 1, 8),\ (1, 1, 2, 11),\ (1, 2, 1, 11),\ (1, 2, 2, 14),\\ (1, 3, 1, 14),\ (2, 1, 1, 12),\ (2, 1, 2, 15),\ (2, 2, 1, 15)\}$$

**3.32.** Each of the following expressions defines a relation on **R**:

(*a*) $y \le x^2$, (*b*) $y < 3 - x$, (*c*) $y > x^3$.

Sketch (by shading the appropriate area) each relation in the plane $\mathbf{R}^2$.

In order to sketch a relation on **R** defined by an expression of the form:

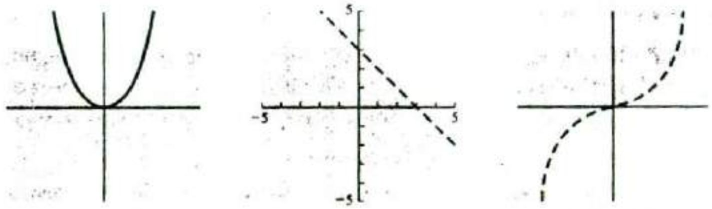
(1) $y > f(x)$, (2) $y \ge f(x)$, (3) $y < f(x)$, (4) $y \le f(x)$

first plot the equation $y = f(x)$ in the usual manner. Then the relation, i.e., the desired set, will consist, respectively, of the points:

(1) above, (2) above and on, (3) below, (4) below and on.

the equation $y = f(x)$.

Figure 3-13 shows the sketches of the three relations. The equations $y = f(x)$ in Fig. 3-13(*b*) and (*c*) are drawn with dashes to indicate that the points on the curve do not belong to the given relation.



(*a*) $y \le x^2$ (*b*) $y < 3 - x$ (*c*) $y > x^3$

Fig. 3-13

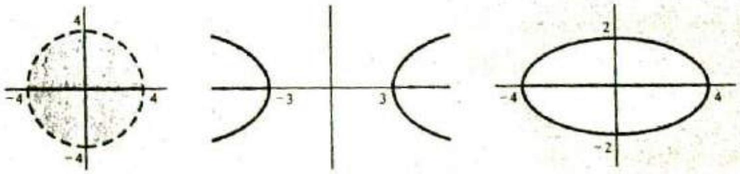
**3.33.** Each of the following expressions defines a relation on **R**:

(*a*) $x^2 + y^2 < 16$, (*b*) $x^2 - 4y^2 \ge 9$, (*c*) $x^2 + 4y^2 \le 16$.

Sketch (by shading the appropriate area) each relation in the plane $\mathbf{R}^2$.

In order to sketch a relation on **R** defined by an expression of the form $E(x, y) < k$ (respectively: $\leq$, $\equiv$, or $\geq$), first plot the equation $E(x, y) = k$. The curve $E(x, y) = k$ will, in simple situations, partition the plane into various regions. The relation will consist of all the points in one or more of the regions. Thus test at least one point in each region to determine whether or not all the points in that region belong to the relation. Also, use a dotted curve to indicate the points on the curve that do not belong to the relation.

Figure 3-14 shows each of the relations.



(a) $x^2 + y^2 < 16$ (b) $x^2 - 4y^2 \geq 9$ (c) $x^2 + 4y^2 \leq 16$

Fig. 3-14

## Supplementary Problems

### ORDERED PAIRS AND PRODUCT SETS

**3.34.** Let $S = \{a, b, c\}$, $T = \{b, c, d\}$, $W = \{a, d\}$. Find $S \times T \times W$ by constructing the tree diagram of $S \times T \times W$.

**3.35.** Let $C = \{\mathrm{H}, \mathrm{T}\}$, the set of possible outcomes if a coin is tossed. Find: (a) $C^2 = C \times C$; (b) $C^3$.

**3.36.** Find $x$ and $y$ if: (a) $(x + 2, 4) = (5, 2x + y)$; (b) $(y - 2,\ 2x + 1) = (x - 1,\ y + 2)$.

**3.37.** Suppose $n(A) = 3$ and $n(B) = 5$. Find the number of elements in:

(a) $A \times B$, $B \times A$, $A^2$, $B^2$; (b) $A \times B \times A$, $A^3$, $B^3$.

**3.38.** Sketch each of the following product sets in the plane $\mathbf{R}^2$ by shading the appropriate area:

(a) $[-3, 3] \times [-1, 2]$; (b) $[-3, 1) \times (-2, 2]$; (c) $(-2, 3] \times [-3, \infty)$.

[Here $[-3, \infty)$ is the infinite interval $\{x : x \geq -3\}$.]

**3.39.** Prove: $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

**3.40.** Suppose $A = B \cap C$. Show that: (a) $A \times A = (B \times B) \cap (C \times C)$; (b) $A \times A = (B \times C) \cap (C \times B)$.

### RELATIONS

**3.41.** Consider the relation $R = \{(1, a), (1, b), (3, b), (3, d), (4, b)\}$ from $X = \{1, 2, 3, 4\}$ to $Y = \{a, b, c, d\}$.

(a) Find $E = \{x : x\,R\,b\}$ and $F = \{x : x\,R\,d\}$. (c) Find the domain and range of $R$.

(b) Find $G = \{y : 1\,R\,y\}$ and $H = \{y : 2\,R\,y\}$. (d) Find $R^{-1}$.

**3.42.** Let $R$ and $S$ be relations from $A = \{1, 2, 3\}$ to $B = \{a, b\}$ defined by

$$R = \{(1, a),\ (3, a),\ (2, b),\ (3, b)\} \quad \text{and} \quad S = \{(1, b),\ (2, b)\}$$

Find: (*a*) $R \cap S$; (*b*) $R \cup S$; (*c*) $R^c$, (*d*) composition $R \circ S$.

**3.43.** Find the number of relations from $A = \{a, b, c, d\}$ to $B = \{x, y\}$.

**3.44.** Let $R$ be the relation on $P$ defined by the equation $x + 3y = 12$.

(*a*) Write $R$ as a set of ordered pairs.

(*b*) Find: (i) domain of $R$, (ii) range of $R$, (iii) $R^{-1}$.

(*c*) Find the composition relation $R \circ R$.

**3.45.** Consider the relation $R = \{(1, 3),\ (1, 4),\ (3, 2),\ (3, 3),\ (3, 4)\}$ on $A = \{1, 2, 3, 4\}$.

(*a*) Find the matrix representation $M_R$ of $R$.

(*b*) Find the domain and range of $R$.

(*c*) Find $R^{-1}$.

(*d*) Draw the directed graph of $R$.

(*e*) Find the composition relation $R \circ R$.

**3.46.** Let $S$ be the following relation on $A = \{1, 2, 3, 4, 5\}$:

$$S = \{(1, 2),\ (2, 2),\ (2, 4),\ (3, 3),\ (3, 5),\ (4, 1),\ (5, 2)\}$$

(*a*) Find the following subsets of $A$:

$$E = \{x : xS2\}, \qquad F = \{x : xS3\}, \qquad G = \{x : 2Sx\}, \qquad H = \{x : 3Sx\}$$

(*b*) Find the matrix representation $M_S$ of $S$.

(*c*) Draw the directed graph of $S$.

(*d*) Find the composition relation $S \circ S$.

**3.47.** Let $R$ be the relation on $X = \{a, b, c, d, e, f\}$ defined by

$$R = \{(a, b),\ (b, b),\ (b, c),\ (c, f),\ (d, b),\ (e, a),\ (e, b),\ (e, f)\}$$

(*a*) Find each of the following subsets of $X$:

$$E = \{x : bRx\}, \qquad F = \{x : xRb\}, \qquad G = \{x : xRe\}, \qquad H = \{x : eRx\}$$

(*b*) Find domain and range of $R$.

(*c*) Find the composition $R \circ R$.

## TYPES OF RELATIONS

**3.48.** Each of the following defines a relation on $\mathbf{P} = \{1, 2, 3, \ldots\}$:

(1) $x > y$, (2) $xy$ is a square, (3) $x + y = 10$, (4) $x + 4y = 10$

Determine which relations are: (*a*) reflexive, (*b*) symmetric, (*c*) antisymmetric, (*d*) transitive.

**3.49.** Consider the relation $R = \{(1, 1),\ (2, 2),\ (2, 3),\ (3, 2),\ (4, 2),\ (4, 4)\}$ on $A = \{1, 2, 3, 4\}$. Show that $R$ is not: (*a*) reflexive, (*b*) symmetric, (*c*) transitive, (*d*) antisymmetric.

**3.50.** Let $R, S, T$ be the relations on $A = \{1, 2, 3\}$ defined by:

$$R = \{(1, 1),\ (2, 2),\ (3, 3)\} = \Delta_A, \qquad S = \{(1, 2),\ (2, 1),\ (3, 3)\} \qquad T = \{(1, 2),\ (2, 3),\ (1, 3)\}$$

Determine which of $R, S, T$ are: (*a*) reflexive, (*b*) symmetric, (*c*) antisymmetric, (*d*) transitive.

**3.51.** Let $R$ be a relation on a set $A$ where $n(A) \geq 3$. State whether each of the following is true or false. If it is false, give a counterexample on the set $A = \{1, 2, 3\}$:

(*a*) If $R$ is symmetric, then $R^c$ is symmetric.

(*b*) If $R$ is reflexive, then $R^c$ is reflexive.

(*c*) If $R$ is transitive, then $R^c$ is transitive.

(*d*) If $R$ is reflexive, then $R \cap R^{-1}$ is not empty.

(*e*) If $R$ is symmetric, then $R \cap R^{-1}$ is not empty.

(*f*) If $R$ is antisymmetric, then $R^{-1}$ is antisymmetric.

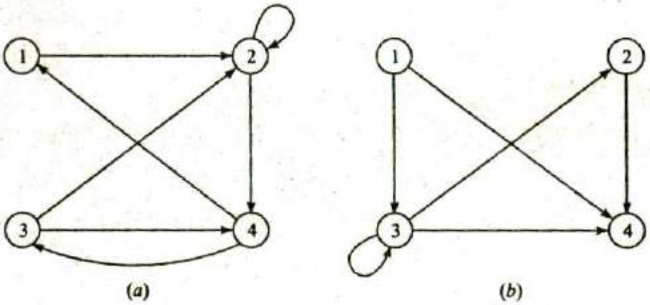
## CLOSURE PROPERTIES

**3.52.** Consider the relation $R = \{(1,1),\ (2,2),\ (2,3),\ (4,2)\}$ on $A = \{1,2,3,4\}$. Find:

(*a*) reflexive closure of $R$; (*b*) symmetric closure of $R$; (*c*) transitive closure of $R$.

**3.53.** Find the transitive closure $R^*$ of the relation $R$ on $A = \{1,2,3,4\}$ defined by the directed graph in:

(*a*) Fig. 3-15(*a*); (*b*) Fig. 3-15(*b*).



(*a*) (*b*)

Fig. 3-15

**3.54.** Suppose $A$ has $n$ elements, say $A = \{1, 2, \ldots, n\}$.

(*a*) Suppose $R$ is a relation on $A$ with $r$ pairs. Find an upper bound for the number of pairs in: (i) reflexive closure of $R$; (ii) symmetric closure of $R$.

(*b*) Find a relation $R$ on $A$ with $n$ pairs such that the transitive closure $R^*$ of $R$ is the universal relation $A \times A$ (containing $n^2$ pairs).

## PARTITIONS

**3.55.** Let $S = \{1,2,3,4,5,6\}$. Determine whether each of the following is a partition of $S$:

(*a*) $[\{1,3,5\},\ \{2,4\},\ \{3,6\}]$,
(*c*) $[\{1\},\ \{3,6\},\ \{2,4,5\},\ \{3,6\}]$,
(*b*) $[\{1,5\},\ \{2\},\ \{3,6\}]$,
(*d*) $[\{1\},\ \{2\},\ \{3\},\ \{4\},\ \{5\},\ \{6\}]$.

**3.56.** Find all partitions of $S = \{1,2,3\}$.

**3.57.** Let $P_1$ and $P_2$ be partitions of a set $S$, and let $P$ be the cross partition.

(*a*) Find bounds on the number $n$ of elements in $P$ if $P_1$ has $r$ elements and $P_2$ has $s$ elements.

(*b*) When will $P = P_1$?

(*c*) Find $P$ when $S = \{1,2,3,\ldots,8,9\}$ and

$$P_1 = [\{1,2,3,4,5\}, \{6,7,8,9\}] \quad \text{and} \quad P_2 = [\{1,3,5\}, \{2,6,7,9\}, \{4,8\}]$$

## EQUIVALENCE RELATIONS AND PARTITIONS

**3.58.** Let $S = \{1, 2, 3, \ldots, 19, 20\}$. Let $\equiv$ be the equivalence relation on $S$ defined by congruence modulo 7.

(*a*) Find the quotient set $S/\equiv$. (*b*) Find a system of equivalence class representatives consisting of even integers.

**3.59.** Let $A$ be a set of integers, and let $\sim$ be the relation on $A \times A$ defined by

$$(a, b) \sim (c, d) \quad \text{if} \quad a + d = b + c$$

(*a*) Prove that $\sim$ is an equivalence relation.

(*b*) Suppose $A = \{1, 2, 3, \ldots, 8, 9\}$. Find $[(2, 5)]$, the equivalence class of $(2, 5)$.

**3.60.** Let $\equiv$ be the relation on the set $R$ of real numbers defined by $a \equiv b$ if $b - a \in \mathbf{Z}$, that is, if $b - a$ is an integer.

(*a*) Show that $\equiv$ is an equivalence relation.

(*b*) Show that the half-open interval $A = [0, 1) = \{x : 0 \leq x < 1\}$ is a system of equivalence class representatives.

## MISCELLANEOUS PROBLEMS

**3.61.** Suppose $R$ is a partial order on a set $A$. Show that $R^{-1}$ is also a partial order on $A$.

**3.62.** Suppose $R_1$ is a partial ordering of a set $A$ and $R_2$ is a partial ordering of a set $B$. Let $R$ be the relation on $A \times B$ defined by

$$(a, b)R(a', b') \quad \text{if} \quad aRa' \text{ and } bR_2b'$$

Show that $R$ is a partial ordering of $A \times B$.

**3.63.** Let $A = \{1, 2, 3, \ldots, 14, 15\}$.

(*a*) Let $R$ be the ternary relation on $A$ defined by the equation $x^3 + y = 5z$. Write $R$ as a set of ordered triples.

(*b*) Let $S$ be the 4-ary relation on $A$ defined by the equation $x_1^2 + 4x_2 + 5x_3 = x_4$. Write $S$ as a set of 4-tuples.

**3.64.** Sketch in the plane $R^2$ (by shading the appropriate area) each of the following relations on $R$:

(*a*) $y < x^2 - 4x + 2$; (*b*) $y \geq \dfrac{x}{2} + 2$.

**3.65.** For each of the following pairs of relations $S$ and $S'$ on $R$, sketch $S \cap S'$ in the plane $\mathbf{R}^2$ and find its domain and range:

(*a*) $S = \{(x, y) : x^2 + y^2 \leq 25, \quad S' = \{(x, y) : y \geq 4x^2/9\}$

(*b*) $S = \{(x, y) : x^2 + y^2 < 25, \quad S' = \{(x, y) : y < 3x/4\}$

**3.66.** Show that a relation $R$ is transitive if and only if $R^n \subseteq R$ for every $n \geq 1$.

## Answers to Supplementary Problems

**3.34.** See Fig. 3-16. Using the notation: $aba = (a, b, a)$,

$S \times T \times W = \{aba, abd, aca, acd, ada, add, bba, bbd, bca, bcd, bda, bdd, cba, cbd, cca, ccd, cda, cdd\}$

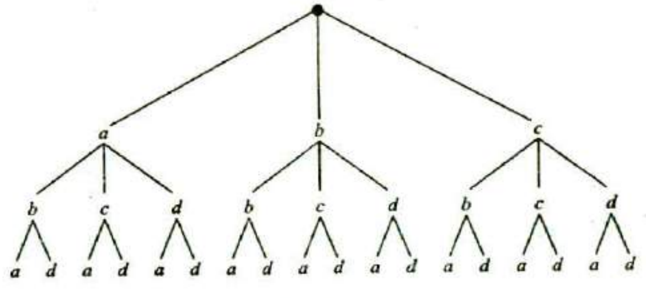


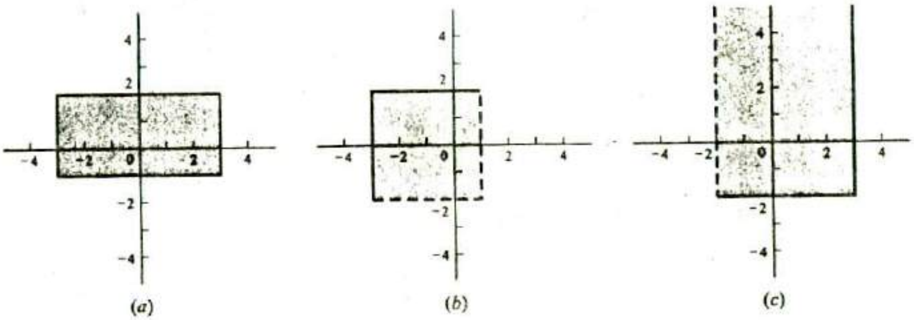
**Fig. 3-16**

**3.35.** (*a*) $C^2 = \{\text{HH}, \text{HT}, \text{TH}, \text{TT}\}$; (*b*) $C^3 = \{\text{HHH}, \text{HHT}, \text{HTH}, \text{HTT}, \text{THH}, \text{THT}, \text{TTH}, \text{TTT}\}$

**3.36.** (*a*) $x = 3,\ y = -2$; (*b*) $x = 2,\ y = 3$

**3.37.** (*a*) 15, 15, 9; (*b*) 45, 27, 125

**3.38.** See Fig. 3-17.



(*a*) (*b*) (*c*)

**Fig. 3-17**

**3.41.** (*a*) $E = \{1, 3, 4\}$, $F = \{3\}$; (*b*) $G = \{a, b\}$, $H = \varnothing$
(*c*) $\text{Dom}(R) = \{1, 3, 4\}$, $\text{Ran}(R) = \{a, b, d\}$
(*d*) $R^{-1} = \{(a, 1),\ (b, 1),\ (b, 3),\ (d, 3),\ (b, 4)\}$

**3.42.** (*a*) $\{(2, b)\}$; (*b*) $\{(1, a),\ (3, a),\ (2, b),\ (3, b),\ (1, b)\}$; (*c*) $\{(2, a),\ (1, b)\}$; (*d*) Not defined

**3.43.** $2^8 = 256$

**3.44.** (*a*) $R = \{(3, 3),\ (6, 2),\ (9, 1)\}$
(*b*) (i) $\{3, 6, 9\}$, (ii) $\{1, 2, 3\}$, (iii) $R^{-1} = \{(3, 3),\ (2, 6),\ (1, 9)\}$
(*c*) $\{3, 3\}$

**3.45.** (*a*) $M_R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

(*b*) Domain $= \{1, 3\}$, range $= \{2, 3, 4\}$

(*c*) $R^{-1} = \{(3,1), (4,1), (2,3), (3,3), (4,3)\}$

(*d*) See Fig. 3-18(*a*)

(*e*) $R \circ R = \{(1,2), (1,3), (1,4), (3,2), (3,3), (3,4)\}$

**3.46.** (*a*) $E = \{1,2,5\}$, $F = \{3\}$, $G = \{2,4\}$, $H = \{3,5\}$

(*b*) $M_S = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$

(*c*) See Fig. 3-18(*b*)

(*d*) $S \circ S = \{(1,2), (1,4), (2,1), (2,2), (2,4), (3,2), (3,3), (3,5), (4,2), (5,2), (5,4)\}$

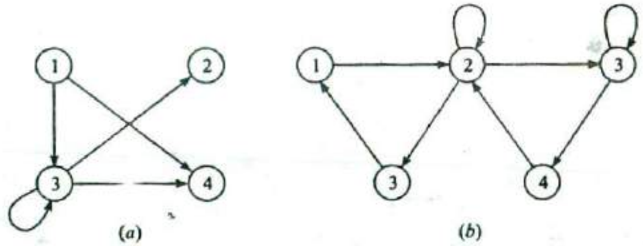


Fig. 3-18

**3.47.** (*a*) $E = \{b, c\}$, $F = \{a, b, d, e\}$, $G = \varnothing$, $H = \{a, b, f\}$

**3.48.** (*a*) None; (*b*) (2) and (3); (*c*) (1) and (4); (*d*) (1), (2), (4)

**3.49.** (*a*) $(3,3) \notin R$; (*b*) $(4,2) \in R$ but $(2,4) \notin R$; (*c*) $(2,3) \in R$, $(3,2) \in R$, but $2 \neq 3$;
(*d*) $(3,2) \in R$, $(2,3) \in R$, but $(3,3) \notin R$

**3.50.** (*a*) $R$; (*b*) $R$ and $S$; (*c*) $R$ and $T$; (*d*) $R$ and $T$

**3.51.** All true except: (*b*) $R = \{(1,1), (2,2), (3,3)\}$, so $(1,1) \notin R^c$; (*c*) and (*f*) $R = \{(2,2)\}$, so $(2,1), (1,2) \in R^c$, but $(2,2) \notin R^c$

**3.52.** (*a*) reflexive$(R) = \{(1,1), (2,2), (2,3), (4,2), (3,3), (4,4)\}$

(*b*) symmetric$(R) = \{(1,1), (2,2), (2,3), (4,2), (3,2), (2,4)\}$

(*c*) transitive$(R) = \{(1,1), (2,2), (2,3), (4,2), (4,3)\}$

**3.53.** (*a*) $A \times A$; (*b*) $\{(1,2), (1,3), (1,4), (3,3), (3,2), (3,4)\}$

**3.54.** (*a*) (i) $r+n$, (ii) $2r$
(*b*) $\{(1,2),\ (2,3), \ldots, (n-1,n),\ (n,1)\}$

**3.55.** (*a*) No; (*b*) no; (*c*) yes; (*d*) yes

**3.56.** There are five: $[S]$, $[\{1\},\ \{2,3\}]$, $[\{2\},\ \{1,3\}]$, $[\{3\},\ \{1,2\}]$, $[\{1\},\ \{2\},\ \{3\}]$.

**3.57.** (*a*) $\operatorname{Max}(r,s) \le n \le rs$. (*b*) Every cell in $P_1$ is a subset of a cell in $P_2$.
(*c*) $[\{1,3,5\},\ \{2\},\ \{4\},\ \{6,7,9\},\ \{8\}]$

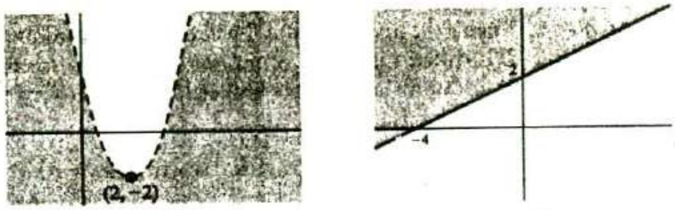
**3.58.** (*a*) $[\{1,8,15\},\ \{2,9,16\},\ \{3,10,17\},\ \{4,11,18\},\ \{5,12,19\},\ \{6,13,20\},\ \{7,14\}]$
(*b*) $\{8,2,10,4,12,6,14\}$

**3.59.** (*b*) $[(2,5)] = \{(1,4),\ (2,5),\ (3,6),\ (4,7),\ (5,8),\ (6,9)\}$

**3.60.** (*b*) If $a,b \in A$, then $b-a \notin A$. If $x \in R$, then $x = n + a$ where $n \in Z$ and $a \in A$.

**3.63.** (*a*) $\{(1,4,1),\ (1,9,2),\ (1,14,3),\ (2,2,2),\ (2,13,3)\}$;
(*b*) $\{(1,1,1,10),\ (1,1,2,15),\ (1,2,1,14),\ (2,1,1,13)\}$

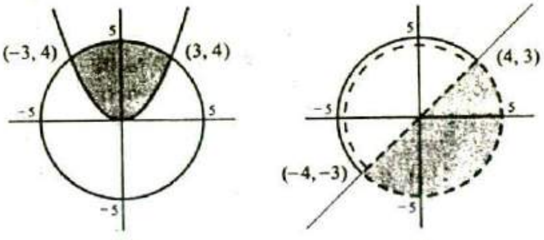
**3.64.** See Fig. 3-19.



(*a*) $y < x^2 - 4x + 2$ (*b*) $y \ge \frac{x}{2} + 2$

Fig. 3-19

**3.65.** (*a*) See Fig. 3-20(*a*); domain $= [-3,3]$, range $= [0,5]$
(*b*) See Fig. 3-20(*b*); domain $= (-4,5)$, range $= (-5,3)$.



(*a*) (*b*)

Fig. 3-20

# Chapter 4

# Functions

## 4.1 INTRODUCTION

One of the most important concepts in mathematics is that of a function. The terms "map", "mapping", "transformation", and many others mean the same thing; the choice of which word to use in a given situation is usually determined by tradition and the mathematical background of the person using the term.

## 4.2 FUNCTIONS

Suppose that to each element of a set $A$ we assign a unique element of a set $B$; the collection of such assignments is called a *function* from $A$ into $B$. The set $A$ is called the *domain* of the function, and the set $B$ is called the *target set*.

Functions are ordinarily denoted by symbols. For example, let $f$ denote a function from $A$ into $B$. Then we write

$$f: A \rightarrow B$$

which is read: "$f$ is a function from $A$ into $B$", or "$f$ takes $A$ into $B$", or "$f$ maps $A$ into $B$".

Suppose $f: A \rightarrow B$ and $a \in A$. Then $f(a)$ [read: "$f$ of $a$"] will denote the unique element of $B$ which $f$ assigns to $a$. This element $f(a)$ in $B$ is called the *image* of $a$ under $f$ or the *value* of $f$ at $a$. We also say that $f$ *sends* or *maps* $a$ into $f(a)$. The set of all such image values is called the *range* or *image* of $f$, and it is denoted by $\mathrm{Ran}(f)$, $\mathrm{Im}(f)$ or $f(A)$. That is,

$$\mathrm{Im}(f) = \{b \in B : \text{there exists } a \in A \text{ for which } f(a) = b\}$$

We emphasize that $\mathrm{Im}(f)$ is a subset of the target set $B$.

Frequently, a function can be expressed by means of a mathematical formula. For example, consider the function which sends each real number into its square. We may describe this function by writing

$$f(x) = x^2 \qquad \text{or} \qquad x \mapsto x^2 \qquad \text{or} \qquad y = x^2$$

In the first notation, $x$ is called a *variable* and the letter $f$ denotes the function. In the second notation, the barred arrow $\mapsto$ is read "goes into". In the last notation, $x$ is called the *independent variable* and $y$ is called the *dependent variable* since the value of $y$ will depend on the value of $x$.

Furthermore, suppose a function is given by a formula in terms of a variable $x$. Then we assume, unless otherwise stated, that the domain of the function is $\mathbf{R}$ or the largest subset of $\mathbf{R}$ for which the formula has meaning, and that the target set is $\mathbf{R}$.

**Remark**: Suppose $f: A \rightarrow B$. If $A'$ is a subset of $A$, then $f(A')$ denotes the set of images of elements in $A'$; and if $B'$ is a subset of $B$, then $f^{-1}(B')$ denotes the set of elements of $A$ each whose image belongs to $B'$. That is,

$$f(A') = \{f(a) : a \in A'\} \qquad \text{and} \qquad f^{-1}(B') = \{a \in A : f(a) \in B'\}$$

We call $f(A')$ the *image* of $A'$, and we call $f^{-1}(B')$ the *inverse image* or *preimage* of $B'$.

**EXAMPLE 4.1**

(*a*) Consider the function $f(x) = x^3$, i.e., $f$ assigns to each real number its cube. Then the image of 2 is 8, and so we may write $f(2) = 8$. Similarly, $f(-3) = -27$, and $f(0) = 0$.

(*b*) Let $g$ assign to each country in the world its capital city. Here the domain of $g$ is the set of all the countries in the world, and the target set is the list of cities in the world. The image of France under $g$ is Paris; that is $g(\text{France}) = \text{Paris}$. Similarly, $g(\text{Denmark}) = \text{Copenhagen}$ and $g(\text{England}) = \text{London}$.

(*c*) Figure 4-1 defines a function $f$ from $A = \{a, b, c, d\}$ into $B = \{r, s, t, u\}$ in the obvious way; that is,

$$f(a) = s, \qquad f(b) = u, \qquad f(c) = r, \qquad f(d) = s$$

The image of $f$ is the set $\{r, s, u\}$. Note that $t$ does not belong to the image of $f$ because $t$ is not the image of any element of $A$ under $f$.

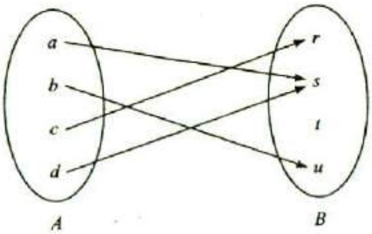


Fig. 4-1

### Identity Function

Consider any set $A$. Then there is a function from $A$ into $A$ which sends each element into itself. It is called the *identity function* on $A$ and it is usually denoted by $1_A$ or simply 1. In other words, the identity function $1_A : A \to A$ is defined by

$$1_A(a) = a$$

for every element $a \in A$.

### Functions as Relations

There is another point of view from which functions may be considered. First of all, every function $f: A \to B$ gvies rise to a relation from $A$ to $B$ called the *graph* of $f$ and defined by

$$\text{Graph of } f = \{(a, b) : a \in A, b = f(a)\}$$

Two functions $f: A \to B$ and $g: A \to B$ are defined to be equal, written $f = g$, if $f(a) = g(a)$ for every $a \in A$; that is, if they have the same graph. Accordingly, we do not distinguish between a function and its graph. Now, such a graph relation has the property that each $a$ in $A$ belongs to a unique ordered pair $(a, b)$ in the relation. On the other hand, any relation $f$ from $A$ to $B$ that has this property gives rise to a function $f: A \to B$, where $f(a) = b$ for each $(a, b)$ in $f$. Consequently, one may equivalently define a function as follows:

**Definition:** A function $f: A \to B$ is a relation from $A$ to $B$ (i.e., a subset of $A \times B$) such that each $a \in A$ belongs to a unique ordered pair $(a, b)$ in $f$.

Although we do not distinguish between a function and its graph, we will still use the terminology "graph of $f$" when referring to $f$ as a set of ordered pairs. Moreover, since the graph of $f$ is a relation, we can draw its picture as was done for relations in general, and this pictorial representation is itself sometimes called the graph of $f$. Also, the defining condition of a function, that each $a \in A$ belongs to a unique pair $(a, b)$ in $f$, is equivalent to the geometrical condition of each vertical line intersecting the graph in exactly one point.

**EXAMPLE 4.2**

(*a*) Let $f\colon A \to B$ be the function in Example 4.1(*c*). Then the graph of $f$ is the following set of ordered pairs:

$$f = \{(a,s),\ (b,u),\ (c,r),\ (d,s)\}$$

(*b*) Consider the following relations on the set $A = \{(1,2,3)\}$

$$f = \{(1,3),\ (2,3),\ (3,1)\}, \qquad g = \{(1,2),\ (3,1)\}, \qquad h = \{(1,3),\ (2,1),\ (1,2),\ (3,1)\}$$

$f$ is a function from $A$ into $A$ since each member of $A$ appears as the first coordinate in exactly one ordered pair in $f$; here $f(1) = 3$, $f(2) = 3$ and $f(3) = 1$. $g$ is not a function from $A$ into $A$ since $2 \in A$ is not the first coordinate of any pair in $g$ and so $g$ does not assign any image to 2. Also $h$ is not a function from $A$ into $A$ since $1 \in A$ appears as the first coordinate of two distinct ordered pairs in $h$, $(1,3)$ and $(1,2)$. If $h$ is to be a function it cannot assign both 3 and 2 to the element $1 \in A$.

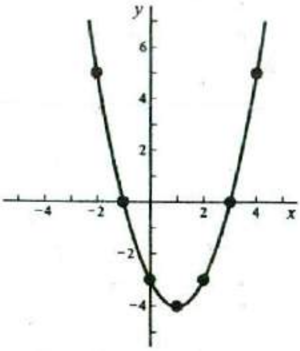
(*c*) By a *real polynomial function*, we mean a function $f : \mathbf{R} \to \mathbf{R}$ of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

where the $a_i$ are real numbers. Since **R** is an infinite set, it would be impossible to plot each point of the graph. However, the graph of such a function can be approximated by first plotting some of its points and then drawing a smooth curve through these points. The points are usually obtained from a table where various values are assigned to $x$ and the corresponding values of $f(x)$ computed.

Figure 4-2 illustrates this technique using the function $f(x) = x^2 - 2x - 3$.

| $x$ | $f(x)$ |
|---|---|
| −2 | 5 |
| −1 | 0 |
| 0 | −3 |
| 1 | −4 |
| 2 | −3 |
| 3 | 0 |
| 4 | 5 |



Graph of $f(x) = x^2 - 2x - 3$

Fig. 4-2

## 4.3 COMPOSITION OF FUNCTIONS

Consider functions $f\colon A \to B$ and $g\colon B \to C$, that is, where the target set $B$ of $f$ is the domain of $g$. This relationship can be pictured by the following diagram:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$$

Let $a \in A$; then its image $f(a)$ under $f$ is in $B$ which is the domain of $g$. Accordingly, we can find the image of $f(a)$ under the function $g$, that is, we can find $g(f(a))$. Thus we have a rule which assigns to each element $a$ in $A$ an element $g(f(a))$ in $C$ or, in other words, $f$ and $g$ give rise to a well defined function from $A$ to $C$. This new function is called the *composition* of $f$ and $g$, and it is denoted by

$$g \circ f$$

More briefly, if $f\colon A \to B$ and $g\colon B \to C$, then we define a new function $g \circ f\colon A \to C$ by

$$(g \circ f)(a) \equiv g(f(a))$$

Here $\equiv$ is used to mean equal by definition.

Note that we can now add the function $g \circ f$ to the above diagram of $f$ and $g$ as follows:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

We emphasize that the composition of $f$ and $g$ is written $g \circ f$, and not $f \circ g$; that is, the composition of functions is read from right to left, and not from left to right.

**EXAMPLE 4.3**

(*a*) Let $f\colon A \to B$ and $g\colon B \to C$ be the functions defined by Fig. 4-3. We compute $g \circ f : A \to C$ by its definition:

$$(g \circ f)(a) \equiv g(f(a)) = g(y) = t, \quad (g \circ f)(b) \equiv g(f(b)) = g(z) = r, \quad (g \circ f)(c) \equiv g(f(c)) = g(y) = t$$

Observe that the composition $g \circ f$ is equivalent to "following the arrows" from $A$ to $C$ in the diagrams of the functions $f$ and $g$.

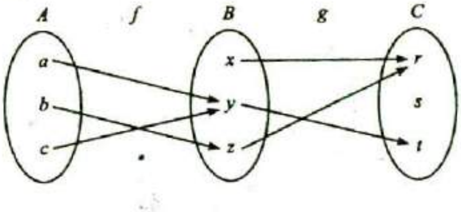


Fig. 4-3

(*b*) Let $f\colon \mathbf{R} \to \mathbf{R}$ and $g\colon \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$ and $g(x) = x + 3$. Then

$$(g \circ f)(2) \equiv g(f(2)) = g(4) = 7; \quad (f \circ g)(2) \equiv f(g(2)) = f(5) = 25$$

Thus the composition functions $g \circ f$ and $f \circ g$ are not the same function. We compute a general formula for these functions:

$$(g \circ f)(x) \equiv g(f(x)) = g(x^2) = x^2 + 3$$
$$(f \circ g)(x) \equiv f(g(x)) = f(x + 3) = (x + 3)^2 = x^2 + 6x + 9$$

(*c*) Consider any function $f : A \to B$. Then one can easily show that

$$f \circ 1_A = f \qquad \text{and} \qquad 1_B \circ f = f$$

where $1_A$ and $1_B$ are the identity functions on $A$ and $B$, respectively. In other words, the composition of any function with the appropriate identity function is the function itself.

### Associativity of Composition of Functions

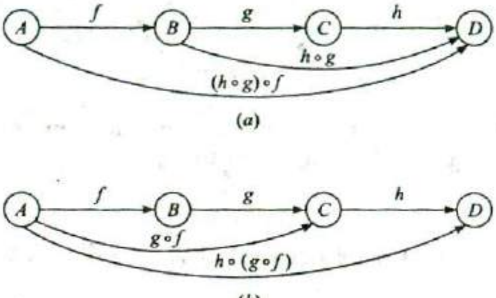
Consider functions $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$. Then, as pictured in Fig. 4-4(*a*), we can form the composition $g \circ f\colon A \to C$, and then the composition $h \circ (g \circ f)\colon A \to D$. Similarly, as pictured in Fig. 4-4(*b*), we can form the composition $h \circ g\colon B \to D$, and then the composition

$(h \circ g) \circ f\colon A \to D$. Both $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are functions with domain $A$ and target set $D$. The next theorem on functions (proved in Problem 4.15) states that these two functions are equal. That is:

**Theorem 4.1**: Let $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$. Then

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

Theorem 4.1 tells us that we can write $h \circ g \circ f\colon A \to D$ without any parentheses.



(a)

(b)

Fig. 4-4

**Remark**: The above definition of the composition of functions and Theorem 4.1 are not really new. Specifically, viewing the functions $f$ and $g$ as relations, then the composition function $g \circ f$ is the same as the composition of $f$ and $g$ as relations (Section 3.5) and Theorem 4.1 is the same as Theorem 3.1. One main difference is that here we use the functional notation $g \circ f$ for the composition of $f$ and $g$ instead of the notation $f \circ g$ which was used for relations.

## 4.4 ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

A function $f\colon A \to B$ is said to be *one-to-one* (written 1-1) if different elements in the domain $A$ have distinct images. Another way of saying the same thing follows:

$$\boxed{f \text{ is one-to-one if } f(a) = f(a') \text{ implies } a = a'}$$

A function $f\colon A \to B$ is said to be an *onto* function if every element of $B$ is the image of some element in $A$ or, in other words, if the image of $f$ is the entire target set $B$. In such a case we say that $f$ is a function of $A$ onto $B$ or that $f$ maps $A$ onto $B$. That is:

$$\boxed{f \text{ maps } A \text{ onto } B \text{ if } \forall b \in B,\ \exists a \in A \text{ such that } f(a) = b}$$

Here

$$\boxed{\forall \text{ means ``for every'', and } \exists \text{ means ``there exist''}}$$

(These quantifiers are discussed in Chapter 10.)

A function $f: A \to B$ is said to be *invertible* if its inverse relation $f^{-1}$ is a function from $B$ to $A$. Equivalently, $f: A \to B$ is *invertible* if there exists a function $f^{-1}: B \to A$, called the *inverse* of $f$, such that

$$f^{-1} \circ f = 1_A \qquad \text{and} \qquad f \circ f^{-1} = 1_B$$

In general, an inverse function $f^{-1}$ need not exist or, equivalently, the inverse relation $f^{-1}$ may not be a function. The following theorem (proved in Problem 4.23) gives simple criteria which tell us when it is.

**Theorem 4.2:** A function $f: A \to B$ is invertible if and only if $f$ is both one-to-one and onto.

If $f: A \to B$ is both one-to-one and onto, then $f$ is called a *one-to-one correspondence* between $A$ and $B$. This terminology comes from the fact that each element of $A$ will correspond to a unique element of $B$ and vice versa.

Some texts use the term *injective* for a one-to-one function, *surjective* for an onto function, and *bijective* for a one-to-one correspondence.

**EXAMPLE 4.4** Consider functions $f_1: A \to B$, $f_2: B \to C$, $f_3: C \to D$, and $f_4: D \to E$ defined by Fig. 4-5. Now $f_1$ is one-to-one since no element of $B$ is the image of more than one element of $A$. Similarly, $f_2$ is one-to-one. However, neither $f_3$ nor $f_4$ is one-to-one since $f_3(r) = f_3(u)$ and $f_4(v) = f_4(w)$.

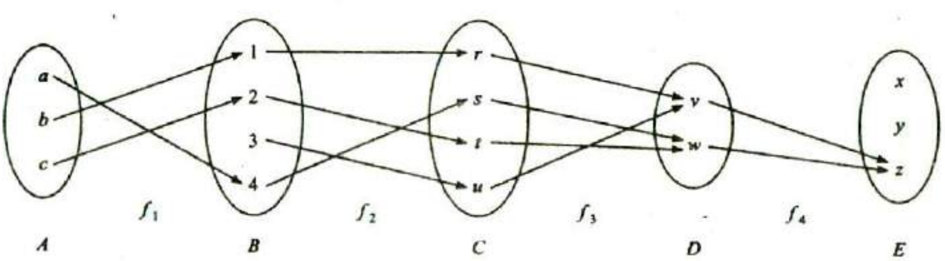


Fig. 4-5

As far as being onto is concerned, $f_2$ and $f_3$ are both onto functions since every element of $C$ is the image under $f_2$ of some element of $B$ and every element of $D$ is the image under $f_3$ of some element of $C$, i.e., $f_2(B) = C$ and $f_3(C) = D$. On the other hand, $f_1$ is not onto since $3 \in B$ but 3 is not the image under $f_1$ of any element of $A$, and $f_4$ is not onto since, for example, $x \in E$ but $x$ is not the image under $f_4$ of any element of $D$.

Thus $f_1$ is one-to-one but not onto, $f_3$ is onto but not one-to-one, and $f_4$ is neither one-to-one nor onto. However, $f_2$ is both one-to-one and onto, i.e., $f_2$ is a one-to-one correspondence between $A$ and $B$. Hence $f_2$ is invertible and $f_2^{-1}$ is a function from $C$ to $B$.

### Geometrical Characterization of One-to-One and Onto Functions

Consider now a real-valued function $f: \mathbf{R} \to \mathbf{R}$. Since $f$ may be identified with its graph and the graph may be plotted in the cartesian plane $\mathbf{R}^2$, we might wonder whether the concepts of being one-to-one and onto have some geometrical meaning. The answer is yes. Specifically:

(*a*) The function $f: \mathbf{R} \to \mathbf{R}$ is one-to-one means that there are no two distinct pairs $(a_1, b)$ and $(a_2, b)$ in the graph of $f$; hence each vertical line in $\mathbf{R}^2$ can intersect the graph of $f$ in at most one point.

(*b*) The function $f: \mathbf{R} \to \mathbf{R}$ is onto means that for every $b \in \mathbf{R}$ there is at least one point $a \in \mathbf{R}$ such that $(a, b)$ belongs to the graph of $f$; hence each vertical line in $\mathbf{R}^2$ must intersect the graph of $f$ at least once.

(*c*) Accordingly, the function $f: \mathbf{R} \to \mathbf{R}$ is one-to-one and onto, i.e., $f$ is invertible, if and only if each horizontal line in $\mathbf{R}^2$ will intersect the graph of $f$ in exactly one point.

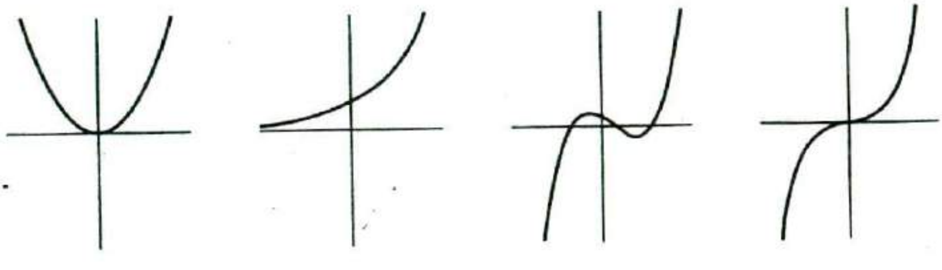
We illustrate the above properties in the next examp

**EXAMPLE 4.5** Consider the following four functions from **R** into **R** whose graphs appear in Fig. 4-6:

$$f_1(x) = x^2, \qquad f_2(x) = 2^x, \qquad f_3(x) = x^3 - 2x^2 - 5x + 6, \qquad f_4(x) = x^3$$

Observe that there are horizontal lines which intersect the graph of $f_1$ twice and there are horizontal lines which do not intersect the graph of $f_1$ at all; hence $f_1$ is neither one-to-one nor onto. Similarly, $f_2$ is one-to-one but not onto, $f_3$ is onto but not one-to-one, and $f_4$ is both one-to-one and onto. The inverse of $f_4$ is the cube root function, that is,

$$f_4^{-1}(x) = \sqrt[3]{x}$$



$f_1(x) = x^2$ $f_2(x) = 2^x$ $f_3(x) = x^3 - 2x^2 - 5x + 6$ $f_4(x) = x^3$

**Fig. 4-6**

**Remark**: Sometimes we restrict the domain and/or target set of a function $f$ in order to obtain an inverse function $f^{-1}$. For example, suppose we restrict the domain and target set of the function $f_1(x) = x^2$ to be the set $D$ of nonnegative real numbers. Then $f_1$ is one-to-one and onto and its inverse is the square root function, that is,

$$f_1^{-1}(x) = \sqrt{x}$$

Similarly, suppose we restrict the target set of the exponential function $f_2(x) = 2^x$ to be the set $\mathbf{R}^+$ of positive real numbers. Then $f_1$ is one-to-one and onto and its inverse is the logarithmic function (to the base 2), that is,

$$f_2^{-1}(x) = \log_2 x$$

(Exponential and logarithmic functions are investigated in Section 4.5.)

## 4.5 MATHEMATICAL FUNCTIONS, EXPONENTIAL AND LOGARITHMIC FUNCTIONS

This section presents various mathematical functions which appear often in mathematics and computer science, together with their notation. We also discuss the exponential and logarithmic functions, and their relationship.

### Integer and Absolute Value Functions

Let $x$ be any real number. The *integer value* of $x$, written $\mathrm{INT}(x)$, converts $x$ into an integer by deleting (truncating) the fractional part of the number. Thus

$$\mathrm{INT}(3.14) = 3, \qquad \mathrm{INT}(\sqrt{5}) = 2, \qquad \mathrm{INT}(-8.5) = -8, \qquad \mathrm{INT}(7) = 7$$

The *absolute value* of the real number $x$, written $\mathrm{ABS}(x)$ or $|x|$, is defined as the greater of $x$ or $-x$. Hence $\mathrm{ABS}(0) = 0$, and, for $x \neq 0$, $\mathrm{ABS}(x) = x$ or $\mathrm{ABS}(x) = -x$, depending on whether $x$ is positive or negative. Thus

$$|-15| = 15, \qquad |7| = 7, \qquad |-3.33| = 3.33, \qquad |4.44| = 4.44, \qquad |-0.975| = 0.075$$

We note that $|x| = |-x|$ and, for $x \neq 0$, $|x|$ is positive.

### Remainder Function; Modular Arithmetic

Let $k$ be any integer and let $M$ be a positive integer. Then

$$k \,(\text{mod } M)$$

(read *$k$ modulo $M$*) will denote the integer remainder when $k$ is divided by $M$. More exactly, $k$ (mod $M$) is the unique integer $r$ such that

$$k = Mq + r \qquad \text{where} \qquad 0 \le r < M$$

When $k$ is positive, simply divide $k$ by $M$ to obtain the remainder $r$. Thus

$$25 \,(\text{mod } 7) = 4, \qquad 25 \,(\text{mod } 5) = 0, \qquad 35 \,(\text{mod } 11) = 2, \qquad 3 \,(\text{mod } 8) = 3$$

Problem 4.25 shows a method to obtain $k$ (mod $M$) when $k$ is negative.

The term "mod" is also used for the mathematical congruence relation, which is denoted and defined as follows:

$$a \equiv b \,(\text{mod } M) \qquad \text{if and only if} \qquad M \text{ divides } b - a$$

$M$ is called the *modulus*, and $a \equiv b$ (mod $M$) is read "$a$ is congruent to $b$ modulo $M$". The following aspects of the congruence relation are frequently useful:

$$0 \equiv M \,(\text{mod } M) \qquad \text{and} \qquad a \pm M \equiv a \,(\text{mod } M)$$

*Arithmetic modulo $M$* refers to the arithmetic operations of addition, multiplication, and subtraction where the arithmetic value is replaced by its equivalent value in the set

$$\{0, 1, 2, \ldots, M - 1\}$$

or in the set

$$\{1, 2, 3, \ldots, M\}$$

For example, in arithmetic modulo 12, sometimes called "clock" arithmetic,

$$6 + 9 \equiv 3, \qquad 7 \times 5 \equiv 11, \qquad 1 - 5 \equiv 8, \qquad 2 + 10 \equiv 0 \equiv 12$$

(The use of 0 or $M$ depends on the application.)

### Exponential Functions

Recall the following definitions for integer exponents (where $m$ is a positive integer):

$$a^m = a \cdot a \ldots a \,(m \text{ times}), \qquad a^0 = 1, \qquad a^{-m} = \frac{1}{a^m}$$

Exponents are extended to include all rational numbers by defining, for any rational number $m/n$,

$$a^{m/n} = \sqrt[n]{a^m} = \left(\sqrt[n]{a}\right)^m$$

For example,

$$2^4 = 16, \qquad 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \qquad 125^{2/3} = 5^2 = 25$$

In fact, exponents are extended to include all real numbers by defining, for any real number $x$,

$$a^x = \lim_{r \to x} a^r \qquad \text{where } r \text{ is a rational number}$$

Accordingly, the exponential function $f(x) = a^x$ is defined for all real numbers.

### Logarithmic Functions

Logarithms are related to exponents as follows. Let $b$ be a positive number. The logarithm of any positive number $x$ to the base $b$, written

$$\log_b x$$

represents the exponent to which $b$ must be raised to obtain $x$. That is,

$$y = \log_b x \quad \text{and} \quad b^y = x$$

are equivalent statements. Accordingly,

$$\log_2 8 = 3 \quad \text{since} \quad 2^3 = 8; \quad \log_{10} 100 = 2 \quad \text{since} \quad 10^2 = 100$$
$$\log_2 64 = 6 \quad \text{since} \quad 2^6 = 64; \quad \log_{10} 0.001 = -3 \quad \text{since} \quad 10^{-3} = 0.001$$

Furthermore, for any base $b$,

$$\log_b 1 = 0 \quad \text{since} \quad b^0 = 1$$
$$\log_b b = 1 \quad \text{since} \quad b^1 = b$$

The logarithm of a negative number and the logarithm of 0 are not defined.

Frequently, logarithms are expressed using approximate values. For example, using tables or calculators, one obtains

$$\log_{10} 300 = 2.4771 \quad \text{and} \quad \log_e 40 = 3.6889$$

as approximate answers. (Here $e = 2.718\,281 \cdots$.)

Three classes of logarithms are of special importance: logarithms to base 10, called *common logarithms*; logarithms to base $e$, called *natural logarithms*; and logarithms to base 2, called *binary logarithms*. Some texts write:

$$\ln x \text{ for } \log_e x \quad \text{and} \quad \lg x \text{ or } \log x \text{ for } \log_2 x$$

The term $\log x$, by itself, usually means $\log_{10} x$; but it is also used for $\log_e x$ in advanced mathematical texts and for $\log_2 x$ in computer science texts.

### Relationship between the Exponential and Logarithmic Functions

The basic relationship between the exponential and the logarithmic functions

$$f(x) = b^x \quad \text{and} \quad g(x) = \log_b x$$

is that they are inverses of each other; hence the graphs of these functions are related geometrically. This relationship is illustrated in Fig. 4-7 where the graphs of the exponential function $f(x) = 2^x$, the logarithmic function $g(x) = \log_2 x$, and the linear function $h(x) = x$ appear on the same coordinate axis. Since $f(x) = 2^x$ and $g(x) = \log_2 x$ are inverse functions, they are symmetric with respect to the linear function $h(x) = x$ or, in other words, the line $y = x$.

Figure 4-7 also indicates another important property of the exponential and logarithmic functions. Specifically, for any positive $c$, we have

$$g(c) < h(c) < f(c)$$

In fact, as $c$ increases in value, the vertical distances $h(c) - g(c)$ and $f(c) - g(c)$ increase in value. Moreover, the logarithmic function $g(x)$ grows very slowly compared with the linear function $h(x)$, and the exponential function $f(x)$ grows very quickly compared with $h(x)$.

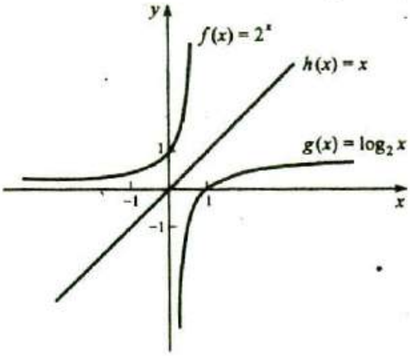


Fig. 4-7

## 4.6 RECURSIVELY DEFINED FUNCTIONS

A function is said to be *recursively defined* if the function definition refers to itself. In order for the definition not to be circular, the function definition must have the following two properties:

(1) There must be certain arguments, called *base values*, for which the function does not refer to itself.

(2) Each time the function does refer to itself, the argument of the function must be closer to a base value.

A recursive function with these two properties is said to be *well-defined.*

The following examples should help clarify these ideas.

### Factorial Function

The product of the positive integers from 1 to $n$, inclusive, is called "$n$ factorial" and is usually denoted by $n!$:

$$n! = 1 \cdot 2 \cdot 3 \ldots (n-2)(n-1)n$$

It is also convenient to define $0! = 1$, so that the function is defined for all nonnegative integers. Thus we have

$$0! = 1, \quad 1! = 1, \quad 2! = 1 \cdot 2 = 2, \quad 3! = 1 \cdot 2 \cdot 3 = 6, \quad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24,$$
$$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120, \quad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$$

and so on. Observe that

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \quad \text{and} \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

This is true for every positive integer $n$; that is,

$$n! = n \cdot (-1)!$$

Accordingly, the factorial function may also be defined as follows:

**Definition 4.1: (Factorial Function)**

(*a*) If $n = 0$, then $n! = 1$.

(*b*) If $n > 0$, then $n! = n \cdot (n-1)!$

Observe that the above definition of $n!$ is recursive, since it refers to itself when it uses $(n-1)!$ However:

(1) The value of $n!$ is explicitly given when $n = 0$ (thus 0 is a base value).
(2) The value of $n!$ for arbitrary $n$ is defined in terms of a smaller value of $n$ which is closer to the base value 0.

Accordingly, the definition is not circular, or, in other words, the function is well-defined.

### Fibonacci Sequence

The celebrated Fibonacci sequence (usually denoted by $F_0, F_1, F_2, \ldots$) is as follows:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

That is, $F_0 = 0$ and $F_1 = 1$ and each succeeding term is the sum of the two preceding terms. For example, the next two terms of the sequence are

$$34 + 55 = 89 \qquad \text{and} \qquad 55 + 89 = 144$$

A formal definition of this function follows:

**Definition 4.2: (Fibonacci Sequence)**
(*a*) If $n = 0$ or $n = 1$, then $F_n = n$.
(*b*) If $n > 1$, then $F_n = F_{n-2} + F_{n-1}$.

This is another example of a recursive definition, since the definition refers to itself when it uses $F_{n-2}$ and $F_{n-1}$. However:

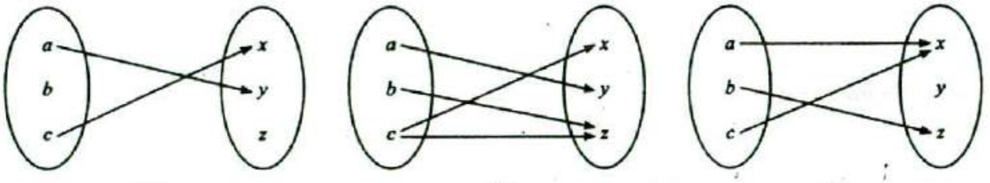
(1) The base values are 0 and 1.
(2) The value of $F_n$ is defined in terms of smaller values of $n$ which are closer to the base values.

Accordingly, this function is well-defined.

## Solved Problems

### FUNCTIONS

**4.1.** State whether or not each diagram in Fig. 4-8 defines a function from $A = \{a, b, c\}$ into $B = \{x, y, z\}$.



(*a*) (*b*) (*c*)

**Fig. 4-8**

(*a*) No. There is nothing assigned to the element $b \in A$.

(*b*) No. Two elements, $x$ and $z$, are assigned to $c \in A$.

(*c*) Yes. Every element in the domain $A = \{a, b, c\}$ is assigned a unique element in the target set $B$.

**4.2.** Let $X = \{1, 2, 3, 4\}$. Determine whether or not each relation below is a function from $X$ into $X$.

(*a*) $f = \{(2,3),\ (1,4),\ (2,1),\ (3,2),\ (4,4)\}$

(*b*) $g = \{(3,1),\ (4,2),\ (1,1)\}$

(*c*) $h = \{(2,1),\ (3,4),\ (1,4),\ (2,1),\ (4,4)\}$

Recall that a subset $f$ of $X \times X$ is a function $f: X \to X$ if and only if each $a \in X$ appears as the first coordinate in exactly one ordered pair in $f$.

(*a*) No. Two different ordered pairs $(2,3)$ and $(2,1)$ in $f$ have the same number 2 as their first coordinate.

(*b*) No. The element $2 \in X$ does not appear as the first coordinate in any ordered pair in $g$.

(*c*) Yes. Although $2 \in X$ appears as the first coordinate in two ordered pairs in $h$, these two ordered pairs are equal.

**4.3.** Let $A$ be the set of students in a school. Determine which of the following assignments defines a function on $A$:

(*a*) To each student assign his age.

(*b*) To each student assign his teacher.

(*c*) To each student assign his sex.

(*d*) To each student assign his spouse.

A collection of assignments is a function on $A$ if and only if each element $a$ in $A$ is assigned exactly one element. Thus:

(*a*) Yes, because each student has one and only one age.

(*b*) Yes, if each student has only one teacher; no, if any student has more than one teacher.

(*c*) Yes.

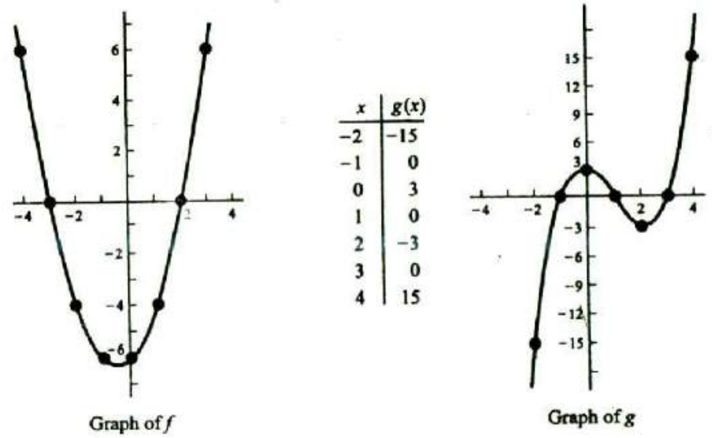
(*d*) No, unless every student is married.

**4.4.** Sketch the graph of: (*a*) $f(x) = x^2 + x - 6$; (*b*) $g(x) = x^3 - 3x^2 - x + 3$.

Set up a table of values for $x$ and then find the corresponding values of the function. Since the functions are polynomials, plot the points in a coordinate diagram and then draw a smooth continuous curve through the points. See Fig. 4-9.

| $x$ | $f(x)$ |
|---|---|
| $-4$ | 6 |
| $-3$ | 0 |
| $-2$ | $-4$ |
| $-1$ | $-6$ |
| 0 | $-6$ |
| 1 | $-4$ |
| 2 | 0 |
| 3 | 6 |

| $x$ | $g(x)$ |
|---|---|
| $-2$ | $-15$ |
| $-1$ | 0 |
| 0 | 3 |
| 1 | 0 |
| 2 | $-3$ |
| 3 | 0 |
| 4 | 15 |



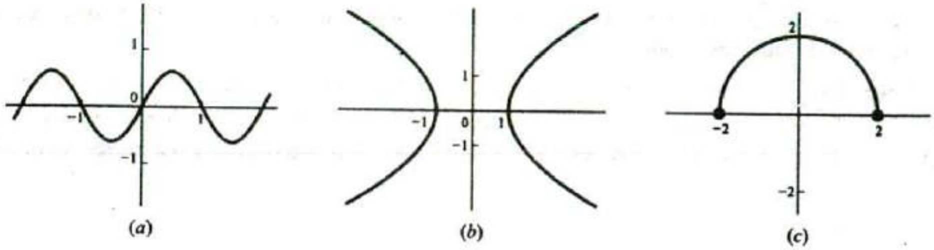
Graph of $f$

Graph of $g$

Fig. 4-9

**4.5.** Determine which of the graphs in Fig. 4-10 are functions from **R** into **R**.

Geometrically speaking, a set of points in the plane $\mathbf{R}^2$ is a function if and only if every vertical line contains exactly one point of the set. Thus: (*a*) Yes. (*b*) No. (*c*) No; however the graph does define a function from $D$ into $\mathbf{R}$ where $D = [-2, 2] = \{x : -2 \le x \le 2\}$.



(*a*) (*b*) (*c*)

**Fig. 4-10**

**4.6.** Let the function $f : \mathbf{R} \to \mathbf{R}$ be defined as follows:

$$f(x) = \begin{cases} 3x - 1 & \text{if } x > 3 \\ x^2 - 2 & \text{if } -2 \le x \le 3 \\ 2x + 3 & \text{if } x < -2 \end{cases}$$

Find: (*a*) $f(2)$, (*b*) $f(4)$, (*c*) $f(-1)$, (*d*) $f(-3)$

Note that there are three formulas used to define the single function $f$. (The reader should not confuse formulas and functions.)

(*a*) Since 2 belongs to the closed interval $[-2, 3]$, we use the formula $f(x) = x^2 - 2$. Hence

$$f(2) = 2^2 - 2 = 4 - 2 = 2$$

(*b*) Since 4 belongs to $(3, \infty)$, we use the formula $f(x) = 3x - 1$. Thus $f(4) = 3(4) - 1 = 12 - 1 = 11$.

(*c*) Since $-1$ is in the interval $[-2, 3]$, we use the formula $f(x) = x^2 - 2$. Computing,

$$f(-1) = (-1)^2 - 2 = 1 - 2 = -1$$

(*d*) Since $-3$ is less than $-2$, i.e., $-3$ belongs to $(-\infty, -2)$, we use the formula $f(x) = 2x + 3$. Thus

$$f(-3) = 2(-3) + 3 = -6 + 3 = -3$$

**4.7.** Find the domain $D$ of each of the following real-valued functions:

(*a*) $f(x) = 1/(x - 2)$; (*b*) $g(x) = x^2 - 3x - 4$; (*c*) $h(x) = \sqrt{25 - x^2}$.

(*a*) $f$ is not defined for $x - 2 = 0$ or $x = 2$; hence $D = \mathbf{R}\backslash\{2\}$.

(*b*) $g$ is defined for every real number; hence $D = \mathbf{R}$.

(*c*) $h$ is not defined when $25 - x^2$ is negative; hence $D = [-5, 5] = \{x : -5 \le x \le 5\}$.

**4.8.** Let $A = \{1, 2, 3, 4, 5\}$ and let $f : A \to A$ be defined by the diagram in Fig. 4-11.

(*a*) Find the graph of $f$, i.e., write $f$ as a set of ordered pairs.

(*b*) Find $f(A)$, the image of $f$.

(*c*) Find $f(S)$ where $S = \{1, 3, 5\}$.

(*d*) Find $f^{-1}(T)$ where $T = \{2, 3\}$.

(*a*) The graph of $f$ consists of all pairs $(a, f(a))$ where $a \in A$. Hence

$$f = \{(1,3),\ (2,5),\ (3,5),\ (4,2),\ (5,3)\}$$

(*b*) $f(A)$ consists of all image points. Since only 2, 3, 5 appear as image points, $f(A) = \{2,3,5\}$.

(*c*) $f(S) = f(\{1,3,5\}) = \{f(1), f(3), f(5)\} = \{3,5,3\} = \{3,5\}$.

(*d*) The element 4 has image 2, and the elements 1 and 5 have image 3; hence $f^{-1}(T) = f^{-1}(\{2,3\}) = \{1,4,5\}$.

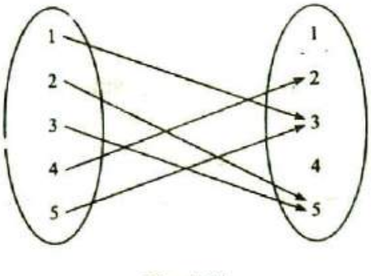


**Fig. 4-11**

**4.9.** Suppose $A = \{a, b\}$ and $B = \{1,2,3\}$. Find the number $m$ of functions:

(*a*) from $A$ into $B$, (*b*) from $B$ into $A$.

(*a*) There are three choices, 1, 2, or 3 for the image of $a$, and three choices for the image of $b$. Hence there are $m = 3 \cdot 3 = 9$ functions from $A$ into $B$.

(*b*) There are two choices, $a$ or $b$, for each of the three elements of $B$. Hence there are $m = 2 \cdot 2 \cdot 2 = 2^3 = 8$ functions from $B$ into $A$.

**4.10.** Suppose $A$ and $B$ are finite sets with $|A|$ elements and $|B|$ elements, respectively. Show there are $|B|^{|A|}$ functions from $A$ into $B$. (For this reason, one sometimes writes $B^A$ for the collection of all functions from $A$ into $B$.)

There are $|B|$ choices for each of the $|A|$ elements of $A$; hence there are $|B|^{|A|}$ possible functions from $A$ into $B$.

## COMPOSITION OF FUNCTIONS

**4.11.** Let the functions $f\colon A \to B$ and $g\colon B \to C$ be defined by Fig. 4-12. Find the composition function $g \circ f\colon A \to C$.

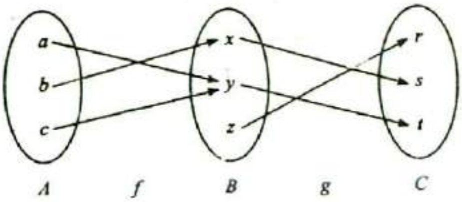


**Fig. 4-12**

Use the definition of the composition function to compute:

$$(g \circ f)(a) = g(f(a)) = g(y) = t, \quad (g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

Note that we arrive at the same answer if we "follow the arrows" in the diagram:

$$a \to y \to t, \qquad b \to x \to s, \qquad c \to y \to t$$

**4.12.** Let the functions $f$ and $g$ be defined by $f(x) = 2x + 1$ and $g(x) = x^2 - 2$. Find the formula defining the composition functions: (*a*) $g \circ f$, (*b*) $f \circ g$.

(*a*) Compute $g \circ f$ as follows:

$$(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1.$$

Observe that the same answer can be found by writing

$$y = f(x) = 2x + 1 \qquad \text{and} \qquad z = g(y) = y^2 - 2$$

and then eliminating $y$ from both equations:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

(*b*) Compute $f \circ g$ as follows:

$$(f \circ g)(x) = f(g(x)) = f(x^2 - 2) = 2(x^2 - 2) + 1 = 2x^2 - 3$$

**4.13.** Let $f\colon A \to B$. When is $f \circ f$ defined?

The composition $f \circ f$ is defined when the domain of $f$ is the same as the target set of $f$; that is, when $A = B$.

**4.14.** Let $f\colon \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2 + 2x$.

(*a*) Find $(f \circ f)$ (2) and $(f \circ f)$ (3). (*b*) Find a formula for $f \circ f$.

(*a*) $(f \circ f)\ (2) = f(f(2)) = f(8) = (8)^2 + 16 = 80$

$(f \circ f)\ (3) = f(f(3)) = f(15) = (15)^2 + 30 = 255$

(*b*)
$$\begin{aligned}(f \circ f)\ (x) &= f(f(x)) = f(x^2 + 2x) = (x^2 + 2x)^2 + 2(x^2 + 2x)\\ &= x^4 + 4x^3 + 4x^2 + 2x^2 + 4x\\ &= x^4 + 4x^3 + 6x^2 + 4x\end{aligned}$$

**4.15.** Prove Theorem 4.1: Let $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$. Then $(f \circ g) \circ h = f \circ (g \circ h)$.

Consider any element $a \in A$. Then:

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) \qquad \text{and} \qquad ((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

Thus $(h \circ (g \circ f))(a) = ((h \circ g) \circ f)(a)$ for every $a \in A$, and so $h \circ (g \circ f) = (h \circ g) \circ f$.

## ONE-TO-ONE, ONTO, AND INVERTIBLE FUNCTIONS

**4.16.** Suppose $f\colon A \to B$. Determine conditions under which:

(*a*) $f$ is not one-to-one (injective); (*b*) $f$ is not onto (surjective).

(*a*) $f$ is not one-to-one if there exist $a, a' \in A$ for which $f(a) = f(a')$ but $a \neq a'$.

(*b*) $f$ is not onto if there exists $b \in B$ such that $f(x) \neq b$ for every $x \in A$.

**4.17.** Determine if each function is one-to-one.

(*a*) To each person on the earth assign the number which corresponds to his age.

(*b*) To each country in the world assign the latitude and longitude of its capital.

(*c*) To each book written by only one author assign the author.

(*d*) To each country in the world which has a prime minister assign its prime minister.

(*a*) No. Many people in the world have the same age.

(*b*) Yes.

(*c*) No. There are different books with the same author.

(*d*) Yes. Different countries in the world have different prime ministers.

**4.18.** Let the functions $f: A \to B$, $g: B \to C$, and $h: C \to D$ be defined by Fig. 4-13.

(*a*) Determine if each function is one-to-one.

(*b*) Determine if each function is onto.

(*c*) Determine if each function is invertible.

(*d*) Find the composition $h \circ g \circ f$.

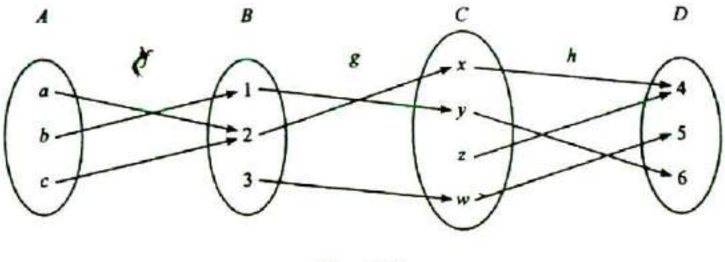


**Fig. 4-13**

(*a*) $f$ is not one-to-one since $f(a) = f(c)$ but $a \neq c$. $h$ is not one-to-one since $h(x) = h(z)$ but $x \neq z$. $g$ is one-to-one, the elements $1, 2, 3 \in B$ have distinct images.

(*b*) $f: A \to B$ is not onto since $3 \in B$ is not the image of any element in $A$.

$g: B \to C$ is not onto since $z \in C$ is not the image of any element in $B$.

$h: C \to D$ is onto since each element in $D$ is the image of some element of $C$.

(*c*) None of the functions are both one-to-one and onto; hence none of the functions are invertible.

(*d*) Now $a \to 2 \to x \to 4$, $b \to 1 \to y \to 6$, $c \to 2 \to x \to 4$. Hence $h \circ g \circ f = \{(a, 4),\ (b, 6),\ (c, 4)\}$.

**4.19.** Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x - 3$. Now $f$ is one-to-one and onto; hence $f$ has an inverse function $f^{-1}$. Find a formula for $f^{-1}$.

Let $y$ be the image of $x$ under the function $f$; that is, set

$$y = f(x) = 2x - 3 \tag{1}$$

Consequently, $x$ will be the image of $y$ under the inverse function $f^{-1}$.

**Method 1:** Solve for $x$ in terms of $y$ in equation (*1*) obtaining

$$x = (y + 3)/2$$

Then $f^{-1}(y) = (y + 3)/2$. Replace $y$ by $x$ to obtain

$$f^{-1}(x) = (x + 3)/2$$

which is the formula for $f^{-1}$ using the usual independent variable $x$.

**Method 2:** First interchange $x$ and $y$ in (*1*) obtaining

$$x = 2y - 3$$

Then solve for $y$ in terms of $x$ to obtain

$$y = (x + 3)/2 \qquad \text{and so} \qquad f^{-1}(x) = (x + 3)/2$$

**4.20.** Find a formula for the inverse of $g(x) = \dfrac{2x - 3}{5x - 7}$.

Set $y = g(x)$ and then interchange $x$ and $y$ as follows:

$$y = \frac{2x - 3}{5x - 7} \qquad \text{and then} \qquad x = \frac{2y - 3}{5y - 7}$$

Now solve for $y$ in terms of $x$:

$$5xy - 7x = 2y - 3 \qquad \text{or} \qquad 5xy - 2y = 7x - 3 \qquad \text{or} \qquad (5x - 2)y = 7x - 3$$

Thus

$$y = \frac{7x - 3}{5x - 2} \qquad \text{and so} \qquad g^{-1}(x) = \frac{7x - 3}{5x - 2}$$

(Here the domain of $g^{-1}$ excludes $x = 2/5$.)

**4.21.** Consider functions $f: A \to B$ and $g: B \to C$. Prove the following:

(*a*) If $f$ and $g$ are one-to-one, then the composition function $g \circ f$ is one-to-one.

(*b*) If $f$ and $g$ are onto functions, then $g \circ f$ is an onto function.

(*a*) Suppose $(g \circ f)(x) = (g \circ f)(y)$; then $g(f(x)) = g(f(y))$. Hence $f(x) = f(y)$ because $g$ is one-to-one. Furthermore, $x = y$ since $f$ is one-to-one. Accordingly, $g \circ f$ is one-to-one.

(*b*) Let $c$ be any arbitrary element of $C$. Since $g$ is onto, there exists a $b \in B$ such that $g(b) = c$. Since $f$ is onto, there exists an $a \in A$ such that $f(a) = b$. But then

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

Hence each $c \in C$ is the image of some element $a \in A$. Accordingly, $g \circ f$ is an onto function.

**4.22.** Consider functions $f: A \to B$ and $g: B \to C$. Prove the following:

(*a*) If $g \circ f$ is one-to-one, then $f$ is one-to-one.

(*b*) If $g \circ f$ is onto, then $g$ is onto.

(*a*) Suppose $f$ is not one-to-one. Then there exist distinct elements $x, y \in A$ for which $f(x) = f(y)$. Thus $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$; hence $g \circ f$ is not one-to-one. Therefore, if $g \circ f$ is one-to-one, t[illegible] must be one-to-one.

(*b*) If $c$ [illegible] then $(g \circ f)(a) = g(f(a)) \in g(B)$; hence $(g \circ f)(A) \subseteq g(B)$. Suppose $g$ is not onto. Then $g(B)$ [illegible] contained in $C$ and so $(g \circ f)(A)$ is properly contained in $C$; thus $g \circ f$ is not onto. Accordingly, if $g \circ f$ is onto, then $g$ must be onto.

**4.23.** Prove Theorem 4.2: A function $f: A \to B$ is invertible if and only if $f$ is bijective (one-to-one and onto).

Suppose $f$ has an inverse, i.e., there exists a function $f^{-1}: B \to A$ for which $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$. Since $1_A$ is one-to-one, $f$ is one-to-one by Problem 4.22; and since $1_B$ is onto, $f$ is onto by Problem 4.22. That is, $f$ is both one-to-one and onto.

Now suppose $f$ is both one-to-one and onto. Then each $b \in B$ is the image of a unique element in $A$, say $\hat{b}$. Thus if $f(a) = b$, then $a = \hat{b}$; hence $f(\hat{b}) = b$. Now let $g$ denote the mapping from $B$ to $A$ defined by $g(b) = \hat{b}$. We have:

(i) $(g \circ f)(a) = g(f(a)) = g(b) = \hat{b} = a$, for every $a \in A$; hence $g \circ f = 1_A$.

(ii) $(f \circ g)(b) = f(g(b)) = f(\hat{b}) = b$, for every $b \in B$; hence $f \circ g = 1_B$.

Accordingly, $f$ has an inverse. Its inverse is the mapping $g$.

## SPECIAL MATHEMATICAL FUNCTIONS, RECURSIVELY DEFINED FUNCTIONS

**4.24.** Find: (*a*) $\lfloor 7.5 \rfloor, \lfloor -7.5 \rfloor, \lfloor -18 \rfloor$, where $\lfloor x \rfloor$, called the *floor* of $x$, denotes the greatest integer that does not exceed $x$; (*b*) $\lceil 7.5 \rceil, \lceil -7.5 \rceil, \lceil -18 \rceil$, where $\lceil x \rceil$, called the *ceiling* of $x$, denotes the least integer that does not exceed $x$.

(*a*) $\lfloor 7.5 \rfloor = 7, \lfloor -7.5 \rfloor = -8, \lfloor -18 \rfloor = -18$.

(*b*) $\lceil 7.5 \rceil = 8, \lceil -7.5 \rceil = -7, \lceil -18 \rceil = -18$.

**4.25.** Find: (*a*) 26 (mod 7), 25 (mod 5), 35 (mod 11);
(*b*) −26 (mod 7), −371 (mod 8), −2345 (mod 6).

(*a*) When $k$ is positive, divide $k$ by the modulus $M$ to obtain the remainder $r$. Then $k \pmod{M} = r$. Thus:

$$26 \pmod{7} = 5, \qquad 25 \pmod{5} = 0, \qquad 35 \pmod{11} = 2$$

(*b*) When $k$ is negative, divide $|k|$ by the modulus $M$ to obtain the remainder $r'$. Then, when $r' \neq 0$, $k \pmod{M} = M - r'$. Thus:

$$-26 \pmod{7} = 7 - 5 = 2, \qquad -371 \pmod{8} = 8 - 3 = 5, \qquad -2345 \pmod{6} = 6 - 5 = 1$$

**4.26.** Using arithmetic modulo $M = 15$, evaluate: (*a*) $9 + 13$, (*b*) $7 + 11$, (*c*) $4 - 9$, (*d*) $2 - 10$.

Use $a \pm M \equiv a \pmod{M}$:

(*a*) $9 + 13 = 22 \equiv 22 - 15 = 7$

(*b*) $7 + 11 = 18 \equiv 18 - 15 = 3$

(*c*) $4 - 9 = -5 \equiv -5 + 15 = 10$

(*d*) $2 - 10 = -8 \equiv -8 + 15 = 7$

**4.27.** Evaluate: (*a*) $\log_2 8$; (*b*) $\log_2 64$; (*c*) $\log_{10} 100$; (*d*) $\log_{10} 0.001$.

(*a*) $\log_2 8 = 3$ since $2^3 = 8$

(*b*) $\log_2 64 = 6$ since $2^6 = 64$

(*c*) $\log_{10} 100 = 2$ since $10^2 = 100$

(*d*) $\log_{10} 0.001 = -3$ since $10^{-3} = 0.001$

**4.28.** Show that: (*a*) $\log_b AB = \log_b A + \log_b B$; (*b*) $\log_b A^n = n \log_b A$.

Let $\log_b A = x$ and $\log_b B = y$. Then $A = b^x$ and $B = b^y$.

(*a*) We have $AB = b^x b^y = b^{x+y}$. Hence

$$\log_b AB = x + y = \log_b A + \log_b B$$

(*b*) We have $A^n = (b^x)^n = b^{nx}$. Hence

$$\log_b A^n = nx = n \log_b A$$

**4.29.** Evaluate: (*a*) $2^5$, (*b*) $3^{-4}$, (*c*) $8^{2/3}$, (*d*) $25^{-3/2}$.

(*a*) $2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$

(*b*) $3^{-4} = \dfrac{1}{3^4} = \dfrac{1}{81}$

(*c*) $8^{2/3} = (\sqrt[3]{8})^2 = 2^2 = 4$

(*d*) $25^{-3/2} = \dfrac{1}{25^{3/2}} = \dfrac{1}{(\sqrt{25})^3} = \dfrac{1}{5^3} = \dfrac{1}{125}$

**4.30.** Let $n$ denote a positive integer. Suppose a function $L$ is defined recursively as follows:

$$L(n) = \begin{cases} 0 & \text{if } n = 1 \\ L(\lfloor n/2 \rfloor) + 1 & \text{if } n > 1 \end{cases}$$

Find $L(25)$ and describe what this function does. (The *floor* function $\lfloor x \rfloor$ is defined in the above Problem 4.24.)

Find $L(25)$ recursively as follows:

$$\begin{aligned} L(25) &= L(12) + 1 \\ &= [L(6) + 1] + 1 = L(6) + 2 \\ &= [L(3) + 1] + 2 = L(3) + 3 \\ &= [L(1) + 1] + 3 = L(1) + 4 \\ &= 0 + 4 = 4 \end{aligned}$$

Each time $n$ is divided by 2, the value of $L$ is increased by 1. Hence $L$ is the greatest integer such that

$$2^L \leq n$$

Accordingly, $L(n) = \lfloor \log_2 n \rfloor$

## Supplementary Problems

### FUNCTIONS

**4.31.** Define each of the following functions from **R** into **R** by a formula:

(*a*) To each number let $f$ assign its square plus 3.

(*b*) To each number let $g$ assign its cube plus twice the number.

(*c*) To each number greater than or equal to 3 let $h$ assign the number squared; and to each number less than 3 let $h$ assign the number $-2$.

**4.32.** Let $f: \mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} x^2 - 3x & \text{if } x \geq 2 \\ x + 2 & \text{if } x < 2 \end{cases}$$

Find $f(5)$, $f(0)$, and $f(-2)$.

**4.33.** Let $W = \{a, b, c, d\}$. Determine whether each set of ordered pairs is a function from $W$ into $W$:

(a) $\{(b,a),\ (c,d),\ (d,a),\ (c,d),\ (a,d)\}$, (c) $\{(a,b),\ (b,b),\ (c,b),\ (d,b)\}$,

(b) $\{(d,d),\ (c,a),\ (a,b),(d,b)\}$, (d) $\{(a,a),\ (b,a),\ (a,b),\ (c,d)\}$.

**4.34.** Let the function $g$ assign to each name in the following set $S$ the number of different letters needed to spell the name:

$$S = \{\text{Britt, Martin, Alan, Audrey, Julianna}\}$$

Find the graph of $g$, i.e., write $g$ as a set of ordered pairs.

**4.35.** Let $A = \{1, 2, 3, 4, 5\}$ and let $f\colon A \to A$ be defined by Fig. 4-14. (a) Write $f$ as a set of ordered pairs. (b) Find the image of $f$. (c) Find $f(S)$ where $S = \{1, 2, 4\}$. (d) Find $f^{-1}(T)$ where $T = \{1, 2, 3\}$.

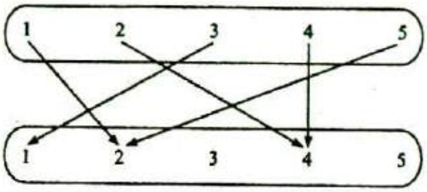


Fig. 4-14

4.36. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$. Find the number of functions from: (a) $A$ into $B$; (b) $B$ into $A$.

**4.37.** Consider any function $f\colon A \to B$. Show $f^{-1}[f[A]] = A$.

**4.38.** A function with domain $A$ is called a *constant* function if every $a \in A$ is assigned the same element. Find the number of constant functions from $A$ into $B$.

## COMPOSITION FUNCTION

**4.39.** Figure 4-15 defines functions $f$, $g$, $h$ from $A = \{1, 2, 3, 4\}$ into itself.

(a) Find the images of $f$, $g$, $h$.

(b) Find the composition functions $f \circ g$, $h \circ f$, $g^2 = g \circ g$.

(c) Find the composition functions $h \circ g \circ f$ and $f \circ g \circ h$.

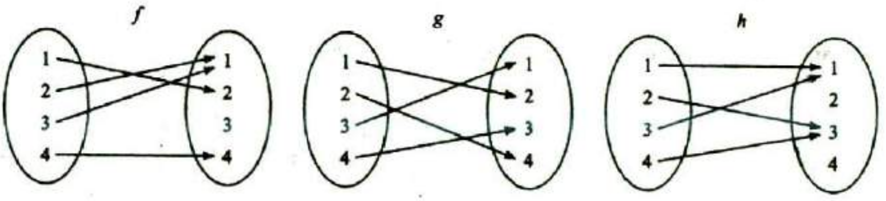


Fig. 4-15

**4.40.** Consider the functions $f(x) = x^2 + 3x + 1$ and $g(x) = 2x - 3$. Find a formula defining the composition function: (a) $f \circ g$; (b) $g \circ f$.

**4.41.** Let $V = \{1,2,3,4\}$ and let

$$f = \{(1,3),\ (2,1),\ (3,4),\ (4,3)\} \quad \text{and} \quad g = \{(1,2),\ (2,3),\ (3,1),\ (4,1)\}$$

Find: (*a*) $f \circ g$; (*b*) $g \circ f$; (*c*) $f \circ f$.

**4.42.** Suppose $f: A \to B$ and $g: B \to C$. Show that $g \circ f$ is a constant function (Problem 4.38) if either $f$ or $g$ is a constant function.

## ONE-TO-ONE, ONTO AND INVERTIBLE FUNCTIONS

**4.43.** Which of the functions in Fig. 4-15 are: (*a*) one-to-one, (*b*) onto, (*c*) invertible?

**4.44.** Consider the formula $f(x) = x^2$.

(*a*) Find the largest interval $D$ such that $f: D \to \mathbf{R}$ is a one-to-one function.

(*b*) Find the smallest target set $T$ such that $f: \mathbf{R} \to T$ is an onto function.

**4.45.** Find the domain $D$ and a formula defining the inverse $f^{-1}$ of each function:
(*a*) $f(x) = x^3 + 5$; (*b*) $f(x) = \dfrac{x-2}{x-3}$.

**4.46.** Suppose $f: A \to B$ is a constant function (Problem 4.38). When will $f$ be: (*a*) one-to-one, (*b*) onto?

**4.47.** Suppose $f: A \to B$ and $g: B \to C$ are invertible functions. Show that $g \circ f: A \to C$ is invertible, and $(g \circ f)^{-1} = g^{-1} \circ f^{-1}$.

**4.48.** Let $W = [0, \infty) = \{x : x \geq 0\}$. Let $f: W \to W$, $g: W \to W$, $h: W \to W$ be defined as follows:

$$f(x) = x^4, \qquad g(x) = x^3 + 1, \qquad h(x) = x + 2$$

Which of the functions are (*a*) one-to-one, (*b*) onto, (*c*) invertible?

## SPECIAL MATHEMATICAL FUNCTIONS, RECURSIVELY DEFINED FUNCTIONS

**4.49.** Find: (*a*) $\lfloor 13.2 \rfloor$, $\lfloor -0.17 \rfloor$, $\lfloor 34 \rfloor$; (*b*) $\lceil 13.2 \rceil$, $\lceil -0.17 \rceil$, $\lceil 34 \rceil$. (See Problem 4.24.)

**4.50.** Find: (*a*) 10 (mod 3), 200 (mod 20), 29 (mod 6); (*b*) −10 (mod 3), −29 (mod 6), −345 (mod 11).

**4.51.** Find: (*a*) $3! + 4!$; (*b*) $3!(3! + 2!)$; (*c*) $6!/5!$; (*d*) $30!/28!$.

**4.52.** Evaluate: (*a*) $\log_2 16$; (*b*) $\log_3 27$; (*c*) $\log_{10} 0.01$.

**4.53.** Find: (*a*) $6^3$; (*b*) $7^{-2}$; (*c*) $4^{5/2}$; (*d*) $27^{-4/3}$.

**4.54.** Let $a$ and $b$ be positive integers. Suppose a function $Q$ is defined recursively as follows:

$$Q(a,b) = \begin{cases} 0 & \text{if } a < b \\ Q(a-b, b) + 1 & \text{if } a \geq b \end{cases}$$

(*a*) Find $Q(2,3)$ and $Q(14,3)$. (*b*) What does the function do? Find $Q(5861, 7)$.

## MISCELLANEOUS PROBLEMS

**4.55.** Find the domain $D$ of each of the following functions:

(*a*) $f(x) = 1/(x+3)$, (*c*) $f(x) = \sqrt{16 - x^2}$,
(*b*) $f(x) = 1/(x-3)$ where $x > 0$, (*d*) $f(x) = \log(x+3)$.

**4.56.** Sketch the graph of each function:

(a) $f(x) = \frac{1}{2}x - 1$

(b) $g(x) = x^3 - 3x + 2$

(c) $h(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1/x & \text{if } x \neq 0 \end{cases}$

## Answers to Supplementary Problems

**4.31.** (a) $f(x) = x^2 + 3$ (b) $g(x) = x^3 + 2x$;
(c) $h(x) = \begin{cases} x^2 & \text{if } x \geq 3 \\ -2 & \text{if } x < 3 \end{cases}$

**4.32.** $f(5) = 10$; $f(0) = 2$; $f(-2) = 0$

**4.33.** (a) Yes; (b) no; (c) yes; (d) no

**4.34.** $g = \{$(Britt, 4), (Martin, 6), (Alan, 3), (Audrey, 6), (Julianna, 6)$\}$

**4.35.** (a) $f = \{(1,2),\ (2,4),\ (3,1),\ (4,4),\ (5,2)\}$; (b) $\text{Im}(f) = \{1,2,4\}$; (c) $f(S) = \{2,4\}$;
(d) $f^{-1}(T) = \{1,3,5\}$

**4.36.** (a) $4^3 = 64$; (b) $3^4 = 81$

**4.37.** $f^{-1}(f(A)) = A$

**4.38.** Number of elements in $B$.

**4.39.** (a) $\text{Im}(f) = \{1,2,4\}$, $\text{Im}(g) = \{1,2,3,4\}$, $\text{Im}(h) = \{1,3\}$
(b) $f \circ g = \{(1,1),\ (2,4),\ (3,2),\ (4,1)\}$
$h \circ f = \{(1,3),\ (2,1),\ (3,1),\ (4,3)\}$
$g^2 = g \circ g = \{(1,4),\ (2,3),\ (3,2),\ (4,1)\}$
(c) $h \circ g \circ f = \{(1,3),\ (2,3),\ (3,3),\ (4,1)\}$
$f \circ g \circ h = \{(1,1),\ (2,2),\ (3,1),\ (4,2)\}$

**4.40.** (a) $(f \circ g)(x) = 4x^2 - 6x + 1$; (b) $(g \circ f)(x) = 2x^2 + 6x - 1$

**4.41.** (a) $f \circ g = \{(1,1),\ (2,4),\ (3,3),\ (4,3)\}$
(b) $g \circ f = \{(1,1),\ (2,2),\ (3,1),\ (4,1)\}$
(c) $f^2 = f \circ f = \{(1,4),\ (2,3),\ (3,3),\ (4,4)\}$

**4.43.** (a) Only $g$; (b) only $g$; (c) only $g$

**4.44.** (a) $D = [0, \infty)$ or $D = (-\infty, 0]$; (b) $T = [0, \infty)$

**4.45.** (a) $f^{-1}(x) = \sqrt[3]{x-5}$, $D = \mathbf{R}$; (b) $f^{-1}(x) = (2-3x)/(1-x)$, $D = \mathbf{R}\backslash\{1\}$

**4.46.** (a) $A$ has one element; (b) $B$ has one element

**4.48.** (*a*) $f, g, h$; (*b*) $f$; (*c*) $f$

**4.49.** (*a*) 13, $-1$, 34; (*b*) 14, 0, 34

**4.50.** (*a*) 1, 0, 5; (*b*) 2, 1, 7

**4.51.** (*a*) 30; (*b*) 48; (*c*) 6; (*d*) 870

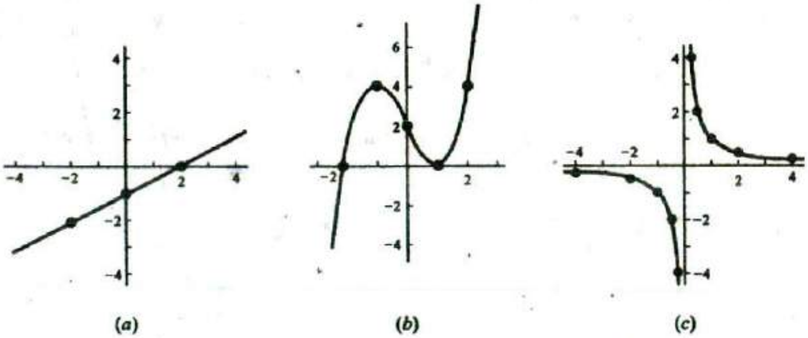
**4.52.** (*a*) 4; (*b*) 3; (*c*) $-2$

**4.53.** (*a*) 216; (*b*) 1/49; (*c*) 32; (*d*) 1/81

**4.54.** (*a*) $Q(2,3) = 0$, $Q(14,3) = 2$; (*b*) $Q(a,b)$ is the remainder when $a$ is divided by $b$, so $Q(5861,7) = 2$.

**4.55.** (*a*) $R\backslash\{-3\}$; (*b*) $D = [0,\infty)\backslash\{-3\}$; (*c*) $D = [-4,4]$; (*d*) $D = (-3,\infty)$

**4.56.** See Fig. 4-16.



(*a*) (*b*) (*c*)

**Fig. 4-16**

# Chapter 5

# Further Theory of Sets and Functions

## 5.1 INTRODUCTION

This chapter investigates some additional properties of sets and functions including set operations on collections of sets and indexed sets. We also discuss the notion of a diagram of functions.

## 5.2 OPERATIONS ON COLLECTIONS OF SETS

Let $\mathscr{A}$ be a collection of sets. The *union* of $\mathscr{A}$, denoted by

$$\bigcup\{A : A \in \mathscr{A}\} \qquad \text{or} \qquad \bigcup_{A \in \mathscr{A}} A \qquad \text{or simply} \qquad \bigcup \mathscr{A}$$

consists of all elements $x$ such that $x$ belongs to at least one set in $\mathscr{A}$; that is,

$$\bigcup\{A : A \in \mathscr{A}\} = \{x : x \in A \text{ for some } A \text{ in } \mathscr{A}\}$$

Analogously, the *intersection* of $\mathscr{A}$, denoted by

$$\bigcap\{A : A \in \mathscr{A}\} \qquad \text{or} \qquad \bigcap_{A \in \mathscr{A}} A \qquad \text{or simply} \qquad \bigcap \mathscr{A}$$

consists of all elements $x$ such that $x$ belongs to all the sets in $\mathscr{A}$; that is,

$$\bigcap\{A : A \in \mathscr{A}\} = \{x : x \in A \text{ for every } A \text{ in } \mathscr{A}\}$$

If $\mathscr{A}$ is empty, then we do not define the intersection of $\mathscr{A}$. In case $\mathscr{A}$ is nonempty and finite, then the above are just the same as our previous definitions of union and intersection.

**EXAMPLE 5.1**

(*a*) Let $\mathscr{A} = [\{1, 2, 3\}, \{2, 3, 4\}, \{2, 3, 5\}]$. Then

$$\bigcup \mathscr{A} = \{1, 2, 3, 4, 5\} \qquad \text{and} \qquad \bigcap \mathscr{A} = \{2, 3\}$$

(*b*) Let $A$ be any set and let $\mathscr{P} = \mathscr{P}(A)$ be the power set of $A$. Then:

$$\bigcup \mathscr{P} = A \qquad \text{and} \qquad \bigcap \mathscr{P} = \varnothing$$

(*c*) Let $\mathscr{A} = \{[-1, 1], [-2, 2], [-3, 3], \ldots, [-n, n], \ldots\}$. Then

$$\bigcup \mathscr{A} = R \qquad \text{and} \qquad \bigcap \mathscr{A} = [-1, 1]$$

## 5.3 INDEXED COLLECTIONS OF SETS

Algebraic properties of unions and intersections are usually presented in the context of one of the main ways of designating collections of sets, that is, as indexed collections of sets. Such collections of sets and the set operations on them are discussed in this section.

### Indexed Collections of Sets

Let $I$ be any nonempty set, and let $\mathscr{L}$ be a collection of sets. An *indexing function* from $I$ to $\mathscr{L}$ is a function $f: I \to \mathscr{L}$. For any $i \in I$, we denote the image $f(i)$ by $A_i$. Thus the indexing function $f$ is usually denoted by

$$\{A_i : i \in I\} \quad \text{or} \quad \{A_i\}_{i \in I} \quad \text{or simply} \quad \{A_i\}$$

The set $I$ is called the *indexing set*, and the elements of $I$ are called *indices*. If $f$ is bijective, that is, one-to-one and onto, then we say that $\mathscr{L}$ is indexed by $I$.

**Remark:** Any nonempty collection $\mathscr{A}$ of distinct sets may be viewed as an indexed collection of sets by letting $\mathscr{A}$ be indexed by itself. Thus a collection of sets is usually given in the form $\{A_i : i \in I\}$, that is, as an indexed collection of sets.

### Operations on Indexed Collections of Sets

Consider any indexed collection $\{A_i : i \in I\}$ of sets. The *union* of the collection $\{A_i : i \in I\}$, denoted by

$$\bigcup\{A_i : i \in I\} \quad \text{or} \quad \bigcup_{i \in I} A_i \quad \text{or simply} \quad \bigcup_i A_i$$

consists of those elements which belong to at least one of the $A_i$. Namely,

$$\bigcup\{A_i : i \in I\} = \{x : x \in A_i \text{ for some } i \in I\}$$

Analogously, the *intersection* of a collection set $\{A_i : i \in I\}$, denoted by

$$\bigcap\{A_i : i \in I\} \quad \text{or} \quad \bigcap_{i \in I} A_i \quad \text{or, simply} \quad \bigcap_i A_i$$

consists of those elements which belong to every $A_i$. Namely,

$$\bigcap\{A_i : i \in I\} = \{x : x \in A_i \text{ for every } i \in I\}$$

In the case that $I$ is a finite set, this is just the same as our previous definitions of union and intersection.

Suppose the indexing set $I$ is the set $\mathbf{P}$ of positive integers. Then $\{A_i\}$ is called a *sequence of sets*, usually denoted by $A_1, A_2, A_3, \ldots$, and the union and intersection of the sets may be denoted by

$$A_1 \cup A_2 \cup \cdots \quad \text{and} \quad A_1 \cap A_2 \cap \cdots$$

respectively.

Suppose $J \subseteq I$. Then the union and intersection of only those sets $A_i$ where $i \in J$ is denoted, respectively, by

$$\bigcup\{A_i : i \in J\} \quad \text{and} \quad \bigcap\{A_i : i \in J\} \quad \text{or} \quad \bigcup_{i \in J} A_i \quad \text{and} \quad \bigcap_{i \in I} A_i$$

We emphasize that $\bigcup_i A_i$ and $\bigcap_i A_i$ can only be used when the entire indexing set $I$ is used in the union and intersection.

**EXAMPLE 5.2**

(*a*) Let $I$ be the set $\mathbf{Z}$ of integers. To each integer $n$ we assign the following subset of $\mathbf{R}$:

$$A_n = \{x : x \leq n\}$$

In other words, $A_n$ is the infinite interval $(-\infty, n]$. For any real number $a$, there exist integers $n_1$ and $n_2$ such that $n_1 < a < n_2$. Hence

$$a \in \bigcup_n A_n \quad \text{but} \quad a \notin \bigcap_n A_n$$

Accordingly,

$$\bigcup_n A_n = \mathbf{R} \quad \text{but} \quad \bigcap_n A_n = \varnothing$$

(*b*) Let $I = \{1, 2, 3, 4, 5\}$ and $J = \{2, 3, 5\}$, and let

$$A_1 = \{1, 9\}, \qquad A_2 = \{2, 4, 6, 9\}, \qquad A_3 = \{3, 6, 7, 9\}, \qquad A_4 = \{4, 8\}, \qquad A_5 = \{5, 6, 9\}$$

Then

$$\bigcap_i A_i = \varnothing \quad \text{and} \quad \bigcup_i A_i = \{1, 2, \ldots, 9\}$$

However,

$$\bigcap_{i \in J} A_i = \{6, 9\} \quad \text{and} \quad \bigcup_{i \in J} A_i = \{2, 3, 4, 5, 6, 7, 9\}$$

The following theorem tells us, in particular, that the distributive laws and DeMorgan's law in Table 1-1 can be generalized to apply to indexed collections of sets.

**Theorem 5.1**: Let $B$ and $\{A_i\}$ with $i \in I$ be subsets of a universal set $\mathbf{U}$. Then:

(i) $B \cap (\cup\{A_i\}) = \cup\{B \cap A_i\}$ and $B \cup (\cap\{A_i\}) = \cap\{B \cup A_i\}$.

(ii) $(\cup\{A_i\})^c = \cap\{A_i^c\}$ and $(\cap\{A_i\})^c = \cup\{A_i^c\}$.

(iii) If $J$ is a subset of $I$, then

$$\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i \quad \text{and} \quad \bigcap_{i \in J} A_i \supseteq \bigcap_{i \in I} A_i$$

Since the empty set $\varnothing$ is a subset of any set, Theorem 5.1(iii) should imply that the empty intersection contains any set $A_i$. Accordingly, one sometimes defines

$$\bigcap_{\varnothing} A_i = \mathbf{U}$$

This may seem strange, but it is similar to defining $0! = 1$ and $a^0 = 1$ in order for general properties to be true.

We also note that Theorem 5.1(i) and (ii) apply to any collection $\mathscr{A}$ of sets.

## 5.4 SEQUENCES, SUMMATION SYMBOL

A *sequence* is a function from the set $\mathbf{P}$ of positive integers into a set $A$. The notation $a_n$ is used to denote the image of the integer $k$. Thus a sequence is usually denoted by

$$a_1, a_2, a_3, \ldots \quad \text{or} \quad \{a_n : n \in \mathbf{P}\} \quad \text{or simply} \quad \{a_n\}$$

Sometimes the domain of a sequence is the set $\mathbf{N} = \{0, 1, 2, \ldots\}$ of nonnegative integers rather than $\mathbf{P}$. In such a case we say that $n$ *begins* with 0 rather than 1.

A *finite sequence* over a set $A$ is a function from $\{1, 2, \ldots, m\}$ into $A$, and it is usually denoted by

$$a_1, a_2, \ldots, a_m$$

Such a finite sequence is sometimes called a *list* or an *m-tuple*.

**EXAMPLE 5.3**

(*a*) The familiar sequences

$$1, 1/2, 1/3, 1/4, \ldots \quad \text{and} \quad 1, 1/2, 1/4, 1/8, \ldots$$

may be formally defined, respectively, by

$$a_n = 1/n \quad \text{and} \quad b_n = 2^{-n}$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*b*) The important sequence $1, -1, 1, -1, \ldots$ may be formally defined by

$$a_n = (-1)^{n+1} \quad \text{or, equivalently, by} \quad b_n = (-1)^n$$

where the first sequence begins with $n = 1$ and the second sequence begins with $n = 0$.

(*c*) (*Strings*): Suppose a set $A$ is finite and $A$ is viewed as a character set or an alphabet. Then a finite sequence over $A$ is called a *string* or *word*, and it is usually written in the form $a_1 a_2 \dots a_m$, that is, without parentheses. The number $m$ of characters in the string is called its *length*. One also views the set with zero characters as a string; it is called the *empty string* or *null string*.

### Summation Symbol, Sums

Consider a sequence $a_1, a_2, a_3, \dots$. Frequently we want to form sums of elements from the sequence. Such sums may sometimes be conveniently represented using the summation symbol $\Sigma$ (the Greek letter sigma). Specifically, the sums

$$a_1 + a_2 + a_3 + \cdots + a_n \qquad \text{and} \qquad a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

will be denoted, respectively, by

$$\sum_{j=1}^{n} a_j \qquad \text{and} \qquad \sum_{j=m}^{n} a_j$$

The letter $j$ in the above expression is called a *dummy index* or *dummy variable*. Other letters frequently used as dummy variables are $i, k, s$, and $t$.

**EXAMPLE 5.4**

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

The last sum in Example 5.4 appears often. It has the value $n(n+1)/2$. Namely,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Thus, for example,

$$1 + 2 + 3 + \cdots + 50 = \frac{50(51)}{2} = 1275$$

The formula may be proved using mathematical induction.

## 5.5 FUNDAMENTAL PRODUCTS

Consider a list $A_1, A_2, \dots, A_n$ of $n$ sets. A *fundamental product* of the sets is a set of the form

$$A_1^* \cap A_2^* \cap \cdots \cap A_m^*$$

where $A_i^*$ is either $A_i$ or $A_i^c$. We note that there are $2^n$ such fundamental products since there is a choice of two sets for each $A_i^*$. One can also show (Problem 5.54) that such fundamental products are disjoint and their union is the universal set $\mathbf{U}$.

There is a geometrical description of these fundamental products which is illustrated below.

**EXAMPLE 5.5** Consider three sets $A, B, C$. The following lists the eight fundamental products of the three sets:

$$P_1 = A \cap B \cap C \qquad P_3 = A \cap B^c \cap C \qquad P_5 = A^c \cap B \cap C \qquad P_7 = A^c \cap B^c \cap C$$
$$P_2 = A \cap B \cap C^c \qquad P_4 = A \cap B^c \cap C^c \qquad P_6 = A^c \cap B \cap C^c \qquad P_8 = A^c \cap B^c \cap C^c$$

These eight products correspond precisely to the eight disjoint regions in the Venn diagram of sets $A, B, C$ in Fig. 5-1 as indicated by the labeling of the regions.

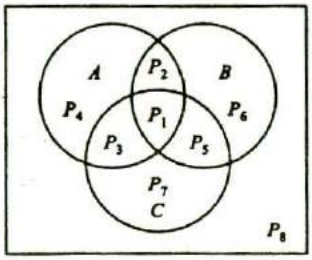


Fig. 5-1

A *Boolean expression* in the sets $A_1, A_2, \ldots, A_n$ is an expression $E = E(A_1, A_2, \ldots, A_n)$ which is built up from the sets using the operations of union, intersection, and complement. For example,

$$E_1 = (A \cup B^c)^c \cap (A^c \cap C)^c \cap (B^c \cup C) \qquad \text{and} \qquad E_2 = [(A \cap B^c) \cup (B^c \cap C)]^c$$

are Boolean expressions in the sets $A, B, C$.

The following theorem applies.

**Theorem 5.2**: Any Boolean expression $E = E(A_1, A_2, \ldots, A_n)$ is equal to the empty set $\varnothing$ or the unique union of a finite number of fundamental products.

This theorem is a special case of Theorem 11.8 on Boolean algebras. So its proof appears there. We indicate a geometrical interpretation here.

Consider sets $A, B, C$. Then any Boolean expression $E = E(A, B, C)$ will be uniquely represented by a finite number of regions in the Venn diagram in Fig. 5-1. Thus $E = E(A, B, C)$ is either the empty set or the union of one or more of the eight fundamental products in Fig. 5-1.

## 5.6 FUNCTIONS AND DIAGRAMS

Recall that we used the following diagram to represent functions $f\colon A \to B$ and $g\colon B \to C$:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$$

Similarly, the following diagram represents functions $f\colon A \to B$, $g\colon B \to C$, and $h\colon A \to C$:

$$\begin{tikzcd} A \arrow[rr, "h"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

Note that the diagram defines two functions from $A$ to $C$, the function $h$ represented by a single arrow, and the composition function $g \circ f$ represented by a sequence of two connected arrows. Each arrow or sequence of arrows connecting $A$ to $C$ is called a *path* from $A$ to $C$.

**Definition:** A diagram of functions is said to be *commutative* if, for any pair of sets $X$ and $Y$ in the diagram, any two paths from $X$ to $Y$ are equal.

**EXAMPLE 5.6**

(*a*) Suppose the diagram of functions in Fig. 5-2(*a*) is commutative. Then:

$$i \circ h = f, \qquad g \circ i = j, \qquad g \circ f = j \circ h = g \circ i \circ h$$

(*b*) The functions $f: A \to B$ and $g: B \to A$ are inverses if and only if the diagrams in Fig. 5-2(*b*) are commutative, that is, if and only if

$$g \circ f = 1_A \quad \text{and} \quad f \circ g = 1_B$$

Here $1_A$ and $1_B$ are the identity functions.

$$\begin{tikzcd}
& D \arrow[d, "i"] \arrow[dr, "j"] & \\
A \arrow[ur, "h"] \arrow[r, "f"'] & B \arrow[r, "g"'] & C
\end{tikzcd}$$

(*a*)

$$\begin{tikzcd}
A \arrow[rr, "1_A"] \arrow[dr, "f"'] & & A \\
& B \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
B \arrow[rr, "1_B"] \arrow[dr, "g"'] & & B \\
& A \arrow[ur, "f"'] &
\end{tikzcd}$$

(*b*)

Fig. 5-2

## 5.7 SPECIAL KINDS OF FUNCTIONS, FUNDAMENTAL FACTORIZATION

This section discusses a number of special kinds of functions which frequently occur in mathematics. We also define and discuss the fundamental factorization of a function.

### Restriction

Consider a function $f: A \to S$. Let $B$ be a subset of $A$. Then $f$ induces a function $f'$ on $B$ defined by

$$f'(b) = f(b)$$

for every $b \in B$. This function $f'$ is called the *restriction* of $f$ to $B$. It is sometimes denoted by

$$f|_B$$

**EXAMPLE 5.7**

(*a*) Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Recall that $f$ is not one-to-one, e.g., $f(2) = f(-2) = 4$. Consider the restriction of $f$ to the nonnegative real numbers $D = [0, \infty)$. Then $f|_D$ is one-to-one. [In fact, $f: D \to D$ is invertible and its inverse is the square root function $f^{-1}(x) = \sqrt{x}$.]

(*b*) Consider the functions

$$g = \{(1,3),\ (2,6),\ (3,11),\ (4,18),\ (5,27)\} \qquad \text{and} \qquad g' = \{(1,3),\ (3,11),\ (5,27)\}$$

Observe that $g'$ is a subset of $g$. Thus $g'$ is the restriction of $g$ to $B = \{1, 3, 5\}$, the set of first elements of $g'$. Note that $B$ is a subset of $A = \{1, 2, 3, 4, 5\}$, the set of first elements of $g$.

### Extension

Consider a function $f: A \to S$. Suppose $B$ to be a superset of $A$, that is, suppose $A \subseteq B$. Let $F: B \to S$ be a function on $B$ such that, for every $a \in A$,

$$F(a) = f(a)$$

This function $F$ is called an *extension* of $f$ to $B$. We note that such an extension is rarely unique.

**EXAMPLE 5.8**

(*a*) Let $f$ be the function on the nonnegative real numbers $D = [0, \infty)$ defined by $f(x) = x$. Then the absolute value function

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

is an extension of $f$ to the set $\mathbf{R}$ of all real numbers. Clearly, the identity function $1_R : \mathbf{R} \to \mathbf{R}$ is also an extension of $f$ to $\mathbf{R}$.

(*b*) Consider the functions

$$f = \{(1,5),\ (3,11),\ (5,17)\} \qquad \text{and} \qquad F = \{(1,5),\ (2,8),\ (3,11),\ (4,14),\ (5,17)\}$$

Observe that $F$ is a superset of $f$. Thus the function $F$ is an extension of $f$ from $\text{dom}(f) = \{1,3,5\}$ to $\text{dom}(F) = \{1,2,3,4,5\}$.

### Inclusion Map

Let $A$ be a subset of a set $S$, that is, $A \subseteq S$. Let $\imath$ be the function from $A$ to $S$ defined by

$$\imath(a) = a$$

for every $a \in A$. Then $\imath$ is called the *inclusion map*. This map is frequently denoted by writing

$$\imath : A \hookrightarrow S$$

For example, the function $f: \mathbf{Z} \to \mathbf{R}$ defined by $f(n) = n$ is the inclusion map from the integers $\mathbf{Z}$ into the real numbers $\mathbf{R}$.

### Characteristic Function

Consider a universal set $\mathbf{U}$. For any subset $A$ of $\mathbf{U}$, let $\chi_A$ be the function from $\mathbf{U}$ to $\{0,1\}$ defined by

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

Then $\chi_A$ is called the *characteristic function* of $A$.

**EXAMPLE 5.9** Let $\mathbf{U} = \{a,b,c,d,e\}$ and $A = \{a,d,e\}$. Then the function

$$\{(a,1),\ (b,0),\ (c,0),\ (d,1),\ (e,1)\}$$

is the characteristic function $\chi_A$.

On the other hand, any function $f: \mathbf{U} \to \{0,1\}$ defines a subset $A_f$ of $\mathbf{U}$ as follows:

$$A_f = \{x : x \in \mathbf{U},\ f(x) = 1\}$$

Furthermore, the characteristic function $\chi_{A_f}$ of $A_f$ is the original function $f$. Thus there is a one-to-one correspondence between the power set $\mathscr{P}(\mathbf{U})$ of $\mathbf{U}$ and the set of all functions from $\mathbf{U}$ into $\{0,1\}$.

### Equivalence Relation and Canonical Map

Let $\equiv$ be an equivalence relation on a set $S$. Recall that $\equiv$ induces a partition of $S$ into equivalence classes, called the quotient set of $S$ by $\equiv$, and denoted and defined by

$$s/\!\equiv\ = \{[a] : a \in S\}$$

Let $\eta : S \to S/\!\equiv$ be the function defined by

$$\eta(a) = [a]$$

that is, $\eta$ sends each element of $S$ into its equivalence class. Then $\eta$ is called the *canonical* or *natural map* from $S$ into $S/\!\equiv$.

**EXAMPLE 5.10** Consider the relation $\equiv$ of congruence modulo 5 on the set $\mathbf{Z}$ of integers; that is,

$$a \equiv b \pmod{5}$$

if 5 divides $a - b$. Then $\equiv$ is an equivalence relation on $\mathbf{Z}$. There are five equivalence classes:

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \qquad [3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} \qquad [4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$

Let $\eta : \mathbf{Z} \to \mathbf{Z}/\equiv$ be the canonical map. Then

$$\eta(7) = [7] = [2], \qquad \eta(19) = [19] = [4], \qquad \eta(-12) = [-12] = [3]$$

### Fundamental Factorization of a Function

Consider any function $f\colon A \to B$. Consider the relation $\sim$ on $A$ defined by

$$a \sim a' \quad \text{if} \quad f(a) = f(a')$$

We show (Problem 5.20) that $\sim$ is an equivalence relation on $A$. We will let $A/f$ denote the quotient set under this relation. Recall that $\mathrm{Im}(f) = f(A)$ denotes the image of $f$ and it is a subset of the target set $B$.

The following lemma and theorem (proved in Problems 5.21 and 5.22) apply.

**Lemma 5.3**: The function $f^*\colon A/f \to f(A)$ defined by

$$f^*([a]) = f(a)$$

is well-defined and bijective.

**Theorem 5.4**: Let $f\colon A \to B$. Then the diagram in Fig. 5-3 is commutative; that is,

$$f = \iota \circ f^* \circ \eta$$

We note that, in Fig. 5-3, $\eta$ is the canonical mapping from $A$ into $A/f$, $f^*$ is the bijective function defined above, and $\iota$ is the inclusion map from $f(A)$ into $B$.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\eta"'] & B \\
A/f \arrow[r, "f^*"] & f(A) \arrow[u, hook, "\iota"']
\end{tikzcd}$$

Fig. 5-3

## 5.8 ASSOCIATED SET FUNCTIONS

Consider a function $f\colon S \to T$. Recall that the *image* $f[A]$ of any subset $A$ of $S$ consists of the elements in $T$ which are images of elements in $A$, that is,

$$f[A] = \{b \in T : \text{there exists } a \in A \text{ such that } f(a) = b\}$$

Also recall that the *preimage* or *inverse image* $f^{-1}[B]$ of any subset $B$ of $T$ consists of all elements in $S$ whose images belong to $B$, that is,

$$f^{-1}[B] = \{a \in S : f(a) \in T\}$$

Thus $f[A]$ is a subset of $T$ and $f^{-1}[B]$ is a subset of $S$.

**EXAMPLE 5.11** Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Then

$$f[\{1,2,3,4\}] = \{1,4,9,16\} \quad \text{and} \quad f[(1,5)] = (1,25)$$

Also,

$$f^{-1}[\{4,9\}] = \{-3,-2,2,3\} \quad \text{and} \quad f^{-1}[(1,4)] = (1,2) \cup (-2,-1)$$

Accordingly, a function $f: S \to T$ induces a function, also denoted by $f$, from the power set $\mathscr{P}(S)$ of $S$ into the power set $\mathscr{P}(T)$ of $T$, and a function $f^{-1}$ from $\mathscr{P}(T)$ back to $\mathscr{P}(S)$. These functions $f$ and $f^{-1}$ are called *set functions* since they map sets into sets, i.e., their domains and target sets are collections of sets.

Observe that brackets [. .] rather than parentheses (. .) are used to distinguish between a function and its associated set functions, i.e., $f(a)$ denotes a value of the original function, whereas $f[A]$ and $f^{-1}[B]$ denote values of the associated set functions.

We note that the associated set function $f^{-1}$ is not in general the inverse of the associated set function $f$. For example, for the above function $f(x) = x^2$, we have

$$f^{-1} \circ f[(1,2)] = f^{-1}[(1,4)] = (1,2) \cup (-2,-1)$$

However, we do have the following theorem.

**Theorem 5.5**: Let $f: S \to T$, and let $A \subseteq S$ and $B \subseteq T$. Then:

(i) $A \subseteq f^{-1} \circ f[A]$.

(ii) $B = f \circ f^{-1}[B]$.

As noted above, the inclusion in (i) cannot in general be replaced by equality.

## 5.9 CHOICE FUNCTIONS

Consider a collection $\{A_i : i \in I\}$ of subsets of a set $B$. A function

$$f: \{A_i\} \to B$$

is called a *choice function* if, for every $i \in I$,

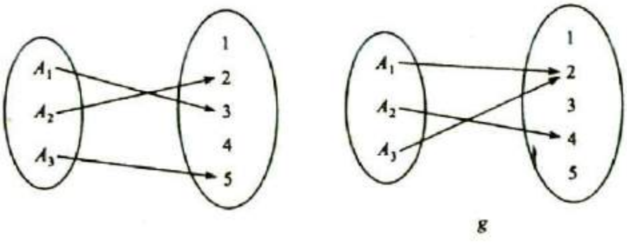
$$f(A_i) \in A_i$$

that is, if the image of each set is an element in the set.

**EXAMPLE 5.12** Consider the following subsets of $B = \{1,2,3,4,5\}$:

$$A_1 = \{1,2,3\}, \qquad A_2 = \{1,3,4\}, \qquad A_3 = \{2,5\}$$

Figure 5-4 shows functions $f$ and $g$ from $\{A_1, A_2, A_3\}$ into $B$. The function $f$ is not a choice function since $f(A_2) = 2$ does not belong to $A_2$, that is $f(A_2) \notin A_2$. On the other hand, $g$ is a choice function. Namely, $g(A_1) = 2$ belongs to $A_1$, $g(A_2) = 4$ belongs to $A_2$, and $g(A_3) = 2$ belongs to $A_3$, that is, $g(A_i) \in A_i$, for $i = 1,2,3$.



g

Fig. 5-4

**Remark**: Essentially, a choice function, for any collection of sets, "chooses" an element from each set in the collection. The question of whether or not a choice function exists for any collection of sets lies at the foundation of set theory. Chapter 9 will be devoted to this question.

## 5.10 ALGORITHMS AND FUNCTIONS

An algorithm $M$ is a finite step-by-step list of well-defined instructions for solving a particular problem, say, to find the output $f(X)$ for a given function $f$ with input $X$. (Here $X$ may be a list or set of values.) Frequently, there may be more than one way to obtain $f(X)$ as illustrated by the following examples. The particular choice of the algorithm $M$ to obtain $f(X)$ may depend on the "efficiency" or "complexity" of the algorithm; this question of the complexity of an algorithm $M$ is discussed in the next section.

**EXAMPLE 5.13** ***(Polynomial Evaluation)*** Suppose, for a given polynomial $f(x)$ and value $x = a$, we want to find $f(a)$, say,

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \qquad \text{and} \qquad a = 5$$

This can be done in the following two ways.

(*a*) (***Direct Method***): Here we substitute $a = 5$ directly in the polynomial to obtain

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe that there are $4 + 3 + 1 = 8$ multiplications and 3 additions. In general, evaluating a polynomial of degree $n$ directly would require approximately

$$n + (n-1) + \cdots + 1 = \frac{n(n-1)}{2} \text{ multiplications and } n \text{ additions.}$$

(*b*) (***Horner's Method or Synthetic Division***): Here we rewrite the polynomial by successively factoring out $x$ (on the right) as follows:

$$f(x) = (2x^2 - 7x + 4)x - 15 = [(2x - 7)x + 4]x - 15$$

Then

$$f(5) = [(3)5 + 4]5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

For those familiar with synthetic division, the above arithmetic is equivalent to the following synthetic division:

$$\begin{array}{r|r} 5 & 2 - 7 + \ \ 4 - 15 \\ & 10 + 15 + 95 \\ \hline & 2 + 3 + 19 + 80 \end{array}$$

Observe that here there are 3 multiplications and 3 additions. In general, evaluating a polynomial of degree $n$ by Horner's method would require approximately

$n$ multiplications and $n$ additions

Clearly Horner's method (*b*) is more efficient than the direct method (*a*).

**EXAMPLE 5.14** (***Greatest Common Divisor***) Let $a$ and $b$ be positive integers with, say, $b < a$; and suppose we want to find $d = \gcd(a, b)$, the greatest common divisor of $a$ and $b$. This can be done in the following two ways.

(*a*) (***Direct Method***): Here we find all the divisors of $a$ and all the divisors of $b$; say, by testing all the numbers from 2 to $a/2$ and from 2 to $b/2$. Then we pick the largest common divisor. For example, suppose $a = 258$ and $b = 60$. The divisors of $a$ and $b$ follow:

$$a = 258; \quad \text{divisors:} \quad 1, 2, 3, 6, 86, 129, 258$$
$$b = 60; \quad \text{divisors:} \quad 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$$

Accordingly, $d = \gcd(258, 60) = 6$.

(*b*) (***Euclidean Algorithm***): Here we divide $a$ by $b$ to obtain a remainder $r_1$ (where $r_1 < b$). Then we divide $b$ by the remainder $r_1$ to obtain a second remainder $r_2$ (where $r_2 < r_1$). Next we divide $r_1$ by $r_2$ to obtain a third remainder $r_3$ (where $r_3 < r_2$). And so on. Since

$$a > b > r_1 > r_2 > r_3 > \cdots \tag{$*$}$$

eventually we obtain a remainder $r_m = 0$. Then $r_{m-1} = \gcd(a, b)$. For example, suppose $a = 258$ and $b = 60$. Then:

(1) Dividing $a = 258$ by $b = 60$ yields the remainder $r_1 = 18$.
(2) Dividing $b = 60$ by $r_1 = 18$ yields the remainder $r_2 = 6$.
(3) Dividing $r_1 = 18$ by $r_2 = 6$ yields the remainder $r_3 = 0$.

Thus $r_2 = 6 = \gcd(258, 60)$.

**Remark:** The Euclidean algorithm is a very efficient way to find the greatest common divisor of two positive integers $a$ and $b$. The fact that the algorithm ends follows from (*). The fact that the algorithm yields $d = \gcd(a, b)$ follows from properties of the integers.

## 5.11 COMPLEXITY OF ALGORITHMS

The analysis of algorithms is a major task in mathematics and computer science. In order to compare algorithms, we must have some criteria to measure the efficiency of our algorithms. This section discusses this important topic.

Suppose $M$ is an algorithm, and suppose $n$ is the size of the input data. The time and space used by the algorithm are the two main measures for the efficiency of $M$. The time is measured by counting the number of "key operations"; for example:

(*a*) In sorting and searching, one counts the number of comparisons.
(*b*) In arithmetic, one counts multiplications and neglects additions.

Key operations are so defined when the time for the other operations is much less than or at most proportional to the time for the key operations. The space is measured by counting the maximum of memory needed by the algorithm.

The *complexity* of an algorithm $M$ is the function $f(n)$ which gives the running time and/or storage space requirement of the algorithm in terms of the size $n$ of the input data. Frequently, the storage space required by an algorithm is simply a multiple of the data size. Accordingly, unless otherwise stated or implied, the term "complexity" shall refer to the running time of the algorithm.

The complexity function $f(n)$, which we assume gives the running time of an algorithm, usually depends not only on the size $n$ of the input data but also on the particular data.

**EXAMPLE 5.15** Suppose we want to search through an English short story TEXT for the first occurrence of a given 3-letter word $W$. Clearly, if $W$ is the 3-letter word "the", then $W$ likely occurs near the beginning of TEXT, so $f(n)$ will be small. On the other hand, if $W$ is the 3-letter word "zoo", then $W$ may not appear in TEXT at all, so $f(n)$ will be large.

The above discussion leads us to the question of finding the complexity function $f(n)$ for certain cases. The two cases one usually investigates in complexity theory follow:

(1) *Worst case*: The maximum value of $f(n)$ for any possible input.
(2) *Average case*: The expected value of $f(n)$.

The analysis of the average case assumes a certain probabilistic distribution for the input data. The average case also uses the following concept in probability theory. Suppose the numbers $n_1, n_2, \ldots, n_k$ occur with respective probabilities $p_1, p_2, \ldots, p_k$. Then the *expectation* or *average value* $E$ is given by

$$E = n_1p_1 + n_2p_2 + \cdots + n_kp_k$$

**Remark**: The complexity of the average case of an algorithm is usually much more complicated to analyze than that of the worst case. Moreover, the probabilistic distribution that one assumes for the average case may not actually apply to real situations. Accordingly, unless otherwise stated or implied, the complexity of an algorithm shall mean the function which gives the running time of the worst case in terms of the input size. This is not too strong an assumption, since the complexity of the average case for many algorithms is proportional to the worst case.

### Rate of Growth; Big $O$ Notation

Suppose $M$ is an algorithm, and suppose $n$ is the size of the input data. Clearly the complexity $f(n)$ of $M$ increases as $n$ increases. It is usually the rate of increase of $f(n)$ that we want to examine. This is usually done by comparing $f(n)$ with some standard function, such as

$$\log_2 n, \qquad n, \qquad n\log_2 n, \qquad n^2, \qquad n^3, \qquad 2^n$$

The rates of growth for these standard functions are indicated in Fig. 5-5, which gives their approximate values for certain values of $n$. Observe that the functions are listed in the order of their rates of growth: the logarithmic function $\log_2 n$ grows most slowly, the exponential function $2^n$ grows most rapidly, and the polynomial functions $n^c$ grows according to the exponent $c$.

| $g(n)$<br>$n$ | $\log n$ | $n$ | $n \log n$ | $n^2$ | $n^3$ | $2^n$ |
|---|---|---|---|---|---|---|
| 5 | 3 | 5 | 15 | 25 | 125 | 32 |
| 10 | 4 | 10 | 40 | 100 | $10^3$ | $10^3$ |
| 100 | 7 | 100 | 700 | $10^4$ | $10^6$ | $10^{30}$ |
| 1000 | 10 | $10^3$ | $10^4$ | $10^6$ | $10^9$ | $10^{300}$ |

**Fig. 5-5** Rate of growth of standard functions.

The way we compare our complexity function $f(n)$ with one of the standard functions is to use the functional "big $O$" notation which we formally define below.

**Definition**: Let $f(x)$ and $g(x)$ be arbitrary functions defined on $R$ or a subset of $R$. We say "$f(x)$ is of order $g(x)$", written

$$f(x) = O(g(x))$$

if there exists a real number $k$ and a positive constant $C$ such that, for all $x > k$, we have

$$|f(x)| \leq C|g(x)|$$

Assuming $f(n)$ and $g(n)$ are functions defined on the positive integers, then

$$f(n) = O(g(n))$$

means that $f(n)$ is bounded by a constant multiple of $g(n)$ for almost all $n$.

**Remark**: The above is called the "big $O$" notation since $f(x) = o(g(x))$ has an entirely different meaning. We also write

$$f(x) = h(x) + O(g(x)) \qquad \text{when} \qquad f(x) - h(x) = O(g(x)).$$

**EXAMPLE 5.16**

(*a*) Let $P(x)$ be a polynomial of degree $m$. We show (Problem 5.24) that $P(x) = O(x^m)$. Thus,

$$7x^2 - 9x + 4 = O(x^2) \quad \text{and} \quad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

(*b*) The following gives the complexity of certain well-known searching and sorting algorithms in computer science:

(1) Linear search: $O(n)$ (3) Bubble sort: $O(n^2)$
(2) Binary search: $O(\log_n)$ (4) Merge-sort: $O(n \log n)$

# Solved Problems

## GENERALIZED OPERATIONS, INDEXED SETS

**5.1.** Let $\mathscr{A} = [\{1,2,3,4\}, \{2,3,4,5\}, \{3,4,5,6\}, \{3,4,7,8,9\}]$.

Find: (*a*) $\bigcup \mathscr{A}$, (*b*) $\bigcap \mathscr{A}$.

(*a*) $\bigcup \mathscr{A}$ consists of all elements which belong to at least one of the sets in $\mathscr{A}$; hence

$$\bigcup \mathscr{A} = \{1, 2, 3, \ldots, 8, 9\}$$

(*b*) $\bigcap \mathscr{A}$ consists of those elements which belong to every set in $\mathscr{A}$; hence

$$\bigcap \mathscr{A} = \{3, 4\}$$

**5.2.** Let $A_m = \{m, 2m, 3m, \ldots\}$ where $m \in \mathbf{P}$; that is, $A_m$ consists of the positive multiples of $m$. Find: (*a*) $A_3 \cap A_5$; (*b*) $A_4 \cap A_6$; (*c*) $A_5 \cup A_{15}$; (*d*) $\bigcup(A_m : m \in S)$ where $S$ is the set of prime numbers.

(*a*) The numbers which are divisible by 3 and divisible by 5 are the multiples of 15. Thus $A_3 \cap A_5 = A_{15}$.

(*b*) The multiples of 12 and no other numbers are contained in $A_4$ and $A_6$; hence $A_4 \cap A_6 = A_{12}$.

(*c*) The multiples of 21 are contained in the multiples of 7, that is, $A_{21} \subseteq A_7$. Hence $A_7 \cup A_{21} = A_7$.

(*d*) Every positive integer except 1 is a multiple of a prime number. Thus

$$\bigcup(A_m : m \in S) = \{2, 3, 4, \ldots\} = \mathbf{P}\backslash\{1\}$$

**5.3.** Let $B_n = [n, n+1]$ where $n \in \mathbf{Z}$, the integers. Find:

(*a*) $B_1 \cup B_2$; (*b*) $B_3 \cap B_4$; (*c*) $\bigcup_{i=7}^{18} B_i = \bigcup(B_i : i \in \{7, 8, \ldots, 18\})$; (*d*) $\bigcup(B_i : i \in \mathbf{Z})$.

(*a*) $B_1 \cup B_2$ consists of all points in the intervals $[1,2]$ and $[2,3]$; hence $B_1 \cup B_2 = [1,3]$.

(*b*) $B_3 \cap B_4$ consists of the points which lie in both $[3,4]$ and $[4,5]$; hence $B_3 \cap B_4 = \{4\}$.

(*c*) $\bigcup_{i=7}^{18} B_i$ means the union of the sets $[7,8], [8,9], \ldots, [18,19]$. Hence

$$\bigcup_{i=7}^{18} B_i = [7, 19]$$

(*d*) Since every real number belongs to at least one interval $[i, i+1]$, we have $\bigcup(B_i : i \in \mathbf{Z}) = \mathbf{R}$.

**5.4.** Prove Theorem 5.1(i) (Distributive Law):

(*a*) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$; (*b*) $B \cup (\cap_i A_i) = \cap_i (B \cup A_i)$.

$$
\begin{aligned}
(a)\quad B \cap (\cup_i A_i) &= \{x : x \in B,\ x \in \cup_i A_i\} \\
&= \{x : x \in B,\ \exists i_0 \text{ s.t. } x \in A_{i_0}\} \\
&= \{x : \exists i_0 \text{ s.t. } x \in B \cap A_{i_0}\} \\
&= \cup_i (B \cap A_i) \\
(b)\quad B \cup (\cap_i A_i) &= \{x : x \in B \text{ or } \forall i,\ x \in A_i\} \\
&= \{x : \forall i,\ x \in B \text{ or } x \in A_i\} \\
&= \{x : \forall i,\ x \in (B \cup \in A_i)\} \\
&= \cap_i (B \cup A_i)
\end{aligned}
$$

Here $\exists$ means "there exists" and $\forall$ means "for every"; these quantifiers are discussed in Chapter 10.

**5.5.** Prove: Let $\{A_i : i \in I\}$ be an indexed collection of sets and let $i_0 \in I$. Then $\bigcap_i A_i \subseteq A_{i_0} \subseteq \bigcup_i A_i$.

Let $x \in \bigcap_i A_i$; then $x \in A_i$ for every $i \in I$. In particular, $x \in A_{i_0}$. Therefore, $\bigcap_i A_i \subseteq A_{i_0}$. Now let $y \in A_{i_0}$. Since $i_0 \in I$, $y \in \bigcup_i A_i$. Hence $A_{i_0} \subseteq \bigcup_i A_i$.

**5.6.** Prove Theorem 5.1(ii) (DeMorgan's law): $(\bigcup_i A_i)^c = \bigcap_i A_i^c$

$$
\begin{aligned}
(\textstyle\bigcup_i A_i)^c &= \{x : x \notin (\textstyle\bigcup_i A_i)\} \\
&= \{x : \forall i,\ x \notin A_i\} \\
&= \{x : \forall i,\ x \in A_i^c\} \\
&= \textstyle\bigcap_i A_i^c
\end{aligned}
$$

## SEQUENCES, SUMMATION SYMBOL

**5.7.** Write out the first six terms of each sequence:

(*a*) $a_n = (-1)^{n+1} n^2$ (*b*) $b_n = \frac{n}{n+1}$

(*c*) $c_n = \begin{cases} 3n & \text{if } n \text{ is odd} \\ 5 & \text{if } n \text{ is even} \end{cases}$

Assuming the sequence begins with $n = 1$, simply substitute $n = 1, 2, \ldots, 6$.

(*a*) 1, −4, 9, −16, 25, −36

(*b*) 1/2, 2/3, 3/4, 4/5, 5/6, 6/7

(*c*) 3, 5, 6, 5, 9, 5

**5.8.** Write out the first six terms of each sequence:

(*a*) $a_1 = 1,\ a_n = n + a_{n-1}$ for $n > 1$.

(*b*) $b_1 = 1,\ b_2 = 2,\ b_n = 3b_{n-2} + 2b_{n-1}$ for $n > 2$.

The sequences are defined recursively in terms of preceding terms of the sequence:

(*a*) 1, 2, 4, 7, 11, 16

(*b*) 1, 2, 7, 20, 61, 221

**5.9.** Find: (*a*) $\sum_{k=1}^{4} k^3$; (*b*) $\sum_{i=1}^{5} x_i$; (*c*) $\sum_{j=1}^{3} (j^4 - j^2)$.

(*a*) $\sum_{k=1}^{4} k^3 = 1^3 + 2^3 + 3^3 + 4^3 = 1 + 8 + 27 + 64 = 100$

(*b*) $\sum_{i=1}^{5} x_i = x_1 + x_2 + x_3 + x_4 + x_5$

(*c*) $\sum_{j=1}^{3} (j^4 - j^2) = (1 - 1) + (16 - 4) + (81 - 9) = 0 + 12 + 72 = 84$

**5.10.** Prove: $\sum_{k=1}^{n} [f(k) + g(k)] = \sum_{k=1}^{n} f(k) + \sum_{k=1}^{n} g(k)$.

The proof is by induction on $n$. For $n = 1$,

$$\sum_{k=1}^{1} [f(k) + g(k)] = f(1) + g(1) = \sum_{k=1}^{1} f(k) + \sum_{k=1}^{1} g(k)$$

Suppose $n > 1$, and the theorem holds for $n - 1$, that is, suppose

$$\sum_{k=1}^{n-1} [f(k) + g(k)] = \sum_{k=1}^{n-1} f(k) + \sum_{k=1}^{n-1} g(k)$$

Then

$$\begin{aligned}
\sum_{k=1}^{n} [f(k) + g(k)] &= \sum_{k=1}^{n-1} [f(k) + g(k)] + [f(n) + g(n)] \\
&= \sum_{k=1}^{n-1} f(k) + \sum_{k=1}^{n-1} g(k) + [f(n)] + [g(n)] \\
&= \sum_{k=1}^{n-1} f(k) + f(n) + \sum_{k=1}^{n-1} g(k) + g(n) \\
&= \sum_{k=1}^{n} f(k) + \sum_{k=1}^{n} g(k)
\end{aligned}$$

Thus the theorem is proved.

## DIAGRAMS AND FUNCTIONS

**5.11.** Consider the diagram in Fig. 5-6(*a*). (*a*) Find the number of paths from $A$ to $E$; what are they? (*b*) How many of the paths represent the same function?

(*a*) There are six paths from $A$ to $E$ as follows:

$A \to B \to E$

$A \to B \to C \to E$

$A \to B \to C \to D \to E$

$A \to C \to E$

$A \to C \to D \to E$

$A \to D \to E$

That is,

$$r \circ f, \quad s \circ i \circ f, \quad t \circ j \circ i \circ f, \quad s \circ h, \quad t \circ j \circ h, \quad t \circ g$$

As noted previously, the functions are written from right to left.

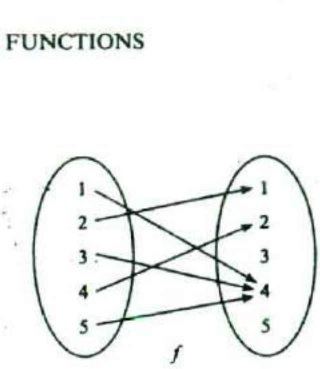
(*b*) If the diagram is commutative, then all six paths (functions) are equal. Otherwise, one cannot say anything about them.

$$\begin{tikzcd}
& B \arrow[d, "i"] \arrow[dr, "r"] & \\
A \arrow[ur, "f"] \arrow[r, "h"] \arrow[dr, "g"'] & C \arrow[r, "s"] \arrow[d, "j"] & E \\
& D \arrow[ur, "t"'] &
\end{tikzcd}$$

(*a*)

$$\begin{tikzcd}
A \arrow[rr, "1_A"] \arrow[dr, "f"'] & & A \\
& B \arrow[ur, "g"'] &
\end{tikzcd}$$

(*b*)



(*c*)

**Fig. 5-6**

**5.12.** Suppose the diagram in Fig. 5-6(*b*) is commutative. (Recall that $1_A$ denotes the identity function on $A$.) State all information that is inferred by the diagram.

First, since the diagram is commutative, $g \circ f = 1_A$.

Furthermore, since $g \circ f$ is one-to-one, $f$ must be one-to-one; and since $g \circ f$ is onto, $g$ must also be onto. It need not be true that $g = f^{-1}$, since we do not know that $f \circ g = 1_B$.

## ASSOCIATED SET FUNCTIONS

**5.13.** Let $A = \{1, 2, 3, 4, 5\}$, and let $f: A \to A$ be defined by Fig. 5-6(*c*). Find:

(*a*) $f[\{1, 2, 5\}]$; (*b*) $f^{-1}[\{2, 3, 4\}]$; (*c*) $f^{-1}[\{3, 5\}]$.

(*a*) $f[\{1, 3, 5\}] = \{f(1), f(2), f(5)\} = \{4, 1, 4\} = \{1, 4\}$.

(*b*) $f^{-1}[\{2, 3, 4\}]$ consists of each element whose image is 2, 3 or 4. Hence $f^{-1}[\{2, 3, 4\} = \{4, 1, 3, 5\}]$.

(*c*) $f^{-1}[\{3, 5\}] = \varnothing$ since no element has 3 or 5 as an image.

**5.14.** Consider the function $f: \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^2$. Find:

(*a*) $f^{-1}[\{25\}]$; (*b*) $f^{-1}[\{-9\}]$; (*c*) $f^{-1}[\{x : x \le 0\}]$; (*d*) $f^{-1}[[4, 25]] = f^{-1}[\{x : 4 \le x \le 25\}]$.

(*a*) $f^{-1}[\{25\}] = \{5, -5\}$ since $f(5) = 25$ and $f(-5) = 25$ and since the square of no other number is 25.

(*b*) $f^{-1}[\{-9\}] = \varnothing$ since the square of no real number is 9.

(*c*) $f^{-1}[\{x : x \le 0\}] = \{0\}$ since $f(0) = 0 \le 0$ and since the square of every other real number is greater than 0.

(*d*) $f^{-1}[\{x : 4 \le x \le 25\}]$ consists of those real numbers $x$ such that $4 \le x^2 \le 25$. Accordingly,

$$f^{-1}[\{x : 4 \le x \le 25\}] = [2, 5] \cup [-5, -2]$$

**5.15.** Suppose $f: S \to T$ is one-to-one. Prove that the associated set function $f: \mathscr{P}(S) \to \mathscr{P}(T)$ is also one-to-one.

Suppose $S = \varnothing$. Then $\mathscr{P}(S) = \{\varnothing\}$ has only one element. Hence $f: \mathscr{P}(S) \to \mathscr{P}(T)$ is one-to-one.

Suppose $S \ne \varnothing$. Then $\mathscr{P}(S)$ has at least two elements. Let $A, B \in \mathscr{P}(S)$, but $A \ne B$. Then there exists $p \in A$ such that $p \notin B$ (or $p \in B$ such that $p \notin A$). Then $f(p) \in f[A]$ and, since $f$ is one-to-one, $f(p) \notin f[B]$. Thus $f[A] \ne f[B]$, and so the associated set function is one-to-one.

**5.16.** Let $f: S \to T$ and let $A$ and $B$ be subsets of $S$. Prove $f[A \cup B] = f[A] \cup f[B]$.

We first show that $f[A \cup B] \subseteq f[A] \cup f[B]$. Let $y \in f[A \cup B]$. Then there exists $x \in S$ such that $f(x) = y$ and $x \in A \cup B$. Then $x \in A$ or $x \in B$. Hence $f(x) \in f[A]$ or $f(x) \in f[B]$. In either case, $y = f(x)$ belongs to $f[A] \cup f[B]$.

Next we prove the reverse inclusion, i.e., $f[A] \cup f[B] \subseteq f[A \cup B]$. Let $y \in f[A] \cup f[B]$. Then $y \in f[A]$ or $y \in f[B]$. If $y \in f[A]$, then there exists $x \in A$ such that $f(x) = y$, and if $y \in f[B]$, then there exists $x \in B$ such that $f(x) = y$. In either case, $y = f(x)$ with $x \in A \cup B$; hence $y \in f[A \cup B]$.

## SPECIAL FUNCTIONS: EXTENSION, CHOICE, CHARACTERISTIC

**5.17.** Consider the function $f(x) = x$ where $x \geq 0$, that is, where $D = [0, \infty)$ is the domain. State whether or not each of the following functions is an extension of $f$:

(*a*) $g_1(x) = x$ where $x \geq -2$; (*b*) $g_2(x) = (x + |x|)/2$; (*c*) $g_3(x) = x$ where $x \in [-1, 1]$.

A function $g$ is an extension of $f$ if the domain $D'$ of $g$ is an extension of the domain $D = [0, \infty)$ of $f$, and if $g(x) = x$ for every $x \in [0, \infty)$.

(*a*) Since $g_1$ satisfies both of the above conditions, $g_1$ is an extension of $f$.

(*b*) Note

$$g_2(x) = \begin{cases} (x+x)/2 = x & \text{if } x \geq 0 \\ (x-x)/2 = 0 & \text{if } x < 0 \end{cases}$$

Hence $g_2$ is an extension of $f$.

(*c*) The domain of $g_3$ is not a superset of the domain of $f$; hence $g_3$ is not an extension of $f$.

**5.18.** Consider the following subsets of $B = \{1, 2, 3, 4, 5\}$:

$$A_1 = \{1, 2, 3\}, \qquad A_2 = \{1, 5\}, \qquad A_3 = \{2, 4, 5\}, \qquad A_4 = \{3, 4\}$$

State whether or not each of the following functions from $\{A_1, A_2, A_3, A_4\}$ into $B$ is a choice function:

(*a*) $f_1 = \{(A_1, 1), (A_2, 2), (A_3, 3), (A_4, 4)\}$
(*b*) $f_2 = \{(A_1, 1), (A_2, 1), (A_3, 4), (A_4, 4)\}$
(*c*) $f_3 = \{(A_1, 2), (A_2, 1), (A_3, 4), (A_4, 3)\}$
(*d*) $f_4 = \{(A_1, 3), (A_2, 5), (A_3, 1), (A_4, 3)\}$

(*a*) Since $f_1(A_2) = 2$ is not an element in $A_2$, $f_1$ is not a choice function.

(*b*) Here $f_2(A_i)$ belongs to $A_i$, for each $i$; hence $f_2$ is a choice function.

(*c*) Also, $f_3(A_i)$ belongs to $A_i$, for each $i$, hence $f_3$ is a choice function.

(*d*) Note that $f_4(A_3) = 1$ does not belong to $A_3$, hence $f_4$ is not a choice function.

**5.19.** Let $A$ and $B$ be subsets of a universal set $\mathbf{U}$. Prove $\chi_{A \cap B} = \chi_A \chi_B$. [Here $\chi_A \chi_B$ is the product of the functions, not the composition, that is, $(\chi_A \chi_B)(x) = \chi_A(x)\chi_B(x)$.]

Let $x \in A \cap B$. Then $x \in A$ and $x \in B$. Hence

$$\chi_{A \cap B}(x) = 1 \qquad \text{and} \qquad (\chi_A \chi_B)(x) = \chi_A(x)\chi_B(x) = (1)(1) = 1$$

Suppose $y \notin A \cap B$. Then $\chi_{A \cap B}(y) = 0$. Also, $y \in (A \cap B)^c = A^c \cup B^c$, and so $y \in A^c$ or $y \in B^c$. This means $\chi_A(y) = 0$ or $\chi_B(y) = 0$, and therefore

$$(\chi_A \chi_B)(y) = \chi_A(y)\chi_B(y) = 0 = \chi_{A \cap B}(y)$$

Accordingly, $\chi_{A \cap B}$ and $\chi_A \chi_B$ assign the same number to each element in $\mathbf{U}$. Therefore, $\chi_{A \cap B} = \chi_A \chi_B$.

## FUNDAMENTAL FACTORIZATION

**5.20.** Let $f: A \to B$. Define $a \sim a'$ if $f(a) = f(a')$. Show that $\sim$ is an equivalence relation on $A$.

We must show that $\sim$ is: (*a*) reflexive, (*b*) symmetric, and (*c*) transitive.

(*a*) For any $a \in A$, we have $f(a) = f(a)$. Hence $a \sim a$, and so $\sim$ is reflexive.

(*b*) Suppose $a \sim a'$. Then $f(a) = f(a')$, and hence $f(a') = f(a)$. Thus $a' \sim a$, and so $\sim$ is symmetric.

(*c*) Suppose $a \sim a'$ and $a' \sim a''$. Then $f(a) = f(a')$ and $f(a') = f(a'')$; hence $f(a) = f(a'')$. Thus $a \sim a''$, and so $\sim$ is transitive.

**5.21.** Prove Lemma 5.3: Let $f: A \to B$. Let $f^* : A/f \to f(A)$ be defined by $f^*([a]) = f(a)$. Then $f^*$ is well-defined and bijective.

Suppose $[a] = [a']$. Then $a \sim a'$. Hence $f(a) = f(a')$, and so $f^*$ is well-defined.

First we show that $f^*$ is one-to-one. Suppose $f^*([a]) = f^*([a'])$. Then $f(a) = f(a')$. Hence $a \sim a'$, and so $[a] = [a']$. Thus $f^*$ is one-to-one.

Next we show that $f^*$ is onto. Suppose $b \in f(A)$. Then there exists $a \in A$ such that $f(a) = b$. Then $f^*([a]) = f(a) = b$. Thus $f^*$ is onto. Therefore, $f^*$ is bijective (one-to-one and onto).

**5.22.** Prove Theorem 5.4: Let $f: A \to B$. Then diagram in Fig. 5-3 is commutative, that is, $f = i \circ f^* \circ \eta$.

Let $a \in A$. Then

$$\begin{aligned}(i \circ f^* \circ \eta)(a) &= (i \circ f^*)(\eta(a)) = (i \circ f^*)([a]) \\ &= i(f^*([a])) = i(f(a)) = f(a)\end{aligned}$$

Hence $f = i \circ f^* \circ \eta$.

**5.23.** Let $A = \{1, 2, 3, 4, 5\}$ and let $f$ be the function in Fig. 5-6(*c*).

(*a*) Find $A/f$ and $f(A)$. (*b*) Find the factorization $f = i \circ f^* \circ \eta$.

(*a*) The elements with the same images are put in the same equivalence class. Hence $A/f = [\{1, 3, 5\},\ \{2\},\ \{4\}]$. Also, $f(A) = \{1, 2, 4\}$. [Note $|A/f| = |f(A)|$.]

(*b*) We have:

$$\begin{array}{l} 1 \xrightarrow{\eta} \{1, 3, 5\} \xrightarrow{f^*} 4 \xrightarrow{i} 4 \\ 2 \xrightarrow{\eta} \{2\} \xrightarrow{f^*} 1 \xrightarrow{i} 1 \\ 3 \xrightarrow{\eta} \{1, 3, 5\} \xrightarrow{f^*} 4 \xrightarrow{i} 4 \\ 4 \xrightarrow{\eta} \{4\} \xrightarrow{f^*} 2 \xrightarrow{i} 2 \\ 5 \xrightarrow{\eta} \{1, 3, 5\} \xrightarrow{f^*} 4 \xrightarrow{i} 4 \end{array}$$

On the other hand:

$$f(1) = 4, \quad f(2) = 1, \quad f(3) = 4, \quad f(4) = 2, \quad f(5) = 5$$

Thus $f = i \circ f^* \circ \eta$.

## ALGORITHMS AND COMPLEXITY

**5.24.** Suppose $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ has degree $m$. Prove $P(x) = O(x^m)$.

Let $b_0 = |a_0|, b_1 = |a_1|, \ldots, b_m = |a_m|$. Then, for $x \geq 1$, we have

$$\begin{aligned} |P(x)| &\leq b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \\ &= \left[\frac{b_0}{x^m} + \frac{b_1}{x^{m-1}} + \cdots + b^m\right]x^m \\ &\leq (b_0 + b_1 + b_2 + \cdots + b_m)x^m = Mx^m \end{aligned}$$

where $M = |a_0| + |a_1| + \cdots + |a_m|$. Thus $P(x) = O(x^m)$.

**5.25.** Compare the factorial function $f(n) = n!$ to the functions in Fig. 5-5.

The factorial function $f(n) = n!$ grows faster than the exponential function $2^n$. Clearly, for $n \geq 4$,

$$2^n = 2 \cdot 2 \cdot \cdots \cdot 2 \geq 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1)n$$

Thus $f(n) = n!$ grows faster than every function in Fig. 5-5. In fact, $f(n) = n!$ grows faster than the exponential function $g(n) = c^n$ for any constant $c$.

**5.26.** Find $f(3)$ where $f(x) = 2x^4 - 5x^3 + 2x^2 - 6x - 7$.

Use synthetic division to obtain:

$$\begin{array}{r|rrrrr} 3 & 2 & -5 & 2 & -6 & -7 \\ & & 6 & 3 & 15 & 27 \\ \hline & 2 & 1 & 5 & 9 & 20 \end{array}$$

Thus $f(3) = 20$.

**5.27.** Suppose a list DATA contains $n$ elements, and suppose a specific NAME which appears in DATA is given. We want to find the location of NAME in the list using a linear search; that is, we compare NAME with DATA[1], DATA[2], and so on. Let $C(n)$ denote the number of comparisons. Find $C(n)$ for: (*a*) the worse case, (*b*) the average case.

(*a*) Clearly the worst case occurs when NAME is the last element in the list. Hence $C(n) = n$ is the worst-case complexity.

(*b*) Here we assume that it is equally likely for NAME to occur in any position in the list. Accordingly, the numbers of comparisons are $1, 2, \ldots, n$ and each number occurs with probability $p = 1/n$. (We do make the last comparison just to make sure that NAME is in the list.) Then:

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

This agrees with our intuitive feeling that the average number of comparisons needed to find NAME is approximately half the number of elements in the list.

## Supplementary Problems

### GENERALIZED OPERATIONS, INDEXED SETS

**5.28.** Let $\mathscr{A} = [\{1,2,3,4\},\ \{1,3,5,7,9\},\ \{1,2,3,6,8\},\ \{1,3,7,8,9\}]$. Find: (*a*) $\bigcup\mathscr{A}$; (*b*) $\bigcap\mathscr{A}$.

**5.29.** For each $m \in \mathbf{P}$, let $A_m$ be the following subset of $\mathbf{P}$:

$$A_m = \{m, 2m, 3m, \ldots\} = \{\text{multiples of } m\}$$

(*a*) Find: (1) $A_2 \cap A_7$; (2) $A_6 \cap A_8$; (3) $A_3 \cup A_{12}$; (4) $A_3 \cap A_{12}$.

(*b*) Prove $\bigcap(A_i : i \in J) = \varnothing$, when $J$ is an infinite subset of $\mathbf{P}$.

**5.30.** For each $n \in \mathbf{Z}$, let $B_n = (n, n+1]$, a half-open interval. Find:

(*a*) $B_4 \cup B_5$; (*b*) $B_h \cap B_7$; (*c*) $\bigcup_{i=4}^{20} B_i$; (*d*) $B_s \cup B_{s+1} \cup B_{s+2}$; (*e*) $\bigcup_{i=0}^{15} B_{s+i}$; (*f*) $\bigcup(B_{s+i} : i \in \mathbf{Z})$.

**5.31.** For each $n \in \mathbf{P}$, let $D_n = [0, 1/n]$, $S_n = (0, 1/n]$, $T_n = [0, 1/n)$. Find: (*a*) $\bigcap_n D_n$; (*b*) $\bigcap_n S_n$; (*c*) $\bigcap_n T_n$.

**5.32.** Prove Theorem 5.1(iii): Suppose $J$ is a subset of $I$. Then

$$\bigcup_{i\in J} A_i \subseteq \bigcup_{i\in I} A_i \qquad \text{and} \qquad \bigcap_{i\in J} A_i \supseteq \bigcap_{i\in I} A_i$$

### SEQUENCES, SUMMATION SYMBOL

**5.33.** Write out the first six terms of each sequence:

(*a*) $a_n = (-1)^{n+1} n^3$

(*b*) $b_n = \dfrac{n^2}{2n+1}$

(*c*) $c_n = \begin{cases} n^2 & \text{if } n \text{ is odd} \\ n+4 & \text{if } n \text{ is even} \end{cases}$

**5.34.** Write out the first six terms of each sequence:

(*a*) $a_1 = 1,\ a_n = n^2 + 2a_{n-1}$ for $n > 1$.

(*b*) $b_1 = 1,\ b_2 = 2,\ b_n = 2b_{n-2} + 3b_{n-1}$ for $n > 2$.

**5.35.** Find: (*a*) $\displaystyle\sum_{k=3}^{5} k^4$; (*b*) $\displaystyle\sum_{k=0}^{4} a_k x^k$; (*c*) $\displaystyle\sum_{j=1}^{3} (j^3 + j^2 - j)$; (*d*) $\displaystyle\sum_{j=1}^{15} 1$.

**5.36.** Rewrite using the summation symbol:

(*a*) $\bar{x} = \dfrac{x_1 f_1 + x_2 f_2 + \cdots + x_n f_n}{f_1 + f_2 + \cdots + f_n}$

(*b*) $c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{in} b_{nj}$

## DIAGRAMS AND FUNCTIONS

**5.37.** Consider the diagram in Fig. 5-7($a$). Find the number of paths from $A$ to $D$ and state what they are.

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d, "f"'] & C \arrow[d, "j"] \\
B \arrow[ur, "h"] \arrow[r, "i"] & D
\end{tikzcd}$$

($a$)

$$\begin{tikzcd}
D \arrow[r, "r"] \arrow[dr, "s"] & E \arrow[dr, "v"] & \\
A \arrow[u, "f"] \arrow[r, "t"] & B \arrow[u, "u"'] \arrow[r, "w"] & C
\end{tikzcd}$$

($b$)

**Fig. 5-7**

**5.38.** Suppose the diagram in Fig. 5-7($b$) is commutative. Which functions are equal?

## ASSOCIATED SET FUNCTIONS

**5.39.** Let $A = \{1, 2, 3, 4, 5\}$, and let $f\colon A \to A$ be defined by

$$f = \{(1,3),\ (2,2),\ (3,5),\ (4,3),\ (5,2)\}$$

Find: ($a$) $f[\{1,2,5\}]$; ($b$) $f^{-1}[\{3,4,5\}]$; ($c$) $f^{-1}[\{1,4\}]$.

**5.40.** Consider the function $f\colon R \to R$ defined by $f(x) = |x|$. Find:
($a$) $f^{-1}[\{7\}]$; ($b$) $f^{-1}[\{-5\}]$; ($c$) $f^{-1}[\{x : x \leq 0\}]$; ($d$) $f^{-1}[[2,3]] = f^{-1}[\{x : 2 \leq x \leq 3\}]$.

**5.41.** Suppose $f\colon S \to T$ is onto. Prove that the associated set function $f\colon \mathscr{P}(S) \to \mathscr{P}(T)$ is also onto.

**5.42.** Let $f\colon S \to T$ and let $A$ and $B$ be subsets of $S$. Prove: ($a$) $f[A \cap B] \subseteq f[A] \cap f[B]$; ($b$) $f[A \backslash B] \supseteq f[A] \backslash f[B]$.

**5.43.** Let $f\colon S \to T$ and let $A$ and $B$ be subsets of $T$. Prove:
($a$) $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$; ($b$) $f^{-1}[A \backslash B] = f^{-1}[A] \backslash f^{-1}[B]$. (Compare with Problem 5.42.)

## EXTENSIONS, RESTRICTIONS, CHOICE FUNCTIONS

**5.44.** Let $f$ be the following function with domain $D = \{1, 3, 5, 7\}$:

$$f = \{(1,6),\ (3,4),\ (5,2),\ (7,4)\}$$

For what values of $x$ and $y$ will the following functions be extensions of $f$:

($a$) $g_1 = \{(1,6),\ (2,2),\ (3,x),\ (4,1),\ (5,y),\ (6,2),\ (7,4)\}$
($b$) $g_2 = \{(1,x),\ (2,4),\ (3,4),\ (4,2),\ (5,2),\ (6,2),\ (7,y)\}$
($c$) $g_3 = \{(1,6),\ (2,x),\ (3,4),\ (4,7),\ (5,y),\ (6,3),\ (7,4)\}$
($d$) $g_4 = \{(1,6),\ (2,5),\ (3,1),\ (4,3), (5,x),\ (6,8),\ (7,y)\}$

**5.45.** Consider the following subsets of $B = \{1, 2, 3, 4, 5\}$:

$$A_1 = \{1,2,3\}, \quad A_2 = \{2,4\}, \quad A_3 = \{5\}, \quad A_4 = \{1,3,4,5\}$$

State whether or not each of the following functions from $\{A_1, A_2, A_3, A_4\}$ into $B$ is a choice function:

($a$) $f_1 = \{(A_1,1),\ (A_2,2),\ (A_3,3),\ (A_4,4)\}$
($b$) $f_2 = \{(A_1,2),\ (A_2,2),\ (A_3,5),\ (A_4,5)\}$
($c$) $f_3 = \{(A_1,3),\ (A_2,1),\ (A_3,5),\ (A_4,3)\}$
($d$) $f_4 = \{(A_1,3),\ (A_2,4),\ (A_3,5),\ (A_4,1)\}$

**5.46.** Let $f$ be the following function with domain $D = \{1, 2, 3, 4, 5, 6\}$:

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

Find the restriction of $f$ to: (*a*) $\{1, 3, 5\}$, (*b*) $\{2, 3, 4, 5\}$, (*c*) $\{1, 2, 5, 6\}$.

## CHARACTERISTIC FUNCTIONS

**5.47.** Let $\mathbf{U} = \{a, b, c, d, e\}$, and let $A = \{a, b, c\}$, $B = \{c, d\}$, and $C = \{a, d, e\}$. Find: (*a*) $\chi_A$; (*b*) $\chi_B$; (*c*) $\chi_C$.

**5.48.** Let $\mathbf{U} = \{a, b, c, d\}$. Each of the following functions from $\mathbf{U}$ into $\{0, 1\}$ is the characteristic function of a subset of $\mathbf{U}$. Find each subset.

(*a*) $\{(a,1),\ (b,0),\ (c,0),\ (d,1)\}$, (*c*) $\{(a,0),\ (b,0),\ (c,0),\ (d,0)\}$,
(*b*) $\{(a,0),\ (b,1),\ (c,0),\ (d,0)\}$, (*d*) $\{(a,1),\ (b,1),\ (c,0),\ (d,1)\}$.

**5.49.** Let $A$ and $B$ be subsets of a universal set $\mathbf{U}$. Prove: (*a*) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}$; (*b*) $\chi_{A\setminus B} = \chi_A - \chi_{A\cap B}$.

## FUNDAMENTAL FACTORIZATION

**5.50.** Let $A = \{\text{Marc, Erik, Audrey, Britt, Emily}\}$. Find $A/\!/f$ and $f(A)$ where $f\colon A \to \mathbf{P}$ is defined by:
(*a*) $f(a)$ = number of letters in $a$; (*b*) $f(a)$ = number of distinct letters in $a$

**5.51.** Suppose $f\colon \mathbf{R} \to \mathbf{R}$ is defined by $f(x) = |x|/x$ when $x \neq 0$ and $f(0) = 0$. Find $\mathbf{R}/\!/f$ and $f(\mathbf{R})$.

## MISCELLANEOUS PROBLEMS

**5.52.** Let $f\colon D \to \mathbf{R}$ and $g : D \to \mathbf{R}$ for some domain $D$. Define $(f + g) : D \to \mathbf{R}$ and $(fg) : D \to \mathbf{R}$ by

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x)$$

(Note $fg$ is not the composition of $f$ and $g$.)

(*a*) Let $0_D : D \to \mathbf{R}$ be the zero function, i.e., for every $x \in D$, $0_D(x) = 0$. Prove that, for any function $f\colon D \to \mathbf{R}$,

$$f + 0_D = 0_D + f = f \quad \text{and} \quad g = f \cdot 0_D = 0_D \cdot f = 0_D$$

(*b*) Consider the following functions on $D = \{1, 2, 3\}$:

$$f = \{(1,3),\ (2,5),\ (3,8)\} \quad \text{and} \quad g = \{(1,5),\ (2,-3),\ (3,4)\}$$

Find $f + g$ and $fg$.

**5.53.** Find $f(a)$ where: (*a*) $a = 4$ and $f(x) = 2x^4 - 5x^3 - 9x^2 + 7$;
(*b*) $a = 7$ and $f(x) = x^5 - 8x^4 + 6x^3 + 9x^2 - 7x - 27$.

**5.54.** Consider $n$ distinct sets $A_1, A_2, \ldots, A_n$ in a universal set $\mathbf{U}$. Prove:

(*a*) There are $2^n$ fundamental products of the $n$ sets.
(*b*) Any two such fundamental products are disjoint.
(*c*) $\mathbf{U}$ is the union of all the fundamental products.

## Answers to Supplementary Problems

**5.28.** (*a*) $\bigcup \mathscr{A} = \{1, 2, 3, \ldots, 89\}$; (*b*) $\bigcap \mathscr{A} = \{1, 3\}$

**5.29.** (*a*) (1) $A_{14}$; (2) $A_{24}$; (3) $A_3$; (4) $A_{12}$

**5.30.** (*a*) $(4, 6]$; (*b*) $(6, 8]$; (*c*) $(4, 21]$; (*d*) $(s, s+3]$; (*e*) $(s, s+16]$; (*f*) $\mathbf{R}$

**5.31.** (*a*) $\{0\}$; (*b*) $\varnothing$; (*c*) $\{0\}$

**5.33.** (*a*) 1, −8, 27, −64, 125, −216; (*b*) 1/3, 4/51, 9/7, 16/9, 25/11, 36/13; (*c*) 1, 6, 9, 8, 25, 10

**5.34.** (*a*) 1, 6, 21, 58, 141, 318; (*b*) 1, 2, 8, 28, 100, 356

**5.35.** (*a*) 962; (*b*) $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$; (*c*) 44; (*d*) 15

**5.36.** (*a*) $\bar{x} = \dfrac{\sum x_i f_i}{\sum f_i}$; (*b*) $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$

**5.37.** Three: $i \circ f$, $j \circ g$, and $j \circ h \circ f$

**5.38.** $t = s \circ f$, $r = u \circ s$, $r \circ f = u \circ s \circ f = u \circ t$, $w = v \circ u$, $w \circ s = v \circ r = v \circ u \circ s$,
$w \circ t = w \circ s \circ f = v \circ u \circ t = v \circ u \circ s \circ f = v \circ r \circ f$

**5.39.** (*a*) $\{2, 3\}$; (*b*) $\{1, 4, 3\}$; (*c*) $\varnothing$

**5.40.** (*a*) $\{7, -7\}$; (*b*) $\varnothing$; (*c*) $\{0\}$; (*d*) $[-3, -2] \cup [2, 3]$

**5.44.** (*a*) $x = 4$, $y = 2$; (*b*) $x = 6$, $y = 4$; (*c*) $x$ any value, $y = 2$; (*d*) $(3, 1)$ means no extension.

**5.45.** (*a*) No; (*b*) yes; (*c*) no; (*d*) yes

**5.46.** (*a*) $\{(1,4), (3,6), (5,4)\}$; (*b*) $\{(2,5), (3,6), (4,5), (5,4)\}$; (*c*) $\{(1,4), (2,5), (5,4), (6,3)\}$

**5.47.** (*a*) $\chi_A = \{(a,1), (b,1), (c,1), (d,0), (e,0)\}$
(*b*) $\chi_B = \{(a,0), (b,0), (c,1), (d,1), (e,0)\}$
(*c*) $\chi_C = \{(a,1), (b,0), (c,0), (d,1), (e,1)\}$

**5.48.** (*a*) $\{a, d\}$; (*b*) $\{b\}$; (*c*) $\varnothing$; (*d*) $\{a, b, d\}$

**5.50.** (*a*) $A/f = [\{$Marc, Erik$\}, \{$Britt, Emily$\}, \{$Audrey$\}]$, $f(a) = \{4, 5, 6\}$
(*b*) $A/f = [\{$Marc, Erik, Britt$\}, \{$Emily$\}, \{$Audrey$\}]$, $f(A) = \{4, 5, 6\}$

**5.51.** $\mathbf{R}/f = \{(-\infty, 0), \{0\}, (0, \infty)\}$; $f(\mathbf{R}) = \{-1, 0, 1\}$

**5.52.** (*b*) $f + g = \{(1,8), (2,2), (3,12)\}$; $fg = \{(1,15), (2,-15), (3,32)\}$

**5.53.** (*a*) $f(4) = 19$; (*b*) $f(7) = 22$