ELEMENTS OF

Modern ALGEBRA

fourth edition

Jimmie Gilbert • Linda Gilbert

FOURTH EDITION

ELEMENTS OF MODERN ALGEBRA

Jimmie Gilbert
Linda Gilbert
University of South Carolina at Spartanburg

PWS Publishing Company

I(T)P **An International Thomson Publishing Company**

Boston ■ Albany ■ Bonn ■ Cincinnati ■ Detroit ■ London ■ Madrid ■ Melbourne
Mexico City ■ New York ■ Paris ■ San Francisco ■ Singapore ■ Tokyo ■ Toronto ■ Washington

PWS PUBLISHING COMPANY
20 Park Plaza, Boston, MA 02116-4324

I(T)P™
International Thomson Publishing
The trademark ITP is used under license.

For more information contact:

PWS Publishing Company
20 Park Plaza
Boston, MA 02116

International Thomson Publishing
Europe
Berkshire House 168-173
High Holborn
London WC1V 7AA
England

Thomas Nelson Australia
102 Dodds Street
South Melbourne, 3205
Victoria, Australia

Nelson Canada
1120 Birchmount Road
Scarborough, Ontario
Canada M1K 5G4

International Thomson Editores
Campos Eliseos 385, Piso 7
Col. Polanco
11560 Mexico D.F., Mexico

International Thomson Publishing
GmbH
Königswinterer Strasse 418
53227 Bonn, Germany

International Thomson Publishing Asia
221 Henderson Road
#05-10 Henderson Building
Singapore 0315

International Thomson Publishing
Japan
Hirakawacho Kyowa Building, 31
2-2-1 Hirakawacho
Chiyoda-ku, Tokyo 102
Japan

Library of Congress Cataloging-in-Publication Data

Gilbert, Jimmie
Elements of modern algebra / Jimmie Gilbert, Linda Gilbert. — 4th ed.
p. cm.
Includes bibliographical references and index.
ISBN 0-534-95196-1 (hardcover)
1. Algebra, Abstract. I. Gilbert, Linda. II. Title.
QA162.G527 1995
512′.02—dc20 95-38567
CIP

Photo credits

p. 133: Smithsonian Institution Photo No. 60,277-D
p. 150: Charles Falco/Science Source/Photo Researchers
p. 244: Courtesy Historical Pictures Service
p. 270: Smithsonian Institution Photo No. 56,865
p. 316: Smithsonian Institution Photo No. 46,834-M

Editorial Assistants: John Ward/Anna Aleksandrowicz
Production Coordinator: Patricia Adams
Production: Hoyt Publishing Services
Market Development Manager: Marianne C.P. Rutter
Manufacturing Coordinator: Wendy Kilborn
Interior Design: John Edeen
Interior Illustrator: George Nichols
Cover Designer: Julie Gecha
Compositor: Weimer Graphics, Inc.
Cover Printer: Coral Graphic Services, Inc.
Text Printer and Binder: Quebecor/Martinsburg

This book is printed on recycled, acid-free paper.

Printed and bound in the United States of America
96 97 98 99 10 9 8 7 6 5 4 3 2

Dedicated to Georgia Phillips
and the memory of Ella Gilbert

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. 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, including two new ones on applications, are marked "optional" and may be skipped by instructors who prefer to spend more time on later topics.

When we approached the preparation of this fourth edition, two thoughts were foremost in our minds. The first thought was one of sincere appreciation to the users of previous editions, and the second was one of concern as to how we might improve the book. These two thoughts came together to give us a goal for this edition: to make this text more *user-friendly.*

Our efforts toward that goal led to the following changes from the third edition. This list reflects the suggestions of users and reviewers of that edition, as well as our ideas as to how we might incorporate their suggestions.

- **Introduction to Coding Theory** (Section 2.7) is an optional new section on the application of modular arithmetic to coding theory. This material includes descriptions of codes used in UPC symbols, passport numbers, bank numbers, and ISBN numbers.
- **Permutation Groups in Science and Art** (Section 4.3) is an optional new section that presents some of the more important applications of permutation groups in the natural sciences and the arts. The four types of symmetries (rotations, reflections, translations, and glide reflections) for plane figures are examined, as well as groups of symmetries of unbounded sets.
- **Descriptive labels and titles** have been placed on definitions and theorems to indicate their content and relevance.
- **Strategy boxes** have been added that give guidance and explanation about techniques of proof. This feature forms a component of the bridge that enables students to become more proficient in their proof construction skills.
- **Symbolic marginal notes** such as "$(p \wedge q) \Rightarrow r$" and "$\sim p \Leftarrow (\sim q \wedge \sim r)$" have been added to help students analyze the logic in the proofs of theorems without interrupting the natural flow of the proof.
- A new **reference system** has been installed that provides guideposts to continuations and interconnections of exercises throughout the text. As an example, consider Exercise 23 in the exercises for Section 4.4. The marginal notation "Sec. 3.1, #26 ⩾" indicates that this exercise is *connected* to Exercise 26 in the *earlier* Section 3.1. The marginal notation "Sec. 4.5, #7⩽" indicates that this exercise has a *continuation* in Exercise 7 in the *later* Section 4.5.

- **New or rewritten material** appears in 18 sections and 22 exercise sets of this edition.
- The topic of **homomorphisms** has been moved to Section 3.5, immediately following the section on **isomorphisms**.
- A modest **increase** in the number of exercises requiring proofs has been made, and we have done some minor **reorganization** in the exercise sets.
- An **updated bibliography** includes the excellent new abstract algebra texts that have appeared in recent years.

The following features, many of which contribute to user-friendliness, are retained from the third edition:

- An **appendix** on the basics of logic and methods of proof
- A **biographical sketch** of a great mathematician whose contributions are relevant to that material concludes each chapter
- **Gradual introduction and development** of concepts, proceeding from the simplest structures to the more complex
- An **abundance of examples**, designed to develop the student's intuition
- Enough **exercises** to allow instructors to make different assignments of approximately the same difficulty
- **Exercise sets** designed to develop the student's maturity and ability to construct proofs, with many problems that are elementary or of a computational nature
- A **summary of key words and phrases** at the end of each chapter
- A **list of special notations** used in the book, on the front endpapers
- **Group tables** for the most common examples, on the back endpapers

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.

Several users of the text have inquired as to what material we teach in our courses. Our basic goal in a single course is 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. We would also omit the optional new sections on applications and optional Section 2.1 (Postulates for the Integers) if class meetings are in short supply. The sections on applications naturally lend themselves well to outside student projects involving additional writing and/or library research.

The problems in an exercise set are, for the most part, 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, both authors 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, a completely optional choice of the instructor.

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 treatment of the set $\mathbf{Z}_n$ of congruence classes modulo n is a unique 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).

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 with 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 mathematics courses.

Acknowledgments

We are grateful to the following persons for their reviews and helpful comments with regard to the first three editions:

Lateef A. Adelani, *Harris-Stowe College*
Philip C. Almes, *Wayland Baptist University*
Edwin F. Baumgartner, *Le Moyne College*
Bruce M. Bemis, *Westminster College*
Louise M. Berard, *Wilkes College*
Thomas D. Bishop, *Arkansas State University*
James C. Bradford, *Abilene Christian University*
Shirley Branan, *Birmingham Southern College*
Gordon Brown, *University of Colorado, Boulder*
Harmon C. Brown, *Harding University*
Marshall Cates, *California State University, Los Angeles*
Patrick Costello, *Eastern Kentucky University*
Richard Cowan, *Shorter College*
Elwyn H. Davis, *Pittsburg State University*
David J. DeVries, *Georgia College*
Paul J. Fairbanks, *Bridgewater State College*
Howard Frisinger, *Colorado State University*
Nickolas Heerema, *Florida State University*
Edward K. Hinson, *University of New Hampshire*
William J. Keane, *Boston College*
Robert E. Kennedy, *Central Missouri State University*
William F. Keigher, *Rutgers University*
Stanley M. Lukawecki, *Clemson University*
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*
Burdette C. Wheaton, *Mankato State University*
Henry Wyzinski, *Indiana University Northwest*

We also express our thanks to these people for their valuable suggestions in reviews of the fourth edition:

Steve Benson, *St. Olaf College*
Edwin F. Baumgartner, *Le Moyne College*
Paul Fairbanks, *Bridgewater State College*
David L. Johnson, *Lehigh University*
Andre E. Kezdy, *University of Louisville*
Joan S. Morrison, *Goucher College*
Carl R. Spitznagel, *John Carroll University*
Ralph C. Steinlage, *University of Dayton*
Carroll G. Wells, *Western Kentucky University*

We are indebted to the following people for suggesting improvements and corrections for this edition:

Brian D. Beasley, *Presbyterian College*
David M. Bloom, *Brooklyn College of the City University of New York*
David J. DeVries, *Georgia College*
J. Taylor Hollist, *State University of New York at Oneida*

Our sincere appreciation goes to Anna Aleksandrowicz for coordinating the project and to David Hoyt for excellent production work.

Jimmie Gilbert
Linda Gilbert

Chapters/Sections Dependency Diagram

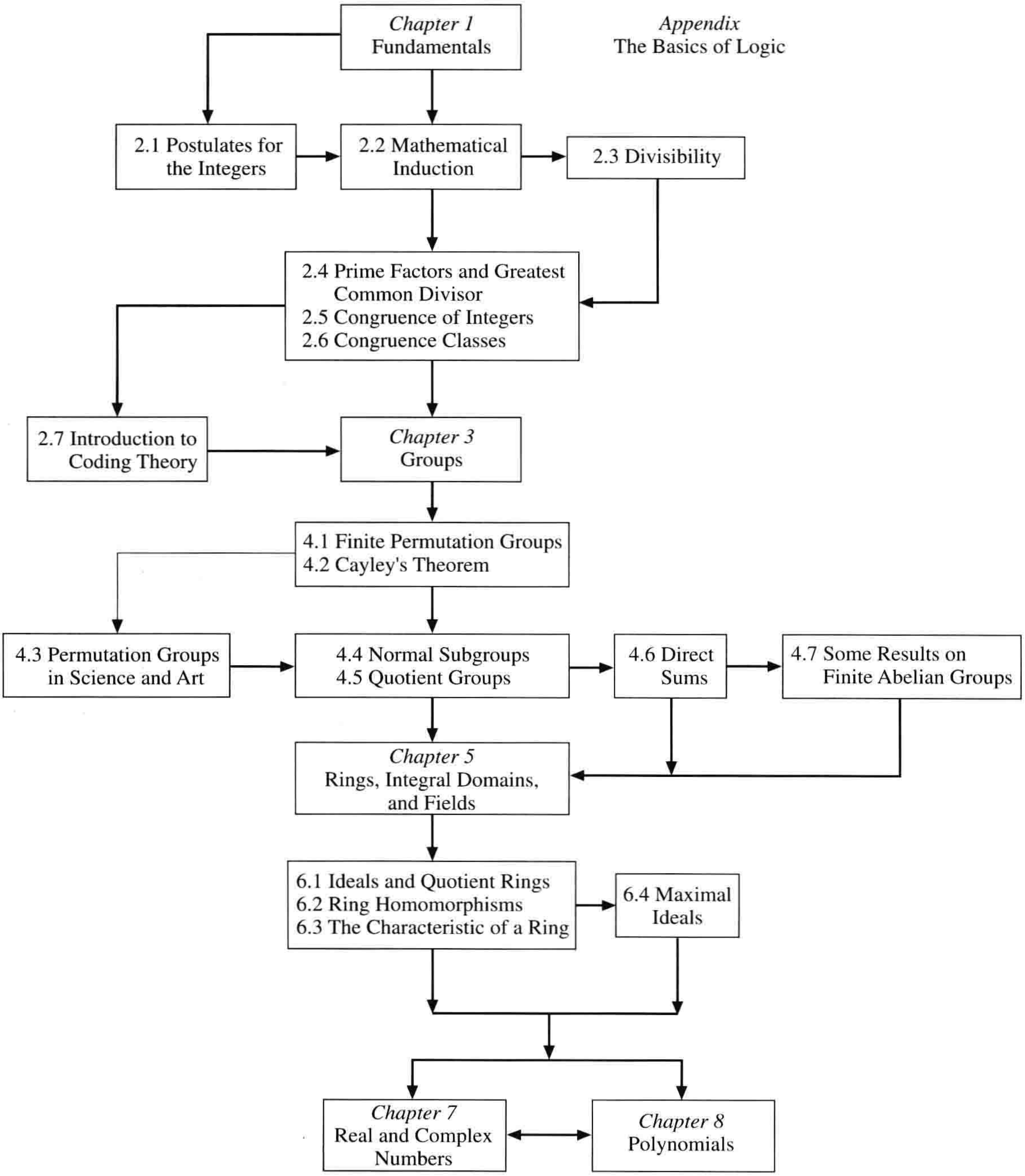
Chapter 1
Fundamentals
Appendix
The Basics of Logic
2.1 Postulates for the Integers
2.2 Mathematical Induction
2.3 Divisibility
2.4 Prime Factors and Greatest Common Divisor
2.5 Congruence of Integers
2.6 Congruence Classes
2.7 Introduction to Coding Theory
Chapter 3
Groups
4.1 Finite Permutation Groups
4.2 Cayley's Theorem
4.3 Permutation Groups in Science and Art
4.4 Normal Subgroups
4.5 Quotient Groups
4.6 Direct Sums
4.7 Some Results on Finite Abelian Groups
Chapter 5
Rings, Integral Domains, and Fields
6.1 Ideals and Quotient Rings
6.2 Ring Homomorphisms
6.3 The Characteristic of a Ring
6.4 Maximal Ideals
Chapter 7
Real and Complex Numbers
Chapter 8
Polynomials

Figure P.1

CONTENTS

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 solve 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 particular 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

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

The three dots . . . , called an *ellipsis,* mean that the pattern established before the dots continues indefinitely. The notation $\{0, 1, 2, 3, \ldots\}$ 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 of the notations $A \subseteq B$ or $B \supseteq A$ indicates that A is a subset of B.

The notation $A \subseteq B$ is read "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.

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. Typically, a proof that two sets are equal is presented in two parts. The first shows that $A \subseteq B$, and the second that $B \subseteq A$. We then conclude that $A = B$. We shall have an example of this type of proof shortly.

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

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

and

$$A \cap B = \{4, 6\}.$$ ■

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

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

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.**

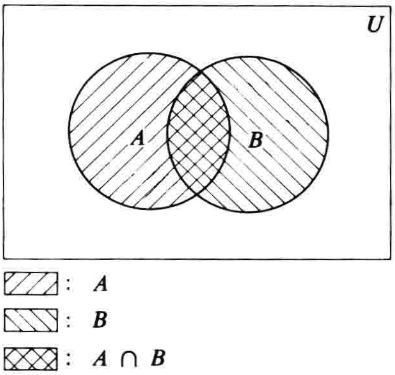

Figure 1.1

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