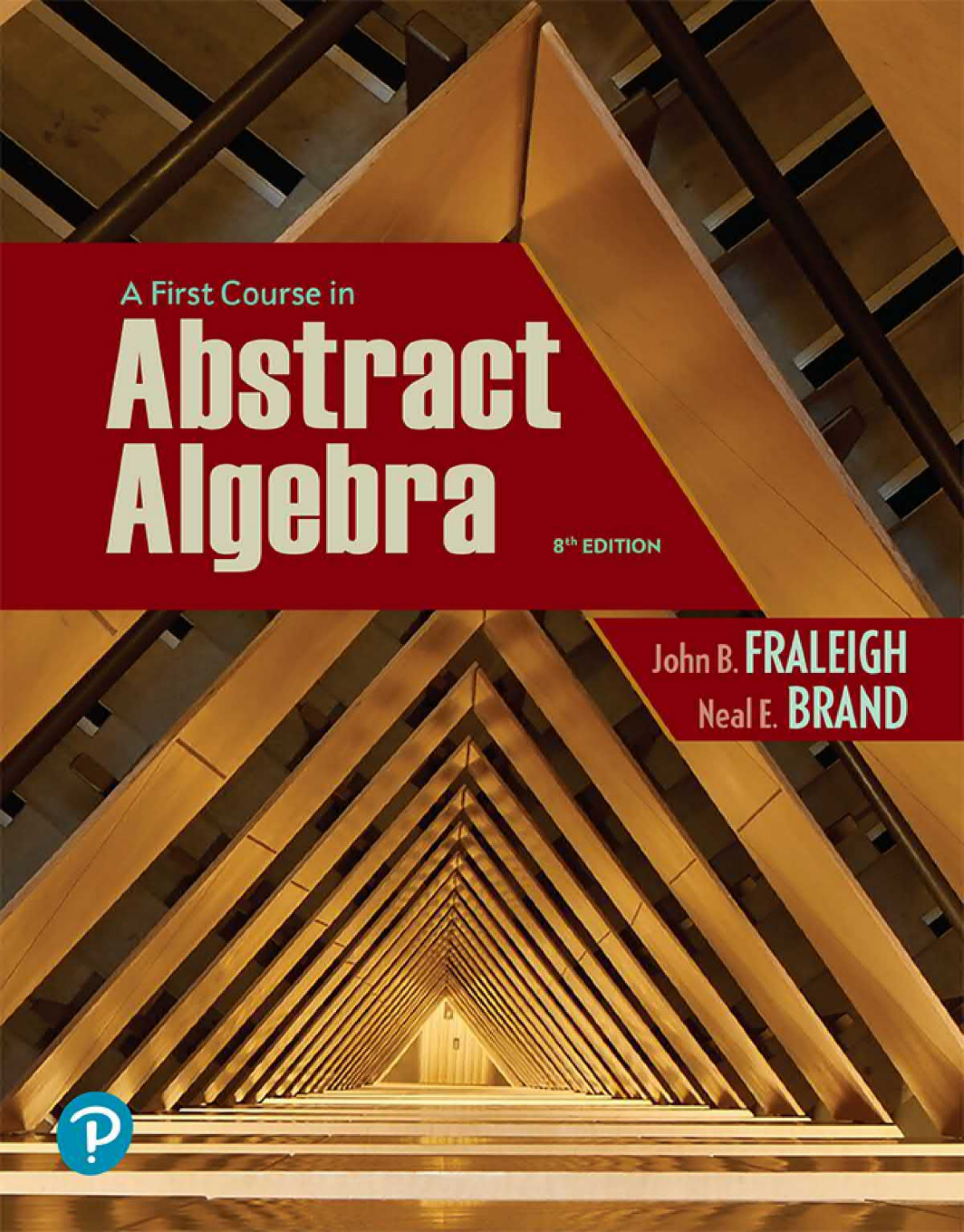

A First Course in
Abstract Algebra
8th EDITION
John B. FRALEIGH
Neal E. BRAND

A First Course in Abstract Algebra

Eighth Edition

John B. Fraleigh
University of Rhode Island

Neal Brand
University of North Texas

Historical Notes by Victor Katz
University of District of Columbia

Pearson

Acknowledgments of third-party content appear on the appropriate page within the text.

Cover image credit: Edmund Sumner/AGE Fotostock

Library of Congress Cataloging-in-Publication Data

Names: Fraleigh, John B., author. | Katz, Victor J., writer of added commentary.
Title: A first course in abstract algebra / John B. Fraleigh ; historical notes by Victor Katz.
Description: Eighth edition. | [Hoboken, New Jersey] : Pearson, [2021] |
Series: World student series | Includes bibliographical references and index.
Identifiers: LCCN 2019038536 | ISBN 9780135758168 (paperback) | ISBN 9780321390363 (ebook)
Subjects: LCSH: Algebra, Abstract.
Classification: LCC QA162 .F7 2020 | DDC 512/.02–dc23
LC record available at https://lccn.loc.gov/2019038536

ScoutAutomatedPrintCode

Pearson

Rental
ISBN-10: 0-13-673162-7
ISBN-13: 978-0-13-673162-7

Loose Leaf Version
ISBN-10: 0-13-575816-5
ISBN-13: 978-0-13-575816-8

Contents

IX

† Not required for the remainder of the text.

‡ This section is a prerequisite for Sections 17 and 36 only.

This page is intentionally left blank

Instructor's Preface

This is an introduction to abstract algebra. It is anticipated that the students have studied calculus and probably linear algebra. However, these are primarily *mathematical maturity* prerequisites; subject matter from calculus and linear algebra appears mostly in illustrative examples and exercises.

As in previous editions of the text, our aim remains to teach students as much about groups, rings, and fields as we can in a first course. For many students, abstract algebra is their first extended exposure to an axiomatic treatment of mathematics. Recognizing this, we have included extensive explanations concerning what we are trying to accomplish, how we are trying to do it, and why we choose these methods. Mastery of this text constitutes a firm foundation for more specialized work in algebra and also provides valuable experience for any further axiomatic study of mathematics.

New to This Edition

[Editor's Note: You may have noticed something new on the cover of the book. Another author! I am thrilled that Neal Brand agreed to update this classic text. He has done so carefully and thoughtfully, staying true to the spirit in which it was written. Neal's years of experience teaching the course with this text at the University of North Texas have helped him produce a meaningful and worthwhile update to John Fraleigh's work.]

Updates for the eText

A focus of this revision was transforming it from a primarily print-based learning tool to a digital learning tool. The eText is therefore filled with content and tools that will help bring the content of the course to life for students in new ways and help you improve instruction. Specifically,

- **Mini lectures.** These brief author-created videos for each section of the text give an overview to the section but not every example or proof. Some sections will have two videos. I have used these videos effectively with my students, who were assigned to watch them ahead of the lecture on that topic. Students came to class with a basic overview of the topic of the day, which had the effect of reducing lecture time and increasing the class time used for discussion and student

presentations. Students reported that the videos were helpful in giving an overview of the topics and a better understanding of the concepts and proofs. Students were also encouraged to view the videos after the topic was covered in class to reinforce what they learned. Many students also used the videos to review topics while preparing for exams. Although I have not attempted to flip the classroom, my intention was to provide sufficient resources in the eText to make it feasible without requiring other resources.

- **Key idea quizzes.** A database of definitions and named theorems will allow students to quiz themselves on these key ideas. The database can be used in the way that flash cards were traditionally used.
- **Self-assessments.** Occasional questions interspersed in the narrative allow students to check their understanding of new ideas.
- **Interactive figures and utilities.** I have added a number of opportunities for students to interact with content in a dynamic manner in order to build or enhance understanding. Interactive figures allow students to explore concepts geometrically or computationally in ways that are not possible without technology.
- **Notes, Labels, and Highlights.** Notes allow instructors to add their personal teaching style to important topics, call out need-to-know information, or clarify difficult concepts. Students can make their eText their own by creating highlights with meaningful labels and notes, helping them focus on what they need to study. The customizable Notebook allows students to filter, arrange, and group their notes in a way that makes sense to them.
- **Dashboard.** Instructors can create reading assignments and see the time spent in the eText so that they can plan more effective instruction.
- **Portability.** Portable access lets students read their eText whenever they have a moment in their day, on Android and iOS mobile phones and tablets. Even without an Internet connection, offline reading ensures students never miss a chance to learn.
- **Ease-of-Use.** Straightforward setup makes it easy for instructors to get their class up and reading quickly on the first day of class. In addition, Learning Management System (LMS) integration provides institutions, instructors, and students with single sign-on access to the eText via many popular LMSs.

Exercises

Many exercises in the text have been updated, and many are new. In order to prevent students from using solutions from the previous edition, I purposefully replaced or reworded some exercises.

I created an Instructor Solutions Manual, which is available online at www.pearson.com to instructors only. Solutions to exercises involving proofs are often sketches or hints, which would not be in the proper form to turn in.

Text Organization Modifications

For each part of the text, I provide an overview of the changes followed by significant changes to sections. In cases where changes to parts or sections were minor, I have not included a list of changes.

Part I: Groups and Subgroups

- Overview of changes: My main goals were to define groups and to introduce the symmetric and dihedral groups as early as possible. The early introduction of these

groups provides students with examples of finite groups that are consistently used throughout the book.

- Section 1 (Binary Operations). Former Section 2. Added definition of an identity for a binary operation.
- Section 2 (Groups). Former Section 4. Included the formal definition of a group isomorphism.
- Section 3 (Abelian Examples). Former Section 1. Included definition of circle group, R_a, and Z_n. Used circle group to show associativity of Z_n and R_a.
- Section 4 (Nonabelian Examples). Based on parts of former Sections 5, 8, and 9. Defined dihedral group and symmetric group. Gave a standardized notation for the dihedral group that is used consistently throughout the book. Introduced both two-row and cycle notation for the symmetric group
- Section 5 (Subgroups). Former Section 5. Included statement of two other conditions that imply a subset is a subgroup and kept the proofs in the exercise section. Made minor modifications using examples from new Section 4.
- Section 6 (Cyclic Groups). Former Section 6. Added examples using dihedral group and symmetric group.
- Section 7 (Generating Sets and Cayley Digraphs). Minor modification of former Section 7.

Part II: Structure of Groups

- Overview of changes: The main goal was to give the formal definition of homomorphism earlier in order to simplify the proofs of Cayley's and Lagrange's theorems.
- Section 8 (Groups of Permutations). Included formal definition of homomorphism. Based on parts of former Sections 8, 9, and 13. Used two-row permutation notation to motivate Cayley's theorem before proof. Deleted first part of section 13 (covered in Section 4). Omitted determinant proof of even/odd permutations since definition of determinant usually uses sign of a permutation. Kept orbit counting proof. Put determinant proof and inversion counting proof in exercises.
- Section 9 (Finitely Generated Abelian Groups). Former Section 11. Added the invariant factor version of the theorem. Showed how to go back and forth between the two versions of the fundamental theorem.
- Section 10 (Cosets and the Theorem of Lagrange). Former Section 10. Changed the order by putting Lagrange's Theorem first, motivating G/H later in the section.
- Section 11 (Plane Isometries). Minor modification of former Section 12.

Part III: Homomorphisms and Factor Groups

- Overview of changes: My main goal was to include a few more examples to motivate the theory and give an introduction to using group actions to prove properties of groups.
- Sections 12-15 are based on former Sections 14-17, respectively.
- Section 12 (Factor Groups). Started section with Z/nZ example to motivate general construction. Defined factor groups from normal subgroups first instead of from homomorphisms. After developing factor groups, showed how they are formed from homomorphisms.
- Section 13 (Factor-Group Computations and Simple Groups). Added a few more examples of computing factor groups. Explicitly used the fundamental homomorphism theorem in computation examples.

- Section 14 (Group Action on a Set). Expanded examples of the general linear group and the dihedral group acting on sets. Added some applications of group actions to finite groups in anticipation of the Sylow Theorems, including Cauchy's Theorem and that fact that p-groups have a nontrivial center.
- Section 15 (Applications of G-sets to Counting). Minor modifications.

Part IV: Advanced Group Theory

- Overview of changes: I moved this part to be closer to the rest of the group theory sections. More examples were included to help clarify the concepts.
- Section 16 (Isomorphism Theorems). Former Section 3. Added two examples and rewrote proofs of two theorems.
- Section 17 (Sylow Theorems). Former Sections 36 and 37. Since Cauchy's Theorem and a few other theorems leading to the Sylow Theorems were covered in new Section 14, this material was removed and the old Sections 36 and 37 were combined. A few examples and exercises were added and a proof was rewritten.
- Section 18 (Series of Groups). Former Section 35. The proof of the Zassenhaus Lemma was placed after the theorem instead of making the argument before stating the theorem. One example added.
- Sections 19 (Free Abelian Groups), 20 (Free Groups), and 21 (Group Presentations). Minor modifications of former Sections 38–40.

Part V: Rings and Fields

- Overview of changes: The previous Part IV was split into two parts, one giving an introduction and the second giving methods of constructing rings and fields.
- Section 22 (Rings and Fields). Minor modification of former Section 18.
- Section 23 (Integral Domains). Former Section 19. Changed former Theorem 19.3 to classify all elements in Z_n. Added corollary that Z_p is a field, anticipating the theorem that all finite integral domains are fields.
- Section 24 (Fermat's and Euler's Theorems). Former Section 20. Simplified proof of Euler's generalization using classification of elements in Z_n.
- Section 25 (Encryption). New section outlining how RSA encryption works. This provides a nice application of the material in Section 24.

Part VI: Constructing Rings and Fields

- Overview of changes: Part VI includes sections from the previous Parts IV and V. The change emphasizes construction techniques used to form rings and fields.
- Section 26 (The Field of Quotients of an Integral Domain). Former Section 21. Rewrote the introduction to include two examples of integral domains and their field of quotients to motivate the general construction.
- Section 27 (Rings of Polynomials). Minor modification of former Section 22.
- Section 28 (Factorization of Polynomials over a Field). Former Section 23. Rewrote former Theorem 23.1 by making a lemma showing how to reduce degree of polynomials in set S. Included proof of former 23.11 in the exercises.
- Section 29 (Algebraic Coding Theory). New section introducing coding theory, focusing on polynomial codes. This gives an application of polynomial computation over a finite field.
- Section 30 (Homomorphisms and Factor Rings). Former Section 26. Motivated why you need the usual conditions for an ideal by starting the section with the example of Z/nZ. Rearranged the order by showing that I an ideal of R gives rise

to the factor ring R/I, then included the material on homomorphisms and factor rings from the kernel. Expanded the statement of former Theorem 26.3 to make it easier to read and more approachable.
- Section 31 (Prime and Maximal Ideals). Minor modification of former Section 27.
- Section 32 (Noncommutative Examples). Minor modification of former Section 24.

Part VII: Commutative Algebra

- Overview of changes: This part includes sections that fit under the general heading of commutative algebra.
- Section 33 (Vector Spaces). Former Section 30. Added two examples and a brief introduction to R-modules over a ring motivated by vector spaces and abelian groups. Moved Former Theorem 30.23 to Section 45 on field extensions.
- Section 34 (Unique Factorization Domains). Former Section 45. Included definition of a Noetherian ring and made other minor changes.
- Section 35 (Euclidean Domains) and Section 36 (Number Theory) are minor modifications of Sections 46 and 47, respectively.
- Section 37 (Algebraic Geometry). Based on the first half of former Section 28. Added a proof of the Hilbert Basis Theorem.
- Section 38 (Gröbner Bases for Ideals). Based on the second half of former Section 28. Added two applications of Gröbner Bases: deriving the formulas for conic sections and determining if a graph can be colored with k colors.

Part VIII: Extension Fields

- Overview of changes: Part VIII consists of minor changes from former Part VI.
- Section 39 (Introduction to Extension Fields). Former Section 29. Divided former Theorem 29.13 into a theorem and a corollary. Rewrote former Theorem 29.18 and its proof to make it easier to follow. Included example moved from former Section 30.
- Section 40 (Algebraic Extensions), Section 41 (Geometric Constructions), and Section 42 (Finite Fields) are minor modifications of former Sections 31–33, respectively.

Part IX: Galois Theory

- Overview of changes: The previous Part X was rewritten to form Part IX. The goal was to improve the readability of the material while maintaining a rigorous development of the theory.
- Section 43 (Introduction to Galois Theory). New section. Uses the field extension $Q(\sqrt{2}, \sqrt{3})$ throughout to motivate and illustrate basic definitions and theorems including field automorphism, field fixed by an automorphism, group of automorphisms fixing a subfield, conjugates, and the conjugate isomorphism theorem. By using an easy-to-understand example consistently throughout, the concepts become more concrete.
- Section 44 (Splitting Fields). Includes the contents of former Sections 49 and 50, but it is completely rewritten. Less emphasis is given to the algebraic closure of a field and more emphasis is given to subfields of splitting fields.
- Section 45 (Separable Extensions). Contents include most of former Section 51 and a little from former Section 53, but material has been rewritten. The notation {E:F} was omitted and definition of separable was given in terms of multiplicity of zeros. Emphasized subfields of the complex numbers.

- Former Section 52 on totally inseparable extensions was omitted since it was not used elsewhere and it detracts from the flow of the rest of Part IX.
- Section 46 (Galois Theory). Former Section 53. Separated the parts of Galois Theory into separate theorems. Continued the same example throughout the section to motivate and illustrate the theorems. By the end of the section, the continued example illustrates how Galois Theory can be used.
- Section 47 (Illustrations of Galois Theory). Minor modification of former Section 54.
- Section 48 (Cyclotomic Extensions). Former Section 55. In order to make the text more readable, restricted the field extensions to subfields of the complex numbers over the rational numbers since this is the only case that is used in the book.
- Section 49 (Insolvability of the Quintic). Former Section 56. Replaced construction of a polynomial that is not solvable by radicals with a specific concrete polynomial. The previous construction of a nonsolvable polynomial was moved to the exercises.

Part X: Groups in Topology (Online at bit.ly/2VBCiej)

- Sections 50-53 are minor modifications of former sections 41-44.

Some Features Retained

I continue to break down most exercise sets into parts consisting of computations, concepts, and theory. Answers to most odd-numbered exercises not requesting a proof again appear at the back of the text. I am supplying the answers to parts a, c, e, g, and i only of our 10-part true-false exercises. The excellent historical notes by Victor Katz are, of course, retained.

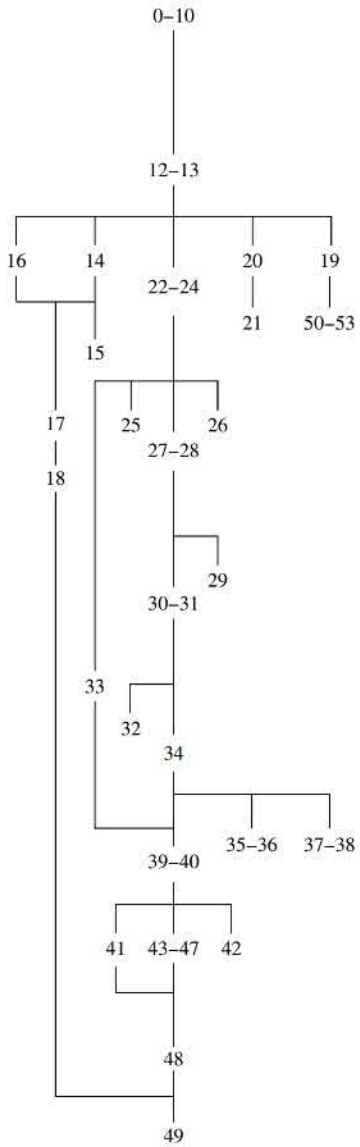
Suggestions for New Instructors of Algebra

Those who have taught algebra several times have discovered the difficulties and developed their own solutions. The comments we make here are not for them.

This course is an abrupt change from the typical undergraduate calculus for the students. A graduate-style lecture presentation, writing out definitions and proofs on the board for most of the class time, will not work with most students. We have found it best to spend at least the first half of each class period answering questions on homework, trying to get a volunteer to give a proof requested in an exercise, and generally checking to see if they seem to understand the material assigned for that class. Typically, we spent only about the last 20 minutes of our 50-minute time talking about new ideas for the next class, and giving at least one proof. The videos for each section can effectively be used to supplement or replace lectures. From a practical point of view, it is a waste of time to try to write on the board all the definitions and proofs. They are in the text.

We suggest that at least half of the assigned exercises consist of the computational ones. Students are used to doing computations in calculus. Although there are many exercises asking for proofs that we would love to assign, we recommend that you assign at most two or three such exercises and try to get someone to explain how each proof is performed in the next class. We do think students should be asked to do at least one proof in each assignment.

Students face a barrage of definitions and theorems, something they have never encountered before. They are not used to mastering this type of material. Grades on tests that seem reasonable to us, requesting a few definitions and proofs, are apt to be low and depressing for most students and instructors. To encourage students to keep up



Dependence Chart

with the basic material, I give approximately ten pop quizzes per semester that typically involve stating a definition, giving an example, or stating a major theorem.

At the University of North Texas, abstract algebra is a two-semester sequence. The first semester is required of all math majors and the second semester is optional. Because most students opt not to continue with the second semester, it is not offered every year. When I teach either class, I give three 50-minute in-class exams. With exam reviews and going over completed exams, this leaves approximately 36 class periods for new material.

In the first-semester class, the base material I always cover includes Sections 0-6, 8, 9, 12, 13, and 22-25. I average approximately two class periods per section, so I can usually cover a few more sections. Options I have used for the remaining time include

Sections 14 and 15, Sections 26-28, Section 17, or Sections 30 and 31. One semester I attempted to cover enough field extension material in order to cover Section 41. This required me to carefully select material in Sections 27, 28, 39, and 40 in order to prepare the students for Section 41.

For the second semester, I usually have as goals proving the impossibility of bisecting an angle using compass and straightedge and the insolvability of quintic polynomials. Assuming that students have seen the basic material in the first semester as described above, these goals require covering material from Sections 16, 18, 27, 28, 30, 31, 33, 34, and 39-49. This turns out to be an ambitious undertaking, but the purpose of rewriting Part IX was to make the material more accessible to students, and therefore make the goal of covering Galois Theory in a second-semester class more feasible.

Acknowledgments

I am very grateful to those who have reviewed the text or who have sent suggestions and corrections. Below is a list of faculty who contributed their thoughts on improving the text.

- Deb Bergstrand, Swarthmore College
- Anthony E. Clement, Brooklyn College
- Richard M. Green, University of Colorado
- Cheryl Grood, Swarthmore College
- Gary Gordon, Lafayette College
- John Harding, New Mexico State University
- Timothy Kohl, Boston University
- Cristian Lenart, University at Albany, SUNY
- Mariana Montiel, Georgia Southern University
- Anne Shiu, Texas A&M University
- Mark Stankus, California Polytechnic State University
- Janet Vassilev, University of New Mexico
- Cassie L. Williams, James Madison University
- T. E. Williamson, Montclair State University
- Michael Zuker, Massachusetts Institute of Technology

I also wish to express appreciation to Jeff Weidenaar, Tara Corpuz, and Jon Krebs at Pearson for their help with this project.

Neal Brand
University of North Texas

Student's Preface

This course may well require a different approach than those you used in previous mathematics courses. You may have become accustomed to working a homework problem by turning back in the text to find a similar problem, and then just changing some numbers. That may work with a few problems in this text, but it will not work for most of them. This is a subject in which understanding is all-important, and where problems should not be tackled without first studying the text.

Let us make some suggestions on studying the text. Notice that the text bristles with definitions, theorems, corollaries, and examples. The definitions are crucial. We must agree on terminology to make any progress. Sometimes a definition is followed by an example that illustrates the concept. Examples are probably the most important aids in studying the text. *Pay attention to the examples.*

Before reading a section, it may be helpful to watch the video associated with the section. I have two general pieces of advice for watching a video or reading the text. First, minimize your distractions. It takes a good deal of concentration for most of us to learn new technical information. Second, have paper and pen (or the electronic equivalent) at hand to take notes and to occasionally work out computations on your own.

I suggest you skip the proofs of the theorems on your first reading of a section, unless you are really "gung-ho" on proofs. You should read the statement of the theorem and try to understand just what it means. Often, a theorem is followed or preceded by an example that illustrates it, which is a great aid in really understanding what the theorem says. Pay particular attention to the summary at the end of each video to get an overview of the topics covered.

In summary, on your first viewing and reading of a section, I suggest you concentrate on what information the section gives and on gaining a real understanding of it. If you do not understand what the statement of a theorem means, it will probably be meaningless for you to read the proof.

Proofs are basic to mathematics. After you feel you understand the information given in a section, you should read and try to understand at least some of the proofs. In the videos you will find a few proofs. Watching the videos a second time after you have a better understanding of the definitions and the statements of the theorems will help to clarify these proofs. Proofs of corollaries are usually the easiest ones, for they often follow directly from the theorem. Many of the exercises under the "Theory" heading

ask for a proof. Try not to be discouraged at the outset. It takes a bit of practice and experience. Proofs in algebra can be more difficult than proofs in geometry and calculus, for there are usually no suggestive pictures that you can draw. Often, a proof falls out easily if you happen to look at just the right expression. Of course, it is hopeless to devise a proof if you do not really understand what it is that you are trying to prove. For example, if an exercise asks you to show that a given thing is a member of a certain set, you must *know* the defining criterion for a thing to be a member of that set, and then show that your given thing satisfies that criterion.

There are several aids for your study at the back of the text. Of course, you will discover the answers to odd-numbered problems that do not involve a proof. If you run into a notation such as Z_n that you do not understand, look in the list of notations that appears after the bibliography. If you run into terminology like *inner automorphism* that you do not understand, look in the index for the first page where the term occurs.

In summary, although an understanding of the subject is important in every mathematics course, it is crucial to your performance in this course. May you find it a rewarding experience.

SECTION 0 SETS AND RELATIONS

On Definitions, and the Notion of a Set

Many students do not realize the great importance of definitions to mathematics. This importance stems from the need for mathematicians to communicate with each other. If two people are trying to communicate about some subject, they must have the same understanding of its technical terms. However, there is an important structural weakness.

It is impossible to define every concept.

Suppose, for example, we define the term *set* as "A **set** is a well-defined collection of objects." One naturally asks what is meant by a *collection.* We could define it as "A collection is an aggregate of things." What, then, is an *aggregate?* Now our language is finite, so after some time we will run out of new words to use and have to repeat some words already examined. The definition is then circular and obviously worthless. Mathematicians realize that there must be some undefined or primitive concept with which to start. At the moment, they have agreed that *set* shall be such a primitive concept. We shall not define *set,* but shall just hope that when such expressions as "the set of all real numbers" or "the set of all members of the United States Senate" are used, people's various ideas of what is meant are sufficiently similar to make communication feasible.

We summarize briefly some of the things we shall simply assume about sets.

1. A set S is made up of **elements,** and if a is one of these elements, we shall denote this fact by $a \in S$.
2. There is exactly one set with no elements. It is the **empty set** and is denoted by $\varnothing$.
3. We may describe a set either by giving a characterizing property of the elements, such as "the set of all members of the United States Senate," or by listing the elements. The standard way to describe a set by listing elements is to enclose the designations of the elements, separated by commas, in braces, for example, $\{1, 2, 15\}$. If a set is described by a characterizing property $P(x)$ of its elements x, the brace notation $\{x \mid P(x)\}$ is also often used, and is read "the set of all x such that the statement $P(x)$ about x is true." Thus

$$\begin{aligned}\{2, 4, 6, 8\} &= \{x \mid x \text{ is an even whole positive number} \leq 8\} \\ &= \{2x \mid x = 1, 2, 3, 4\}.\end{aligned}$$

   The notation $\{x \mid P(x)\}$ is often called "set-builder notation."
4. A set is **well defined,** meaning that if S is a set and a is some object, then either a is definitely in S, denoted by $a \in S$, or a is definitely not in S, denoted by $a \notin S$. Thus, we should never say, "Consider the set S of some positive numbers," for it is not definite whether $2 \in S$ or $2 \notin S$. On the other hand, we can consider the set T of all prime positive integers. Every positive integer is definitely either prime or not prime. Thus $5 \in T$ and $14 \notin T$. It may be hard to actually determine whether an object is in a set. For example, as this book goes to press it is probably unknown whether $2^{(2^{65})} + 1$ is in T. However, $2^{(2^{65})} + 1$ is certainly either prime or not prime.

It is not feasible for this text to push the definition of everything we use all the way back to the concept of a set. For example, we will never define the number π in terms of a set.

Every definition is an *if and only if* type of statement.

With this understanding, definitions are often stated with the *only if* suppressed, but it is always to be understood as part of the definition. Thus we may define an isosceles triangle as follows: "A triangle is **isosceles** if it has two congruent sides" when we really mean that a triangle is isosceles *if and only if* it has two congruent sides.

In our text, we have to define many terms. We use specifically labeled and numbered definitions for the main algebraic concepts with which we are concerned. To avoid an overwhelming quantity of such labels and numberings, we define many terms within the body of the text and exercises using boldface type.

Boldface Convention

A term printed **in boldface** in a sentence is being defined by that sentence.

Do not feel that you have to memorize a definition word for word. The important thing is to *understand* the concept, so that you can define precisely the same concept in your own words. Thus the definition "An **isosceles** triangle is one having two sides of equal length" is perfectly correct. Of course, we had to delay stating our boldface convention until we had finished using boldface in the preceding discussion of sets, because we do not define a set!

In this section, we do define some familiar concepts as sets, both for illustration and for review of the concepts. First we give a few definitions and some notation.

0.1 Definition A set B is a **subset of a set** A, denoted by $B \subseteq A$ or $A \supseteq B$, if every element of B is in A. The notations $B \subset A$ or $A \supset B$ will be used for $B \subseteq A$ but $B \neq A$. ■

Note that according to this definition, for any set A, A itself and $\varnothing$ are both subsets of A.

0.2 Definition If A is any set, then A is the **improper subset of** A. Any other subset of A is a **proper subset of** A. ■

0.3 Example Let $S = \{1, 2, 3\}$. This set S has a total of eight subsets, namely $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, and $\{1, 2, 3\}$. ▲

0.4 Definition Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ is the **Cartesian product** of A and B. ■

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

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

Throughout this text, much work will be done involving familiar sets of numbers. Let us take care of notation for these sets once and for all.

$\mathbb{Z}$ is the set of all integers (that is, whole numbers: positive, negative, and zero).

$\mathbb{Q}$ is the set of all rational numbers (that is, numbers that can be expressed as quotients m/n of integers, where $n \neq 0$).

$\mathbb{R}$ is the set of all real numbers.

$\mathbb{Z}^+$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ are the sets of positive members of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, respectively.

$\mathbb{C}$ is the set of all complex numbers.

$\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ are the sets of nonzero members of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively.

0.6 Example The set $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane that we use in first-semester calculus to draw graphs of functions. ▲

Relations Between Sets

We introduce the notion of an element a of set A being *related* to an element b of set B, which we might denote by $a \mathscr{R} b$. The notation $a \mathscr{R} b$ exhibits the elements a and b in left-to-right order, just as the notation (a, b) for an element in $A \times B$. This leads us to the following definition of a relation $\mathscr{R}$ as a *set*.

0.7 Definition A **relation** between sets A and B is a subset $\mathscr{R}$ of $A \times B$. We read $(a, b) \in \mathscr{R}$ as "a is related to b" and write $a \mathscr{R} b$. ■

0.8 Example Let S be any set. We can define an **Equality Relation** $=$ between S and itself as the subset $\{(x, x) \mid x \in S\}$. Of course, this is nothing new. It is simply the usual idea of what it means for two "things" to be equal. So if $x, y \in S$ are different elements, then they are not related by the equality relation and we write $x \neq y$, but if x and y are the same then we write $x = y$. ▲

We will refer to any relation between a set S and itself, as in the preceding example, as a **relation on** S.

0.9 Example The graph of the function f where $f(x) = x^3$ for all $x \in \mathbb{R}$, is the subset $\{(x, x^3) \mid x \in \mathbb{R}\}$ of $\mathbb{R} \times \mathbb{R}$. Thus it is a relation on $\mathbb{R}$. The function is completely determined by its graph. ▲

The preceding example suggests that rather than define a "function" $y = f(x)$ to be a "rule" that assigns to each $x \in \mathbb{R}$ exactly one $y \in \mathbb{R}$, we can easily describe it as a certain type of subset of $\mathbb{R} \times \mathbb{R}$, that is, as a type of relation. We free ourselves from $\mathbb{R}$ and deal with any sets X and Y.

0.10 Definition A **function** ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ. Such a function is also called a **map** or **mapping** of X into Y. We write $\phi : X \to Y$ and express $(x, y) \in \phi$ by $\phi(x) = y$. The **domain** of ϕ is the set X and the set Y is the **codomain** of ϕ. The **range** of ϕ is $\phi[X] = \{\phi(x) \mid x \in X\}$. ■

0.11 Example We can view the addition of real numbers as a function $+ : (\mathbb{R} \times \mathbb{R}) \to \mathbb{R}$, that is, as a mapping of $\mathbb{R} \times \mathbb{R}$ into $\mathbb{R}$. For example, the action of $+$ on $(2, 3) \in \mathbb{R} \times \mathbb{R}$ is given in function notation by $+((2, 3)) = 5$. In set notation we write $((2, 3), 5) \in +$. Of course, our familiar notation is $2 + 3 = 5$. ▲

Cardinality

The number of elements in a set X is the **cardinality** of X and is often denoted by $|X|$. For example, we have $|\{2, 5, 7\}| = 3$. It will be important for us to know whether two sets have the same cardinality. If both sets are finite, there is no problem; we can simply count the elements in each set. But do $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ have the same cardinality?

To convince ourselves that two sets X and Y have the same cardinality, we try to exhibit a pairing of each x in X with only one y in Y in such a way that each element of Y is also used only once in this pairing. For the sets $X = \{2, 5, 7\}$ and $Y = \{?, !, \#\}$, the pairing

$$2 \leftrightarrow ?, \quad 5 \leftrightarrow \#, \quad 7 \leftrightarrow !$$

shows they have the same cardinality. Notice that we could also exhibit this pairing as $\{(2, ?), (5, \#), (7, !)\}$ which, as a subset of $X \times Y$, is a *relation* between X and Y. The pairing

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & -4 & 4 & -5 & \cdots \end{array}$$

shows that the sets $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinality. Such a pairing, showing that sets X and Y have the same cardinality, is a special type of relation $\leftrightarrow$ between X and Y called a **one-to-one correspondence.** Since each element x of X appears precisely once in this relation, we can regard this one-to-one correspondence as a *function* with domain X. The range of the function is Y because each y in Y also appears in some pairing $x \leftrightarrow y$. We formalize this discussion in a definition.

0.12 Definition *A function $\phi : X \to Y$ is **one-to-one** or **injective** if $\phi(x_1) = \phi(x_2)$ only when $x_1 = x_2$. The function ϕ is **onto** or **surjective** if the range of ϕ is Y. If ϕ is both injective and surjective, ϕ is said to be **bijective**. ■

If a subset of $X \times Y$ is a *one-to-one* function ϕ mapping X *onto* Y, then each $x \in X$ appears as the first member of exactly one ordered pair in ϕ and also each $y \in Y$ appears as the second member of exactly one ordered pair in ϕ. Thus if we interchange the first and second members of all ordered pairs (x, y) in ϕ to obtain a set of ordered pairs (y, x), we get a subset of $Y \times X$, which gives a one-to-one function mapping Y onto X. This function is called the **inverse function** of ϕ, and is denoted by ϕ^{-1}. Summarizing, if ϕ maps X one-to-one onto Y and $\phi(x) = y$, then ϕ^{-1} maps Y one-to-one onto X, and $\phi^{-1}(y) = x$.

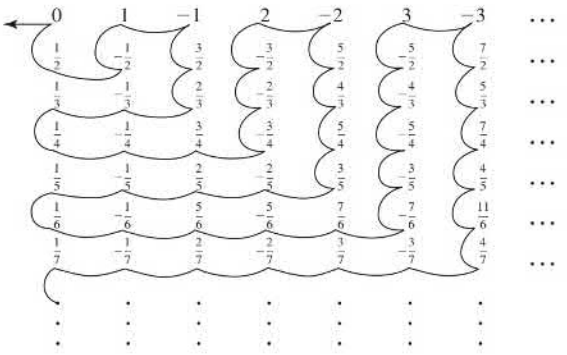
0.13 Definition Two sets X and Y have the **same cardinality** if there exists a one-to-one function mapping X onto Y, that is, if there exists a one-to-one correspondence between X and Y. ■

0.14 Example The function $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$ is not one-to-one because $f(2) = f(-2) = 4$ but $2 \neq -2$. Also, it is not onto $\mathbb{R}$ because the range is the proper subset of all nonnegative numbers in $\mathbb{R}$. However, $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$ is both one-to-one and onto $\mathbb{R}$. ▲

We showed that $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinality. We denote this cardinal number by $\aleph_0$, so that $|\mathbb{Z}| = |\mathbb{Z}^+| = \aleph_0$. It is fascinating that a proper subset of an infinite set may have the same number of elements as the whole set; an **infinite set** can be defined as a set having this property.

We naturally wonder whether all infinite sets have the same cardinality as the set $\mathbb{Z}$. A set has cardinality $\aleph_0$ if and only if *all* of its elements could be listed in an infinite row, so that we could "number them" using $\mathbb{Z}^+$. Figure 0.15 indicates that this is possible for the set $\mathbb{Q}$. The square array of fractions extends infinitely to the right and infinitely

* We should mention another terminology, used by the disciples of N. Bourbaki, in case you encounter it elsewhere. In Bourbaki's terminology, a one-to-one map is an **injection,** an onto map is a **surjection,** and a map that is both one-to-one and onto is a **bijection.**



0.15 Figure

downward, and contains all members of $\mathbb{Q}$. We have shown a string winding its way through this array. Imagine the fractions to be glued to this string. Taking the beginning of the string and pulling to the left in the direction of the arrow, the string straightens out and all elements of $\mathbb{Q}$ appear on it in an infinite row as $0, \frac{1}{2}, -\frac{1}{2}, 1, -1, \frac{3}{2}, \cdots$. Thus $|\mathbb{Q}| = \aleph_0$ also.

If the set $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$ has cardinality $\aleph_0$, all its elements could be listed as unending decimals in a column extending infinitely downward, perhaps as

$$\begin{array}{l} 0.3659663426\cdots \\ 0.7103958453\cdots \\ 0.0358493553\cdots \\ 0.9968452214\cdots \\ \vdots \end{array}$$

We now argue that any such array must omit some number in S. Surely S contains a number r having as its nth digit after the decimal point a number different from 0, from 9, and from the nth digit of the nth number in this list. For example, r might start $.5637\cdots$. The 5 rather than 3 after the decimal point shows r cannot be the first number in S listed in the array shown. The 6 rather than 1 in the second digit shows r cannot be the second number listed, and so on. Because we could make this argument with *any list,* we see that S has too many elements to be paired with those in $\mathbb{Z}^+$. Exercise 15 indicates that $\mathbb{R}$ has the same number of elements as S. We just denote the cardinality of $\mathbb{R}$ by $|\mathbb{R}|$. Exercise 19 indicates that there are infinitely many different cardinal numbers even greater than $|\mathbb{R}|$.

Partitions and Equivalence Relations

Sets are **disjoint** if no two of them share a common element. In Example 0.17 we break up the integers into subsets. Eventually we will see how to define an algebraic structure on these subsets of $\mathbb{Z}$. That is, we will be able to "add" two of these subsets to get another subset. We will find that breaking a set into subsets is a valuable tool in a number of settings, so we conclude this section with a brief study of *partitions* of sets.

0.16 Definition A **partition** of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. The subsets are the **cells** of the partition. ■

When discussing a partition of a set S, we denote by $\bar{x}$ the cell containing the element x of S.

0.17 Example Splitting $\mathbb{Z}$ into the subset of even integers and the subset of odd integers, we obtain a partition of $\mathbb{Z}$ into the two cells listed below.

$$\overline{0} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, \ldots\}$$
$$\overline{1} = \{\ldots, -7, -5, -3, -1, 1, 3, 5, \ldots\}$$

We can think of $\overline{0}$ as being the integers that are divisible by 2 and $\overline{1}$ as the integers that when divided by 2 yield a remainder of 1. This idea can be used for positive integers other than 2. For example, we can partition $\mathbb{Z}$ into three cells:

$$\overline{0} = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\},$$
$$\overline{1} = \{x \in \mathbb{Z} \mid \text{the remainder of } x \text{ divided by 3 is } 1\}, \text{ and}$$
$$\overline{2} = \{x \in \mathbb{Z} \mid \text{the remainder of } x \text{ divided by 3 is } 2\}.$$

Note that when dividing a negative number by 3, we still obtain a non-negative remainder. For example, $-5 \div 3$ is -2 with remainder 1, which says that $\overline{-5} = \overline{1}$.

Generalizing, for each $n \in \mathbb{Z}^+$, we obtain a partition of $\mathbb{Z}$ consisting of n cells, $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$. For each $0 \leq r \leq n-1$, an integer x is in the cell $\bar{r}$ exactly when the remainder of $x \div n$ is r. These cells are the **residue classes modulo *n*** in $\mathbb{Z}$ and n is called the **modulus**. We define the set $\mathbb{Z}/n\mathbb{Z}$ as the set containing the cells in this partition. So, for example, $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. As we can see, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ has exactly n elements. ▲

Each partition of a set S yields a relation $\mathscr{R}$ on S in a natural way: namely, for $x, y \in S$, let $x \mathscr{R} y$ if and only if x and y are in the same cell of the partition. In set notation, we would write $x \mathscr{R} y$ as $(x, y) \in \mathscr{R}$ (see Definition 0.7). A bit of thought shows that this relation $\mathscr{R}$ on S satisfies the three properties of an *equivalence relation* in the following definition.

0.18 Definition An **equivalence relation** $\mathscr{R}$ on a set S is one that satisfies these three properties for all $x, y, z \in S$.

1. (Reflexive) $x \mathscr{R} x$.
2. (Symmetric) If $x \mathscr{R} y$, then $y \mathscr{R} x$.
3. (Transitive) If $x \mathscr{R} y$ and $y \mathscr{R} z$ then $x \mathscr{R} z$. ■

To illustrate why the relation $\mathscr{R}$ corresponding to a partition of S satisfies the symmetric condition in the definition, we need only observe that if y is in the same cell as x (that is, if $x \mathscr{R} y$), then x is in the same cell as y (that is, $y \mathscr{R} x$). We leave the similar observations to verify the reflexive and transitive properties to Exercise 28.

0.19 Example For any nonempty set S, the equality relation $=$ defined by the subset $\{(x, x) \mid x \in S\}$ of $S \times S$ is an equivalence relation. ▲

0.20 Example **(Congruence Modulo *n*)** Let $n \in \mathbb{Z}^+$. The equivalence relation on $\mathbb{Z}$ corresponding to the partition of $\mathbb{Z}$ into residue classes modulo n, discussed in Example 0.17, is **congruence modulo *n***. It is sometimes denoted by $\equiv_n$. Rather than write $a \equiv_n b$, we usually write $a \equiv b \pmod{n}$, read, "a is congruent to b modulo n." For example, we have $15 \equiv 27 \pmod{4}$ because both 15 and 27 have remainder 3 when divided by 4. ▲

0.21 Example Let a relation $\mathscr{R}$ on the set $\mathbb{Z}$ be defined by $n \mathscr{R} m$ if and only if $nm \geq 0$, and let us determine whether $\mathscr{R}$ is an equivalence relation.

Reflexive $a \mathscr{R} a$, because $a^2 \geq 0$ for all $a \in \mathbb{Z}$.

Symmetric If $a \mathscr{R} b$, then $ab \geq 0$, so $ba \geq 0$ and $b \mathscr{R} a$.

Transitive If $a \mathscr{R} b$ and $b \mathscr{R} c$, then $ab \geq 0$ and $bc \geq 0$. Thus $ab^2c = acb^2 \geq 0$.

If we knew $b^2 > 0$, we could deduce $ac \geq 0$ whence $a \mathscr{R} c$. We have to examine the case $b = 0$ separately. A moment of thought shows that $-3 \mathscr{R} 0$ and $0 \mathscr{R} 5$, but we do *not* have $-3 \mathscr{R} 5$. Thus the relation $\mathscr{R}$ is not transitive, and hence is not an equivalence relation. ▲

We observed above that a partition yields a natural equivalence relation. We now show that an equivalence relation on a set yields a natural partition of the set. The theorem that follows states both results for reference.

0.22 Theorem **(Equivalence Relations and Partitions)** Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition of S, where

$$\bar{a} = \{x \in S \mid x \sim a\}.$$

Also, each partition of S gives rise to an equivalence relation $\sim$ on S where $a \sim b$ if and only if a and b are in the same cell of the partition.

Proof We must show that the different cells $\bar{a} = \{x \in S \mid x \sim a\}$ for $a \in S$ do give a partition of S, so that every element of S is in some cell and so that if $a \in \bar{b}$, then $\bar{a} = \bar{b}$. Let $a \in S$. Then $a \in \bar{a}$ by the reflexive condition (1), so a is in *at least one* cell.

Suppose now that $a \in \bar{b}$. We need to show that $\bar{a} = \bar{b}$ as sets; this will show that a cannot be in more than one cell. There is a standard way to show that two sets are the same:

Show that each set is a subset of the other.

We show that $\bar{a} \subseteq \bar{b}$. Let $x \in \bar{a}$. Then $x \sim a$. But $a \in \bar{b}$, so $a \sim b$. Then, by the transitive condition (3), $x \sim b$, so $x \in \bar{b}$. Thus $\bar{a} \subseteq \bar{b}$. Now we show that $\bar{b} \subseteq \bar{a}$. Let $y \in \bar{b}$. Then $y \sim b$. But $a \in \bar{b}$, so $a \sim b$ and, by symmetry (2), $b \sim a$. Then by transitivity (3), $y \sim a$, so $y \in \bar{a}$. Hence $\bar{b} \subseteq \bar{a}$ also, so $\bar{b} = \bar{a}$ and our proof is complete. ◆

Each cell in the partition arising from an equivalence relation is an **equivalence class**.

EXERCISES 0

In Exercises 1 through 4, describe the set by listing its elements.

1. $\{x \in \mathbb{R} \mid x^2 = 3\}$

2. $\{m \in \mathbb{Z} \mid m^2 + m = 6\}$

3. $\{m \in \mathbb{Z} \mid mn = 60 \text{ for some } n \in \mathbb{Z}\}$

4. $\{x \in \mathbb{Z} \mid x^2 - 10x + 16 \leq 0\}$

In Exercises 5 through 10, decide whether the object described is indeed a set (is well defined). Give an alternate description of each set.

5. $\{n \in \mathbb{Z}^+ \mid n \text{ is a large number}\}$

6. $\{n \in \mathbb{Z} \mid n^2 < 0\}$

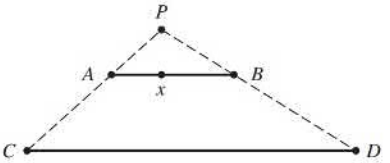
7. $\{n \in \mathbb{Z} \mid 39 < n^3 < 57\}$

8. $\{r \in \mathbb{Q} \mid$ When r is multiplied by a sufficiently large power of 2, one obtains a whole number.$\}$

9. $\{x \in \mathbb{Z}^+ \mid x \text{ is an easy number to factor}\}$

10. $\{x \in \mathbb{Q} \mid x \text{ may be written with positive denominator less than 4}\}$

11. List the elements in $\{a, b, c\} \times \{1, 2, c\}$.



0.23 Figure

12. Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$. For each relation between A and B given as a subset of $A \times B$, decide whether it is a function mapping A into B. If it is a function, decide whether it is one-to-one and whether it is onto B.

a. $\{\{1, 2\}, \{2, 6\}, \{3, 4\}\}$
b. [[1,3] and [5,7]]
c. $\{(1, 6), (1, 2), (1, 4)\}$
d. $\{\{2, 2\}, \{3, 6\}, \{1, 6\}\}$
e. $\{(1, 6), (2, 6), (3, 6)\}$
f. $\{\{1, 2\}, \{2, 6\}\}$

13. Illustrate geometrically that two line segments AB and CD of different lengths have the same number of points by indicating in Fig. 0.23 what point y of CD might be paired with point x of AB.

14. Recall that for $a, b \in \mathbb{R}$ and $a < b$, the **closed interval** $[a, b]$ in $\mathbb{R}$ is defined by $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$. Show that the given intervals have the same cardinality by giving a formula for a one-to-one function f mapping the first interval onto the second.

a. [0, 1] and [0, 2]
b. [1, 3] and [5, 7]
c. $[a, b]$ and $[c, d]$

15. Show that $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$ has the same cardinality as $\mathbb{R}$. [*Hint:* Find an elementary function of calculus that maps an interval one-to-one onto $\mathbb{R}$, and then translate and scale appropriately to make the domain the set S.]

For any set A, we denote by $\mathscr{P}(A)$ the collection of all subsets of A. For example, if $A = \{a, b, c, d\}$, then $\{a, b, d\} \in \mathscr{P}(A)$. The set $\mathscr{P}(A)$ is the **power set** of A. Exercises 16 through 19 deal with the notion of the power set of a set A.

16. List the elements of the power set of the given set and give the cardinality of the power set.

a. $\varnothing$
b. $\{a\}$
c. $\{a, b\}$
d. $\{a, b, c\}$

17. Let A be a finite set, and let $|A| = s$. Based on the preceding exercise, make a conjecture about the value of $|\mathscr{P}(A)|$. Then try to prove your conjecture.

18. For any set A, finite or infinite, let B^A be the set of all functions mapping A into the set $B = \{0, 1\}$. Show that the cardinality of B^A is the same as the cardinality of the set $\mathscr{P}(A)$. [*Hint:* Each element of B^A determines a subset of A in a natural way.]

19. Show that the power set of a set A, finite or infinite, has too many elements to be able to be put in a one-to-one correspondence with A. Explain why this intuitively means that there are an infinite number of infinite cardinal numbers. [*Hint:* Imagine a one-to-one function ϕ mapping A into $\mathscr{P}(A)$ to be given. Show that ϕ cannot be onto $\mathscr{P}(A)$ by considering, for each $x \in A$, whether $x \in \phi(x)$ and using this idea to define a subset S of A that is not in the range of ϕ.] Is *the set of everything* a logically acceptable concept? Why or why not?

20. Let $A = \{1, 2\}$ and let $B = \{3, 4, 5\}$.

a. Illustrate, using A and B, why we consider that $2 + 3 = 5$. Use similar reasoning with sets of your own choice to decide what you would consider to be the value of

i. $3 + \aleph_0$,
ii. $\aleph_0 + \aleph_0$.

b. Illustrate why we consider that $2 \cdot 3 = 6$ by plotting the points of $A \times B$ in the plane $\mathbb{R} \times \mathbb{R}$. Use similar reasoning with a figure in the text to decide what you would consider to be the value of $\aleph_0 \cdot \aleph_0$.

21. How many numbers in the interval $0 \leq x \leq 1$ can be expressed in the form .##, where each # is a digit $0, 1, 2, 3, \cdots, 9$? How many are there of the form .#####? Following this idea, and Exercise 15, decide what you would consider to be the value of $10^{\aleph_0}$. How about $12^{\aleph_0}$ and $2^{\aleph_0}$?

22. Continuing the idea in the preceding exercise and using Exercises 18 and 19, use exponential notation to fill in the three blanks to give a list of five cardinal numbers, each of which is greater than the preceding one.

$$\aleph_0, |\mathbb{R}|, \_\_, \_\_, \_\_.$$

In Exercises 23 through 27, find the number of different partitions of a set having the given number of elements.

23. 1 element **24.** 2 elements **25.** 3 elements

26. 4 elements **27.** 5 elements

28. Consider a partition of a set S. The paragraph following Definition 0.18 explained why the relation

$$x \mathscr{R} y \text{ if and only if } x \text{ and } y \text{ are in the same cell}$$

satisfies the symmetric condition for an equivalence relation. Write similar explanations of why the reflexive and transitive properties are also satisifed.

In Exercises 29 through 34, determine whether the given relation is an equivalence relation on the set. Describe the partition arising from each equivalence relation.

29. $n \mathscr{R} m$ in $\mathbb{Z}$ if $nm > 0$ **30.** $x \mathscr{R} y$ in $\mathbb{R}$ if $x \geq y$

31. $x \mathscr{R} y$ in $\mathbb{Z}^+$ if the greatest common divisor of x and y is greater than 1

32. $(x_1, y_1) \mathscr{R} (x_2, y_2)$ in $\mathbb{R} \times \mathbb{R}$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$

33. $n \mathscr{R} m$ in $\mathbb{Z}^+$ if n and m have the same number of digits in the usual base ten notation

34. $n \mathscr{R} m$ in $\mathbb{Z}^+$ if n and m have the same final digit in the usual base ten notation

35. Using set notation of the form $\{\ldots, \#, \#, \#, \cdots\}$, write the residue classes modulo n in $\mathbb{Z}$ as discussed in Example 0.17 for the indicated values of n.

a. 3 **b.** 4 **c.** 5

36. Write each set by listing its elements.

a. $\mathbb{Z}/3\mathbb{Z}$ **b.** $\mathbb{Z}/4\mathbb{Z}$ **c.** $\mathbb{Z}/5\mathbb{Z}$

37. When discussing residue classes, $\overline{1}$ is not well defined until the modulus n is given. Explain.

38. Let $n \in \mathbb{Z}^+$ and let $\sim$ be defined on $\mathbb{Z}$ by $r \sim s$ if and only if $r - s$ is divisible by n, that is, if and only if $r - s = nq$ for some $q \in \mathbb{Z}$.

a. Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

b. Show that this $\sim$ is the equivalence relation, *congruence modulo n*, of Example 0.20.

39. Let $n \in \mathbb{Z}^+$. Using the relation from Exercise 38, show that if $a_1 \sim a_2$ and $b_1 \sim b_2$, then $(a_1 + b_1) \sim (a_2 + b_2)$.

40. Let $n \in \mathbb{Z}^+$. Using the relation from Exercise 38, show that if $a_1 \sim a_2$ and $b_1 \sim b_2$, then $(a_1 b_1) \sim (a_2 b_2)$.

41. Students often misunderstand the concept of a one-to-one function (mapping). I think I know the reason. You see, a mapping $\phi : A \to B$ has a *direction* associated with it, from A to B. It seems reasonable to expect a one-to-one mapping simply to be a mapping that carries one point of A into one point of B, in the direction indicated by the arrow. But of course, *every* mapping of A into B does this, and Definition 0.12 did not say that at all. With this unfortunate situation in mind, make as good a pedagogical case as you can for calling the functions described in Definition 0.12 *two-to-two functions* instead. (Unfortunately, it is almost impossible to get widely used terminology changed.)

This page is intentionally left blank

PART I

Groups and Subgroups

SECTION 1 BINARY OPERATIONS

The transition from elementary school arithmetic to high school algebra involves using letters to represent unknown numbers and studying the basic properties of equations and expressions. The two main binary operations used in high school algebra are addition and multiplication. Abstract algebra takes the next step in abstraction. Not only are the variables unknown, but the actual operations involved may be unknown! We will study sets that have binary operations with properties similar to those of addition and multiplication of numbers. In Part I, our goal will be to develop some of the basic properties of a group. In this section we start our investigation of groups by defining binary operations, naming properties possessed by some binary operations, and giving examples.

Definitions and Examples

The first step in our journey to understand groups is to give a precise mathematical definition of a binary operation that generalizes the familiar addition and multiplication of numbers. Recall that for any set S, Definition 0.4 defines the set $S \times S$ to contain all ordered pairs (a, b) with $a, b \in S$.

1.1 Definition A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$. ■

Intuitively, we may regard a binary operation $*$ on S as assigning, to each ordered pair (a, b) of elements of S, an element $a * b$ of S.

Binary refers to the fact that we are mapping *pairs* of elements from S into S. We could also define a ternary operation as a function mapping triples of elements of S to S, but we will have no need for this type of operation. Throughout this book we will often drop the term binary and use the term operation to mean binary operation.

1.2 Example Our usual addition $+$ is an operation on the set $\mathbb{R}$. Our usual multiplication $\cdot$ is a different operation on $\mathbb{R}$. In this example, we could replace $\mathbb{R}$ by any of the sets $\mathbb{C}, \mathbb{Z}$, $\mathbb{R}^+$, or $\mathbb{Z}^+$. ▲

Note that we require an operation on a set S to be defined for *every* ordered pair (a, b) of elements from S.

1.3 Example Let $M(\mathbb{R})$ be the set of all matrices[†] with real entries. The usual matrix addition $+$ is *not* an operation on this set since $A + B$ is not defined for an ordered pair (A, B) of matrices having different numbers of rows or of columns. ▲

Sometimes an operation on S provides an operation on a subset H of S also. We make a formal definition.

1.4 Definition Let $*$ be an operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H. ■

By our very definition of an operation $*$ on S, the set S is closed under $*$, but a subset may not be, as the following example shows.

1.5 Example Our usual addition $+$ on the set $\mathbb{R}$ of real numbers does not induce an operation on the set $\mathbb{R}^*$ of nonzero real numbers because $2 \in \mathbb{R}^*$ and $-2 \in \mathbb{R}^*$, but $2 + (-2) = 0$ and $0 \notin \mathbb{R}^*$. Thus $\mathbb{R}^*$ is not closed under $*$. ▲

In our text, we will often have occasion to decide whether a subset H of S is closed under a binary operation $*$ on S. To arrive at a correct conclusion, *we have to know what it means for an element to be in H*, and to use this fact. Students often have trouble here. Be sure you understand the next example.

1.6 Example Let $+$ and $\cdot$ be the usual operations of addition and multiplication on the set $\mathbb{Z}$, and let $H = \{n^2 | n \in \mathbb{Z}^+\}$. Determine whether H is closed under (a) addition and (b) multiplication.

For part (a), we need only observe that $1^2 = 1$ and $2^2 = 4$ are in H, but that $1 + 4 = 5$ and $5 \notin H$. Thus H is not closed under addition.

For part (b), suppose that $r \in H$ and $s \in H$. Using what it means for r and s to be in H, we see that there must be integers n and m in $\mathbb{Z}^+$ such that $r = n^2$ and $s = m^2$. Consequently, $rs = n^2m^2 = (nm)^2$. By the characterization of elements in H and the fact that $nm \in \mathbb{Z}^+$, this means that $rs \in H$, so H is closed under multiplication. ▲

1.7 Example Let F be the set of all real-valued functions f having as domain the set $\mathbb{R}$ of real numbers. We are familiar from calculus with the operations $+$, $-$, $\cdot$, and $\circ$ on F. Namely, for each ordered pair (f, g) of functions in F, we define for each $x \in \mathbb{R}$

$$\begin{array}{rll} f + g \text{ by } (f + g)(x) = f(x) + g(x) & & \text{addition,} \\ f - g \text{ by } (f - g)(x) = f(x) - g(x) & & \text{subtraction,} \\ f \cdot g \text{ by } (f \cdot g)(x) = f(x)g(x) & & \text{multiplication, and} \\ f \circ g \text{ by } (f \circ g)(x) = f(g(x)) & & \text{composition.} \end{array}$$

All four of these functions are again real valued with domain $\mathbb{R}$, so F is closed under all four operations $+$, $-$, $\cdot$, and $\circ$. ▲

The operations described in the examples above are very familiar to you. In this text, we want to *abstract* basic structural concepts from our familiar algebra. To empha-

[†] Most students of abstract algebra have studied linear algebra and are familiar with matrices and matrix operations. For the benefit of those students, examples involving matrices are often given. The reader who is not familiar with matrices can either skip all references to them or turn to the Appendix at the back of the text, where there is a short summary.