Elements *of* MODERN ALGEBRA

EIGHTH EDITION

Gilbert ♦ Gilbert

Special Notations

The following is a list of the special notations used in this text, arranged in order of their first appearance in the text. Numbers refer to the pages where the notations are defined.

$\{a\}$	set with a as its only element, 1
$x \in A$	x is an element of the set A, 2
$x \notin A$	x is not an element of the set A, 2
$A \subseteq B$ or $B \supseteq A$	A is a subset of B, 2
$A \subset B$	A is a proper subset of B, 3
$A \cup B$	union of A and B, 3
$A \cap B$	intersection of A and B, 3
$\emptyset$	empty set, 4
$\mathcal{P}(A)$	power set of A, 4
U	universal set, 5
$A - B$	complement of B in A, 5
A'	complement of A, 5
$\mathbf{Z}$	set of all integers, 6
$\mathbf{Z}^+$	set of all positive integers, 6
$\mathbf{Q}$	set of all rational numbers, 6
$\mathbf{R}$	set of all real numbers, 6
$\mathbf{R}^+$	set of all positive real numbers, 6
$\mathbf{C}$	set of all complex numbers, 6
$\Rightarrow$	"implies," 8
$\Leftarrow$	"is implied by," 8
$\Leftrightarrow$	"if and only if," 9
$A + B$	sum of subsets A and B, 13
$A \times B$	Cartesian product of A and B, 13
$f(a)$	image of the element a under f, 14
$f: A \rightarrow B$ or $A \xrightarrow{f} B$	f is a mapping from A to B, 14
$f(S)$	image of the set S under f, 15
$f^{-1}(T)$	inverse image of the set T under f, 15
$\mathbf{E}$	set of all even integers, 18
$f \circ g$	composition mapping, 20
$\mathcal{S}(A)$	set of all permutations on A, 38
$\mathcal{M}(A)$	set of all mappings from A to A, 38
I_A	identity mapping from A to A, 38
f^{-1}	inverse of a mapping, 42
$[a_{ij}]_{m \times n}$	matrix with m rows, n columns, and elements a_{ij}, 44
$M_{m \times n}(S)$	set of all $m \times n$ matrices over S, 45
$M_n(S)$	set of all square matrices of order n over S, 45
$\sum_{i=1}^{n} a_i$	sigma notation, 49
I_n	identity matrix of order n, 51
δ_{ij}	Kronecker delta, 51
A^{-1}	multiplicative inverse of the matrix A, 52
aRb	element a has the relation R to element b, 57
$[a]$	equivalence class containing a, 59
$\bigcup_{\lambda \in \mathcal{L}} A_\lambda$	union of the collection of sets A_λ, 60

$\bigcap_{\lambda \in \mathcal{L}} A_\lambda$	intersection of the collection of sets A_λ, 60
$a \mid b$, $a \nmid b$	a divides b, a does not divide b, 84
(a, b), gcd (a, b)	greatest common divisor of a and b, 91
$[a, b]$, lcm (a, b)	least common multiple of a and b, 96
$x \equiv y \pmod{n}$	x is congruent to y modulo n, 99
$[0], [1], \ldots, [n-1]$	congruence classes modulo n, 101
$\mathbf{Z}_n$	set of congruence classes modulo n, 111
$a \bmod n$	remainder when a is divided by n, 129
$o(G), \lvert G \rvert$	order of the group G, 145
$GL(n, \mathbf{R})$	general linear group of degree n over $\mathbf{R}$, 147
$Z(G)$	center of the group G, 164
C_a	centralizer of the element a in G, 165
$\langle a \rangle$	subgroup generated by the element a, 165
$SL(2, \mathbf{R})$	special linear group of order 2 over $\mathbf{R}$, 168
$o(a), \lvert a \rvert$	order of the element a, 174
$\mathbf{U}_n$	group of units in $\mathbf{Z}_n$, 175
ker ϕ	kernel of ϕ, 194
S_n	symmetric group on n elements, 200
$(i_1, i_2, \ldots, i_r)$	cycle, 200
A_n	alternating group on n elements, 207
stab(a)	stabilizer of a, 212
D_n	dihedral group of order n, 218
AB	product of subsets of a group, 223
aH, Ha	left coset of H, right coset of H, 225
$[G:H]$	index of H in G, 227
$\langle A \rangle$	subgroup generated by the subset A, 234
$\mathcal{N}(H)$	normalizer of the subgroup H, 237
$a \equiv b \pmod{H}$	congruence modulo the subgroup H, 237
G/H	quotient group or factor group, 239
$H \times K$	internal direct product, 246
$H \otimes K$	external direct product, 246
$H_1 + H_2 + \cdots + H_n$	sum of subgroups of an abelian group, 247
$H_1 \oplus H_2 \oplus \cdots \oplus H_n$	direct sum of subgroups of an abelian group, 248
G_p	set of elements of G with order a power of p, 255
D^+	set of positive elements in D, 293
$x > y$ or $y < x$	order relation in an integral domain, 293
(a)	principal ideal generated by a, 304
$(a_1, a_2, \ldots, a_k)$	ideal generated by $a_1, a_2, \ldots, a_k$, 305
R/I	quotient ring, 306
$I_1 + I_2$	sum of two ideals, 308
$I_1 I_2$	product of two ideals, 309
l.u.b.	least upper bound, 333
$\bar{z}$	conjugate of the complex number z, 344
$R[x]$	ring of polynomials in x over R, 361
$f(x) \mid g(x), f(x) \nmid g(x)$	$f(x)$ divides $g(x)$, $f(x)$ does not divide $g(x)$, 373
D^2	discriminant of $f(x) = (x - c_1)(x - c_2)(x - c_3)$, 411
$(p(x))$	principal ideal generated by $p(x)$, 415
$F(\alpha)$	simple algebraic extension of F, 422
$\forall$	universal quantifier, 429
$\exists$	existential quantifier, 429
$\ni$	"such that," 429
$\sim p$	negation of p, 431
$\wedge$	conjuction, 432
$\vee$	disjunction, 432

EIGHTH EDITION

Elements of Modern Algebra

Linda Gilbert
University of South Carolina Upstate
Jimmie Gilbert
Late of University of South Carolina Upstate

CENGAGE Learning®

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

CENGAGE Learning

Elements of Modern Algebra, Eighth Edition
Linda Gilbert, Jimmie Gilbert

Senior Product Team Manager: Richard Stratton

Senior Product Manager: Molly Taylor

Senior Content Developer: Erin Brown

Content Coordinators: Lauren Crosby and Cynthia Ashton

Product Assistants: Danielle Hallock and Shaylin Walsh

Media Developer: Andrew Coppola

Senior Marketing Manager: Gordon Lee

Market Development Manager: Ryan Ahern

Art and Cover Direction, Production Management, and Composition: PreMediaGlobal

Manufacturing Planner: Doug Bertke

Rights Acquisitions Specialist: Shalice Shah-Caldwell

Cover Image: © echo3005/Shutterstock

Library of Congress Control Number: 2013942826

ISBN-13: 978-1-285-46323-0

ISBN-10: 1-285-46323-4

Cengage Learning
200 First Stamford Place, 4th Floor
Stamford, CT 06902
USA

Printed in the United States of America
1 2 3 4 5 6 7 17 16 15 14 13

To: Jimmie

~~Linda

Contents

Preface

As the earlier editions were, this book is intended as a text for an introductory course in algebraic structures (groups, rings, fields, and so forth). Such a course is often used to bridge the gap from manipulative to theoretical mathematics and to help prepare secondary mathematics teachers for their careers.

A minimal amount of mathematical maturity is assumed in the text; a major goal is to develop mathematical maturity. The material is presented in a theorem-proof format, with definitions and major results easily located, thanks to a user-friendly format. The treatment is rigorous and self-contained, in keeping with the objectives of training the student in the techniques of algebra and providing a bridge to higher-level mathematical courses.

Groups appear in the text before rings. The standard topics in elementary group theory are included, and the last two sections in Chapter 4 provide an optional sample of more advanced work in finite abelian groups.

The treatment of the set $\mathbf{Z}_n$ of congruence classes modulo n is a unique and popular feature of this text, in that it threads throughout most of the book. The first contact with $\mathbf{Z}_n$ is early in Chapter 2, where it appears as a set of equivalence classes. Binary operations of addition and multiplication are defined in $\mathbf{Z}_n$ at a later point in that chapter. Both the additive and multiplicative structures are drawn upon for examples in Chapters 3 and 4. The development of $\mathbf{Z}_n$ continues in Chapter 5, where it appears in its familiar context as a ring. This development culminates in Chapter 6 with the final description of $\mathbf{Z}_n$ as a quotient ring of the integers by the principal ideal (n). Later, in Chapter 8, the use of $\mathbf{Z}_n$ as a ring over which polynomials are defined, provides some interesting results.

Some flexibility is provided by including more material than would normally be taught in one course, and a dependency diagram of the chapters/sections (Figure P.1) is included at the end of this preface. Several sections are marked "optional" and may be skipped by instructors who prefer to spend more time on later topics.

Several users of the text have inquired as to what material the authors themselves teach in their courses. Our basic goal in a single course has always been to reach the end of Section 5.3 "The Field of Quotients of an Integral Domain," omitting the last two sections of Chapter 4 along the way. Other optional sections could also be omitted if class meetings are in short supply. The sections on applications naturally lend themselves well to outside student projects involving additional writing and research.

For the most part, the problems in an exercise set are arranged in order of difficulty, with easier problems first, but exceptions to this arrangement occur if it violates logical order. If one problem is needed or useful in another problem, the more basic problem appears first. When teaching from this text, we use a ground rule that any previous result, including prior exercises, may be used in constructing a proof. Whether to adopt this ground rule is, of course, completely optional.

Some users have indicated that they omit Chapter 7 (Real and Complex Numbers) because their students are already familiar with it. Others cover Chapter 8 (Polynomials) before Chapter 7. These and other options are diagrammed in Figure P.1 at the end of this preface.

The following *user-friendly* features are retained from the seventh edition:

- **Descriptive labels and titles** are placed on definitions and theorems to indicate their content and relevance.
- **Strategy boxes** that give guidance and explanation about techniques of proof are included. This feature forms a component of the bridge that enables students to become more proficient in constructing proofs.
- **Marginal labels and symbolic notes** such as Existence, Uniqueness, Induction, "$(p \wedge q) \Rightarrow r$" and "$\sim p \Leftarrow (\sim q \wedge \sim r)$" are used to help students analyze the logic in the proofs of theorems without interrupting the natural flow of the proof.
- A **reference system** provides guideposts to continuations and interconnections of exercises throughout the text. For example, consider Exercise 14 in Section 4.4. The marginal notation "Sec. 3.3, #11 $\gg$" indicates that Exercise 14 of Section 4.4 is *connected* to Exercise 11 in the *earlier* Section 3.3. The marginal notation "Sec. 4.8, #7 $\ll$" indicates that Exercise 14 of Section 4.4 has a *continuation* in Exercise 7 of Section 4.8. Instructors, as well as students, have found this system useful in anticipating which exercises are needed or helpful in later sections/chapters.
- An **appendix** on the basics of logic and methods of proof is included.
- A **biographical sketch** of a great mathematician whose contributions are relevant to that material concludes each chapter.
- A **gradual introduction and development** of concepts is used, proceeding from the simplest structures to the more complex.
- **Repeated exposure** to topics occurs, whenever possible, to reinforce concepts and enhance learning.
- An **abundance of examples** that are designed to develop the student's intuition are included.
- Enough **exercises** to allow instructors to make different assignments of approximately the same difficulty are included.
- **Exercise sets** are designed to develop the student's maturity and ability to construct proofs. They contain many problems that are elementary or of a computational nature.
- **True/False** statements that encourage the students to thoroughly understand the statements of definitions and the results of theorems are placed at the beginning of the exercise sets.
- A **summary of key words and phrases** is included at the end of each chapter.
- A **list of special notations** used in the book appears on the front endpapers.
- **Group tables** for the most common examples are on the back endpapers.
- An **updated bibliography** is included.

I am very grateful to the reviewers for their thoughtful suggestions and have incorporated many in this edition. The most notable include the following:

- **Alerts** that draw attention to counterexamples, special cases, proper symbol or terminology usage, and common misconceptions. Frequently these alerts lead to True/False statements in the exercises that further reinforce the precision required in mathematical communication.
- More emphasis placed on **special groups** such as the general linear and special linear groups, the dihedral groups, and the group of units.
- Moving some **definitions** from the exercises to the sections for greater emphasis.
- Using marginal notes to outline the **steps of the induction arguments** required in the examples.
- Adding over **200 new exercises**, both theoretical and computational in nature.
- Minor rewriting throughout, including many **new examples**.

Acknowledgments

Jimmie and I have been extremely fortunate to have had such knowledgeable reviewers offering helpful comments, suggestions for improvements, and corrections for this and earlier editions. Those reviewers and their affiliations are as follows:

Lateef A. Adelani, *Harris-Stowe College*
Philip C. Almes, *Wayland Baptist University*
John Barkanic, *Desales University*
Edwin F. Baumgartner, *Le Moyne College*
Dave Bayer, *Barnard College*
Brian Beasley, *Presbyterian College*
Joan E. Bell, *Northeastern State University*
Bruce M. Bemis, *Westminster College*
Steve Benson, *St. Olaf College*
Louise M. Berard, *Wilkes College*
Thomas D. Bishop, *Arkansas State University*
David M. Bloom, *Brooklyn College of the City University of New York*
Elizabeth Bodine, *Cabrini College*
James C. Bradford, *Abilene Christian University*
Shirley Branan, *Birmingham Southern College*
Joel Brawley, *Clemson University*
Gordon Brown, *University of Colorado, Boulder*
Harmon C. Brown, *Harding University*
Holly Buchanan, *West Liberty University*
Marshall Cates, *California State University, Los Angeles*
Patrick Costello, *Eastern Kentucky University*
Richard Cowan, *Shorter College*
Daniel Daly, *Southeast Missouri State University*
Elwyn H. Davis, *Pittsburg State University*
David J. DeVries, *Georgia College*
Jill DeWitt, *Baker College of Muskegon*
John D. Elwin, *San Diego State University*
Sharon Emerson-Stonnell, *Longwood University*
Paul J. Fairbanks, *Bridgewater State College*
Howard Frisinger, *Colorado State University*
Marcus Greferath, *San Diego State University*
Jacqueline Hall, *Longwood University*
Nickolas Heerema, *Florida State University*
Edward K. Hinson, *University of New Hampshire*

J. Taylor Hollist, *State University of New York at Oneonta*
David L. Johnson, *Lehigh University*
Kenneth Kalmanson, *Montclair State University*
William J. Keane, *Boston College*
William F. Keigher, *Rutgers University*
Robert E. Kennedy, *Central Missouri State University*
Andre E. Kezdy, *University of Louisville*
Stanley M. Lukawecki, *Clemson University*
Joan S. Morrison, *Goucher College*
Richard J. Painter, *Colorado State University*
Carl R. Spitznagel, *John Carroll University*
Ralph C. Steinlage, *University of Dayton*
James J. Tattersall, *Providence College*
Mark L. Teply, *University of Wisconsin–Milwaukee*
Krishnanand Verma, *University of Minnesota, Duluth*
Robert P. Webber, *Longwood College*
Diana Y. Wei, *Norfolk State University*
Carroll G. Wells, *Western Kentucky University*
Burdette C. Wheaton, *Mankato State University*
John Woods, *Southwestern Oklahoma State University*
Henry Wyzinski, *Indiana University Northwest*

Special thanks go to Molly Taylor, whose encouragement brought this project to life; to Erin Brown, who nurtured it to maturity; and to Arul Joseph Raj, whose efficient production supervision groomed the final product. Additionally, I wish to express my most sincere gratitude to others: Richard Stratton, Shaylin Walsh, Lauren Crosby, and Danielle Hallock for their outstanding editorial guidance; to Margaret Bridges, Cathy Richmond Robinson, and Kristina Mose-Libon for their excellent work in production; to Ryan Ahern and Lauren Beck for their expert marketing efforts; and, to Ian Crewe and Eric Howe for their remarkable accuracy checks.

Finally, my sincere thanks go to Beckie who is so dear to me; to Matt, who never wavered in his support of me; and to Morgan, who very patiently waited, and waited, and waited for me to complete this project so that we could go fishing.

Linda Gilbert

Chapters/Sections Dependency Diagram

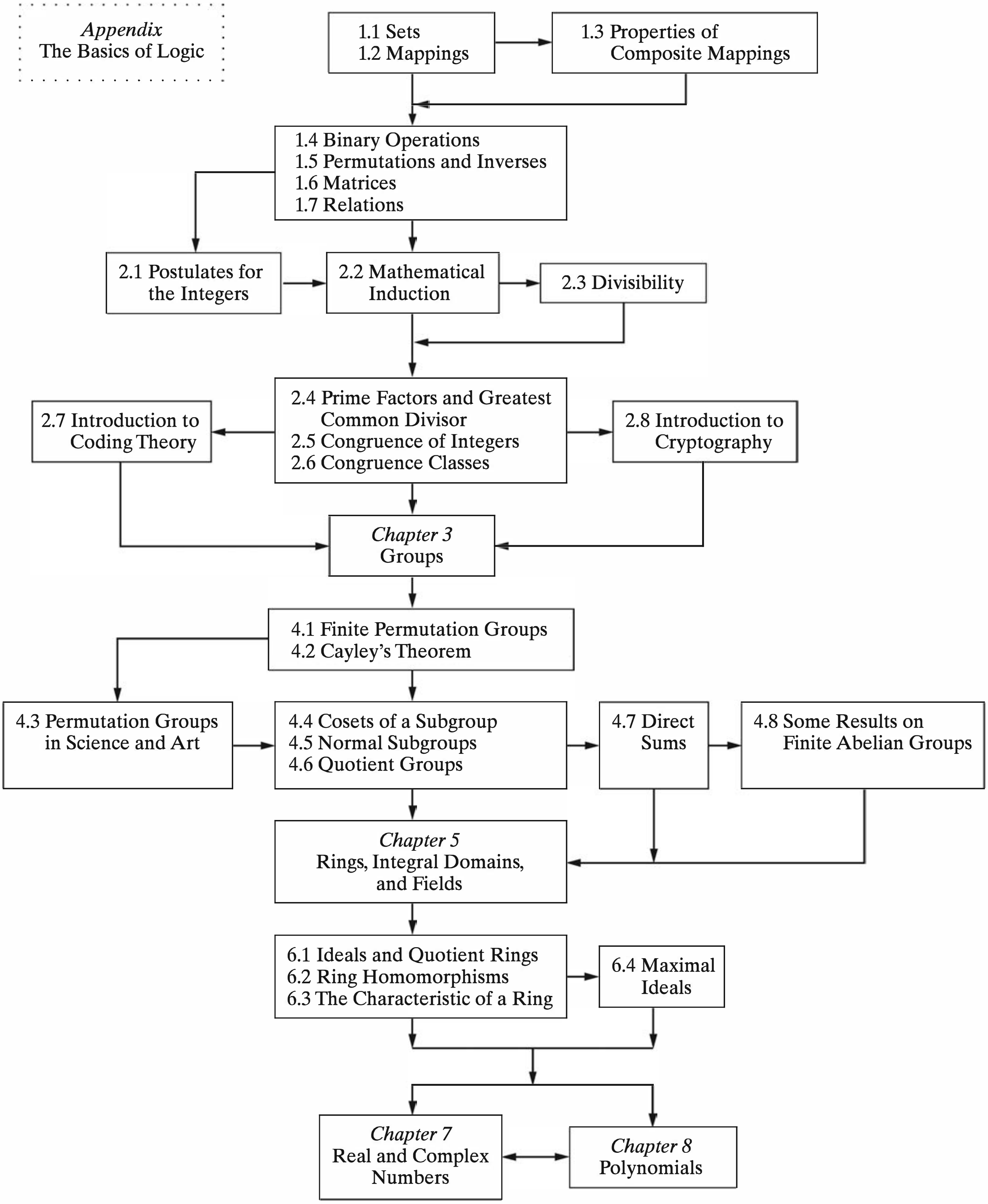


Figure P.1

CHAPTER ONE

Fundamentals

Introduction

This chapter presents the fundamental concepts of set, mapping, binary operation, and relation. It also contains a section on matrices, which will serve as a basis for examples and exercises from time to time in the remainder of the text. Much of the material in this chapter may be familiar from earlier courses. If that is the case, appropriate omissions can be made to expedite the study of later topics.

1.1 Sets

Abstract algebra had its beginnings in attempts to address mathematical problems such as the solution of polynomial equations by radicals and geometric constructions with straightedge and compass. From the solutions of specific problems, general techniques evolved that could be used to solve problems of the same type, and treatments were generalized to deal with whole classes of problems rather than individual ones.

In our study of abstract algebra, we shall make use of our knowledge of the various number systems. At the same time, in many cases we wish to examine how certain properties are consequences of other, known properties. This sort of examination deepens our understanding of the system. As we proceed, we shall be careful to distinguish between the properties we have assumed and made available for use and those that must be deduced from these properties. We must accept without definition some terms that are basic objects in our mathematical systems. Initial assumptions about each system are formulated using these undefined terms.

One such undefined term is **set**. We think of a set as a collection of objects about which it is possible to determine whether or not a particular object is a member of the set. Sets are usually denoted by capital letters and are sometimes described by a list of their elements, as illustrated in the following examples.

Example 1 We write

$$A = \{0, 1, 2, 3\}$$

to indicate that the set A contains the elements 0, 1, 2, 3, and no other elements. The notation $\{0, 1, 2, 3\}$ is read as "the set with elements 0, 1, 2, and 3." ■

Example 2 The set B, consisting of all the nonnegative integers, is written as

$$B = \{0, 1, 2, 3, \dots\}.$$

The three dots $\dots$, called an *ellipsis*, mean that the pattern established before the dots continues indefinitely. The notation $\{0, 1, 2, 3, \dots\}$ is read as "the set with elements 0, 1, 2, 3, and so on." ■

As in Examples 1 and 2, it is customary to avoid repetition when listing the elements of a set. Another way of describing sets is called *set-builder notation*. Set-builder notation uses braces to enclose a property that is the qualification for membership in the set.

Example 3 The set B in Example 2 can be described using set-builder notation as

$$B = \{x \mid x \text{ is a nonnegative integer}\}.$$

The vertical slash is shorthand for "such that," and we read "B is the set of all x such that x is a nonnegative integer." ■

There is also a shorthand notation for "is an element of." We write "$x \in A$" to mean "x is an element of the set A." We write "$x \notin A$" to mean "x is not an element of the set A." For the set A in Example 1, we can write

$$2 \in A \quad \text{and} \quad 7 \notin A.$$

Definition 1.1 ■ Subset

Let A and B be sets. Then A is called a **subset** of B if and only if every element of A is an element of B. Either the notation $A \subseteq B$ or the notation $B \supseteq A$ indicates that A is a subset of B.

The notation $A \subseteq B$ is read as "A is a subset of B" or "A is contained in B." Also, $B \supseteq A$ is read as "B contains A." The symbol $\in$ is reserved for elements, whereas the symbol $\subseteq$ is reserved for subsets.

ALERT

Example 4 We write

$$a \in \{a, b, c, d\} \quad \text{or} \quad \{a\} \subseteq \{a, b, c, d\}.$$

However,

$$a \subseteq \{a, b, c, d\} \quad \text{and} \quad \{a\} \in \{a, b, c, d\}$$

are both *incorrect* uses of set notation. ■

Definition 1.2 ■ Equality of Sets

Two sets are **equal** if and only if they contain exactly the same elements.

The sets A and B are equal, and we write $A = B$, if each member of A is also a member of B and if each member of B is also a member of A.

Strategy ■ Typically, a proof that two sets are equal is presented in two parts. The first shows that $A \subseteq B$, the second that $B \subseteq A$. We then conclude that $A = B$. On the other hand, to prove that $A \neq B$, one method that can be used is to exhibit an element that is in either set A or set B but is not in both.

We illustrate this strategy in the next example.

Example 5 Suppose $A = \{1, 1\}$, $B = \{-1, 1\}$, and $C = \{1\}$. Now $A = C$ since $A \subseteq C$ and $A \supseteq C$, whereas $A \neq B$ since $-1 \in B$ but $-1 \notin A$. ■

Definition 1.3 ■ Proper Subset

If A and B are sets, then A is a **proper subset** of B if and only if $A \subseteq B$ and $A \neq B$.

We sometimes write $A \subset B$ to denote that A is a proper subset of B.

Example 6 The following statements illustrate the notation for proper subsets and equality of sets.

$$\{1, 2, 4\} \subset \{1, 2, 3, 4, 5\} \qquad \{a, c\} = \{c, a\}$$ ■

There are two basic operations, *union* and *intersection*, that are used to combine sets. These operations are defined as follows.

Definition 1.4 ■ Union, Intersection

If A and B are sets, the **union** of A and B is the set $A \cup B$ (read "A union B"), given by

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

The **intersection** of A and B is the set $A \cap B$ (read "A intersection B"), given by

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

The union of two sets A and B is the set whose elements are either in A or in B or are in both A and B. The intersection of sets A and B is the set of those elements common to both A and B.

Example 7 Suppose $A = \{2, 4, 6\}$ and $B = \{4, 5, 6, 7\}$. Then

$$A \cup B = \{2, 4, 5, 6, 7\}$$

and

$$A \cap B = \{4, 6\}.$$ ■

The operations of union and intersection of two sets have some properties that are analagous to properties of addition and multiplication of numbers.

Example 8 It is easy to see that for any sets A and B, $A \cup B = B \cup A$:

$$\begin{aligned} A \cup B &= \{x \mid x \in A \text{ or } x \in B\} \\ &= \{x \mid x \in B \text{ or } x \in A\} \\ &= B \cup A. \end{aligned}$$

Because of the fact that $A \cup B = B \cup A$, we say that the operation union has the **commutative property**. It is just as easy to show that $A \cap B = B \cap A$, and we say also that the operation intersection has the commutative property. ■

It is easy to find sets that have no elements at all in common. For example, the sets

$$A = \{1, -1\} \quad \text{and} \quad B = \{0, 2, 3\}$$

have no elements in common. Hence, there are no elements in their intersection, $A \cap B$, and we say that the intersection is *empty*. Thus it is logical to introduce the *empty set*.

Definition 1.5 ■ Empty Set, Disjoint Sets

The **empty set** is the set that has no elements, and the empty set is denoted by $\emptyset$ or $\{\ \}$. Two sets A and B are called **disjoint** if and only if $A \cap B = \emptyset$.

The sets $\{1, -1\}$ and $\{0, 2, 3\}$ are disjoint, since

$$\{1, -1\} \cap \{0, 2, 3\} = \emptyset.$$

There is only one empty set $\emptyset$, and $\emptyset$ is a subset of every set.

Strategy ■ To show that A is not a subset of B, we must find an element in A that is not in B.

That the empty set $\emptyset$ is a subset of any set A follows from the fact that $a \in \emptyset$ is always false. Thus

$$a \in \emptyset \text{ implies } a \in A$$

must be true. (See the truth table in Figure A.4 of the appendix.)

For a set A with n elements (n a nonnegative integer), we can write out all the subsets of A. For example, if

$$A = \{a, b, c\},$$

then the subsets of A are

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A.$$

Definition 1.6 ■ Power Set

For any set A, the **power set** of A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A and is written

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Example 9 For $A = \{a, b, c\}$, the power set of A is

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A\}. \qquad \blacksquare$$

It is often helpful to draw a picture or diagram of the sets under discussion. When we do this, we assume that all the sets we are dealing with, along with all possible unions and intersections of those sets, are subsets of some **universal set**, denoted by U. In Figure 1.1, we let two overlapping circles represent the two sets A and B. The sets A and B are subsets of the universal set U, represented by the rectangle. Hence the circles are contained in the rectangle. The intersection of A and B, $A \cap B$, is the crosshatched region where the two circles overlap. This type of pictorial representation is called a **Venn diagram**.

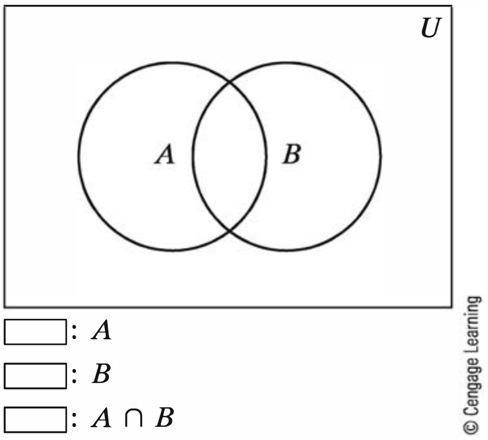


Figure 1.1

Another special subset is defined next.

Definition 1.7 ■ Complement

For arbitrary subsets A and B of the universal set U, the **complement** of B in A is

$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}.$$

The special notation A' is reserved for a particular complement, $U - A$:

$$A' = U - A = \{x \in U \mid x \notin A\}.$$

We read A' simply as "the complement of A" rather than as "the complement of A in U."

Example 10 Let

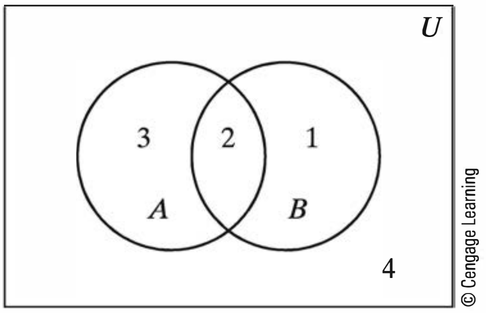
$$U = \{x \mid x \text{ is an integer}\}$$
$$A = \{x \mid x \text{ is an even integer}\}$$
$$B = \{x \mid x \text{ is a positive integer}\}.$$

Then

$$\begin{aligned} B - A &= \{x \mid x \text{ is a positive odd integer}\} \\ &= \{1, 3, 5, 7, \ldots\} \\ A - B &= \{x \mid x \text{ is a nonpositive even integer}\} \\ &= \{0, -2, -4, -6, \ldots\} \\ A' &= \{x \mid x \text{ is an odd integer}\} \\ &= \{\ldots, -3, -1, 1, 3, \ldots\} \\ B' &= \{x \mid x \text{ is a nonpositive integer}\} \\ &= \{0, -1, -2, -3, \ldots\}. \end{aligned}$$

■

Example 11 The overlapping circles representing the sets A and B separate the interior of the rectangle representing U into four regions, labeled 1, 2, 3, and 4, in the Venn diagram in Figure 1.2. Each region represents a particular subset of U.



■ **Figure 1.2**

Region 1: $B - A$
Region 2: $A \cap B$
Region 3: $A - B$
Region 4: $(A \cup B)'$

■

Many of the examples and exercises in this book involve familiar systems of numbers, and we adopt the following standard notations for some of these systems:

Z denotes the set of all **integers**.

$\mathbf{Z}^+$ denotes the set of all **positive integers**.

Q denotes the set of all **rational numbers**.

R denotes the set of all **real numbers**.

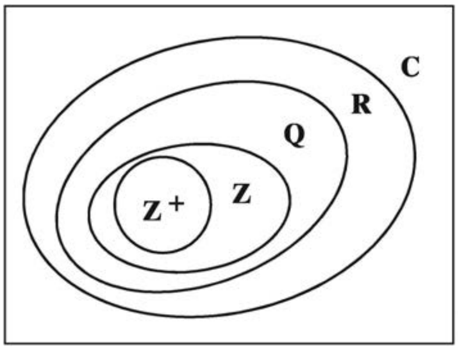
$\mathbf{R}^+$ denotes the set of all **positive real numbers**.

C denotes the set of all **complex numbers**.

We recall that a **complex number** is defined as a number of the form $a + bi$, where a and b are real numbers and $i = \sqrt{-1}$. Also, a real number x is **rational** if and only if x can be written as a quotient of integers that has a nonzero denominator. That is,

$$\mathbf{Q} = \left\{ \frac{m}{n} \;\middle|\; m \in \mathbf{Z}, n \in \mathbf{Z}, \text{ and } n \neq 0 \right\}.$$

The relationships that some of the number systems have to each other are indicated by the Venn diagram in Figure 1.3.



© Cengage Learning

■ **Figure 1.3** $\mathbf{Z}^+ \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$

Our work in this book usually assumes a knowledge of the various number systems that would be familiar from a precalculus or college algebra course. Some exceptions occur when we wish to examine how certain properties are consequences of other properties in a particular system. Exceptions of this kind occur with the integers in Chapter 2 and the complex numbers in Chapter 7, and these exceptions are clearly indicated when they occur.

The operations of union and intersection can be applied repeatedly. For instance, we might form the intersection of A and B, obtaining $A \cap B$, and then form the intersection of this set with a third set C: $(A \cap B) \cap C$.

Example 12 The sets $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are equal, since

$$\begin{aligned}(A \cap B) \cap C &= \{x \mid x \in A \text{ and } x \in B\} \cap C \\ &= \{x \mid x \in A \text{ and } x \in B \text{ and } x \in C\} \\ &= A \cap \{x \mid x \in B \text{ and } x \in C\} \\ &= A \cap (B \cap C).\end{aligned}$$

In analogy with the associative property

$$(x + y) + z = x + (y + z)$$

for addition of numbers, we say that the operation of intersection is **associative**. When we work with numbers, we drop the parentheses for convenience and write

$$x + y + z = x + (y + z) = (x + y) + z.$$

Similarly, for sets A, B, and C, we write

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

■

Just as simply, we can show (see Exercise 18 in this section) that the union of sets is an associative operation. We write

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

Example 13 A separation of a nonempty set A into mutually disjoint nonempty subsets is called a **partition** of the set A. If

$$A = \{a, b, c, d, e, f\},$$

then one partition of A is

$$X_1 = \{a, d\}, \qquad X_2 = \{b, c, f\}, \qquad X_3 = \{e\},$$

since

$$A = X_1 \cup X_2 \cup X_3$$

with $X_1 \neq \emptyset$, $X_2 \neq \emptyset$, $X_3 \neq \emptyset$, and

$$X_1 \cap X_2 = \emptyset, \qquad X_1 \cap X_3 = \emptyset, \qquad X_2 \cap X_3 = \emptyset.$$

The concept of a partition is fundamental to many of the topics encountered later in this book. ■

The operations of intersection, union, and forming complements can be combined in all sorts of ways, and several nice equalities that relate some of these results can be obtained. For example, it can be shown that

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

and that

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

Because of the resemblance between these equations and the familiar distributive property $x(y + z) = xy + xz$ for numbers, we call these equations **distributive properties**.

We shall prove the first of these distributive properties in the next example and leave the last one as an exercise. To prove the first, we shall show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. This illustrates the point made earlier in the discussion of equality of sets, highlighted in the strategy box, after Definition 1.2.

The symbol $\Rightarrow$ is shorthand for "implies," and $\Leftarrow$ is shorthand for "is implied by." We use them in the next example.

Example 14 To prove

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

we first let $x \in A \cap (B \cup C)$. Now

$$\begin{aligned}
x \in A \cap (B \cup C) &\Rightarrow x \in A \quad \text{and} \quad x \in (B \cup C) \\
&\Rightarrow x \in A, \quad \text{and} \quad x \in B \quad \text{or} \quad x \in C \\
&\Rightarrow x \in A \quad \text{and} \quad x \in B, \quad \text{or} \quad x \in A \quad \text{and} \quad x \in C \\
&\Rightarrow x \in A \cap B, \quad \text{or} \quad x \in A \cap C \\
&\Rightarrow x \in (A \cap B) \cup (A \cap C).
\end{aligned}$$

Thus $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Conversely, suppose $x \in (A \cap B) \cup (A \cap C)$. Then

$$\begin{aligned} x \in (A \cap B) \cup (A \cap C) &\Rightarrow x \in A \cap B, \quad \text{or} \quad x \in A \cap C \\ &\Rightarrow x \in A \quad \text{and} \quad x \in B, \quad \text{or} \quad x \in A \quad \text{and} \quad x \in C \\ &\Rightarrow x \in A, \quad \text{and} \quad x \in B \quad \text{or} \quad x \in C \\ &\Rightarrow x \in A \quad \text{and} \quad x \in (B \cup C) \\ &\Rightarrow x \in A \cap (B \cup C). \end{aligned}$$

Therefore, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, and we have shown that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

It should be evident that the second part of the proof can be obtained from the first simply by reversing the steps. That is, when each $\Rightarrow$ is replaced by $\Leftarrow$, a valid implication results. In fact, then, we could obtain a proof of both parts by replacing $\Rightarrow$ with $\Leftrightarrow$, where $\Leftrightarrow$ is short for "if and only if." Thus

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \quad \text{and} \quad x \in (B \cup C) \\ &\Leftrightarrow x \in A, \quad \text{and} \quad x \in B \quad \text{or} \quad x \in C \\ &\Leftrightarrow x \in A \quad \text{and} \quad x \in B, \quad \text{or} \quad x \in A \quad \text{and} \quad x \in C \\ &\Leftrightarrow x \in A \cap B, \quad \text{or} \quad x \in A \cap C \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

■

Strategy ■ In proving an equality of sets S and T, we can often use the technique of showing that $S \subseteq T$ and then check to see whether the steps are reversible. In many cases, the steps are indeed reversible, and we obtain the other part of the proof easily. However, this method should not obscure the fact that there are still two parts to the argument: $S \subseteq T$ and $T \subseteq S$.

There are some interesting relations between complements and unions or intersections. For example, it is true that

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

This statement is one of two that are known as **De Morgan's† Laws**. De Morgan's other law is the statement that

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

Stated somewhat loosely in words, the first law says that the complement of an intersection is the union of the individual complements. The second similarly says that the complement of a union is the intersection of the individual complements.

†Augustus De Morgan (1806–1871) coined the term mathematical induction and is responsible for rigorously defining the concept. Not only does he have laws of logic bearing his name but also the headquarters of the London Mathematical Society and a crater on the moon.

Exercises 1.1

True or False

Label each of the following statements as either true or false.

1. Two sets are equal if and only if they contain exactly the same elements.
2. If A is a subset of B and B is a subset of A, then A and B are equal.
3. The empty set is a subset of every set except itself.
4. $A - A = \emptyset$ for all sets A.
5. $A \cup A = A \cap A$ for all sets A.
6. $A \subset A$ for all sets A.
7. $\{a, b\} = \{b, a\}$
8. $\{a, b\} = \{b, a, b\}$
9. $A - B = C - B$ implies $A = C$, for all sets A, B, and C.
10. $A - B = A - C$ implies $B = C$, for all sets A, B, and C.

Exercises

1. For each set A, describe A by indicating a property that is a qualification for membership in A.

   a. $A = \{0, 2, 4, 6, 8, 10\}$ **b.** $A = \{1, -1\}$

   c. $A = \{-1, -2, -3, \dots\}$ **d.** $A = \{1, 4, 9, 16, 25, \dots\}$

2. Decide whether or not each statement is true for $A = \{2, 7, 11\}$ and $B = \{1, 2, 9, 10, 11\}$.

   a. $2 \subseteq A$ **b.** $\{11, 2, 7\} \subseteq A$

   c. $2 = A \cap B$ **d.** $\{7, 11\} \in A$

   e. $A \subseteq B$ **f.** $\{7, 11, 2\} = A$

3. Decide whether or not each statement is true.

   a. $a \in \{a, \{a\}\}$ **b.** $\{a\} \in \{a, \{a\}\}$

   c. $\{a\} \subseteq \{a, \{a\}\}$ **d.** $\{\{a\}\} \subseteq \{a, \{a\}\}$

   e. $\emptyset \subseteq A$ **f.** $0 \in \emptyset$

   g. $\emptyset \in \{\emptyset\}$ **h.** $\emptyset \subseteq \{\emptyset\}$

   i. $\{\emptyset\} \subseteq \emptyset$ **j.** $\{\emptyset\} = \emptyset$

   k. $\emptyset \in \emptyset$ **l.** $\emptyset \subseteq \emptyset$

4. Decide whether or not each of the following is true for all sets A, B, and C.

   a. $B \cup A \subseteq A$ **b.** $B \cap A \subseteq A \cup B$

   c. $A \subseteq A \cup B$ **d.** $A \cup B \subseteq A \cap B$

   e. $A \cap A' = \emptyset$ **f.** $A \cap \emptyset = A \cup \emptyset$

   g. $A \cap (B \cup C) = A \cup (B \cap C)$ **h.** $A \cup (B' \cap C') = A \cup (B \cup C)'$

i. $A \cup (B \cap C) = (A \cup B) \cap C$ **j.** $(A \cap B) \cup C = A \cap (B \cup C)$

k. $A \cup (B \cap C) = (A \cap C) \cup (B \cap C)$ **l.** $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$

5. Evaluate each of the following sets, where

$$U = \{0, 1, 2, 3, \ldots, 10\}$$
$$A = \{0, 1, 2, 3, 4, 5\}$$
$$B = \{0, 2, 4, 6, 8, 10\}$$
$$C = \{2, 3, 5, 7\}.$$

a. $A \cup B$ **b.** $A \cap C$ **c.** $A' \cup B$

d. $A \cap B \cap C$ **e.** $A' \cap B \cap C$ **f.** $A \cup (B \cap C)$

g. $A \cap (B \cup C)$ **h.** $(A \cup B')'$ **i.** $A - B$

j. $B - A$ **k.** $A - (B - C)$ **l.** $C - (B - A)$

m. $(A - B) \cap (C - B)$ **n.** $(A - B) \cap (A - C)$

6. Determine whether each of the following is either A, A', U, or $\varnothing$, where A is an arbitrary subset of the universal set U.

a. $A \cap A$ **b.** $A \cup A$

c. $A \cap A'$ **d.** $A \cup A'$

e. $A \cup \varnothing$ **f.** $A \cap \varnothing$

g. $A \cap U$ **h.** $A \cup U$

i. $U \cup A'$ **j.** $A - \varnothing$

k. $\varnothing'$ **l.** U'

m. $(A')'$ **n.** $\varnothing - A$

7. Write out the power set, $\mathcal{P}(A)$, for each set A.

a. $A = \{a\}$ **b.** $A = \{0, 1\}$

Sec. 3.1, #43–45 ⋞ **c.** $A = \{a, b, c\}$ **d.** $A = \{1, 2, 3, 4\}$

e. $A = \{1, \{1\}\}$ **f.** $A = \{\{1\}\}$

g. $A = \{\varnothing\}$ **h.** $A = \{\varnothing, \{\varnothing\}\}$

8. Describe two partitions of each of the following sets.

a. $\{x \mid x \text{ is an integer}\}$ **b.** $\{a, b, c, d\}$

c. $\{1, 5, 9, 11, 15\}$ **d.** $\{x \mid x \text{ is a complex number}\}$

9. Write out all the different partitions of the given set A.

a. $A = \{1, 2, 3\}$ **b.** $A = \{1, 2, 3, 4\}$

10. Suppose the set A has n elements where $n \in \mathbf{Z}^+$.

a. How many elements does the power set $\mathcal{P}(A)$ have?

Sec. 2.2, #37–40 ⋞ **b.** If $0 \le k \le n$, how many elements of the power set $\mathcal{P}(A)$ contain exactly k elements?

11. State the most general conditions on the subsets A and B of U under which the given equality holds.

a. $A \cap B = A$
b. $A \cup B' = A$
c. $A \cup B = A$
d. $A \cap B' = A$
e. $A \cap B = U$
f. $A' \cap B' = \emptyset$
g. $A \cup \emptyset = U$
h. $A' \cap U = \emptyset$

12. Let $\mathbf{Z}$ denote the set of all integers, and let

$$A = \{x \mid x = 3p - 2 \text{ for some } p \in \mathbf{Z}\}$$
$$B = \{x \mid x = 3q + 1 \text{ for some } q \in \mathbf{Z}\}.$$

Prove that $A = B$.

13. Let $\mathbf{Z}$ denote the set of all integers, and let

$$C = \{x \mid x = 3r - 1 \text{ for some } r \in \mathbf{Z}\}$$
$$D = \{x \mid x = 3s + 2 \text{ for some } s \in \mathbf{Z}\}.$$

Prove that $C = D$.

In Exercises 14–35, prove each statement.

14. $A \cap B \subseteq A \cup B$

15. $(A')' = A$

16. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

17. $A \subseteq B$ if and only if $B' \subseteq A'$.

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

19. $(A \cup B)' = A' \cap B'$

20. $(A \cap B)' = A' \cup B'$

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

22. $A \cap (A' \cup B) = A \cap B$

23. $A \cup (A' \cap B) = A \cup B$

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

25. If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.

26. If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

27. $B - A = B \cap A'$

28. $A \cap (B - A) = \emptyset$

29. $A \cup (B - A) = A \cup B$

30. $(A \cup B) - C = (A - C) \cup (B - C)$

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

32. $U - (A \cap B) = (U - A) \cup (U - B)$

33. $U - (A \cup B) = (U - A) \cap (U - B)$

34. $A \subseteq B$ if and only if $A \cup B = B$.

35. $A \subseteq B$ if and only if $A \cap B = A$.

36. Prove or disprove that $A \cup B = A \cup C$ implies $B = C$.

37. Prove or disprove that $A \cap B = A \cap C$ implies $B = C$.

38. Prove or disprove that $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

39. Prove or disprove that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

40. Prove or disprove that $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$.

41. Express $(A \cup B) - (A \cap B)$ in terms of unions and intersections that involve A, A', B, and B'.

42. Let the operation of addition be defined on subsets A and B of U by $A + B = (A \cup B) - (A \cap B)$. Use a Venn diagram with labeled regions to illustrate each of the following statements.

a. $A + B = (A - B) \cup (B - A)$

b. $A + (B + C) = (A + B) + C$

c. $A \cap (B + C) = (A \cap B) + (A \cap C)$.

43. Let the operation of addition be as defined in Exercise 42. Prove each of the following statements.

a. $A + A = \emptyset$

b. $A + \emptyset = A$

1.2 Mappings

The concept of a function is fundamental to nearly all areas of mathematics. The term *function* is the one most widely used for the concept that we have in mind, but it has become traditional to use the terms *mapping* and *transformation* in algebra. It is likely that these words are used because they express an intuitive feel for the association between the elements involved. The basic idea is that correspondences of a certain type exist between the elements of two sets. There is to be a rule of association between the elements of a first set and those of a second set. The association is to be such that for each element in the first set, there is one and only one associated element in the second set. This rule of association leads to a natural pairing of the elements that are to correspond, and then to the formal statement in Definition 1.9.

By an **ordered pair** of elements we mean a pairing (a, b), where there is to be a distinction between the pair (a, b) and the pair (b, a), if a and b are different. That is, there is to be a first position and a second position such that $(a, b) = (c, d)$ if and only if both $a = c$ and $b = d$. This ordering is altogether different from listing the elements of a set, for there the order of listing is of no consequence at all. The sets $\{1, 2\}$ and $\{2, 1\}$ have exactly the same elements, and $\{1, 2\} = \{2, 1\}$. When we speak of ordered pairs, however, we do not consider $(1, 2)$ and $(2, 1)$ equal. With these ideas in mind, we make the following definition.

ALERT

Definition 1.8 ■ Cartesian† Product

For two nonempty sets A and B, the **Cartesian product** $A \times B$ is the set of all ordered pairs (a, b) of elements $a \in A$ and $b \in B$. That is,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Example 1 If $A = \{1, 2\}$ and $B = \{3, 4, 5\}$, then

$$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}.$$

†The Cartesian product is named for René Descartes (1596–1650), who has been called the "Father of Modern Philosophy" and the "Father of Modern Mathematics."

ALERT We observe that the order in which the sets appear is important. In this example,

$$B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2), (5, 1), (5, 2)\},$$

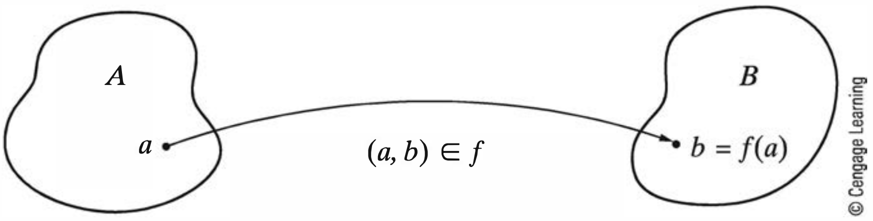
so $A \times B$ and $B \times A$ are quite distinct from each other. ■

We now make our formal definition of a mapping.

Definition 1.9 ■ Mapping, Image

Let A and B be nonempty sets. A subset f of $A \times B$ is a **mapping** from A to B if and only if for each $a \in A$ there is a unique (one and only one) element $b \in B$ such that $(a, b) \in f$. If f is a mapping from A to B and the pair (a, b) belongs to f, we write $b = f(a)$ and call b the **image** of a under f.

Figure 1.4 illustrates the pairing between a and $f(a)$. A mapping f from A to B is the same as a function from A to B, and the image of $a \in A$ under f is the same as the value of the function f at a. Two mappings f from A to B and g from A to B are **equal** if and only if $f(x) = g(x)$ for all $x \in A$.



■ **Figure 1.4**

Example 2 Let $A = \{-2, 1, 2\}$, and let $B = \{1, 4, 9\}$. The set f given by

$$f = \{(-2, 4), (1, 1), (2, 4)\}$$

is a mapping from A to B, since for each $a \in A$ there is a unique element $b \in B$ such that $(a, b) \in f$. As is frequently the case, this mapping can be efficiently described by giving the rule for the image under f. In this case, $f(a) = a^2$, $a \in A$. This mapping is illustrated in Figure 1.5.

■ **Figure 1.5** $f(a) = a^2, a \in A$ ■

When it is possible to describe a mapping by giving a simple rule for the image of an element, it is certainly desirable to do so. We must keep in mind, however, that the set A, the set B, and the rule must all be known before the mapping is determined. If f is a mapping from A to B, we write $f: A \to B$ or $A \xrightarrow{f} B$ to indicate this.

ALERT