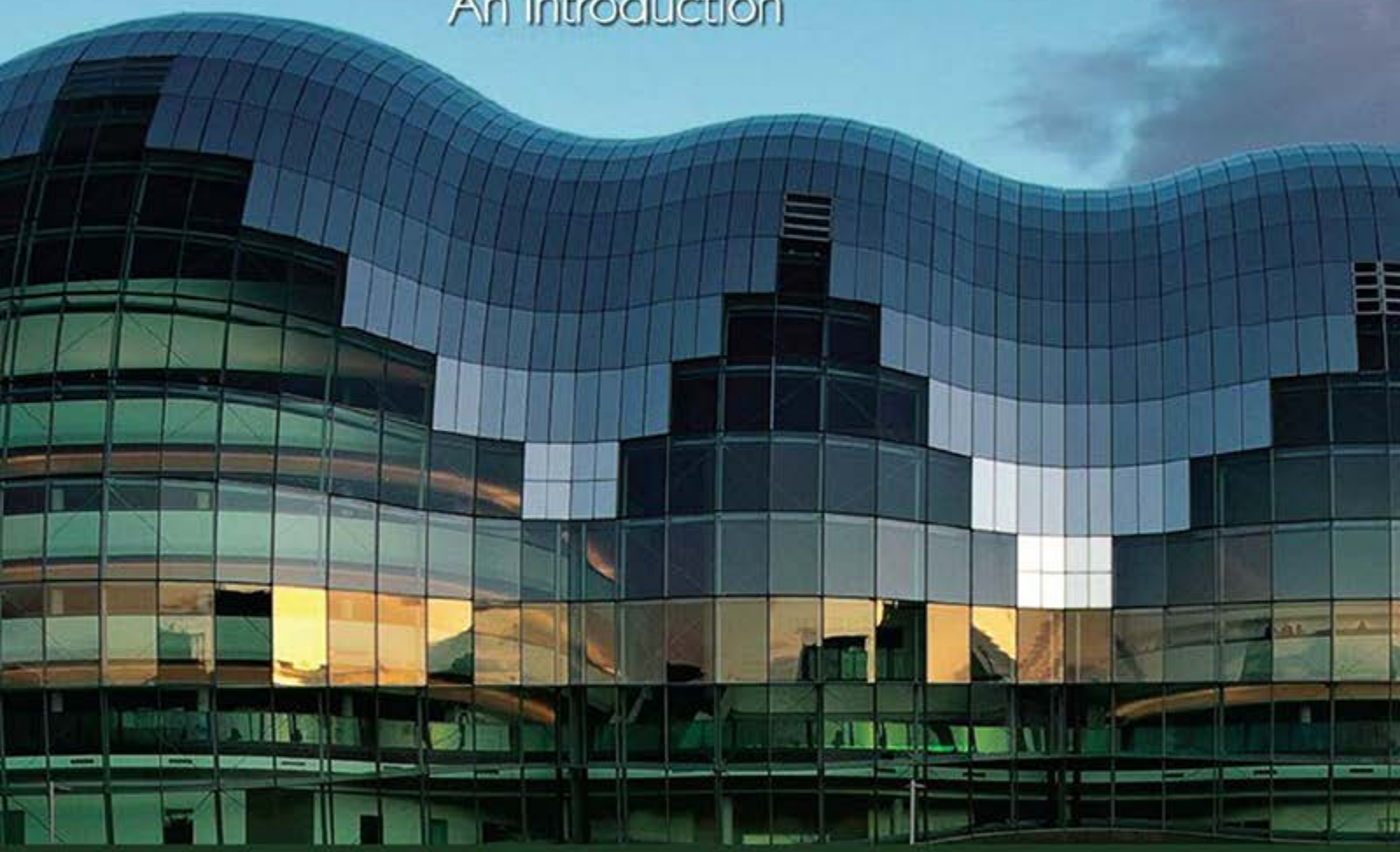
Third Edition

Abstract Algebra

An Introduction



Thomas W. Hungerford

NOTATIONS

The number after each entry refers to a page where the symbol is explained in the text.

Sets and Functions

$c \in B$	c is an element of the set B, 509
$c \notin B$	c is not an element of the set B, 509
$\varnothing$	Empty set [or null set], 510
$B \subseteq C$	B is a subset of C, 510
$B - C$	Relative complement of set C in set B, 511
$B \cap C$	Intersection of sets B and C, 511
$\bigcap_{i \in I} A_i$	Intersection of the sets A_i with $i \in I$, 511
$B \cup C$	Union of sets B and C, 511
$\bigcup_{i \in I} A_i$	Union of the sets A_i with $i \in I$, 511
$B \times C$	Cartesian product of sets B and C, 512
$f: B \to C$	Function [or mapping] from set B to set C, 512
$f(b)$	Image of b under the function $f: B \to C$, or the value of f at b, 512
$\iota_B: B \to B$	Identity map on the set B, 512
$g \circ f$	Composite function of $f: B \to C$ and $g: C \to D$, 512–513
$\operatorname{Im} f$	Image of the function $f: B \to C$, which is a subset of C, 517

Important Sets

$\mathbb{N}$	Nonnegative integers, 523
$\mathbb{Z}$	Integers, 3
$\mathbb{Q}$	Rational Numbers, 49, 191
$\mathbb{R}$	Real Numbers, 45, 191
$\mathbb{C}$	Complex numbers, 49, 191
$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	Nonzero elements of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively, 178, 192
$\mathbb{Q}^{**}, \mathbb{R}^{**}$	Positive elements of $\mathbb{Q}$, $\mathbb{R}$ respectively, 178, 192

Integers

$b \mid a$	b divides a [or b is a factor of a], 9
(a, b)	Greatest common divisor (gcd) of a and b, 10
$(a_1, a_2, \ldots, a_n)$	Greatest common divisor (gcd) of $a_1, a_2, \ldots, a_n$, 16
$[a, b]$	Least common multiple (lcm) of a and b, 16

$[a_1, a_2, \ldots, a_n]$	Least common multiple (lcm) of $a_1, a_2, \ldots, a_n$, 16
$a \equiv b \pmod{n}$	a is congruent to b modulo n, 25
$[a]$ or $[a]_n$	Congruence class of a modulo n, 27, 28
$\mathbb{Z}_n$	Set of congruence classes modulo n, 30

Rings and Ideals

1_R	Multiplicative identity element in a ring with identity, 44
$M(\mathbb{R})$	Ring of 2×2 matrices over the real numbers $\mathbb{R}$, 46
$M(\mathbb{Z})$, $M(\mathbb{Q})$, $M(\mathbb{C})$, $M(\mathbb{Z}_n)$	Ring of 2×2 matrices over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_n$ respectively, 48
0	Zero matrix in $M(\mathbb{R})$, 47
$M(R)$	Ring of 2×2 matrices over a commutative ring R with identity, 48
$R \cong S$	Ring R is isomorphic to ring S, 72
(c)	Principal ideal generated by c, 144
$(c_1, c_2, \ldots, c_n)$	Ideal generated by $c_1, c_2, \ldots, c_n$, 145
$a \equiv b \pmod{I}$	a is congruent to b modulo the ideal I, 145
$a + I$	Coset [congruence class] of a modulo the ideal I, 147
R/I	Quotient ring [or factor ring] of the ring R by the ideal I, 147, 154
$I + J$	Sum of ideals I and J (which is also an ideal), 149
IJ	Product of ideals I and J (which is also an ideal), 150
$\mathbb{Z}[\sqrt{d}]$	The subring $\{r + s\sqrt{d} \mid d, r, s \in \mathbb{Z}\}$ of $\mathbb{C}$, 322
$\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-1}]$	Ring of Gaussian integers, 322
$\mathbb{Q}_{\mathbb{Z}}[x]$	Ring of polynomials in $\mathbb{Q}[x]$ whose constant term is an integer, 336
$N: \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$	Norm function, 346
$F(x)$	Field of quotients [or field of rational functions] of the polynomial ring $F[x]$ over the field F, 358

Polynomials

$R[x]$	Ring of polynomials with coefficients in the ring R, 86
$\deg f(x)$	Degree of the polynomial $f(x)$, 88
$f(x) \mid g(x)$	$f(x)$ divides [or is a factor of] $g(x)$, 96
$f(x) \equiv g(x) \pmod{p(x)}$	$f(x)$ is congruent to $g(x)$ modulo $p(x)$, 125
$[f(x)]$ or $[f(x)]_{p(x)}$	Congruence class [or residue class] of $f(x)$ modulo $p(x)$, 126
$F[x]/p(x)$	Ring of congruence classes modulo $p(x)$, 128, 131

List continues on inside back cover.

ABSTRACT ALGEBRA

An Introduction

THIRD EDITION

THOMAS W. HUNGERFORD
Saint Louis University

BROOKS/COLE
CENGAGE Learning

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

BROOKS/COLE
CENGAGE Learning

***Abstract Algebra: An Introduction*, Third Edition**
Thomas H. Hungerford

Publisher/Executive Editor: Richard Stratton
Acquisitions Editor: Molly Taylor
Assistant Editor: Shaylin Walsh
Editorial Assistant: Alex Gontar
Media Editor: Andrew Coppola
Content Project Manager: Cathy Brooks
Production Manager: Suzanne St. Clair
Art Director: Linda May
Rights Acquisition Specialist: Shalice Shah-Caldwell
Manufacturing Planner: Doug Bertke
Manufacturing Manager: Marcia Locke
Marketing Manager: Jennifer Jones
Marketing Director: Mandee Eckersley
Marketing Coordinator: Lauren Beck
Marketing Communications Manager: Mary Anne Payumo
Production Service and Compositor: MPS Ltd.
Text Designer: Pier 1 Design
Cover Designer: Rokusek Design
Cover Image: Shutterstock

Library of Congress Control Number: 2012940761

ISBN-13: 978-1-111-56962-4

ISBN-10: 1-111-56962-2

Brooks/Cole
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil and Japan. Locate your local office at **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your course and learning solutions, visit **www.cengage.com**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**
Instructors: Please visit **login.cengage.com** and log in to access instructor-specific resources.

Printed in the United States of America.
1 2 3 4 5 6 7 16 15 14 13 12

Dedicated to the memory of

Vincent O. McBrien

and

Raymond J. Swords, S.J.

College of the Holy Cross

TABLE OF CONTENTS

***Sections in the Core Course marked * may be omitted or postponed. See the beginning of each such section for specifics.**

PREFACE

This book is intended for a first undergraduate course in modern abstract algebra. Linear algebra is not a prerequisite. The flexible design makes the text suitable for courses of various lengths and different levels of mathematical sophistication, including (but not limited to) a traditional abstract algebra course, or one with a more applied flavor, or a course for prospective secondary school teachers. As in previous editions, the emphasis is on clarity of exposition and the goal is to produce a book that an average student can read with minimal outside assistance.

New in the Third Edition

Groups First Option Those who believe (as I do) that covering rings before groups is the better pedagogical approach to abstract algebra can use this edition exactly as they used the previous ones.

Nevertheless, anecdotal evidence indicates that some instructors have used the second edition for a "groups first" course, which presumably means that they liked other aspects of the book enough that they were willing to take on the burden of adapting it to their needs. To make life easier for them (and for anyone else who prefers "groups first")

It is now possible (though not necessary) to use this text for a course that covers groups before rings.

See the TO THE INSTRUCTOR section for details.

Much of the rewriting needed to make this option feasible also benefits the "rings first" users. A number of them have suggested that complete proofs were needed in parts of the group theory chapters instead of directions that said in effect "adapt the proof of the analogous theorem for rings". The full proofs are now there.

Proofs for Beginners Many students entering a first abstract algebra course have had little (or no) experience in reading and writing proofs. To assist such students (and better prepared students as well), a number of proofs (especially in Chapters 1 and 2) have been rewritten and expanded. They are broken into several steps, each of which is carefully explained and proved in detail. Such proofs take up more space, but I think it's worth it if they provide better understanding.

So that students can better concentrate on the essential topics, various items from number theory that play no role in the remainder of the book have been eliminated from Chapters 1 and 2 (though some remain as exercises).

More Examples and Exercises In the core course (Chapters 1–8), there are 35% more examples than in the previous edition and 13% more exercises. Some older exercises have been replaced, so 18% of the exercises are new. The entire text has about 350 examples and 1600 exercises. For easier reference, the examples are now numbered.

Coverage The breadth of coverage in this edition is substantially the same as in the preceding ones, with one minor exception. The chapter on Lattices and Boolean Algebra (which apparently was rarely used) has been eliminated. However, it is available at our website (www.CengageBrain.com) for those who want to use it.

The coverage of groups is much the same as before, but the first group theory chapter in the second edition (the longest one in the book by far) has been divided into two chapters of more manageable size. This arrangement has the added advantage of making the parallel development of integers, polynomials, groups, and rings more apparent.

Endpapers The endpapers now provide a useful catalog of symbols and notations.

Website The website (www.CengageBrain.com) provides several downloadable programs for TI graphing calculators that make otherwise lengthy calculations in Chapters 1 and 14 quite easy. It also contains a chapter on Lattices and Boolean Algebra, whose prerequisites are Chapter 3 and Appendices A and B.

Continuing Features

Thematic Development The Core Course (Chapters 1–8) is organized around two themes: Arithmetic and Congruence. The themes are developed for integers (Chapters 1 and 2), polynomials (Chapters 4 and 5), rings (Chapters 3 and 6), and groups (Chapters 7 and 8). See the **Thematic Table of Contents** in the TO THE STUDENT section for a fuller picture.

Congruence The Congruence theme is strongly emphasized hi the development of quotient rings and quotient groups. Consequently, students can see more clearly that ideals, normal subgroups, quotient rings, and quotient groups are simply an extension of familiar concepts in the integers, rather than an unmotivated mystery.

Useful Appendices These contain prerequisite material (e.g., logic, proof, sets, functions, and induction) and optional material that some instructors may wish to introduce (e.g., equivalence relations and the Binomial Theorem).

Acknowledgments

This edition has benefited from the comments of many students and mathematicians over the years, and particularly from the reviewers for this edition. My warm thanks to

Ross Abraham, *South Dakota State University*
George DeRise, *Thomas Nelson Community College*
Kimberly Elce, *California State University, Sacramento*
Sherry Ettlich, *Southern Oregon University*
Lenny Jones, *Shippensburg University*
Anton Kaul, *California Polytechnic University, San Luis Obispo*
Wojciech Komornicki, *Hamline University*

Ronald Merritt, *Athens State University*
Bogdan Nita, *Montclair State University*
Tara Smith, *University of Cincinnati*

It is a particular pleasure to acknowledge the invaluable assistance of the Cengage staff, especially Molly Taylor, Shaylin Walsh, Cathy Brooks, and Alex Gontar. I also want to express my appreciation to my copyeditor, Martha Williams, whose thorough reading of the manuscript significantly improved the final text. Charu Khanna and the MPS Limited production staff did an excellent job.

John Oprea (Cleveland State University), Greg Marks (Saint Louis University), and David Leep (University of Kentucky) provided assistance on several points, for which I am grateful.

Finally, a very special thank you to my wife Mary Alice for her patience, understanding, and support during the preparation of this revision.

T. W. H.

TO THE INSTRUCTOR

Here are some items that will assist you in making up your syllabus.

Course Planning

Using the chart on the opposite page, the Table of Contents (in which optional sections are marked), and the chapter introductions, you can easily plan courses of varying length, emphasis, and order of topics. If you plan to cover groups before rings, please note that Section 7.1 should be replaced by Section 7.1. A (which appears immediately after 7.1).

Appendices

Appendix A (Logic and Proof) is a prerequisite for the entire text. Prerequisites for various parts of the text are in Appendices B–F. Depending on the preparation of your students and your syllabus, you may want to incorporate some of this material into your course. Note the following.

- *Appendix B (Sets and Functions):* The middle part (Cartesian products and binary operations) is first used in Section 3.1 [7.1.A].* The last five pages (injective and surjective functions) are first used in Section 3.3 [7.4].
- *Appendix C (Induction):* Ordinary induction (Theorem C.1) is first used in Section 4.4. Complete Induction (Theorem C.2) is first used in Section 4.1 [9.2]. The equivalence of induction and well-ordering (Theorem C.4) is not needed in the body of the text.
- *Appendix D (Equivalence Relations):* Important examples of equivalence relations are presented in Sections 2.1, 5.1, 6.1, and 8.1, but the formal definition is not needed until Section 10.4 [9.4].
- *Appendix E (The Binomial Theorem):* This is used only in Section 11.6 and occasional exercises earlier.
- *Appendix F (Matrix Algebra):* This is a prerequisite for Chapter 16 but is not needed by students who have had a linear algebra course.

Finally, Appendix G presents a formal development of polynomials and indeterminates. I personally think it's a bit much for beginners, but some people like it.

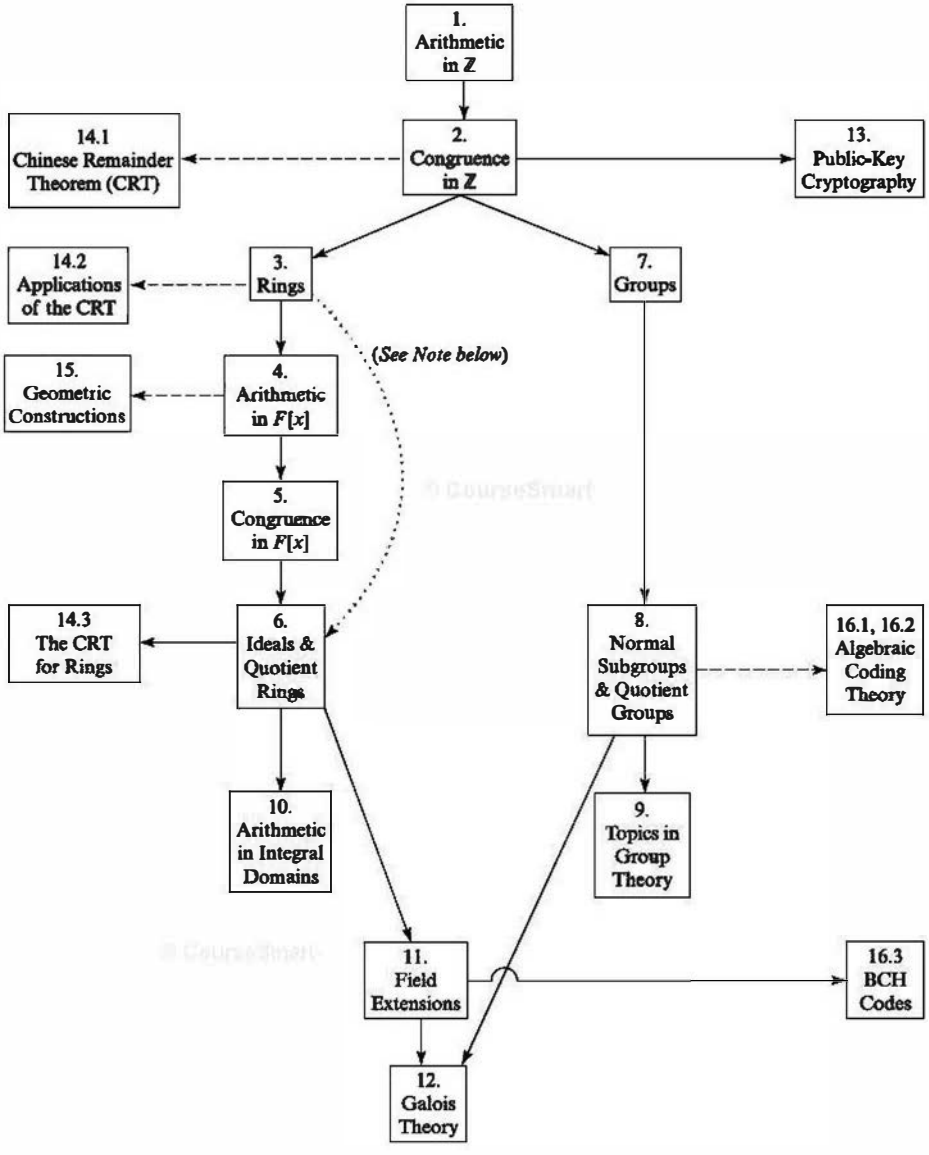
Exercises

The exercises in Group A involve routine calculations or short straightforward proofs. Those in Group B require a reasonable amount of thought, but the vast majority should be accessible to most students. Group C consists of difficult exercises.

Answers (or hints) for more than half of the odd-numbered exercises are given at the end of the book. Answers for the remaining exercises are in the Instructor's Manual available to adopters of the text.

*The section numbers in brackets are for groups-first courses.

CHAPTER INTERDEPENDENCE*



NOTE: To go quickly from Chapter 3 to Chapter 6, first cover Section 4.1 (except the proof of the Division Algorithm), then proceed to Chapter 6. If you plan to cover Chapter 11, however, you will need to cover Chapter 4 first.

---

*A solid arrow $A \rightarrow B$ means that A is a prerequisite for B; a dashed arrow $A \dashrightarrow B$ means that B depends only on parts of A (see the Table of Contents for specifics). For the dotted arrow 3 $\cdots\!\rightarrow$ 6, see the Note at the bottom of the chart.

TO THE STUDENT

Overview

This book begins with grade-school arithmetic and the algebra of polynomials from high school (from a more advanced viewpoint, of course). In later chapters of the book, you will see how these familiar topics fit into a larger framework of abstract algebraic systems. This presentation is organized around these two themes:

Arithmetic You will see how the familiar properties of division, remainders, factorization, and primes in the integers carry over to polynomials, and then to more general algebraic systems.

Congruence You may be familiar with "clock arithmetic".* This is an example of congruence and leads to new finite arithmetic systems that provide a model for what can be done for polynomials and other algebraic systems. Congruence and the related concept of a quotient object are the keys to understanding abstract algebra.

Proofs

The emphasis in this course, much more than in high-school algebra, is on the rigorous logical development of the subject. If you have had little experience with reading or writing proofs, you would do well to read Appendix A, which summarizes the basic rules of logic and the proof techniques that are used throughout the book.

You should first concentrate on understanding the proofs in the text (which is quite different from constructing a proof yourself). Just as you can appreciate a new building without being an architect or a contractor, you can verify the validity of proofs presented by others, *even if you can't see how anyone ever thought of doing it this way in the first place.*

Begin by skimming through the proof to get an idea of its general outline before worrying about the details in each step. It's easier to understand an argument if you know approximately where it's headed. Then go back to the beginning and read the proof carefully, line by line. If it says "such and such is true by Theorem 5.18", check to see just what Theorem 5.18 says and be sure you understand why it applies here. If you get stuck, take that part on faith and finish the rest of the proof. Then go back and see if you can figure out the sticky point.

---

*When the hour hand of a clock moves 3 hours or 15 hours from 12, it ends in the same position, so $3 = 15$ on the clock. If the hour hand starts at 12 and moves 8 hours, then moves an additional 9 hours, it finishes at 5; so $8 + 9 = 5$ on the clock.

When you're really stuck, *ask your instructor.* He or she will welcome questions that arise from a serious effort on your part.

Exercises

Mathematics is not a spectator sport. You can't expect to learn mathematics without *doing* mathematics, any more than you could learn to swim without getting in the water. That's why there are so many exercises in this book.

The exercises in group A are usually straightforward. If you can't do almost all of them, you don't really understand the material. The exercises in group B often require a reasonable amount of thought—and for most of us, some trial and error as well. But the vast majority of them are within your grasp. The exercises in group C are usually difficult . . . a good test for strong students.

Many exercises will ask you to prove something. As you build up your skill in understanding the proofs of others (as discussed above), you will find it easier to make proofs of your own. The proofs that you will be asked to provide will usually be much simpler than proofs in the text (which can, nevertheless, serve as models).

Answers (or hints) for more than half of the odd-numbered exercises are given at the back of the book.

Keeping It All Straight

In the Core Course (Chapters 1–8), students often have trouble seeing how the various topics tie together, or even *if* they do. The *Thematic Table of Contents* on the next two pages is arranged according to the themes of arithmetic and congruence, so you *can* see how things fit together.

THEMATIC TABLE OF CONTENTS FOR THE CORE COURSE

TOPICS ▶ THEME ▼	INTEGERS	POLYNOMIALS	
ARITHMETIC *Division Algorithm*	**1. Arithmetic in $\mathbb{Z}$ Revisited** 1.1 The Division Algorithm	**4. Arithmetic in $F[x]$** 4.1 Polynomial Arithmetic and the Division Algorithm	
Divisibility	1.2 Divisibility	4.2 Divisibility in $F[x]$	
Primes and Factorization	1.3 Primes and Unique Factorization	4.3 Irreducibles and Unique Factorization	
Primality Testing	1.3 Theorem 1.10	4.4 Polynomial Functions, Roots, and Reducibility 4.5 Irreducibility in $\mathbb{Q}[x]$ 4.6 Irreducibility in $\mathbb{R}[x]$ and $\mathbb{C}[x]$	
CONGRUENCE *Congruence*	**2. Congruence in $\mathbb{Z}$ and Modular Arithmetic** 2.1 Congruence and Congruence Classes	**5. Congruence in $F[x]$ and Congruence Class Arithmetic** 5.1 Congruence in $F[x]$ and Congruence Classes	
Congruence-Class Arithmetic	2.2 Modular Arithmetic	5.2 Congruence-Class Arithmetic	
Quotient Structures	2.3 The Structure of $\mathbb{Z}_p$ When p Is Prime	5.3 The Structure of $F[x]/p(x)$ When $p(x)$ Is Irreducible	
OTHER *Isomorphism and Homomorphism*			

Directions: Reading from left to right across these two pages shows how the theme or subtheme in the left-hand column is developed in the four algebraic systems listed in the top row. Each vertical column shows how the themes are carried out for the system listed at the top of the column.

RINGS*	GROUPS*
3. Rings 3.1 Rings	**7. Groups** 7.1 Definition and Examples of Groups 7.5 The Symmetric and Alternating Groups
3.2 Basic Properties of Rings	7.2 Basic Properties of Groups 7.3 Subgroups
6. Ideals and Quotient Rings 6.1 Ideals and Congruence	**8. Normal Subgroups and Quotient Groups** 8.1 Congruence 8.2 Normal Subgroups 8.5 The Simplicity of A_n
6.2 Quotient Rings and Homomorphisms	8.3 Quotient Groups 8.4 Quotient Groups and Homomorphisms
6.3 The Structure of R/I When I Is Prime or Maximal	
3.3 Isomorphisms and Homomorphisms	7.4 Isomorphisms and Homomorphisms

*In the Arithmetic Theme, the sections of Chapters 3 (Rings) and 8 (Groups) do not correspond to the individual subthemes (as do the sections of Chapters 1 and 4). For integral domains, however, there is a correspondence, as you will see in Chapter 10 (Arithmetic in Integral Domains).

PART 1

THE CORE COURSE

CHAPTER 1

Arithmetic in $\mathbb{Z}$ Revisited

Algebra grew out of arithmetic and depends heavily on it. So we begin our study of abstract algebra with a review of those facts from arithmetic that are used frequently in the rest of this book and provide a model for much of the work we do. We stress primarily the underlying pattern and properties rather than methods of computation. Nevertheless, the fundamental concepts are ones that you have seen before.

1.1 The Division Algorithm

Our starting point is the set of all integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. We assume that you are familiar with the arithmetic of integers and with the usual order relation ($<$) on the set $\mathbb{Z}$. We also assume the

WELL-ORDERING AXIOM *Every nonempty subset of the set of nonnegative integers contains a smallest element.*

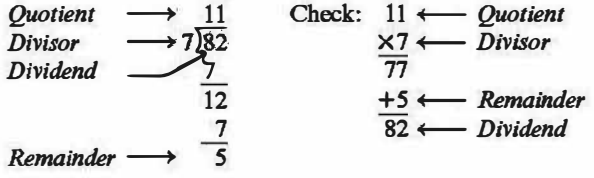
If you think of the nonnegative integers laid out on the usual number line, it is intuitively plausible that each subset contains an element that lies to the left of all the other elements in the subset—that is the smallest element. On the other hand, the Well-Ordering Axiom does not hold in the set $\mathbb{Z}$ of all integers (there is no smallest negative integer). Nor does it hold in the set of all nonnegative rational numbers (the subset of all positive rationals does not contain a smallest element because, for any positive rational number r, there is always a smaller positive rational—for instance, $r/2$).

NOTE: The rest of this chapter and the next require Theorem 1.1, which is stated below. Unfortunately, its proof is a bit more complicated than is desirable at the beginning of the course, since some readers may not have seen many (or any) formal mathematical proofs. To alleviate this

situation, we shall first look at the origins of Theorem 1.1 and explain the idea of its proof. Unless you have a strong mathematical background, we suggest that you read this additional material carefully before beginning the proof.

To ease the beginner's way, the proof itself will be broken into several steps and given in more detail than is customary in most books. However, because the proof does not show how the theorem is actually used in practice, some instructors may wish to postpone the proof until the class has more experience in proving results. In any case, all students should at least read the outline of the proof (its first three lines and the statements of Steps 1–4).

So here we go. Consider the following grade-school division problem:



The division process stops when we reach a remainder that is less than the divisor. All the essential facts are contained in the checking procedure, which may be verbally summarized like this:

$$\text{dividend} = (\text{divisor})\,(\text{quotient}) + (\text{remainder}).$$

Here is a formal statement of this idea, in which the dividend is denoted by a, the divisor by b, the quotient by q, and the remainder by r:

Theorem 1.1 The Division Algorithm

Let a, b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

Theorem 1.1 allows the possibility that the dividend a might be negative but requires that the remainder r must not only be less than the divisor b but also must be *nonnegative*. To see why this last requirement is necessary, suppose $a = -14$ is divided by $b = 3$, so that $-14 = 3q + r$. If we only require that the remainder be less than the divisor 3, then there are many possibilities for the quotient q and remainder r, including these three:

$$-14 = 3(-3) + (-5), \quad \text{with } -5 < 3 \qquad [\textit{Here } q = -3 \textit{ and } r = -5.]$$
$$-14 = 3(-4) + (-2), \quad \text{with } -2 < 3 \qquad [\textit{Here } q = -4 \textit{ and } r = -2.]$$
$$-14 = 3(-5) + 1, \quad \text{with } 1 < 3 \qquad [\textit{Here } q = -5 \textit{ and } r = 1.].$$

When the remainder is also required to be nonnegative as in Theorem 1.1, then there is exactly one quotient q and one remainder r, namely, $q = -5$ and $r = 1$, as will be shown in the proof.

The fundamental idea underlying the proof of Theorem 1.1 is that division is just repeated subtraction. For example, the division of 82 by 7 is just a shorthand method for repeatedly subtracting 7:

$$
\begin{array}{ll}
82 & \\
-7 & \\
\hline
75 \longleftarrow 82 - 7 \cdot 1 & 40 \\
-7 & -7 \\
\hline
68 \longleftarrow 82 - 7 \cdot 2 & 33 \longleftarrow 82 - 7 \cdot 7 \\
-7 & -7 \\
\hline
61 \longleftarrow 82 - 7 \cdot 3 & 26 \longleftarrow 82 - 7 \cdot 8 \\
-7 & -7 \\
\hline
54 \longleftarrow 82 - 7 \cdot 4 & 19 \longleftarrow 82 - 7 \cdot 9 \\
-7 & -7 \\
\hline
47 \longleftarrow 82 - 7 \cdot 5 & 12 \longleftarrow 82 - 7 \cdot 10 \\
-7 & -7 \\
\hline
40 \longleftarrow 82 - 7 \cdot 6 & 5 \longleftarrow 82 - 7 \cdot 11
\end{array}
$$

The subtractions continue until you reach a nonnegative number less than 7 (in this case 5). The number 5 is the remainder, and the *number* of multiples of 7 that were subtracted (namely, 11, as shown at the right of the subtractions) is the quotient.

In the preceding example we looked at the numbers

$$82 - 7 \cdot 1, \quad 82 - 7 \cdot 2, \quad 82 - 7 \cdot 3, \text{ and so on.}$$

In other words, we looked at numbers of the form $82 - 7x$ for $x = 1, 2, 3, \ldots$ and found the smallest nonnegative one (namely, 5). In the proof of Theorem 1.1 we shall do something very similar.

Proof of Theorem 1.1* ▸ Let a and b be fixed integers with $b > 0$. Consider the set S of all integers of the form

$$a - bx, \qquad \text{where } x \text{ is an integer and } a - bx \geq 0.$$

Note that x may be any integer—positive, negative, or 0—but $a - bx$ must be nonnegative. There are four main steps in the proof, as indicated below.

Step 1 *Show that S is nonempty by finding a value for x such that $a - bx \geq 0$.*

Proof of Step 1: We first show that $a + b|a| \geq 0$. Since b is a positive integer by hypothesis, we must have

$$
\begin{aligned}
b &\geq 1 \\
b|a| &\geq |a| && [\textit{Multiply both sides of the preceding inequality by } |a|.] \\
b|a| &\geq -a && [\textit{Because } |a| \geq -a \textit{ by the definition of absolute value.}] \\
a + b|a| &\geq 0.
\end{aligned}
$$

---

*For an alternate proof by induction of part of the theorem, see Example 2 in Appendix C.

Now let $x = -|a|$. Then

$$a - bx = a - b(-|a|) = a + b|a| \geq 0.$$

Hence, $a - bx$ is in S when $x = -|a|$, which means that S is nonempty.

Step 2 *Find q and r such that $a = bq + r$ and $r \geq 0$.*

Proof of Step 2: By the Well-Ordering Axiom, S contains a smallest element—call it r. Since $r \in S$, we know that $r \geq 0$ and $r = a - bx$ for some x, say $x = q$. Thus,

$$r = a - bq \text{ and } r \geq 0, \quad \text{or, equivalently,} \quad a = bq + r \text{ and } r \geq 0.$$

Step 3 *Show that $r < b$.*

Proof of Step 3: We shall use a "proof by contradiction" (which is explained on page 506 of Appendix A). We want to show that $r < b$. So suppose, on the contrary, that $r \geq b$. Then $r - b \geq 0$, so that

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

Since $a - b(q + 1)$ is nonnegative, it is an element of S by definition. But since b is positive, it is certainly true that $r - b < r$. Thus

$$a - b(q + 1) = r - b < r.$$

The last inequality states that $a - b(q + 1)$—which is an element of S—is less than r, the *smallest* element of S. This is a contradiction. So our assumption that $r \geq b$ is false, and we conclude that $r < b$. Therefore, we have found integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Step 4 *Show that r and q are the only numbers with these properties (that's what "unique" means in the statement of the theorem).*

Proof of Step 4: To prove uniqueness, we suppose that there are integers q_1 and r_1 such that $a = bq_1 + r_1$ and $0 \leq r_1 < b$, and prove that $q_1 = q$ and $r_1 = r$.

Since $a = bq + r$ and $a = bq_1 + r_1$, we have

$$bq + r = bq_1 + r_1$$

so that

$$(*) \qquad b(q - q_1) = r_1 - r.$$

Furthermore,

$$0 \leq r < b$$
$$0 \leq r_1 < b.$$

Multiplying the first inequality by -1 (and reversing the direction of the inequality), we obtain

$$-b < -r \le 0$$
$$0 \le r_1 < b.$$

Adding these two inequalities produces

$$\begin{aligned} -b &< r_1 - r < b \\ -b &< b(q - q_1) < b \quad [\textit{By Equation } (*)] \\ -1 &< q - q_1 < 1 \quad [\textit{Divide each term by } b.] \end{aligned}$$

But $q - q_1$ is an *integer* (because q and q_1 are integers) and the only integer strictly between -1 and 1 is 0. Therefore $q - q_1 = 0$ and $q = q_1$. Substituting $q - q_1 = 0$ in Equation (*) shows that $r_1 - r = 0$ and hence $r = r_1$. Thus the quotient and remainder are unique, and the proof is complete. ■*

When both the dividend a and the divisor b in a division problem are positive, then the quotient and remainder are easily found either by long division (as on page 4) or with a calculator when the integers involved are larger.

EXAMPLE 1

Suppose $a = 4327$ is divided by $b = 281$. Entering a/b in a calculator produces $15.39857 \cdots$. The integer to the left of the decimal point (15 here) is the quotient q and the remainder is

$$r = a - bq = 4327 - 281 \cdot 15 = 112.$$

These calculations are shown on the graphing calculator screen in Figure 1.

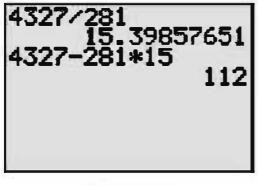


FIGURE 1

When the dividend a is negative, a slightly different procedure is needed so that the remainder will be nonnegative.

*The symbol ■ indicates the end of a proof.

EXAMPLE 2

Suppose $a = -7432$ is divided by $b = 453$. Entering a/b in a calculator produces $-16.40618\cdots$. In this case the quotient q is *not* -16; instead,

$$q = (\text{the integer to the left of the decimal point}) - 1 = -16 - 1 = -17.$$

(Without this adjustment, you will end up with a negative remainder.) Now, as usual,

$$r = a - bq = -7432 - 453 \cdot (-17) = 269.$$

The preceding calculations are summarized in the calculator screen in Figure 2.

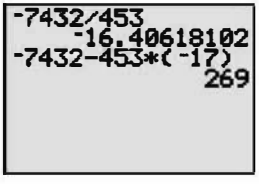


FIGURE 2

■ Exercises

A. *In Exercises 1 and 2, find the quotient q and remainder r when a is divided by b, without using technology. Check your answers.*

1. **(a)** $a = 17; b = 4$ **(b)** $a = 0; b = 19$ **(c)** $a = -17; b = 4$

2. **(a)** $a = -51; b = 6$ **(b)** $a = 302; b = 19$ **(c)** $a = 2000; b = 17$

In Exercises 3 and 4, use a calculator to find the quotient q and remainder r when a is divided by b.

3. **(a)** $a = 517; b = 83$ **(b)** $a = -612; b = 74$

(c) $a = 7{,}965{,}532; b = 127$

4. **(a)** $a = 8{,}126{,}493; b = 541$ **(b)** $a = -9{,}217{,}645; b = 617$

(c) $a = 171{,}819{,}920; b = 4321$

5. Let a be any integer and let b and c be positive integers. Suppose that when a is divided by b, the quotient is q and the remainder is r, so that

$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

If ac is divided by bc, show that the quotient is q and the remainder is rc.

B. **6.** Let a, b, c, and q be as in Exercise 5. Suppose that when q is divided by c, the quotient is k. Prove that when a is divided by bc, then the quotient is also k.

7. Prove that the square of any integer a is either of the form $3k$ or of the form $3k + 1$ for some integer k. [*Hint:* By the Division Algorithm, a must be of the form $3q$ or $3q + 1$ or $3q + 2$.]