JOSEPH A. GALLIAN

CONTEMPORARY ABSTRACT ALGEBRA

8th Edition

Notations

(The number after the item indicates the page where the notation is defined.)

SET THEORY

$\cap_{i\in I}S_i$	intersection of sets S_i, $i \in I$
$\cup_{i\in I}S_i$	union of sets S_i, $i \in I$
$[a]$	$\{x \in S \mid x \sim a\}$, equivalence class of S containing a, 18
$\lvert s\rvert$	number of elements in the set of S

SPECIAL SETS

Z	integers, additive groups of integers, ring of integers
Q	rational numbers, field of rational numbers
Q^+	multiplicative group of positive rational numbers
F^*	set of nonzero elements of F
$\mathbf{R}$	real numbers, field of real numbers
$\mathbf{R}^+$	multiplicative group of positive real numbers
$\mathbf{C}$	complex numbers

FUNCTIONS AND ARITHMETIC

f^{-1}	inverse of the function f
$t \mid s$	t divides s, 3
$t \nmid s$	t does not divide s, 3
$\gcd(a, b)$	greatest common divisor of the integers a and b, 4
$\text{lcm}(a, b)$	least common multiple of the integers a and b, 6
$\lvert a + b\rvert$	$\sqrt{a^2 + b^2}$, 13
$\phi(a)$	image of a under ϕ, 20
$\phi\colon A \to B$	mapping of A to B, 20
gf, $\alpha\beta$	composite function, 21

ALGEBRAIC SYSTEMS

D_4	group of symmetries of a square, dihedral group of order 8, 33
D_n	dihedral group of order $2n$, 34
e	identity element, 43
Z_n	group $\{0, 1, \ldots, n-1\}$ under addition modulo n, 44
$\det A$	the determinant of A, 45
$U(n)$	group of units modulo n (that is, the set of integers less than n and relatively prime to n under multiplication modulo n), 46
$\mathbf{R}^n$	$\{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbf{R}\}$, 47
$SL(2, F)$	group of 2×2 matrices over F with determinant 1, 48
$GL(2, F)$	2×2 matrices of nonzero determinants with coefficients from the field F (the general linear group), 48
g^{-1}	multiplicative inverse of g, 51
$-g$	additive inverse of g, 52
$\lvert G\rvert$	order of the group G, 60
$\lvert g\rvert$	order of the element g, 60
$H \leq G$	subgroup inclusion, 61
$H < G$	subgroup $H \neq G$, 61
$\langle a\rangle$	$\{a^n \mid n \in Z\}$, cyclic group generated by a, 65
$Z(G)$	$\{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$, the center of G, 66

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

$C(a)$	$\{g \in G \mid ga = ag\}$, the centralizer of a in G, 68
$\langle S \rangle$	subgroup generated by the set S, 71
$C(H)$	$\{x \in G \mid xh = hx \text{ for all } h \in H\}$, the centralizer of H, 72
$\phi(n)$	Euler phi function of n, 84
$N(H)$	$\{x \in G \mid xHx^{-1} = H\} = \{x \in G \mid Hx = xH\}$, the normalizer of H in G, 95
$\text{cl}(a)$	conjugacy class of a, 95
G^n	$\{g^n \mid g \in G\}$, 96
S_n	group of one-to-one functions from $\{1, 2, \ldots, n\}$ to itself, 101
A_n	alternating group of degree n, 110
$G \approx \overline{G}$	G and $\overline{G}$ are isomorphic, 128
ϕ_a	mapping given by $\phi_a(x) = axa^{-1}$ for all x, 135
$\text{Aut}(G)$	group of automorphisms of the group G, 136
$\text{Inn}(G)$	group of inner automorphisms of G, 136
aH	$\{ah \mid h \in H\}$, 144
aHa^{-1}	$\{aha^{-1} \mid h \in H\}$, 144
$\lvert G{:}H \rvert$	the index of H in G, 148
HK	$\{hk \mid h \in H, k \in K\}$, 150
$\text{stab}_G(i)$	$\{\phi \in G \mid \phi(i) = i\}$, the stabilizer of i under the permutation group G, 151
$\text{orb}_G(i)$	$\{\phi(i) \mid \phi \in G\}$, the orbit of i under the permutation group G, 151
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$	external direct product of groups $G_1, G_2, \ldots, G_n$, 162
$U_k(n)$	$\{x \in U(n) \mid x \bmod k = 1\}$, 166
G'	commutator subgroup, 181
$H \lhd G$	H is a normal subgroup of G, 185
G/H	factor group, 187
$H \times K$	internal direct product of H and K, 196
$H_1 \times H_2 \times \cdots \times H_n$	internal direct product of $H_1, \ldots, H_n$, 197
$\text{Ker } \phi$	kernel of the homomorphism ϕ, 208
$\phi^{-1}(g')$	inverse image of g' under ϕ, 210
$\phi^{-1}(\overline{K})$	inverse image of $\overline{K}$ under ϕ, 211
$Z[x]$	ring of polynomials with integer coefficients, 246
$M_2(Z)$	ring of all 2×2 matrices with integer entries, 246
$R_1 \oplus R_2 \oplus \cdots \oplus R_n$	direct sum of rings, 247
nZ	ring of multiples of n, 249
$Z[i]$	ring of Gaussian integers, 249
$U(R)$	group of units of the ring R, 251
$\text{char } R$	characteristic of R, 258
$\langle a \rangle$	principal ideal generated by a, 268
$\langle a_1, a_2, \ldots, a_n \rangle$	ideal generated by $a_1, a_2, \ldots, a_n$, 268
R/A	factor ring, 268
$A + B$	sum of ideals A and B, 275
AB	product of ideals A and B, 275
$\text{Ann}(A)$	annihilator of A, 277
$N(A)$	nil radical of A, 277
$F(x)$	field of quotients of $F[x]$, 291
$R[x]$	ring of polynomials over R, 298

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

$\deg f(x)$	degree of the polynomial, 300
$\Phi_p(x)$	pth cyclotomic polynomial, 316
$M_2(Q)$	ring of 2×2 matrices over Q, 352
$\langle v_1, v_2, \ldots, v_n \rangle$	subspace spanned by $v_1, v_2, \ldots, v_n$, 353
$F(a_1, a_2, \ldots, a_n)$	extension of F by $a_1, a_2, \ldots, a_n$, 363
$f'(x)$	the derivative of $f(x)$, 368
$[E{:}F]$	degree of E over F, 378
$\mathrm{GF}(p^n)$	Galois field of order p^n, 389
$\mathrm{GF}(p^n)^*$	nonzero elements of $\mathrm{GF}(p^n)$, 390
$\mathrm{cl}(a)$	$\{xax^{-1} \mid x \in G\}$, the conjugacy class of a, 409
$\Pr(G)$	probability that two elements from G commute, 411
n_p	the number of Sylow p-subgroups of a group, 416
$W(S)$	set of all words from S, 446
$\langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t \rangle$	group with generators $a_1, a_2, \ldots, a_n$ and relations $w_1 = w_2 = \cdots = w_t$, 449
Q_4	quarternions, 453
Q_6	dicyclic group of order 12, 453
D_∞	infinite dihedral group, 454
$\mathrm{fix}(\phi)$	$\{i \in S \mid \phi(i) = i\}$, elements fixed by ϕ, 497
$\mathrm{Cay}(S{:}G)$	Cayley digraph of the group G with generating set S, 506
$k * (a, b, \ldots, c)$	concatenation of k copies of $(a, b, \ldots, c)$, 514
(n, k)	linear code, k-dimensional subspace of F^n, 531
F^n	$F \oplus F \oplus \cdots \oplus F$, direct product of n copies of the field F, 531
$d(u, v)$	Hamming distance between vectors u and v, 532
$\mathrm{wt}(u)$	the number of nonzero components of the vector u (the Hamming weight of u), 532
$\mathrm{Gal}(E/F)$	the automorphism group of E fixing F, 554
E_H	fixed field of H, 554
$\Phi_n(x)$	nth cyclotomic polynomial, 571
$C^\perp$	dual code of a code C, 582

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Contemporary Abstract Algebra

EIGHTH EDITION

Joseph A. Gallian
University of Minnesota Duluth

BROOKS/COLE
CENGAGE Learning

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

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

BROOKS/COLE
CENGAGE Learning

Contemporary Abstract Algebra, Eighth Edition
Joseph A. Gallian

Publisher/Executive Editor: Richard Stratton
Senior Sponsoring Editor: Molly Taylor
Assistant Editor: Shaylin Walsh Hogan
Editorial Assistant: Alex Gontar
Media Editor: Andrew Coppola
Content Project Manager: Katie Costello
Production Manager: Suzanne St. Clair
Art Director: Linda May
Rights Acquisition Specialist: Shalice Shah-Caldwell
Manufacturing Planner: Doug Bertke
Manufacturing Manager: Marcia Locke
Marketing Communications Manager: Mary Anne Payumo
Rights Acquisition Director: Tim Sisler
Marketing Coordinator: Michael Ledesma
Inventory Analyst: Anna Matos
Content Manager: Rachel Wimberly

© 2013, 2010, 2006 Brooks/Cole, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means, graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at **Cengage Learning Customer & Sales Support, 1-800-354-9706**

For permission to use material from this text or product, submit all requests online at **www.cengage.com/permissions**
Further permissions questions can be emailed to **permissionrequest@cengage.com**

Library of Congress Control Number: 2012938179
Student Edition:
ISBN-13: 978-1-133-59970-8
ISBN-10: 1-133-59970-2

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

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

To my wonderful grandson, Joey Yapel.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Contents

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Preface

Dear Sir or Madam, will you read my book, it took me years to write, will you take a look?

John Lennon and Paul McCartney, *"Paperback Writer," single, 1966**

Although I wrote the first edition of this book more than 25 years ago, my goals for it remain the same. I want students to receive a solid introduction to the traditional topics. I want readers to come away with the view that abstract algebra is a contemporary subject—that its concepts and methodologies are being used by working mathematicians, computer scientists, physicists, and chemists. I want students to see the connections between abstract algebra and number theory and geometry. I want students to be able to do computations and to write proofs. I want students to enjoy reading the book. And I want to convey to the reader my enthusiasm for this beautiful subject.

Educational research has shown that an effective way of learning mathematics is to interweave worked-out examples and practice problems. Thus, I have made examples and exercises the heart of the book. The examples elucidate the definitions, theorems, and proof techniques. The exercises facilitate understanding, provide insight, and develop the ability of the students to do proofs. The exercises often foreshadow definitions, concepts, and theorems to come. Many exercises focus on special cases and ask the reader to generalize. Generalizing is a skill that students should develop but rarely do. Even if an instructor chooses not to spend class time on the applications in the book, I feel that having them there demonstrates to students the utility of the theory.

Changes for the eighth edition include 200 new exercises, new examples, and a freshening of the quotations, historical notes, and biographies. These changes accentuate and enhance the hallmark features that have made previous editions of the book a comprehensive, lively, and engaging introduction to the subject:

- Extensive coverage of groups, rings, and fields, plus a variety of nontraditional special topics

*Copyright © 1966 (Renewed) Stony/ATV Tunes LLC. All rights administered by Sony/ATV Music Publishing, 8 Music Square West, Nashville, TN 37203. All rights reserved. Used by permission.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- A good mixture of nearly 2000 computational and theoretical exercises appearing in each chapter and in Supplementary Exercise sets that synthesize concepts from multiple chapters
- Back-of-the-book skeleton solutions and hints to the odd-numbered exercises
- Worked-out examples—now totaling nearly 300—ranging from routine computations to quite challenging problems
- Computer exercises, which utilize interactive software available on my website, that stress guessing and making conjectures
- A large number of applications from scientific and computing fields, as well as from everyday life
- Numerous historical notes and biographies that spotlight the people and events behind the mathematics
- Lines from popular songs, poems, and quotations
- Scores of photographs, hundreds of figures, numerous tables and charts, and reproductions of stamps and currency that honor mathematicians
- Annotated suggested readings and media for interesting further exploration of topics

To make room for the new material, the computer exercises from previous editions are available at **www.d.umn.edu/~jgallian** or through Cengage's book companion site at **www.cengage.com/math/gallian**. The first website also offers a wealth of additional online resources supporting the book, including:

- True/false questions with comments
- Flash cards
- Essays on learning abstract algebra, doing proofs, and reasons why abstract algebra is a valuable subject to learn
- Links to abstract algebra–related websites and software packages and much, much more

Additionally, Cengage offers the following student and instructor ancillaries to accompany the book:

- A *Student Solutions Manual*, available for purchase separately, with detailed solutions to the odd-numbered exercises in the book (ISBN:978-1-133-60853-0)
- Solution Builder, an online instructor database that offers complete, worked-out solutions to all exercises in the text, which allows you to create customized, secure solutions printouts (in PDF format) matched exactly to the problems you assign in class. Sign up for access at www.cengage.com/solutionbuilder.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- An *Instructor's Solutions Manual* with solutions to all the exercises in the book and additional test questions and solutions
- An online laboratory manual, written by Julianne Rainbolt, with exercises designed to be done with the free computer algebra system software GAP
- Online instructor answer keys to the book's computer exercises and the exercises in the GAP lab manual

Special thanks go to my copy editor for this edition, Jeff Anderson, and the accuracy checker, Roger Lipsett. I am grateful to each for their careful attention to the manuscript. My appreciation also goes to Molly Taylor, Shaylin Hogan, and Alex Gontar from Cengage Learning, as well as Katie Costello and the Cengage production staff.

The thoughtful input of the following people, who served as reviewers for the eighth edition, is also sincerely appreciated: Homer Austin, Salisbury University; David Barth-Hart, Rochester Institute of Technology; Bret Benesh, College of St. Benedict and St. John's University; Daniel Daly, Southeast Missouri State University; Paul Felt, University of Texas of the Permian Basin; Donald Hartig, California Polytechnic State University, San Luis Obispo; Nancy Ann Neudauer, Pacific University; Bingwu Wang, Eastern Michigan University; Dana Williams, Dartmouth College; and Norbert Youmbi, Saint Francis University.

Over the years, many faculty and students have kindly sent me valuable comments and suggestions. They have helped to make each edition better. I owe many thanks to my UMD colleague Robert McFarland for giving me numerous exercises and comments that have been included in this edition. Douglas Dunham, another UMD colleague, has generously provided the spectacular cover image for this edition. For an explanation of the mathematics underlying this image see **www.d.umn.edu/~jgallian/Dunhamimage**. Please send any comments and suggestions you have to me at **jgallian@d.umn.edu**

Joseph A. Gallian

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PART 1

Integers and Equivalence Relations

For online student resources, visit this textbook's website at www.CengageBrain.com

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

0 Preliminaries

The whole of science is nothing more than a refinement of everyday thinking.

ALBERT EINSTEIN, *Physics and Reality*

Properties of Integers

Much of abstract algebra involves properties of integers and sets. In this chapter we collect the properties we need for future reference.

An important property of the integers, which we will often use, is the so-called Well Ordering Principle. Since this property cannot be proved from the usual properties of arithmetic, we will take it as an axiom.

Well Ordering Principle

Every nonempty set of positive integers contains a smallest member.

The concept of divisibility plays a fundamental role in the theory of numbers. We say a nonzero integer t is a *divisor* of an integer s if there is an integer u such that $s = tu$. In this case, we write $t \mid s$ (read "t divides s"). When t is not a divisor of s, we write $t \nmid s$. A *prime* is a positive integer greater than 1 whose only positive divisors are 1 and itself. We say an integer s is a *multiple* of an integer t if there is an integer u such that $s = tu$ or, equivalently, if t is a divisor of s.

As our first application of the Well Ordering Principle, we establish a fundamental property of integers that we will use often.

Theorem 0.1 Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

PROOF We begin with the existence portion of the theorem. Consider the set $S = \{a - bk \mid k \text{ is an integer and } a - bk \geq 0\}$. If $0 \in S$, then b

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

divides a and we may obtain the desired result with $q = a/b$ and $r = 0$. Now assume $0 \notin S$. Since S is nonempty [if $a > 0$, $a - b \cdot 0 \in S$; if $a < 0$, $a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \notin S$], we may apply the Well Ordering Principle to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$, so all that remains to be proved is that $r < b$.

If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, so that $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, and $a - bq$ is the *smallest* member of S. So, $r < b$.

To establish the uniqueness of q and r, let us suppose that there are integers q, q', r, and r' such that

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

For convenience, we may also suppose that $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. So, b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$, and therefore $r' = r$ and $q = q'$. ∎

The integer q in the division algorithm is called the *quotient* upon dividing a by b; the integer r is called the *remainder* upon dividing a by b.

EXAMPLE 1 For $a = 17$ and $b = 5$, the division algorithm gives $17 = 5 \cdot 3 + 2$; for $a = -23$ and $b = 6$, the division algorithm gives $-23 = 6(-4) + 1$. ∎

Definitions Greatest Common Divisor, Relatively Prime Integers
The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $\gcd(a, b)$. When $\gcd(a, b) = 1$, we say a and b are *relatively prime*.

The following property of the greatest common divisor of two integers plays a critical role in abstract algebra. The proof provides an application of the division algorithm and our second application of the Well Ordering Principle.

Theorem 0.2 GCD Is a Linear Combination

For any nonzero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

PROOF Consider the set $S = \{am + bn \mid m, n \text{ are integers and } am + bn > 0\}$. Since S is obviously nonempty (if some choice of m

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

and n makes $am + bn < 0$, then replace m and n by $-m$ and $-n$), the Well Ordering Principle asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = \gcd(a, b)$. To verify this claim, use the division algorithm to write $a = dq + r$, where $0 \leq r < d$. If $r > 0$, then $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$, contradicting the fact that d is the smallest member of S. So, $r = 0$ and d divides a. Analogously (or, better yet, by symmetry), d divides b as well. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a and b and write $a = d'h$ and $b = d'k$. Then $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$, so that d' is a divisor of d. Thus, among all common divisors of a and b, d is the greatest. ∎

The special case of Theorem 0.2 when a and b are relatively prime is so important in abstract algebra that we single it out as a corollary.

Corollary

If a and b are relatively prime, then there exist integers s and t such that as + bt = 1.

EXAMPLE 2 $\gcd(4, 15) = 1$; $\gcd(4, 10) = 2$; $\gcd(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$. Note that 4 and 15 are relatively prime, whereas 4 and 10 are not. Also, $4 \cdot 4 + 15(-1) = 1$ and $4(-2) + 10 \cdot 1 = 2$. ∎

The next lemma is frequently used. It appeared in Euclid's *Elements*.

Euclid's Lemma $p \mid ab$ Implies $p \mid a$ or $p \mid b$

If p is a prime that divides ab, then p divides a or p divides b.

PROOF Suppose p is a prime that divides ab but does not divide a. We must show that p divides b. Since p does not divide a, there are integers s and t such that $1 = as + pt$. Then $b = abs + ptb$, and since p divides the right-hand side of this equation, p also divides b. ∎

Note that Euclid's Lemma may fail when p is not a prime, since $6 \mid (4 \cdot 3)$ but $6 \nmid 4$ and $6 \nmid 3$.

Our next property shows that the primes are the building blocks for all integers. We will often use this property without explicitly saying so.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 0.3 Fundamental Theorem of Arithmetic

Every integer greater than 1 *is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if* $n = p_1 p_2 \cdots p_r$ *and* $n = q_1 q_2 \cdots q_s$*, where the p's and q's are primes, then* $r = s$ *and, after renumbering the q's, we have* $p_i = q_i$ *for all i.*

We will prove the existence portion of Theorem 0.3 later in this chapter (Example 11). The uniqueness portion is a consequence of Euclid's Lemma (Exercise 31).

Another concept that frequently arises is that of the least common multiple of two integers.

Definition Least Common Multiple
The *least common multiple* of two nonzero integers *a* and *b* is the smallest positive integer that is a multiple of both *a* and *b*. We will denote this integer by lcm(*a*, *b*).

We leave it as an exercise (Exercise 10) to prove that every common multiple of a and b is a multiple of lcm(a, b).

EXAMPLE 3 lcm(4, 6) = 12; lcm(4, 8) = 8; lcm(10, 12) = 60; lcm(6, 5) = 30; $\text{lcm}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2$. ∎

Modular Arithmetic

Another application of the division algorithm that will be important to us is modular arithmetic. Modular arithmetic is an abstraction of a method of counting that you often use. For example, if it is now September, what month will it be 25 months from now? Of course, the answer is October, but the interesting fact is that you didn't arrive at the answer by starting with September and counting off 25 months. Instead, without even thinking about it, you simply observed that $25 = 2 \cdot 12 + 1$, and you added 1 month to September. Similarly, if it is now Wednesday, you know that in 23 days it will be Friday. This time, you arrived at your answer by noting that $23 = 7 \cdot 3 + 2$, so you added 2 days to Wednesday instead of counting off 23 days. If your electricity is off for 26 hours, you must advance your clock 2 hours, since $26 = 2 \cdot 12 + 2$. Surprisingly, this simple idea has numerous

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

important applications in mathematics and computer science. You will see a few of them in this section. The following notation is convenient.

When $a = qn + r$, where q is the quotient and r is the remainder upon dividing a by n, we write $a \bmod n = r$. Thus,

$$\begin{aligned} 3 \bmod 2 &= 1 \text{ since } 3 = 1 \cdot 2 + 1, \\ 6 \bmod 2 &= 0 \text{ since } 6 = 3 \cdot 2 + 0, \\ 11 \bmod 3 &= 2 \text{ since } 11 = 3 \cdot 3 + 2, \\ 62 \bmod 85 &= 62 \text{ since } 62 = 0 \cdot 85 + 62, \\ -2 \bmod 15 &= 13 \text{ since } -2 = (-1)15 + 13. \end{aligned}$$

In general, if a and b are integers and n is a positive integer, then $a \bmod n = b \bmod n$ if and only if n divides $a - b$ (Exercise 7).

In our applications, we will use addition and multiplication mod n. When you wish to compute $ab \bmod n$ or $(a + b) \bmod n$, and a or b is greater than n, it is easier to "mod first." For example, to compute $(27 \cdot 36) \bmod 11$, we note that $27 \bmod 11 = 5$ and $36 \bmod 11 = 3$, so $(27 \cdot 36) \bmod 11 = (5 \cdot 3) \bmod 11 = 4$. (See Exercise 9.)

Modular arithmetic is often used in assigning an extra digit to identification numbers for the purpose of detecting forgery or errors. We present two such applications.

EXAMPLE 4 The United States Postal Service money order shown in Figure 0.1 has an identification number consisting of 10 digits together with an extra digit called a *check.* The check digit is the 10-digit number modulo 9. Thus, the number 3953988164 has the check digit 2, since

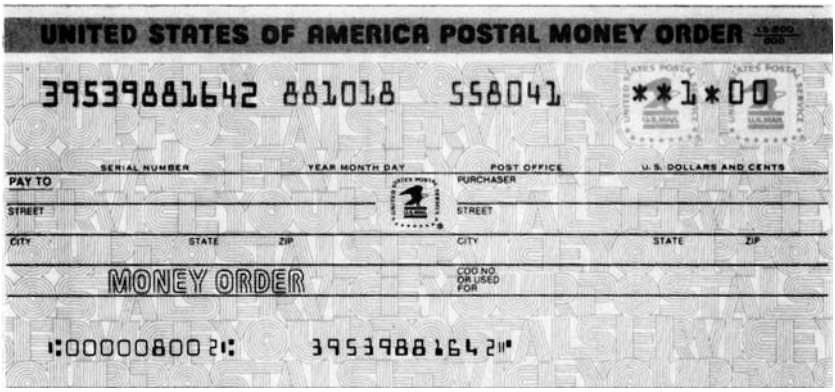


Figure 0.1

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

3953988164 mod 9 = 2.† If the number 39539881642 were incorrectly entered into a computer (programmed to calculate the check digit) as, say, 39559881642 (an error in the fourth position), the machine would calculate the check digit as 4, whereas the entered check digit would be 2. Thus, the error would be detected. ∎

∎ **EXAMPLE 5** Airline companies, the United Parcel Service, and the rental-car companies Avis and National use the mod 7 values of identification numbers to assign check digits. Thus, the identification number 00121373147367 (see Figure 0.2) has the check digit 3 appended

Figure 0.2

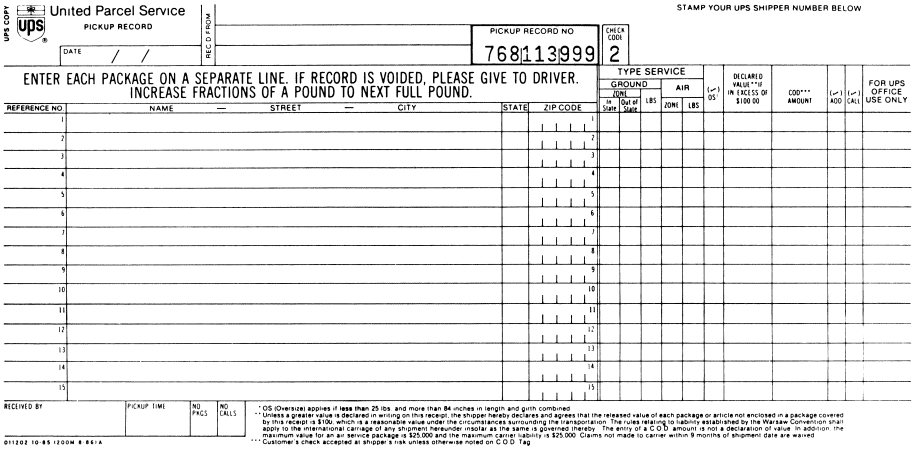


Figure 0.3

†The value of N mod 9 is easy to compute with a calculator. If $N = 9q + r$, where r is the remainder upon dividing N by 9, then on a calculator screen $N \div 9$ appears as $q.rrrrr\ldots$, so the first decimal digit is the check digit. For example, $3953988164 \div 9 = 439332018.222$, so 2 is the check digit. If N has too many digits for your calculator, replace N by the sum of its digits and divide that number by 9. Thus, 3953988164 mod 9 = 56 mod 9 = 2. The value of 3953988164 mod 9 can also be computed by searching Google for "3953988164 mod 9."

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

to it because 121373147367 mod 7 = 3. Similarly, the UPS pickup record number 768113999, shown in Figure 0.3, has the check digit 2 appended to it. ∎

The methods used by the Postal Service and the airline companies do not detect all single-digit errors (see Exercises 41 and 45). However, detection of all single-digit errors, as well as nearly all errors involving the transposition of two adjacent digits, is easily achieved. One method that does this is the one used to assign the so-called Universal Product Code (UPC) to most retail items (see Figure 0.4). A UPC identification number has 12 digits. The first six digits identify the manufacturer, the next five identify the product, and the last is a check. (For many items, the 12th digit is not printed, but it is always bar-coded.) In Figure 0.4, the check digit is 8.

Figure 0.4

To explain how the check digit is calculated, it is convenient to introduce the dot product notation for two k-tuples:

$$(a_1, a_2, \ldots, a_k) \cdot (w_1, w_2, \ldots, w_k) = a_1w_1 + a_2w_2 + \cdots + a_kw_k.$$

An item with the UPC identification number $a_1a_2 \cdots a_{12}$ satisfies the condition

$$(a_1, a_2, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10 = 0.$$

To verify that the number in Figure 0.4 satisfies this condition, we calculate

$$\begin{aligned}(0 \cdot 3 + 2 \cdot 1 + 1 \cdot 3 + 0 \cdot 1 + 0 \cdot 3 + 0 \cdot 1 + 6 \cdot 3 + 5 \cdot 1 \\ + 8 \cdot 3 + 9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1) \bmod 10 = 90 \bmod 10 = 0.\end{aligned}$$

The fixed k-tuple used in the calculation of check digits is called the *weighting vector.*

Now suppose a single error is made in entering the number in Figure 0.4 into a computer. Say, for instance, that 021000958978 is

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

entered (notice that the seventh digit is incorrect). Then the computer calculates

$$0 \cdot 3 + 2 \cdot 1 + 1 \cdot 3 + 0 \cdot 1 + 0 \cdot 3 + 0 \cdot 1 + 9 \cdot 3 + 5 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1 = 99.$$

Since $99 \bmod 10 \neq 0$, the entered number cannot be correct.

In general, any single error will result in a sum that is not 0 modulo 10.

The advantage of the UPC scheme is that it will detect nearly all errors involving the transposition of two adjacent digits as well as all errors involving one digit. For doubters, let us say that the identification number given in Figure 0.4 is entered as 021000658798. Notice that the last two digits preceding the check digit have been transposed. But by calculating the dot product, we obtain $94 \bmod 10 \neq 0$, so we have detected an error. In fact, the only undetected transposition errors of adjacent digits a and b are those where $|a - b| = 5$. To verify this, we observe that a transposition error of the form

$$a_1 a_2 \cdots a_i a_{i+1} \cdots a_{12} \rightarrow a_1 a_2 \cdots a_{i+1} a_i \cdots a_{12}$$

is undetected if and only if

$$(a_1, a_2, \ldots, a_{i+1}, a_i, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10 = 0.$$

That is, the error is undetected if and only if

$$(a_1, a_2, \ldots, a_{i+1}, a_i, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10 = (a_1, a_2, \ldots, a_i, a_{i+1}, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10.$$

This equality simplifies to either

$$(3a_{i+1} + a_i) \bmod 10 = (3a_i + a_{i+1}) \bmod 10$$

or

$$(a_{i+1} + 3a_i) \bmod 10 = (a_i + 3a_{i+1}) \bmod 10,$$

depending on whether i is even or odd. Both cases reduce to $2(a_{i+1} - a_i) \bmod 10 = 0$. It follows that $|a_{i+1} - a_i| = 5$, if $a_{i+1} \neq a_i$.

In 2005, United States companies began to phase in the use of a 13th digit to be in conformance with the 13-digit product identification numbers used in Europe. The weighting vector for 13-digit numbers is (1, 3, 1, 3, . . . , 3, 1).

Identification numbers printed on bank checks (on the bottom left between the two colons) consist of an eight-digit number $a_1 a_2 \cdots a_8$ and a check digit a_9, so that

$$(a_1, a_2, \ldots, a_9) \cdot (7, 3, 9, 7, 3, 9, 7, 3, 9) \bmod 10 = 0.$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

As is the case for the UPC scheme, this method detects all single-digit errors and all errors involving the transposition of adjacent digits a and b except when $|a - b| = 5$. But it also detects most errors of the form $\cdots abc \cdots \rightarrow \cdots cba \cdots$, whereas the UPC method detects no errors of this form.

In Chapter 5, we will examine more sophisticated means of assigning check digits to numbers.

What about error correction? Suppose you have a number such as 73245018 and you would like to be sure that if even a single mistake were made in entering this number into a computer, the computer would nevertheless be able to determine the correct number. (Think of it. You could make a mistake in dialing a telephone number but still get the correct phone to ring!) This is possible using two check digits. One of the check digits determines the magnitude of any single-digit error, while the other check digit locates the position of the error. With these two pieces of information, you can fix the error. To illustrate the idea, let us say that we have the eight-digit identification number $a_1a_2 \cdots a_8$. We assign two check digits a_9 and a_{10} so that

$$(a_1 + a_2 + \cdots + a_9 + a_{10}) \bmod 11 = 0$$

and

$$(a_1, a_2, \ldots, a_9, a_{10}) \cdot (1, 2, 3, \ldots, 10) \bmod 11 = 0$$

are satisfied.

Let's do an example. Say our number before appending the two check digits is 73245018. Then a_9 and a_{10} are chosen to satisfy

$$(7 + 3 + 2 + 4 + 5 + 0 + 1 + 8 + a_9 + a_{10}) \bmod 11 = 0 \qquad (1)$$

and

$$\begin{aligned}(7 \cdot 1 + 3 \cdot 2 + 2 \cdot 3 + 4 \cdot 4 + 5 \cdot 5 + 0 \cdot 6 \\ + 1 \cdot 7 + 8 \cdot 8 + a_9 \cdot 9 + a_{10} \cdot 10) \bmod 11 = 0.\end{aligned} \qquad (2)$$

Since $7 + 3 + 2 + 4 + 5 + 0 + 1 + 8 = 30$ and $30 \bmod 11 = 8$, Equation (1) reduces to

$$(8 + a_9 + a_{10}) \bmod 11 = 0. \qquad (1')$$

Likewise, since $(7 \cdot 1 + 3 \cdot 2 + 2 \cdot 3 + 4 \cdot 4 + 5 \cdot 5 + 0 \cdot 6 + 1 \cdot 7 + 8 \cdot 8) \bmod 11 = 10$, Equation (2) reduces to

$$(10 + 9a_9 + 10a_{10}) \bmod 11 = 0. \qquad (2')$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Since we are using mod 11, we may rewrite Equation (2′) as

$$(-1 - 2a_9 - a_{10}) \bmod 11 = 0$$

and add this to Equation (1′) to obtain $7 - a_9 = 0$. Thus $a_9 = 7$. Now substituting $a_9 = 7$ into Equation (1′) or Equation (2′), we obtain $a_{10} = 7$ as well. So, the number is encoded as 7324501877.

Now let us suppose that this number is erroneously entered into a computer programmed with our encoding scheme as 7824501877 (an error in position 2). Since the sum of the digits of the received number mod 11 is 5, we know that some digit is 5 too large (assuming only one error has been made). But which one? Say the error is in position i. Then the second dot product has the form $a_1 \cdot 1 + a_2 \cdot 2 + \ldots + (a_i + 5)i + a_{i+1} \cdot (i + 1) + \ldots + a_{10} \cdot 10 = (a_1, a_2, \ldots, a_{10}) \cdot (1, 2, \ldots, 10) + 5i$. So, $(7, 8, 2, 4, 5, 0, 1, 8, 7, 7) \cdot (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \bmod 11 = 5i \bmod 11$. Since the left-hand side mod 11 is 10, we see that $i = 2$. Our conclusion: The digit in position 2 is 5 too large. We have successfully corrected the error.

Modular arithmetic is often used to verify the validity of statements about divisibility regarding all positive integers by checking only finitely many cases.

EXAMPLE 6 Consider the statement, "The sum of the cubes of any three consecutive integers is divisible by 9." This statement is equivalent to checking that the equation $(n^3 + (n + 1)^3 + (n + 2)^3) \bmod 9 = 0$ is true for all integers n. Because of properties of modular arithmetic, to prove this, all we need do is check the validity of the equation for $n = 0$, 1, …, 8. ∎

Modular arithmetic is occasionally used to show that certain equations have no rational number solutions.

EXAMPLE 7 We use mod 3 arithmetic to show that there are no integers a and b such that $a^2 - 6b = 2$. To see this, suppose that there are such integers. Then, taking both sides modulo 3, there is an integer solution to $a^2 \bmod 3 = 2$. But trying $a = 0$, 1, and 2 we obtain a contradiction. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

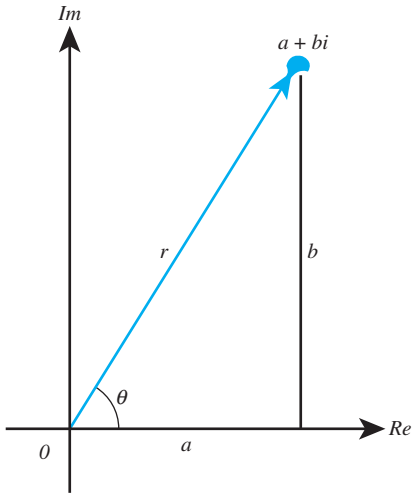


Figure 0.5

Complex Numbers

Recall that complex numbers are expressions of the form $a + b\sqrt{-1}$, where a and b are real numbers. The number $\sqrt{-1}$ is defined to have the property $\sqrt{-1}^2 = -1$. It is customary to use i to denote $\sqrt{-1}$. Then, $i^2 = -1$. Complex numbers written in the form $a + bi$ are said to be in *standard* form. In some instances it is convenient to write a complex number $a + bi$ in another form. To do this we represent $a + bi$ as the point (a,b) in a plane coordinatized by a horizontal axis called the *real* axis and a vertical i axis called the *imaginary* axis. The distance from the point $a + bi$ to the origin is $r = \sqrt{a^2 + b^2}$ and is often denoted by $|a + bi|$. If we draw the line segment from the origin to $a + bi$ and denote the angle formed by the line segment and the positive real axis by θ, we can write $a + bi$ as $r(\cos\theta + i \sin\theta)$ (see Figure 0.5). This form of $a + bi$ is called the *polar* form. An advantage of the polar form is demonstrated in parts 5 and 6 of Theorem 0.4.

Theorem 0.4 Properties of Complex Numbers

1. Closure under addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$
2. Closure under multiplication: $(a + bi)(c + di) = (ac) + (ad)i + (bc)i + (bd)i^2 = (ac - bd) + (ad + bc)i$
3. Closure under division $(c + di \neq 0)$: $\dfrac{(a + bi)}{(c + di)} = \dfrac{(a + bi)}{(c + di)}\dfrac{(c - di)}{(c - di)} = \dfrac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \dfrac{(ac + bd)}{c^2 + d^2} + \dfrac{(bc - ad)}{c^2 + d^2}i$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

4. Complex conjugation: $(a + bi)(a - bi) = a^2 + b^2$
5. Inverses: For every nonzero complex number $a + bi$ there is a complex number $c + di$ such that $(a + bi)(c + di) = 1$. (That is, $(a + bi)^{-1}$ exists in C.)
6. Powers: For every complex number $a + bi = r(\cos\theta + i\sin\theta)$ and every positive integer n, we have $(a + bi)^n = [r(\cos\theta + i\sin\theta)]^n = r^n(\cos n\theta + i\sin n\theta)$.
7. Radicals: For every complex number $a + bi = r(\cos\theta + i\sin\theta)$ and every positive integer n, we have $(a + bi)^{\frac{1}{n}} = [r(\cos\theta + i\sin\theta)]^{\frac{1}{n}} = r^{\frac{1}{n}}(\cos\frac{\theta}{n} + i\sin\frac{\theta}{n})$.

PROOF Parts 1 and 2 are definitions. Part 4 follows from part 2. Part 6 is proved in Example 10 in the next section of this chapter. Part 7 follows from Exercise 25 in this chapter. ∎

The next example illustrates properties of complex numbers.

EXAMPLE 8 $(3 + 5i) + (-5 + 2i) = -2 + 7i$;

$(3 + 5i)(-5 + 2i) = -25 + (-19)i = -25 - 19i$;

$$\frac{3 + 5i}{-2 + 7i} = \frac{3 + 5i}{-2 + 7i}\,\frac{-2 - 7i}{-2 - 7i} = \frac{29 - 31i}{53} = \frac{29}{53} + \frac{-31}{53}i;$$

$(3 + 5i)(3 - 5i) = 9 + 25 = 34$;

$$(3 + 5i)^{-1} = \frac{3}{34} - \frac{5}{34}i.$$

To find $(3 + 5i)^4$ and $(3 + 5i)^{\frac{1}{4}}$ we first note that if $\theta = \arctan\frac{5}{3}$, then $\cos\theta = \frac{3}{\sqrt{34}}$ and $\sin\theta = \frac{5}{\sqrt{34}}$. Thus, $(3 + 5i)^4 = ((\sqrt{34}(\cos\theta + i\sin\theta))^4 = \sqrt{34}^4(\cos 4\theta + i\sin 4\theta)$ and $(3 + 5i)^{\frac{1}{4}} = (\sqrt{34}(\cos\theta + i\sin\theta))^{\frac{1}{4}} = \sqrt{34}^{\frac{1}{4}}(\cos\frac{\theta}{4} + i\sin\frac{\theta}{4})$.

Mathematical Induction

There are two forms of proof by mathematical induction that we will use. Both are equivalent to the Well Ordering Principle. The explicit formulation of the method of mathematical induction came in the 16th century. Francisco Maurolico (1494–1575), a teacher of Galileo, used it in 1575 to prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$, and Blaise Pascal (1623–1662) used it when he presented what we now call Pascal's triangle for the coefficients of the binomial expansion. The term *mathematical induction* was coined by Augustus De Morgan.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 0.5 First Principle of Mathematical Induction

Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

PROOF The proof is left as an exercise (Exercise 33). ∎

So, to use induction to prove that a statement involving positive integers is true for every positive integer, we must first verify that the statement is true for the integer 1. We then *assume* the statement is true for the integer n and use this assumption to prove that the statement is true for the integer $n + 1$.

Our next example uses some facts about plane geometry. Recall that given a straightedge and compass, we can construct a right angle.

EXAMPLE 9 We use induction to prove that given a straightedge, a compass, and a unit length, we can construct a line segment of length $\sqrt{n}$ for every positive integer n. The case when $n = 1$ is given. Now we assume that we can construct a line segment of length $\sqrt{n}$. Then use the straightedge and compass to construct a right triangle with height 1 and base $\sqrt{n}$. The hypotenuse of the triangle has length $\sqrt{n+1}$. So, by induction, we can construct a line segment of length $\sqrt{n}$ for every positive integer n. ∎

EXAMPLE 10 DeMOIVRE'S THEOREM We use induction to prove that for every positive integer n and every real number θ, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$, where i is the complex number $\sqrt{-1}$. Obviously, the statement is true for $n = 1$. Now assume it is true for n. We must prove that $(\cos\theta + i\sin\theta)^{n+1} = \cos(n+1)\theta + i\sin(n+1)\theta$. Observe that

$$\begin{aligned}(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta)\\ &= (\cos n\theta + i\sin n\theta)(\cos\theta + i\sin\theta)\\ &= \cos n\theta\cos\theta + i(\sin n\theta\cos\theta\\ &\quad + \sin\theta\cos n\theta) - \sin n\theta\sin\theta.\end{aligned}$$

Now, using trigonometric identities for $\cos(\alpha + \beta)$ and $\sin(\alpha + \beta)$, we see that this last term is $\cos(n+1)\theta + i\sin(n+1)\theta$. So, by induction, the statement is true for all positive integers. ∎

In many instances, the assumption that a statement is true for an integer n does not readily lend itself to a proof that the statement is true

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

for the integer $n + 1$. In such cases, the following equivalent form of induction may be more convenient. Some authors call this formulation the *strong form* of induction.

Theorem 0.6 Second Principle of Mathematical Induction

Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

PROOF The proof is left to the reader. ∎

To use this form of induction, we first show that the statement is true for the integer a. We then *assume* that the statement is true for *all* integers that are greater than or equal to a and less than n, and use this assumption to prove that the statement is true for n.

EXAMPLE 11 We will use the Second Principle of Mathematical Induction with $a = 2$ to prove the existence portion of the Fundamental Theorem of Arithmetic. Let S be the set of integers greater than 1 that are primes or products of primes. Clearly, $2 \in S$. Now we assume that for some integer n, S contains all integers k with $2 \leq k < n$. We must show that $n \in S$. If n is a prime, then $n \in S$ by definition. If n is not a prime, then n can be written in the form ab, where $1 < a < n$ and $1 < b < n$. Since we are assuming that both a and b belong to S, we know that each of them is a prime or a product of primes. Thus, n is also a product of primes. This completes the proof. ∎

Notice that it is more natural to prove the Fundamental Theorem of Arithmetic with the Second Principle of Mathematical Induction than with the First Principle. Knowing that a particular integer factors as a product of primes does not tell you anything about factoring the next larger integer. (Does knowing that 5280 is a product of primes help you to factor 5281 as a product of primes?)

The following problem appeared in the "Brain Boggler" section of the January 1988 issue of the science magazine *Discover.**

EXAMPLE 12 The Quakertown Poker Club plays with blue chips worth \$5.00 and red chips worth \$8.00. What is the largest bet that cannot be made?

*"Brain Boggler" by Maxwell Carver. Copyright © 1988 by *Discover Magazine*. Used by permission.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

To gain insight into this problem, we try various combinations of blue and red chips and obtain 5, 8, 10, 13, 15, 16, 18, 20, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40. It appears that the answer is 27. But how can we be sure? Well, we need only prove that every integer greater than 27 can be written in the form $a \cdot 5 + b \cdot 8$, where a and b are nonnegative integers. This will solve the problem, since a represents the number of blue chips and b the number of red chips needed to make a bet of $a \cdot 5 + b \cdot 8$. For the purpose of contrast, we will give two proofs—one using the First Principle of Mathematical Induction and one using the Second Principle.

Let S be the set of all integers greater than or equal to 28 of the form $a \cdot 5 + b \cdot 8$, where a and b are nonnegative. Obviously, $28 \in S$. Now assume that some integer $n \in S$, say, $n = a \cdot 5 + b \cdot 8$. We must show that $n + 1 \in S$. First, note that since $n \geq 28$, we cannot have both a and b less than 3. If $a \geq 3$, then

$$\begin{aligned} n + 1 &= (a \cdot 5 + b \cdot 8) + (-3 \cdot 5 + 2 \cdot 8) \\ &= (a - 3) \cdot 5 + (b + 2) \cdot 8. \end{aligned}$$

(Regarding chips, this last equation says that we may increase a bet from n to $n + 1$ by removing three blue chips from the pot and adding two red chips.) If $b \geq 3$, then

$$\begin{aligned} n + 1 &= (a \cdot 5 + b \cdot 8) + (5 \cdot 5 - 3 \cdot 8) \\ &= (a + 5) \cdot 5 + (b - 3) \cdot 8. \end{aligned}$$

(The bet can be increased by 1 by removing three red chips and adding five blue chips.) This completes the proof.

To prove the same statement by the Second Principle, we note that each of the integers 28, 29, 30, 31, and 32 is in S. Now assume that for some integer $n > 32$, S contains all integers k with $28 \leq k < n$. We must show that $n \in S$. Since $n - 5 \in S$, there are nonnegative integers a and b such that $n - 5 = a \cdot 5 + b \cdot 8$. But then $n = (a + 1) \cdot 5 + b \cdot 8$. Thus n is in S. ∎

Equivalence Relations

In mathematics, things that are considered different in one context may be viewed as equivalent in another context. We have already seen one such example. Indeed, the sums $2 + 1$ and $4 + 4$ are certainly different in ordinary arithmetic, but are the same under modulo 5 arithmetic. Congruent triangles that are situated differently in the plane are not the same, but they are often considered to be the same in plane geometry. In physics, vectors of the same magnitude and direction can produce

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

different effects—a 10-pound weight placed 2 feet from a fulcrum produces a different effect than a 10-pound weight placed 1 foot from a fulcrum. But in linear algebra, vectors of the same magnitude and direction are considered to be the same. What is needed to make these distinctions precise is an appropriate generalization of the notion of equality; that is, we need a formal mechanism for specifying whether or not two quantities are the same in a given setting. This mechanism is an equivalence relation.

Definition Equivalence Relation
An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that

1. **$(a, a) \in R$ for all $a \in S$ (reflexive property).**
2. **$(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).**
3. **$(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).**

When R is an equivalence relation on a set S, it is customary to write aRb instead of $(a, b) \in R$. Also, since an equivalence relation is just a generalization of equality, a suggestive symbol such as $\approx$, $\equiv$, or $\sim$ is usually used to denote the relation. Using this notation, the three conditions for an equivalence relation become $a \sim a$; $a \sim b$ implies $b \sim a$; and $a \sim b$ and $b \sim c$ imply $a \sim c$. If $\sim$ is an equivalence relation on a set S and $a \in S$, then the set $[a] = \{x \in S \mid x \sim a\}$ is called the *equivalence class of S containing a*.

EXAMPLE 13 Let S be the set of all triangles in a plane. If $a, b \in S$, define $a \sim b$ if a and b are similar—that is, if a and b have corresponding angles that are the same. Then $\sim$ is an equivalence relation on S. ∎

EXAMPLE 14 Let S be the set of all polynomials with real coefficients. If $f, g \in S$, define $f \sim g$ if $f' = g'$, where f' is the derivative of f. Then $\sim$ is an equivalence relation on S. Since two polynomials with equal derivatives differ by a constant, we see that for any f in S, $[f] = \{f + c \mid c \text{ is real}\}$. ∎

EXAMPLE 15 Let S be the set of integers and let n be a positive integer. If $a, b \in S$, define $a \equiv b$ if $a \bmod n = b \bmod n$ (that is, if $a - b$ is divisible by n). Then $\equiv$ is an equivalence relation on S and $[a] = \{a + kn \mid k \in S\}$. Since this particular relation is important in abstract algebra, we will take the trouble to verify that it is indeed an equivalence relation. Certainly, $a - a$ is divisible by n, so that $a \equiv a$ for all a in S. Next, assume that $a \equiv b$, say, $a - b = rn$. Then, $b - a = (-r)n$, and

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

therefore $b \equiv a$. Finally, assume that $a \equiv b$ and $b \equiv c$, say, $a - b = rn$ and $b - c = sn$. Then, we have $a - c = (a - b) + (b - c) = rn + sn = (r + s)n$, so that $a \equiv c$. ∎

∎ **EXAMPLE 16** Let $\equiv$ be as in Example 15 and let $n = 7$. Then we have $16 \equiv 2$; $9 \equiv -5$; and $24 \equiv 3$. Also, $[1] = \{\ldots, -20, -13, -6, 1, 8, 15, \ldots\}$ and $[4] = \{\ldots, -17, -10, -3, 4, 11, 18, \ldots\}$. ∎

∎ **EXAMPLE 17** Let $S = \{(a, b) \mid a, b \text{ are integers, } b \neq 0\}$. If $(a, b), (c, d) \in S$, define $(a, b) \approx (c, d)$ if $ad = bc$. Then $\approx$ is an equivalence relation on S. [The motivation for this example comes from fractions. In fact, the pairs (a, b) and (c, d) are equivalent if the fractions a/b and c/d are equal.]

To verify that $\approx$ is an equivalence relation on S, note that $(a, b) \approx (a, b)$ requires that $ab = ba$, which is true. Next, we assume that $(a, b) \approx (c, d)$, so that $ad = bc$. We have $(c, d) \approx (a, b)$ provided that $cb = da$, which is true from commutativity of multiplication. Finally, we assume that $(a, b) \approx (c, d)$ and $(c, d) \approx (e, f)$ and prove that $(a, b) \approx (e, f)$. This amounts to using $ad = bc$ and $cf = de$ to show that $af = be$. Multiplying both sides of $ad = bc$ by f and replacing cf by de, we obtain $adf = bcf = bde$. Since $d \neq 0$, we can cancel d from the first and last terms. ∎

Definition Partition

A *partition* of a set S is a collection of nonempty disjoint subsets of S whose union is S. Figure 0.6 illustrates a partition of a set into four subsets.

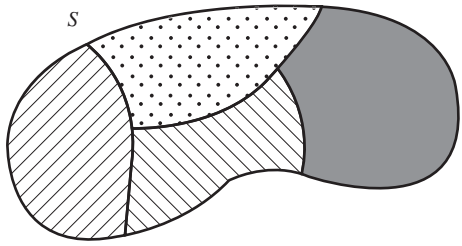


Figure 0.6 Partition of S into four subsets.

∎ **EXAMPLE 18** The sets $\{0\}$, $\{1, 2, 3, \ldots\}$, and $\{\ldots, -3, -2, -1\}$ constitute a partition of the set of integers. ∎

∎ **EXAMPLE 19** The set of nonnegative integers and the set of nonpositive integers do not partition the integers, since both contain 0. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The next theorem reveals that equivalence relations and partitions are intimately intertwined.

Theorem 0.7 Equivalence Classes Partition

The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

PROOF Let $\sim$ be an equivalence relation on a set S. For any $a \in S$, the reflexive property shows that $a \in [a]$. So, $[a]$ is nonempty and the union of all equivalence classes is S. Now, suppose that $[a]$ and $[b]$ are distinct equivalence classes. We must show that $[a] \cap [b] = \emptyset$. On the contrary, assume $c \in [a] \cap [b]$. We will show that $[a] \subseteq [b]$. To this end, let $x \in [a]$. We then have $c \sim a$, $c \sim b$, and $x \sim a$. By the symmetric property, we also have $a \sim c$. Thus, by transitivity, $x \sim c$, and by transitivity again, $x \sim b$. This proves $[a] \subseteq [b]$. Analogously, $[b] \subseteq [a]$. Thus, $[a] = [b]$, in contradiction to our assumption that $[a]$ and $[b]$ are distinct equivalence classes.

To prove the converse, let P be a collection of nonempty disjoint subsets of S whose union is S. Define $a \sim b$ if a and b belong to the same subset in the collection. We leave it to the reader to show that $\sim$ is an equivalence relation on S (Exercise 61). ∎

Functions (Mappings)

Although the concept of a function plays a central role in nearly every branch of mathematics, the terminology and notation associated with functions vary quite a bit. In this section, we establish ours.

Definition Function (Mapping)
A *function* (or *mapping*) ϕ *from a set A to a set B* is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain of* ϕ, and B is called the *range of* ϕ. If ϕ assigns b to a, then b is called the *image of a under* ϕ. The subset of B comprising all the images of elements of A is called the *image of A under* ϕ.

We use the shorthand $\phi: A \to B$ to mean that ϕ is a mapping from A to B. We will write $\phi(a) = b$ or $\phi: a \to b$ to indicate that ϕ carries a to b.

There are often different ways to denote the same element of a set. In defining a function in such cases one must verify that the function

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

values assigned to the elements depend not on the way the elements are expressed but on only the elements themselves. For example, the correspondence ϕ from the rational numbers to the integers given by $\phi(a/b) = a + b$ does not define a function since $1/2 = 2/4$ but $\phi(1/2) \neq \phi(2/4)$. To verify that a correspondence is a function, you assume that $x_1 = x_2$ and prove that $\phi(x_1) = \phi(x_2)$.

Definition Composition of Functions
Let $\phi: A \to B$ and $\psi: B \to C$. The *composition* $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A. The composition function $\psi\phi$ can be visualized as in Figure 0.7.

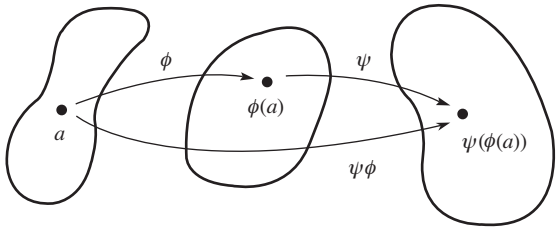


Figure 0.7 Composition of functions ϕ and ψ.

In calculus courses, the composition of f with g is written $(f \circ g)(x)$ and is defined by $(f \circ g)(x) = f(g(x))$. When we compose functions, we omit the "circle."

■ **EXAMPLE 20** Let $f(x) = 2x + 3$ and $g(x) = x^2 + 1$. Then $(fg)(5) = f(g(5)) = f(26) = 55$; $(gf)(5) = g(f(5)) = g(13) = 170$. More generally, $(fg)(x) = f(g(x)) = f(x^2 + 1) = 2(x^2 + 1) + 3 = 2x^2 + 5$ and $(gf)(x) = g(f(x)) = g(2x + 3) = (2x + 3)^2 + 1 = 4x^2 + 12x + 9 + 1 = 4x^2 + 12x + 10$. Note that the function fg is not the same as the function gf. ■

There are several kinds of functions that occur often enough to be given names.

Definition One-to-One Function
A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

The term *one-to-one* is suggestive, since the definition ensures that one element of B can be the image of only one element of A. Alternatively, ϕ is one-to-one if $a_1 \neq a_2$ implies $\phi(a_1) \neq \phi(a_2)$. That is, different elements of A map to different elements of B. See Figure 0.8.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

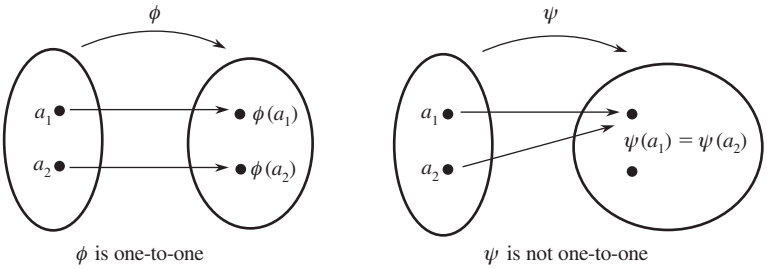


Figure 0.8

Definition Function from A onto B

A function ϕ from a set A to a set B is said to be *onto* B if each element of B is the image of at least one element of A. In symbols, $\phi: A \to B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$. See Figure 0.9.

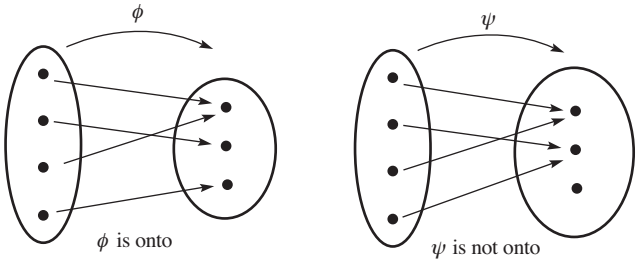


Figure 0.9

The next theorem summarizes the facts about functions we will need.

Theorem 0.8 Properties of Functions

Given functions $\alpha: A \to B$, $\beta: B \to C$, and $\gamma: C \to D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ *(associativity).*
2. *If α and β are one-to-one, then $\beta\alpha$ is one-to-one.*
3. *If α and β are onto, then $\beta\alpha$ is onto.*
4. *If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.*

PROOF We prove only part 1. The remaining parts are left as exercises (Exercise 57). Let $a \in A$. Then $(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$. On the other hand, $((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$. So, $\gamma(\beta\alpha) = (\gamma\beta)\alpha$. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

It is useful to note that if α is one-to-one and onto, the function α^{-1} described in part 4 of Theorem 0.8 has the property that if $\alpha(s) = t$, then $\alpha^{-1}(t) = s$. That is, the image of t under α^{-1} is the unique element s that maps to t under α. In effect, α^{-1} "undoes" what α does.

EXAMPLE 21 Let **Z** denote the set of integers, **R** the set of real numbers, and **N** the set of nonnegative integers. The following table illustrates the properties of one-to-one and onto.

Domain	Range	Rule	One-to-One	Onto
Z	**Z**	$x \to x^3$	Yes	No
R	**R**	$x \to x^3$	Yes	Yes
Z	**N**	$x \to \lvert x \rvert$	No	Yes
Z	**Z**	$x \to x^2$	No	No

To verify that $x \to x^3$ is one-to-one in the first two cases, notice that if $x^3 = y^3$, we may take the cube roots of both sides of the equation to obtain $x = y$. Clearly, the mapping from **Z** to **Z** given by $x \to x^3$ is not onto, since 2 is the cube of no integer. However, $x \to x^3$ defines an onto function from **R** to **R**, since every real number is the cube of its cube root (that is, $\sqrt[3]{b} \to b$). The remaining verifications are left to the reader. ∎

Exercises

I was interviewed in the Israeli Radio for five minutes and I said that more than 2000 years ago, Euclid proved that there are infinitely many primes. Immediately the host interrupted me and asked: "Are there still infinitely many primes?"

NOGA ALON

1. For $n = 5$, 8, 12, 20, and 25, find all positive integers less than n and relatively prime to n.
2. Determine $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ and $\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$.
3. Determine 51 mod 13, 342 mod 85, 62 mod 15, 10 mod 15, $(82 \cdot 73) \bmod 7$, $(51 + 68) \bmod 7$, $(35 \cdot 24) \bmod 11$, and $(47 + 68) \bmod 11$.
4. Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.
5. Show that if a and b are positive integers, then $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.
6. Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

7. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

8. Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

9. Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$. (This exercise is referred to in Chapters 6, 8, 10, and 15.)

10. Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

11. Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \bmod n = 1$ has a solution if and only if $d = 1$. (This exercise is referred to in Chapter 2.)

12. Show that $5n + 3$ and $7n + 4$ are relatively prime for all n.

13. Suppose that m and n are relatively prime and r is any integer. Show that there are integers x and y such that $mx + ny = r$.

14. Let p, q, and r be primes other than 3. Show that 3 divides $p^2 + q^2 + r^2$.

15. Prove that every prime greater than 3 can be written in the form $6n + 1$ or $6n + 5$.

16. Determine $7^{1000} \bmod 6$ and $6^{1001} \bmod 7$.

17. Let a, b, s, and t be integers. If $a \bmod st = b \bmod st$, show that $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$. What condition on s and t is needed to make the converse true? (This exercise is referred to in Chapter 8.)

18. Determine $8^{402} \bmod 5$.

19. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. (This exercise is referred to in Chapter 8.)

20. Let $p_1, p_2, \ldots, p_n$ be primes. Show that $p_1 p_2 \cdots p_n + 1$ is divisible by none of these primes.

21. Prove that there are infinitely many primes. (*Hint:* Use Exercise 20.)

22. Express $(-7 - 3i)^{-1}$ in standard form.

23. Express $\dfrac{-5 + 2i}{4 - 5i}$ in standard form.

24. Express $(\cos 360^\circ + i \sin 360^\circ)^{1/8}$ in standard form without trig expressions. (Note that $\cos 360^\circ + i \sin 360^\circ = 1$.)

25. Prove that for any positive integer n, $(\cos \theta + i \sin \theta)^{1/n} = \cos \dfrac{\theta}{n} + i \sin \dfrac{\theta}{n}$.

26. For every positive integer n, prove that $1 + 2 + \cdots + n = n(n + 1)/2$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

27. For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

28. Prove that $2^n 3^{2n} - 1$ is always divisible by 17.

29. Prove that there is some positive integer n such that $n, n + 1, n + 2, \ldots, n + 200$ are all composite.

30. (Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \cdots a_n$, prove that p divides a_i for some i.

31. Use the Generalized Euclid's Lemma (see Exercise 30) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

32. What is the largest bet that cannot be made with chips worth \$7.00 and \$9.00? Verify that your answer is correct with both forms of induction.

33. Prove that the First Principle of Mathematical Induction is a consequence of the Well Ordering Principle.

34. The Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, 21, 34, ... In general, the Fibonacci numbers are defined by $f_1 = 1$, $f_2 = 1$, and for $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Prove that the nth Fibonacci number f_n satisfies $f_n < 2^n$.

35. Prove by induction on n that for all positive integers n, $n^3 + (n + 1)^3 + (n + 2)^3$ is a multiple of 9.

36. Suppose that there is a statement involving a positive integer parameter n and you have an argument that shows that whenever the statement is true for a particular n it is also true for $n + 2$. What remains to be done to prove the statement is true for every positive integer? Describe a situation in which this strategy would be applicable.

37. In the cut "As" from *Songs in the Key of Life*, Stevie Wonder mentions the equation $8 \times 8 \times 8 = 4$. Find all integers n for which this statement is true, modulo n.

38. Prove that for every integer n, $n^3 \bmod 6 = n \bmod 6$.

39. If it is 2:00 A.M. now, what time will it be 3736 hours from now?

40. Determine the check digit for a money order with identification number 7234541780.

41. Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9 or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.

42. Suppose that a money order identification number and check digit of 21720421168 is erroneously copied as 27750421168. Will the check digit detect the error?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

43. A transposition error involving distinct adjacent digits is one of the form $\ldots ab \ldots \rightarrow \ldots ba \ldots$ with $a \neq b$. Prove that the money order check-digit scheme will not detect such errors unless the check digit itself is transposed.

44. Determine the check digit for the Avis rental car with identification number 540047. (See Example 5.)

45. Show that a substitution of a digit a_i' for the digit a_i ($a_i' \neq a_i$) in a noncheck position of a UPS number is detected if and only if $|a_i - a_i'| \neq 7$.

46. Determine which transposition errors involving adjacent digits are detected by the UPS check digit.

47. Use the UPC scheme to determine the check digit for the number 07312400508.

48. Explain why the check digit for a money order for the number N is the repeated decimal digit in the real number $N \div 9$.

49. The 10-digit International Standard Book Number (ISBN-10) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ has the property $(a_1, a_2, \ldots, a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \bmod 11 = 0$. The digit a_{10} is the check digit. When a_{10} is required to be 10 to make the dot product 0, the character X is used as the check digit. Verify the check digit for the ISBN-10 assigned to this book.

50. Suppose that an ISBN-10 has a smudged entry where the question mark appears in the number 0-716?-2841-9. Determine the missing digit.

51. Suppose three consecutive digits *abc* of an ISBN-10 are scrambled as *bca*. Which such errors will go undetected?

52. The ISBN-10 0-669-03925-4 is the result of a transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN-10.

53. Suppose the weighting vector for ISBN-10s were changed to (1, 2, 3, 4, 5, 6, 7, 8, 9, 10). Explain how this would affect the check digit.

54. Use the two-check-digit error-correction method described in this chapter to append two check digits to the number 73445860.

55. Suppose that an eight-digit number has two check digits appended using the error-correction method described in this chapter and it is incorrectly transcribed as 4302511568. If exactly one digit is incorrect, determine the correct number.

56. The state of Utah appends a ninth digit a_9 to an eight-digit driver's license number $a_1a_2 \ldots a_8$ so that $(9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 + a_9) \bmod 10 = 0$. If you know that the license number 149105267 has exactly one digit incorrect, explain why the error cannot be in position 2, 4, 6, or 8.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

57. Complete the proof of Theorem 0.8.

58. Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

59. Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

60. Let S be the set of integers. If $a, b \in S$, define aRb if $a + b$ is even. Prove that R is an equivalence relation and determine the equivalence classes of S.

61. Complete the proof of Theorem 0.7 by showing that $\sim$ is an equivalence relation on S.

62. Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.

63. What is the last digit of 3^{100}? What is the last digit of 2^{100}?

64. Prove that none of the integers 11, 111, 1111, 11111, . . . is a square of an integer.

65. (Cancellation Property) Suppose α, β, and γ are functions. If $\alpha\gamma = \beta\gamma$ and γ is one-to-one and onto, prove that $\alpha = \beta$.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Readings

Linda Deneen, "Secret Encryption with Public Keys," *The UMAP Journal* 8 (1987): 9–29.

This well-written article describes several ways in which modular arithmetic can be used to code secret messages. They range from a simple scheme used by Julius Caesar to a highly sophisticated scheme invented in 1978 and based on modular n arithmetic, where n has more than 200 digits.

J. A. Gallian, "Assigning Driver's License Numbers," *Mathematics Magazine* 64 (1991): 13–22.

This article describes various methods used by the states to assign driver's license numbers. Several include check digits for error detection. This article can be downloaded at **http://www.d.umn.edu/~jgallian/license.pdf**

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

J. A. Gallian, "The Mathematics of Identification Numbers," *The College Mathematics Journal* 22 (1991): 194–202.

This article is a comprehensive survey of check-digit schemes that are associated with identification numbers. This article can be downloaded at **http://www.d.umn.edu/~jgallian/ident.pdf**

J. A. Gallian and S. Winters, "Modular Arithmetic in the Marketplace," *The American Mathematical Monthly* 95 (1988): 548–551.

This article provides a more detailed analysis of the check-digit schemes presented in this chapter. In particular, the error detection rates for the various schemes are given. This article can be downloaded at **http://www.d.umn.edu/~jgallian/marketplace.pdf**

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PART 2

Groups

For online student resources, visit this textbook's website at www.CengageBrain.com

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

1 Introduction to Groups

Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root, and it would be hard to find a better one on which to demonstrate the working of the mathematical intellect.

HERMANN WEYL, *Symmetry*

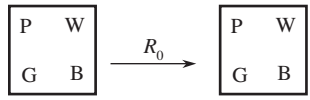
Symmetries of a Square

Suppose we remove a square region from a plane, move it in some way, then put the square back into the space it originally occupied. Our goal in this chapter is to describe all possible ways in which this can be done. More specifically, we want to describe the possible relationships between the starting position of the square and its final position in terms of motions. However, we are interested in the net effect of a motion, rather than in the motion itself. Thus, for example, we consider a 90° rotation and a 450° rotation as equal, since they have the same net effect on every point. With this simplifying convention, it is an easy matter to achieve our goal.

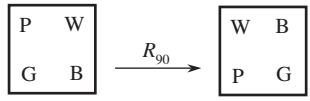
To begin, we can think of the square region as being transparent (glass, say), with the corners marked on one side with the colors blue, white, pink, and green. This makes it easy to distinguish between motions that have different effects. With this marking scheme, we are now in a position to describe, in simple fashion, all possible ways in which a square object can be repositioned. See Figure 1.1. We now claim that any motion—no matter how complicated—is equivalent to one of these eight. To verify this claim, observe that the final position of the square is completely determined by the location and orientation (that is, face up or face down) of any particular corner. But, clearly, there are only four locations and two orientations for a given corner, so there are exactly eight distinct final positions for the corner.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

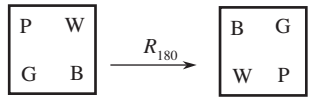
R_0 = Rotation of 0° (no change in position)



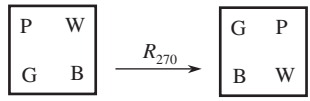
R_{90} = Rotation of 90° (counterclockwise)



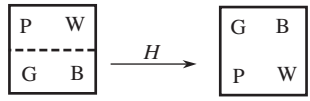
R_{180} = Rotation of 180°



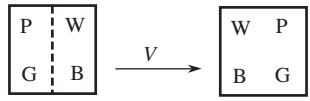
R_{270} = Rotation of 270°



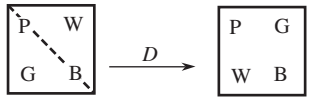
H = Flip about a horizontal axis



V = Flip about a vertical axis



D = Flip about the main diagonal



D' = Flip about the other diagonal

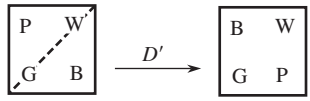
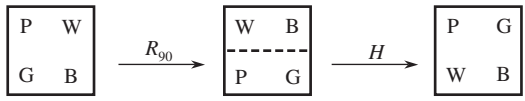


Figure 1.1

Let's investigate some consequences of the fact that every motion is equal to one of the eight listed in Figure 1.1. Suppose a square is repositioned by a rotation of 90° followed by a flip about the horizontal axis of symmetry.



Thus, we see that this pair of motions—taken together—is equal to the single motion D. This observation suggests that we can compose two motions to obtain a single motion. And indeed we can, since the

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

eight motions may be viewed as functions from the square region to itself, and as such we can combine them using function composition.

With this in mind, we write $H\,R_{90} = D$ because in lower level math courses function composition $f \circ g$ means "g followed by f." The eight motions R_0, R_{90}, R_{180}, R_{270}, H, V, D, and D', together with the operation composition, form a mathematical system called the *dihedral group of order 8* (the order of a group is the number of elements it contains). It is denoted by D_4. Rather than introduce the formal definition of a group here, let's look at some properties of groups by way of the example D_4.

To facilitate future computations, we construct an *operation table* or *Cayley table* (so named in honor of the prolific English mathematician Arthur Cayley, who first introduced them in 1854) for D_4 below. The circled entry represents the fact that $D = HR_{90}$. (In general, ab denotes the entry at the intersection of the row with a at the left and the column with b at the top.)

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	$\textcircled{D}$	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Notice how orderly this table looks! This is no accident. Perhaps the most important feature of this table is that it has been completely filled in without introducing any new motions. Of course, this is because, as we have already pointed out, any sequence of motions turns out to be the same as one of these eight. Algebraically, this says that if A and B are in D_4, then so is AB. This property is called *closure*, and it is one of the requirements for a mathematical system to be a group. Next, notice that if A is any element of D_4, then $AR_0 = R_0A = A$. Thus, combining any element A on either side with R_0 yields A back again. An element R_0 with this property is called an *identity*, and every group must have one. Moreover, we see that for each element A in D_4, there is exactly one element B in D_4 such that $AB = BA = R_0$. In this case, B is said to be the *inverse* of A and vice versa. For example, R_{90} and R_{270} are inverses of each other, and H is its own inverse. The term *inverse* is a descriptive one, for if A and B are inverses of each other, then B "undoes" whatever A "does," in the sense that A and B taken together in either order produce R_0, representing no change. Another striking feature

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

of the table is that every element of D_4 appears exactly once in each row and column. This feature is something that all groups must have, and, indeed, it is quite useful to keep this fact in mind when constructing the table in the first place.

Another property of D_4 deserves special comment. Observe that $HD \neq DH$ but $R_{90}R_{180} = R_{180}R_{90}$. Thus, in a group, ab may or may not be the same as ba. If it happens that $ab = ba$ for *all* choices of group elements a and b, we say the group is *commutative* or—better yet—*Abelian* (in honor of the great Norwegian mathematician Niels Abel). Otherwise, we say the group is *non-Abelian.*

Thus far, we have illustrated, by way of D_4, three of the four conditions that define a group—namely, closure, existence of an identity, and existence of inverses. The remaining condition required for a group is *associativity*; that is, $(ab)c = a(bc)$ for all a, b, c in the set. To be sure that D_4 is indeed a group, we should check this equation for each of the $8^3 = 512$ possible choices of a, b, and c in D_4. In practice, however, this is rarely done! Here, for example, we simply observe that the eight motions are functions and the operation is function composition. Then, since function composition is associative, we do not have to check the equations.

The Dihedral Groups

The analysis carried out above for a square can similarly be done for an equilateral triangle or regular pentagon or, indeed, any regular n-gon ($n \geq 3$). The corresponding group is denoted by D_n and is called the *dihedral group of order 2n.*

The dihedral groups arise frequently in art and nature. Many of the decorative designs used on floor coverings, pottery, and buildings have one of the dihedral groups as a group of symmetry. Corporation logos are rich sources of dihedral symmetry [1]. Chrysler's logo has D_5 as a symmetry group, and that of Mercedes-Benz has D_3. The ubiquitous five-pointed star has symmetry group D_5. The phylum Echinodermata contains many sea animals (such as starfish, sea cucumbers, feather stars, and sand dollars) that exhibit patterns with D_5 symmetry.

Chemists classify molecules according to their symmetry. Moreover, symmetry considerations are applied in orbital calculations, in determining energy levels of atoms and molecules, and in the study of molecular vibrations. The symmetry group of a pyramidal molecule such as ammonia (NH_3), depicted in Figure 1.2, is D_3.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

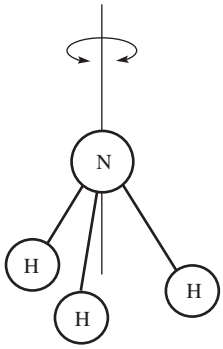
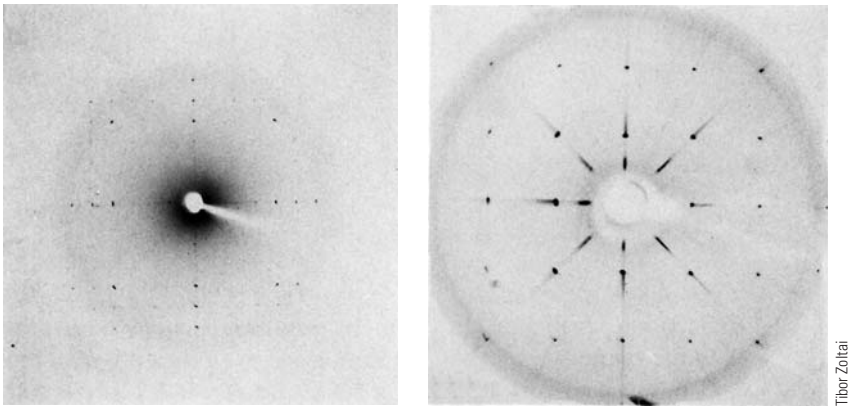


Figure 1.2 A pyramidal molecule with symmetry group D_3.

Mineralogists determine the internal structures of crystals (that is, rigid bodies in which the particles are arranged in three-dimensional repeating patterns—table salt and table sugar are two examples) by studying two-dimensional x-ray projections of the atomic makeup of the crystals. The symmetry present in the projections reveals the internal symmetry of the crystals themselves. Commonly occurring symmetry patterns are D_4 and D_6 (see Figure 1.3). Interestingly, it is mathematically impossible for a crystal to possess a D_n symmetry pattern with $n = 5$ or $n > 6$.



Tibor Zoltai

Figure 1.3 X-ray diffraction photos revealing D_4 symmetry patterns in crystals.

The dihedral group of order $2n$ is often called the *group of symmetries of a regular n-gon.* A *plane symmetry* of a figure F in a plane is a function from the plane to itself that carries F onto F and preserves distances; that is, for any points p and q in the plane, the distance from the image of p to the image of q is the same as the

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

distance from p to q. (The term *symmetry* is from the Greek word *symmetros*, meaning "of like measure.") The *symmetry group* of a plane figure is the set of all symmetries of the figure. Symmetries in three dimensions are defined analogously. Obviously, a rotation of a plane about a point in the plane is a symmetry of the plane, and a rotation about a line in three dimensions is a symmetry in three-dimensional space. Similarly, any translation of a plane or of three-dimensional space is a symmetry. A *reflection across a line L* is that function that leaves every point of L fixed and takes any point q, not on L, to the point q' so that L is the perpendicular bisector of the line segment joining q and q' (see Figure 1.4). A reflection across a plane in three dimensions is defined analogously. Notice that the restriction of a 180° rotation about a line L in three dimensions to a plane containing L is a reflection across L in the plane. Thus, in the dihedral groups, the motions that we described as flips about axes of symmetry in three dimensions (for example, H, V, D, D') are reflections across lines in two dimensions. Just as a reflection across a line is a plane symmetry that cannot be achieved by a physical motion of the plane in two dimensions, a reflection across a plane is a three-dimensional symmetry that cannot be achieved by a physical motion of three-dimensional space. A cup, for instance, has reflective symmetry across the plane bisecting the cup, but this symmetry cannot be duplicated with a physical motion in three dimensions.

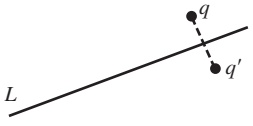


Figure 1.4

Many objects and figures have rotational symmetry but not reflective symmetry. A symmetry group consisting of the rotational symmetries of 0°, 360°/n, 2(360°)/n, . . . , (n − 1)360°/n, and no other symmetries, is called a *cyclic rotation group of order n* and is denoted by $\langle R_{360/n} \rangle$. Cyclic rotation groups, along with dihedral groups, are favorites of artists, designers, and nature. Figure 1.5 illustrates with corporate logos the cyclic rotation groups of orders 2, 3, 4, 5, 6, 8, 16, and 20.

A study of symmetry in greater depth is given in Chapters 27 and 28.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

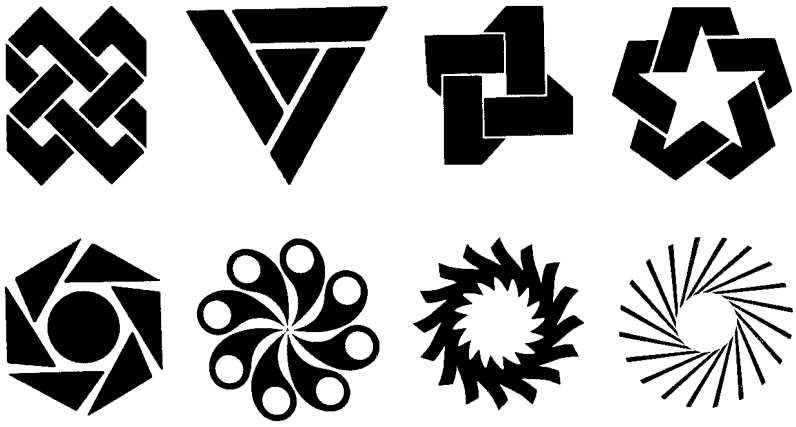


Figure 1.5 Logos with cyclic rotation symmetry groups.

Exercises

The only way to learn mathematics is to do mathematics.

PAUL R. HALMOS, *A Hilbert Space Problem Book*

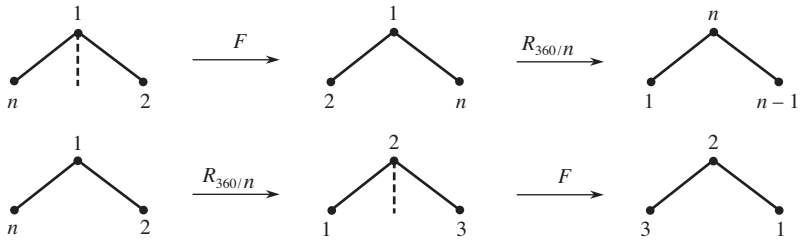
1. With pictures and words, describe each symmetry in D_3 (the set of symmetries of an equilateral triangle).
2. Write out a complete Cayley table for D_3. Is D_3 Abelian?
3. In D_4, find all elements X such that
   a. $X^3 = V$;
   b. $X^3 = R_{90}$;
   c. $X^3 = R_0$;
   d. $X^2 = R_0$;
   e. $X^2 = H$.
4. Describe in pictures or words the elements of D_5 (symmetries of a regular pentagon).
5. For $n \geq 3$, describe the elements of D_n. (*Hint:* You will need to consider two cases—n even and n odd.) How many elements does D_n have?
6. In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.
7. In D_n, explain geometrically why a rotation followed by a rotation must be a rotation.
8. In D_n, explain geometrically why a rotation and a reflection taken together in either order must be a reflection.
9. Associate the number 1 with a rotation and the number -1 with a reflection. Describe an analogy between multiplying these two numbers and multiplying elements of D_n.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

10. If r_1, r_2, and r_3 represent rotations from D_n and f_1, f_2, and f_3 represent reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

11. Find elements A, B, and C in D_4 such that $AB = BC$ but $A \neq C$. (Thus, "cross cancellation" is not valid.)

12. Explain what the following diagram proves about the group D_n.



13. Describe the symmetries of a nonsquare rectangle. Construct the corresponding Cayley table.

14. Describe the symmetries of a parallelogram that is neither a rectangle nor a rhombus. Describe the symmetries of a rhombus that is not a rectangle.

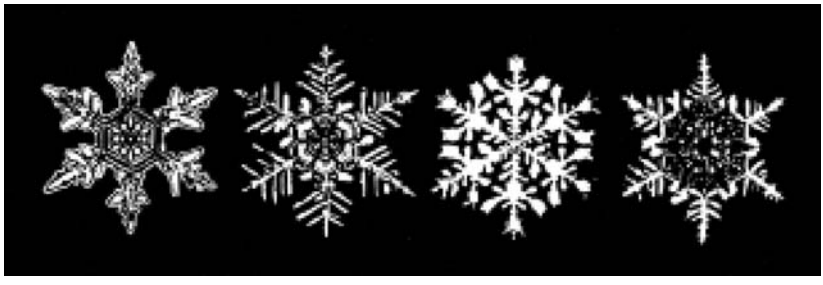
15. Describe the symmetries of a noncircular ellipse. Do the same for a hyperbola.

16. Consider an infinitely long strip of equally spaced H's:

$$\cdots \text{H H H H} \cdots$$

Describe the symmetries of this strip. Is the group of symmetries of the strip Abelian?

17. For each of the snowflakes in the figure, find the symmetry group and locate the axes of reflective symmetry (disregard imperfections).

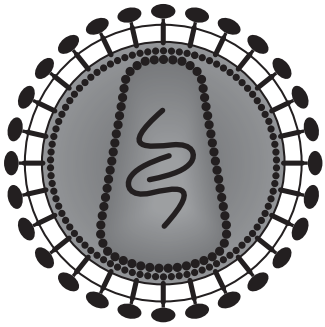


Snow Crystals, by W. A. Bentley & W. J. Humphreys © Dover Publications

Photographs of snowflakes from the Bentley and Humphreys atlas.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

18. Determine the symmetry group of the outer shell of the cross section of the human immunodeficiency virus (HIV) shown below.



19. Does a fan blade have a cyclic symmetry group or a dihedral symmetry group?

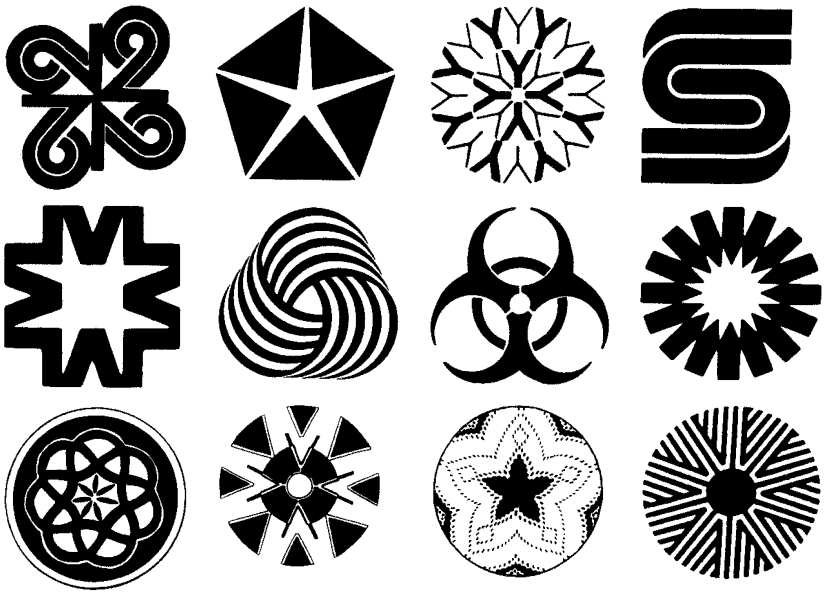
20. Bottle caps that are pried off typically have 22 ridges around the rim. Find the symmetry group of such a cap.

21. What group theoretic property do uppercase letters F, G, J, L, P, Q, R have that is not shared by the remaining uppercase letters in the alphabet?

22. What symmetry property does the word "zoonosis" have when written in uppercase letters? (It means a disease of humans acquired from animals.)

23. What symmetry property do the words "mow," "sis," and "swims" have when written in uppercase letters?

24. For each design below, determine the symmetry group (ignore imperfections).



Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Suggested Reading

Michael Field and Martin Golubitsky, *Symmetry in Chaos*, Oxford University Press, 1992.

This book has many beautiful symmetric designs that arise in chaotic dynamic systems.

Suggested Website

http://britton.disted.camosun.bc.ca/jbsymteslk.htm

This spectacular website on symmetry and tessellations has numerous activities and links to many other sites on related topics. It is a wonderful website for K–12 teachers and students.

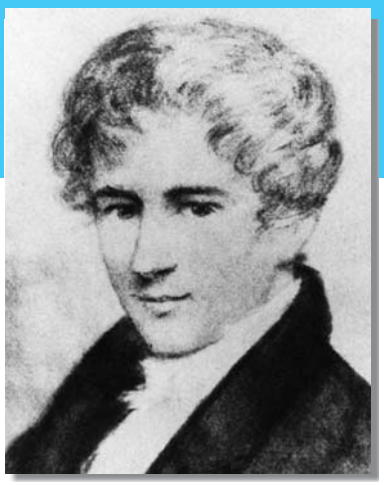
Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Niels Abel

He [Abel] has left mathematicians something to keep them busy for five hundred years.

CHARLES HERMITE

A 500-kroner bank note first issued by Norway in 1948.



Stock Montage

This stamp was issued in 1929 to commemorate the 100th anniversary of Abel's death.

NIELS HENRIK ABEL, one of the foremost mathematicians of the 19th century, was born in Norway on August 5, 1802. At the age of 16, he began reading the classic mathematical works of Newton, Euler, Lagrange, and Gauss. When Abel was 18 years old, his father died, and the burden of supporting the family fell upon him. He took in private pupils and did odd jobs, while continuing to do mathematical research. At the age of 19, Abel solved a problem that had vexed leading mathematicians for hundreds of years. He proved that, unlike the situation for equations of degree 4 or less, there is no finite (closed) formula for the solution of the general fifth-degree equation.

Although Abel died long before the advent of the subjects that now make up abstract algebra, his solution to the quintic problem laid the groundwork for many of these subjects. Just when his work was beginning to receive the attention it deserved, Abel contracted tuberculosis. He died on April 6, 1829, at the age of 26.

In recognition of the fact that there is no Nobel Prize for mathematics, in 2002 Norway established the Abel Prize as the "Nobel Prize in mathematics" in honor of its native son. At approximately the $1,000,000 level, the Abel Prize is now seen as an award equivalent to a Nobel Prize.

To find more information about Abel, visit:

http://www-groups.dcs.st-and.ac.uk/~history/

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

2 Groups

A good stock of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one.

PAUL R. HALMOS

Definition and Examples of Groups

The term *group* was used by Galois around 1830 to describe sets of one-to-one functions on finite sets that could be grouped together to form a set closed under composition. As is the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the result of a long evolutionary process. Although this definition was given by both Heinrich Weber and Walther von Dyck in 1882, it did not gain universal acceptance until the 20th century.

Definition Binary Operation
Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.

A binary operation on a set G, then, is simply a method (or formula) by which the members of an ordered pair from G combine to yield a new member of G. This condition is called *closure*. The most familiar binary operations are ordinary addition, subtraction, and multiplication of integers. Division of integers is not a binary operation on the integers because an integer divided by an integer need not be an integer.

The binary operations addition modulo n and multiplication modulo n on the set $\{0, 1, 2, \ldots, n - 1\}$, which we denote by Z_n, play an extremely important role in abstract algebra. In certain situations we will want to combine the elements of Z_n by addition modulo n only; in other situations we will want to use both addition modulo n and multiplication modulo n to combine the elements. It will be clear

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

from the context whether we are using addition only or addition and multiplication. For example, when multiplying matrices with entries from Z_n, we will need both addition modulo n and multiplication modulo n.

Definition Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.

1. ***Associativity.*** **The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.**
2. ***Identity.*** **There is an element e (called the *identity*) in G such that $ae = ea = a$ for all a in G.**
3. ***Inverses.*** **For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.**

In words, then, a group is a set together with an associative operation such that there is an identity, every element has an inverse, and any pair of elements can be combined without going outside the set. Be sure to verify closure when testing for a group (see Example 5). Notice that if a is the inverse of b, then b is the inverse of a.

If a group has the property that $ab = ba$ for every pair of elements a and b, we say the group is *Abelian.* A group is *non-Abelian* if there is some pair of elements a and b for which $ab \neq ba$. When encountering a particular group for the first time, one should determine whether or not it is Abelian.

Now that we have the formal definition of a group, our first job is to build a good stock of examples. These examples will be used throughout the text to illustrate the theorems. (The best way to grasp the meat of a theorem is to see what it says in specific cases.) As we progress, the reader is bound to have hunches and conjectures that can be tested against the stock of examples. To develop a better understanding of the following examples, the reader should supply the missing details.

■ **EXAMPLE 1** The set of integers Z (so denoted because the German word for numbers is *Zahlen*), the set of rational numbers Q (for quotient), and the set of real numbers $\mathbf{R}$ are all groups under ordinary addition. In each case, the identity is 0 and the inverse of a is $-a$. ■

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 2 The set of integers under ordinary multiplication is not a group. Since the number 1 is the identity, property 3 fails. For example, there is no integer b such that $5b = 1$.

EXAMPLE 3 The subset $\{1, -1, i, -i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, whereas the inverse of i is $-i$, and vice versa.

EXAMPLE 4 The set Q^+ of positive rationals is a group under ordinary multiplication. The inverse of any a is $1/a = a^{-1}$.

EXAMPLE 5 The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} \cdot \sqrt{2} = 2$, so S is not closed under multiplication.

EXAMPLE 6 A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is called a 2×2 *matrix*. The set of all 2×2 matrices with real entries is a group under componentwise addition. That is,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

EXAMPLE 7 The set $Z_n = \{0, 1, \ldots, n - 1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in Z_n, the inverse of j is $n - j$. This group is usually referred to as the *group of integers modulo n.*

As we have seen, the real numbers, the 2×2 matrices with real entries, and the integers modulo n are all groups under the appropriate addition. But what about multiplication? In each case, the existence of some elements that do not have inverses prevents the set from being a group under the usual multiplication. However, we can form a group in each case by simply throwing out the rascals. Examples 8, 9, and 11 illustrate this.

EXAMPLE 8 The set $\mathbf{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 9† The *determinant* of the 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $ad - bc$. If A is a 2×2 matrix, $\det A$ denotes the determinant of A. The set

$$GL(2, \mathbf{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbf{R}, ad - bc \neq 0 \right\}$$

of 2×2 matrices with real entries and nonzero determinants is a non-Abelian group under the operation

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}.$$

The first step in verifying that this set is a group is to show that the product of two matrices with nonzero determinants also has a nonzero determinant. This follows from the fact that for any pair of 2×2 matrices A and B, $\det(AB) = (\det A)(\det B)$.

Associativity can be verified by direct (but cumbersome) calculations. The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is

$$\begin{bmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{bmatrix}$$

(explaining the requirement that $ad - bc \neq 0$). This very important non-Abelian group is called the *general linear group* of 2×2 matrices over $\mathbf{R}$. ∎

EXAMPLE 10 The set of all 2×2 matrices with real entries is not a group under the operation defined in Example 9. Inverses do not exist when the determinant is 0. ∎

Now that we have shown how to make subsets of the real numbers and subsets of the set of 2×2 matrices into multiplicative groups, we next consider the integers under multiplication modulo n.

†For simplicity, we have restricted our matrix examples to the 2×2 case. However, readers who have had linear algebra can readily generalize to $n \times n$ matrices.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 11 (L. EULER, 1761) By Exercise 11 in Chapter 0, an integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime. So, for each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n. (We leave it to the reader to check that this set is closed under this operation.)

For $n = 10$, we have $U(10) = \{1, 3, 7, 9\}$. The Cayley table for $U(10)$ is

mod 10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(Recall that ab mod n is the unique integer r with the property $a \cdot b = nq + r$, where $0 \leq r < n$ and $a \cdot b$ is ordinary multiplication.) In the case that n is a prime, $U(n) = \{1, 2, \ldots, n - 1\}$. ∎

In his classic book *Lehrbuch der Algebra*, published in 1895, Heinrich Weber gave an extensive treatment of the groups $U(n)$ and described them as the most important examples of finite Abelian groups.

EXAMPLE 12 The set $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not. ∎

EXAMPLE 13 The set of integers under subtraction is not a group, since the operation is not associative. ∎

With the examples given thus far as a guide, it is wise for the reader to pause here and think of his or her own examples. Study actively! Don't just read along and be spoon-fed by the book.

EXAMPLE 14 The complex numbers $\mathbf{C} + \{a + bi \mid a, b \in \mathbf{R}, i^2 = -1\}$ are a group under the operation $(a + bi) + (c + di) = (a + c) + (b + d)i$. The inverse of $a + bi$ is $-a - bi$. The nonzero complex numbers $\mathbf{C}^*$ are a group under the operation $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$. The inverse of $a + bi$ is $\dfrac{1}{a + bi} = \dfrac{1}{a + bi}\dfrac{a - bi}{a - bi} = \dfrac{1}{a^2 + b^2}a - \dfrac{1}{a^2 + b^2}bi$. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 15 For all integers $n \geq 1$, the set of complex nth roots of unity

$$\left\{ \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n} \,\middle|\, k = 0, 1, 2, \ldots, n-1 \right\}$$

(i.e., complex zeros of $x^n - 1$) is a group under multiplication. (See DeMoivre's Theorem—Example 10 in Chapter 0.) Compare this group with the one in Example 3.

Recall from Chapter 0 that the complex number $\cos\theta + i \sin\theta$ can be represented geometrically as the point $(\cos\theta, \sin\theta)$ in a plane coordinatized by a real horizontal axis and a vertical imaginary axis, where θ is the angle formed by the line segment joining the origin and the point $(\cos\theta, \sin\theta)$ and the positive real axis. Thus, the six complex zeros of $x^6 = 1$ are located at points around the circle of radius 1, 60° apart, as shown in Figure 2.1.

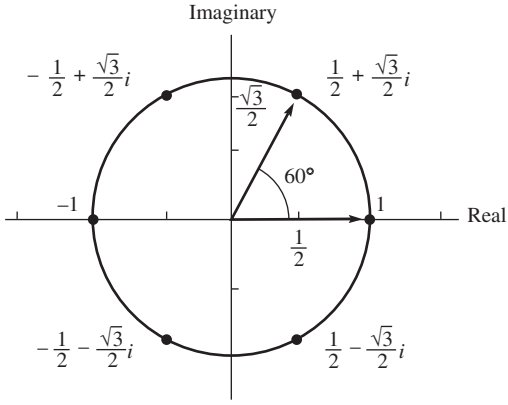


Figure 2.1

EXAMPLE 16 The set $\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbf{R}\}$ is a group under componentwise addition [i.e., $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$].

EXAMPLE 17 For a fixed point (a, b) in $\mathbf{R}^2$, define $T_{a,b}: \mathbf{R}^2 \to \mathbf{R}^2$ by $(x, y) \to (x + a, y + b)$. Then $G = \{T_{a,b} \mid a, b \in \mathbf{R}\}$ is a group under function composition. Straightforward calculations show that $T_{a,b}T_{c,d} = T_{a+c,b+d}$. From this formula we may observe that G is closed, $T_{0,0}$ is the identity, the inverse of $T_{a,b}$ is $T_{-a,-b}$, and G is Abelian. Function composition is always associative. The elements of G are called *translations.*

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 18 The set of all 2×2 matrices with determinant 1 with entries from Q (rationals), $\mathbf{R}$ (reals), $\mathbf{C}$ (complex numbers), or Z_p (p a prime) is a non-Abelian group under matrix multiplication. This group is called the *special linear group* of 2×2 matrices over Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p, respectively. If the entries are from F, where F is any of the above, we denote this group by $SL(2, F)$. For the group $SL(2, F)$, the formula given in Example 9 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ simplifies to $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. When the matrix entries are from Z_p, we use modulo p arithmetic to compute determinants, matrix products, and inverses. To illustrate the case $SL(2, Z_5)$, consider the element $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$. Then $\det A = (3 \cdot 4 - 4 \cdot 4) \bmod 5 = -4 \bmod 5 = 1$, and the inverse of A is $\begin{bmatrix} 4 & -4 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$. Note that $\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ when the arithmetic is done modulo 5. ∎

Example 9 is a special case of the following general construction.

EXAMPLE 19 Let F be any of Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p (p a prime). The set $GL(2, F)$ of all 2×2 matrices with nonzero determinants and entries from F is a non-Abelian group under matrix multiplication. As in Example 18, when F is Z_p, modulo p arithmetic is used to calculate determinants, matrix products, and inverses. The formula given in Example 9 for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ remains valid for elements from $GL(2, Z_p)$, provided we interpret division by $ad - bc$ as multiplication by the inverse of $(ad - bc)$ modulo p. For example, in $GL(2, Z_7)$, consider $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$. Then the determinant $(ad - bc) \bmod 7$ is $(12 - 30) \bmod 7 = -18 \bmod 7 = 3$ and the inverse of 3 is 5 [since $(3 \cdot 5) \bmod 7 = 1$]. So, the inverse of $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ is $\begin{bmatrix} 3 \cdot 5 & 2 \cdot 5 \\ 1 \cdot 5 & 4 \cdot 5 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$. [The reader should check that $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $GL(2, Z_7)$]. ∎

The group $GL(n, F)$ is called the *general linear group* of $n \times n$ matrices over F.

EXAMPLE 20 The set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime. ∎

EXAMPLE 21 The set of all symmetries of the infinite ornamental pattern in which arrowheads are spaced uniformly a unit apart along

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

a line is an Abelian group under composition. Let T denote a translation to the right by one unit, T^{-1} a translation to the left by one unit, and H a reflection across the horizontal line of the figure. Then, every member of the group is of the form $x_1x_2 \cdot \cdot \cdot x_n$, where each $x_i \in \{T, T^{-1}, H\}$. In this case, we say that T, T^{-1}, and H *generate* the group. ∎

Table 2.1 summarizes many of the specific groups that we have presented thus far.

As the previous examples demonstrate, the notion of a group is a very broad one indeed. The goal of the axiomatic approach is to find properties general enough to permit many diverse examples having these properties and specific enough to allow one to deduce many interesting consequences.

The goal of abstract algebra is to discover truths about algebraic systems (that is, sets with one or more binary operations) that are independent of the specific nature of the operations. All one knows or needs to know is that these operations, whatever they may be, have

Table 2.1 Summary of Group Examples (F can be any of Q, $\mathbf{R}$, $\mathbf{C}$, or Z_p; L is a reflection)

Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
$\mathbf{R}^*$	Multiplication	1	x	$1/x$	Yes
$\mathbf{C}^*$	Multiplication	1	$a + bi$	$\frac{1}{a^2 + b^2}a - \frac{1}{a^2 - b^2}bi$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbf{R}^n$	Componentwise addition	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - \alpha}$, L	No

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

certain properties. We then seek to deduce consequences of these properties. This is why this branch of mathematics is called *abstract* algebra. It must be remembered, however, that when a specific group is being discussed, a specific operation must be given (at least implicitly).

Elementary Properties of Groups

Now that we have seen many diverse examples of groups, we wish to deduce some properties that they share. The definition itself raises some fundamental questions. Every group has *an* identity. Could a group have more than one? Every group element has *an* inverse. Could an element have more than one? The examples suggest not. But examples can only suggest. One cannot prove that every group has a unique identity by looking at examples, because each example inherently has properties that may not be shared by all groups. We are forced to restrict ourselves to the properties that all groups have; that is, we must view groups as abstract entities rather than argue by example. The next three theorems illustrate the abstract approach.

Theorem 2.1 Uniqueness of the Identity

In a group G, there is only one identity element.

PROOF Suppose both e and e' are identities of G. Then,

1. $ae = a$ for all a in G, and
2. $e'a = a$ for all a in G.

The choices of $a = e'$ in (part 1) and $a = e$ in (part 2) yield $e'e = e'$ and $e'e = e$**.** Thus, e and e' are both equal to $e'e$ and so are equal to each other. ∎

Because of this theorem, we may unambiguously speak of "the identity" of a group and denote it by 'e' (because the German word for identity is *Einheit*).

Theorem 2.2 Cancellation

In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PROOF Suppose $ba = ca$. Let a' be an inverse of a. Then multiplying on the right by a' yields $(ba)a' = (ca)a'$. Associativity yields $b(aa') = c(aa')$. Then $be = ce$ and, therefore, $b = c$ as desired. Similarly, one can prove that $ab = ac$ implies $b = c$ by multiplying by a' on the left. ∎

A consequence of the cancellation property is the fact that in a Cayley table for a group, each group element occurs exactly once in each row and column (see Exercise 31). Another consequence of the cancellation property is the uniqueness of inverses.

Theorem 2.3 Uniqueness of Inverses

For each element a in a group G, there is a unique element b in G such that ab = ba = e.

PROOF Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so that $ab = ac$. Canceling the a on both sides gives $b = c$, as desired. ∎

As was the case with the identity element, it is reasonable, in view of Theorem 2.3, to speak of "the inverse" of an element g of a group; in fact, we may unambiguously denote it by g^{-1}. This notation is suggested by that used for ordinary real numbers under multiplication. Similarly, when n is a positive integer, the associative law allows us to use g^n to denote the unambiguous product

$$\underbrace{gg \cdots g}_{n \text{ factors}}.$$

We define $g^0 = e$. When n is negative, we define $g^n = (g^{-1})^{|n|}$ [for example, $g^{-3} = (g^{-1})^3$]. Unlike for real numbers, in an abstract group we do not permit noninteger exponents such as $g^{1/2}$. With this notation, the familiar laws of exponents hold for groups; that is, for all integers m and n and any group element g, we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$. Although the way one manipulates the group expressions $g^m g^n$ and $(g^m)^n$ coincides with the laws of exponents for real numbers, the laws of exponents fail to hold for expressions involving two group elements. Thus, for groups in general, $(ab)^n \neq a^n b^n$ (see Exercise 23).

The important thing about the existence of a unique inverse for each group element a is that for every element b in the group there is a unique solution in the group of the equations $ax = b$ and $xa = b$. Namely, $x = a^{-1}b$ in the first case and $x = ba^{-1}$ in the second case. In contrast,

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

in the set $\{0, 1, 2, 3, 4, 5\}$, the equation $2x = 4$ has the solutions $x = 2$ and $x = 5$ under the operation multiplication mod 6. However, this set is not a group under multiplication mod 6.

Also, one must be careful with this notation when dealing with a specific group whose binary operation is addition and is denoted by "+." In this case, the definitions and group properties expressed in multiplicative notation must be translated to additive notation. For example, the inverse of g is written as $-g$. Likewise, for example, g^3 means $g + g + g$ and is usually written as $3g$, whereas g^{-3} means $(-g) + (-g) + (-g)$ and is written as $-3g$. When additive notation is used, do not interpret "ng" as combining n and g under the group operation; n may not even be an element of the group! Table 2.2 shows the common notation and corresponding terminology for groups under multiplication and groups under addition. As is the case for real numbers, we use $a - b$ as an abbreviation for $a + (-b)$.

Table **2.2**

Multiplicative Group		Additive Group	
$a \cdot b$ or ab	Multiplication	$a + b$	Addition
e or 1	Identity or one	0	Zero
a^{-1}	Multiplicative inverse of a	$-a$	Additive inverse of a
a^n	Power of a	na	Multiple of a
ab^{-1}	Quotient	$a - b$	Difference

Because of the associative property, we may unambiguously write the expression abc, for this can be reasonably interpreted as only $(ab)c$ or $a(bc)$, which are equal. In fact, by using induction and repeated application of the associative property, one can prove a general associative property that essentially means that parentheses can be inserted or deleted at will without affecting the value of a product involving any number of group elements. Thus,

$$a^2(bcdb^2) = a^2b(cd)b^2 = (a^2b)(cd)b^2 = a(abcdb)b,$$

and so on.

Although groups do not have the property that $(ab)^n = a^nb^n$, there is a simple relationship between $(ab)^{-1}$ and a^{-1} and b^{-1}.

Theorem 2.4 Socks–Shoes Property

For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

PROOF Since $(ab)(ab)^{-1} = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, we have by Theorem 2.3 that $(ab)^{-1} = b^{-1}a^{-1}$. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Historical Note

We conclude this chapter with a bit of history concerning the noncommutativity of matrix multiplication. In 1925, quantum theory was replete with annoying and puzzling ambiguities. It was Werner Heisenberg who recognized the cause. He observed that the product of the quantum-theoretical analogs of the classical Fourier series did not necessarily commute. For all his boldness, this shook Heisenberg. As he later recalled [2, p. 94]:

> In my paper the fact that *XY* was not equal to *YX* was very disagreeable to me. I felt this was the only point of difficulty in the whole scheme, otherwise I would be perfectly happy. But this difficulty had worried me and I was not able to solve it.

Heisenberg asked his teacher, Max Born, if his ideas were worth publishing. Born was fascinated and deeply impressed by Heisenberg's new approach. Born wrote [1, p. 217]:

> After having sent off Heisenberg's paper to the *Zeitschrift für Physik* for publication, I began to ponder over his symbolic multiplication, and was soon so involved in it that I thought about it for the whole day and could hardly sleep at night. For I felt there was something fundamental behind it, the consummation of our endeavors of many years. And one morning, about the 10 July 1925, I suddenly saw light: Heisenberg's symbolic multiplication was nothing but the matrix calculus, well-known to me since my student days from Rosanes' lectures in Breslau.

Born and his student, Pascual Jordan, reformulated Heisenberg's ideas in terms of matrices, but it was Heisenberg who was credited with the formulation. In his autobiography, Born lamented [1, p. 219]:

> Nowadays the textbooks speak without exception of Heisenberg's matrices, Heisenberg's commutation law, and Dirac's field quantization.
>
> In fact, Heisenberg knew at that time very little of matrices and had to study them.

Upon learning in 1933 that he was to receive the Nobel Prize with Dirac and Schrödinger for this work, Heisenberg wrote to Born [1, p. 220]:

> If I have not written to you for such a long time, and have not thanked you for your congratulations, it was partly because of my rather bad conscience with respect to you. The fact that I am to receive the Nobel Prize alone, for work done in Göttingen in collaboration—you, Jordan, and I—this fact depresses me and I hardly know what to write to you. I am, of course, glad that our common efforts are now appreciated, and I enjoy the recollection of the beautiful time of collaboration. I also believe that all good physicists know how great was your and Jordan's contribution to the structure of quantum mechanics—and this remains unchanged by a wrong decision from outside. Yet I myself can do nothing but thank you again for all the fine collaboration, and feel a little ashamed.

The story has a happy ending, however, because Born received the Nobel Prize in 1954 for his fundamental work in quantum mechanics.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Exercises

"For example" is not proof.

JEWISH PROVERB

1. Which of the following binary operations are closed?
- **a.** subtraction of positive integers
- **b.** division of nonzero integers
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with integer entries

2. Which of the following binary operations are associative?
- **a.** multiplication mod n
- **b.** division of nonzero rationals
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with integer entries

3. Which of the following binary operations are commutative?
- **a.** substraction of integers
- **b.** division of nonzero real numbers
- **c.** function composition of polynomials with real coefficients
- **d.** multiplication of 2×2 matrices with real entries

4. Which of the following sets are closed under the given operation?
- **a.** $\{0, 4, 8, 12\}$ addition mod 16
- **b.** $\{0, 4, 8, 12\}$ addition mod 15
- **c.** $\{1, 4, 7, 13\}$ multiplication mod 15
- **d.** $\{1, 4, 5, 7\}$ multiplication mod 9

5. In each case, find the inverse of the element under the given operation.
- **a.** 13 in Z_{20}
- **b.** 13 in $U(14)$
- **c.** $n-1$ in $U(n)$ $(n > 2)$
- **d.** $3-2i$ in $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication

6. In each case, perform the indicated operation.
- **a.** In $\mathbf{C}^*$, $(7 + 5i)(-3 + 2i)$
- **b.** In $GL(2, Z_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$
- **c.** In $GL(2, \mathrm{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$
- **d.** In $GL(2, Z_{13})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

7. Give two reasons why the set of odd integers under addition is not a group.

8. Referring to Example 13, verify the assertion that subtraction is not associative.

9. Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

10. Show that the group $GL(2, \mathbf{R})$ of Example 9 is non-Abelian by exhibiting a pair of matrices A and B in $GL(2, \mathbf{R})$ such that $AB \neq BA$.

11. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, Z_{11})$.

12. Give an example of group elements a and b with the property that $a^{-1}ba \neq b$.

13. Translate each of the following multiplicative expressions into its additive counterpart. Assume that the operation is commutative.

a. a^2b^3

b. $a^{-2}(b^{-1}c)^2$

c. $(ab^2)^{-3}c^2 = e$

14. For group elements a, b, and c, express $(ab)^3$ and $(ab^{-2}\, c)^{-2}$ without parentheses.

15. Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Show that $G = H$ as sets.

16. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

17. (From the GRE Practice Exam)* Let p and q be distinct primes. Suppose that H is a proper subset of the integers that is a group under addition that contains exactly three elements of the set $\{p, p + q, pq, p^q, q^p\}$. Determine which of the following are the three elements in H.

a. pq, p^q, q^p

b. $p + q, pq, p^q$

c. $p, p + q, pq$

d. p, p^q, q^p

e. p, pq, p^q

18. List the members of $H = \{x^2 \mid x \in D_4\}$ and $K = \{x \in D_4 \mid x^2 = e\}$.

19. Prove that the set of all 2×2 matrices with entries from $\mathbf{R}$ and determinant $+1$ is a group under matrix multiplication.

20. For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

21. An abstract algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead,

*GRE materials selected from the GRE Practice Exam, Question 9 by Educational Testing Service. Reprinted by permission of Educational Testing Service, the copyright owner.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

one of the nine integers was inadvertently left out, so that the list appeared as 1, 9, 16, 22, 53, 74, 79, 81. Which integer was left out? (This really happened!)

22. Let G be a group with the property that for any x, y, z in the group, $xy = zx$ implies $y = z$. Prove that G is Abelian. ("Left-right cancellation" implies commutativity.)

23. (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

24. (Socks–Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. What would be an appropriate name for the group property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

25. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

26. Prove that in a group, $(a^{-1})^{-1} = a$ for all a.

27. For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

28. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?

29. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12.

30. Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

31. Prove that every group table is a *Latin square*[†]; that is, each element of the group appears exactly once in each row and each column.

32. Construct a Cayley table for $U(12)$.

33. Suppose the table below is a group table. Fill in the blank entries.

	e	***a***	***b***	***c***	***d***
e	*e*	—	—	—	—
a	—	*b*	—	—	*e*
b	—	*c*	*d*	*e*	—
c	—	*d*	—	*a*	*b*
d	—	—	—	—	—

[†]Latin squares are useful in designing statistical experiments. There is also a close connection between Latin squares and finite geometries.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

34. Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

35. Let a, b, and c be elements of a group. Solve the equation $axb = c$ for x. Solve $a^{-1}xa = c$ for x.

36. Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.

37. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

38. Give an example of a group with elements a, b, c, d, and x such that $axb = cxd$ but $ab \neq cd$. (Hence "middle cancellation" is not valid in groups.)

39. Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian. ("Middle cancellation" implies commutativity.)

40. Find an element X in D_4 such that $R_{90}VXH = D'$.

41. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n. Prove that $F_1F_2 \neq R_0$.

42. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.

43. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $R^kFR^k = F$.

44. Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $FR^kF = R^{-k}$. Why does this imply that D_n is non-Abelian?

45. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.

a. In D_4, $FR^{-2}FR^5$

b. In D_5, $R^{-3}FR^4FR^{-2}$

c. In D_6, $FR^5FR^{-2}F$

46. Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.

47. Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian. (This exercise is referred to in Chapter 26.)

48. Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

is a group. (Multiplication is defined by

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + a' & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{bmatrix}.$$

This group, sometimes called the *Heisenberg group* after the Nobel Prize–winning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of quantum physics.)

49. Prove the assertion made in Example 20 that the set $\{1, 2, \ldots, n - 1\}$ is a group under multiplication modulo n if and only if n is prime.

50. In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 5. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

51. List the six elements of $\mathrm{GL}(2, Z_2)$. Show that this group is non-Abelian by finding two elements that do not commute. (This exercise is referred to in Chapter 7.)

52. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with Example 10.)

53. Suppose that in the definition of a group G, the condition that there exists an element e with the property $ae = ea = a$ for all a in G is replaced by $ae = a$ for all a in G. Show that $ea = a$ for all a in G. (Thus, a one-sided identity is a two-sided identity.)

54. Suppose that in the definition of a group G, the condition that for each element a in G there exists an element b in G with the property $ab = ba = e$ is replaced by the condition $ab = e$. Show that $ba = e$. (Thus, a one-sided inverse is a two-sided inverse.)

Computer Exercises

Software for the computer exercises in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

References

1. Max Born, *My Life: Recollections of a Nobel Laureate*, New York: Charles Scribner's Sons, 1978.
2. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, Vol. 3, New York: Springer-Verlag, 1982.

Suggested Readings

Marcia Ascher, *Ethnomathematics*, Pacific Grove, CA: Brooks/Cole, 1991.

Chapter 3 of this book describes how the dihedral group of order 8 can be used to encode the social structure of the kin system of family relationships among a tribe of native people of Australia.

Arie Bialostocki, "An Application of Elementary Group Theory to Central Solitaire," *The College Mathematics Journal*, May 1998: 208–212.

The author uses properties of groups to analyze the peg board game central solitaire (which also goes by the name peg solitaire).

J. E. White, "Introduction to Group Theory for Chemists," *Journal of Chemical Education* 44 (1967): 128–135.

Students interested in the physical sciences may find this article worthwhile. It begins with easy examples of groups and builds up to applications of group theory concepts and terminology to chemistry.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

3 Finite Groups; Subgroups

In our own time, in the period 1960–1980, we have seen particle physics emerge as the playground of group theory.

FREEMAN DYSON

Terminology and Notation

As we will soon discover, finite groups—that is, groups with finitely many elements—have interesting arithmetic properties. To facilitate the study of finite groups, it is convenient to introduce some terminology and notation.

Definition Order of a Group
The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

Thus, the group Z of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

Definition Order of an Element
The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

So, to find the order of a group element g, you need only compute the sequence of products $g, g^2, g^3, \ldots$, until you reach the identity for the first time. The exponent of this product (or coefficient if the operation is addition) is the order of g. If the identity never appears in the sequence, then g has infinite order.

EXAMPLE 1 Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. This group has order 8. To find the order of

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

the element 7, say, we compute the sequence $7^1 = 7$, $7^2 = 4$, $7^3 = 13$, $7^4 = 1$, so $|7| = 4$. To find the order of 11, we compute $11^1 = 11$, $11^2 = 1$, so $|11| = 2$. Similar computations show that $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$, $|14| = 2$. [Here is a trick that makes these calculations easier. Rather than compute the sequence 13^1, 13^2, 13^3, 13^4, we may observe that $13 = -2 \bmod 15$, so that $13^2 = (-2)^2 = 4$, $13^3 = -2 \cdot 4 = -8$, $13^4 = (-2)(-8) = 1$.][†] ∎

∎ **EXAMPLE 2** Consider Z_{10} under addition modulo 10. Since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, we know that $|2| = 5$. Similar computations show that $|0| = 1$, $|7| = 10$, $|5| = 2$, $|6| = 5$. (Here $2 \cdot 2$ is an abbreviation for $2 + 2$, $3 \cdot 2$ is an abbreviation for $2 + 2 + 2$, etc.) ∎

∎ **EXAMPLE 3** Consider Z under ordinary addition. Here every nonzero element has infinite order, since the sequence a, $2a$, $3a$, . . . never includes 0 when $a \neq 0$. ∎

The perceptive reader may have noticed among our examples of groups in Chapter 2 that some are subsets of others with the same binary operation. The group $SL(2, \mathbf{R})$ in Example 18, for instance, is a subset of the group $GL(2, \mathbf{R})$ in Example 9. Similarly, the group of complex numbers $\{1, -1, i, -i\}$ under multiplication is a subset of the group described in Example 15 for n equal to any multiple of 4. This situation arises so often that we introduce a special term to describe it.

Definition Subgroup

If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

We use the notation $H \leq G$ to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. Such a subgroup is called a *proper subgroup*. The subgroup $\{e\}$ is called the *trivial subgroup* of G; a subgroup that is not $\{e\}$ is called a *nontrivial subgroup* of G.

Notice that Z_n under addition modulo n is *not* a subgroup of Z under addition, since addition modulo n is not the operation of Z.

Subgroup Tests

When determining whether or not a subset H of a group G is a subgroup of G, one need not directly verify the group axioms. The next

[†] The website **http://www.google.com** provides a convenient way to do modular arithmetic. For example, to compute 13^4 mod 15, just type "13^4 mod 15" in the search box.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

three results provide simple tests that suffice to show that a subset of a group is a subgroup.

Theorem 3.1 One-Step Subgroup Test

Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H is a subgroup of G.)

PROOF Since the operation of H is the same as that of G, it is clear that this operation is associative. Next, we show that e is in H. Since H is nonempty, we may pick some x in H. Then, letting $a = x$ and $b = x$ in the hypothesis, we have $e = xx^{-1} = ab^{-1}$ is in H. To verify that x^{-1} is in H whenever x is in H, all we need to do is to choose $a = e$ and $b = x$ in the statement of the theorem. Finally, the proof will be complete when we show that H is closed; that is, if x, y belong to H, we must show that xy is in H also. Well, we have already shown that y^{-1} is in H whenever y is; so, letting $a = x$ and $b = y^{-1}$, we have $xy = x(y^{-1})^{-1} = ab^{-1}$ is in H. ∎

Although we have dubbed Theorem 3.1 the One-Step Subgroup Test, there are actually four steps involved in applying the theorem. (After you gain some experience, the first three steps will be routine.) Notice the similarity between the last three steps listed below and the three steps involved in the Second Principle of Mathematical Induction.

1. Identify the property P that distinguishes the elements of H; that is, identify a defining condition.
2. Prove that the identity has property P. (This verifies that H is nonempty.)
3. *Assume* that two elements a and b have property P.
4. Use the assumption that a and b have property P to show that ab^{-1} has property P.

The procedure is illustrated in Examples 4 and 5.

EXAMPLE 4 Let G be an Abelian group with identity e. Then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G. Here, the defining property of H is the condition $x^2 = e$. So, we first note that $e^2 = e$, so that H is nonempty. Now we assume that a and b belong to H. This means that $a^2 = e$ and $b^2 = e$. Finally, we must show that $(ab^{-1})^2 = e$. Since G is Abelian, $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$. Therefore, ab^{-1} belongs to H and, by the One-Step Subgroup Test, H is a subgroup of G. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In many instances, a subgroup will consist of all elements that have a particular form. Then the property P is that the elements have that particular form. This is illustrated in the following example.

EXAMPLE 5 Let G be an Abelian group under multiplication with identity e. Then $H = \{x^2 \mid x \in G\}$ is a subgroup of G. (In words, H is the set of all "squares.") Since $e^2 = e$, the identity has the correct form. Next, we write two elements of H in the correct form, say, a^2 and b^2. We must show that $a^2(b^2)^{-1}$ also has the correct form; that is, $a^2(b^2)^{-1}$ is the square of some element. Since G is Abelian, we may write $a^2(b^2)^{-1}$ as $(ab^{-1})^2$, which is the correct form. Thus, H is a subgroup of G. ∎

Beginning students often prefer to use the next theorem instead of Theorem 3.1.

Theorem 3.2 Two-Step Subgroup Test

Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

PROOF By Theorem 3.1, it suffices to show that $a, b \in H$ implies $ab^{-1} \in H$. So, we suppose that $a, b \in H$. Since H is closed under taking inverses, we also have $b^{-1} \in H$. Thus, $ab^{-1} \in H$ by closure under multiplication. ∎

When applying the Two-Step Subgroup Test, we proceed exactly as in the case of the One-Step Subgroup Test, except we use the assumption that a and b have property P to prove that ab has property P and that a^{-1} has property P.

EXAMPLE 6 Let G be an Abelian group. Then $H = \{x \in G \mid |x| \text{ is finite}\}$ is a subgroup of G. Since $e^1 = e$, $H \neq \theta$. To apply the Two-Step Subgroup Test we assume that a and b belong to H and prove that ab and a^{-1} belong to H. Let $|a| = m$ and $|b| = n$. Then, because G is Abelian, we have $(ab)^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. Thus, ab has finite order (this does not show that $|ab| = mn$). Moveover, $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$ shows that a^{-1} has finite order. ∎

We next illustrate how to use the Two-Step Subgroup Test by introducing an important technique for creating new subgroups of Abelian

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

groups from existing ones. The method will be extended to some subgroups of non-Abelian groups in later chapters.

EXAMPLE 7 Let G be an Abelian group and H and K be subgroups of G. Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G. First note that $e = ee$ belongs to HK because e is in both H and K. Now suppose that a and b are in HK. Then by definition of H there are elements h_1, $h_2 \in H$ and k_1, $k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$. We must prove that $ab \in HK$ and $a^{-1} \in HK$. Observe that because G is Abelian and H and K are subgroups of G, we have $ab = h_1k_1h_2k_2 = (h_1h_2)(k_1k_2) \in HK$. Likewise, $a^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}k_1^{-1} \in HK$. ∎

How do you prove that a subset of a group is *not* a subgroup? Here are three possible ways, any one of which guarantees that the subset is not a subgroup:

1. Show that the identity is not in the set.
2. Exhibit an element of the set whose inverse is not in the set.
3. Exhibit two elements of the set whose product is not in the set.

EXAMPLE 8 Let G be the group of nonzero real numbers under multiplication, $H = \{x \in G \mid x = 1 \text{ or } x \text{ is irrational}\}$ and $K = \{x \in G \mid x \geq 1\}$. Then H is not a subgroup of G, since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$. Also, K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$. ∎

When dealing with finite groups, it is easier to use the following subgroup test.

Theorem 3.3 Finite Subgroup Test

Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

PROOF In view of Theorem 3.2, we need only prove that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, consider the sequence a, a^2, ... By closure, all of these elements belong to H. Since H is finite, not all of these elements are distinct. Say $a^i = a^j$ and $i > j$. Then, $a^{i-j} = e$; and since $a \neq e$, $i - j > 1$. Thus, $aa^{i-j-1} = a^{i-j} = e$ and, therefore, $a^{i-j-1} = a^{-1}$. But $i - j - 1 \geq 1$ implies $a^{i-j-1} \in H$ and we are done. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Examples of Subgroups

The proofs of the next few theorems show how our subgroup tests work. We first introduce an important notation. For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n \mid n \in Z\}$. In particular, observe that the exponents of a include all negative integers as well as 0 and the positive integers (a^0 is defined to be the identity).

Theorem 3.4 $\langle a \rangle$ Is a Subgroup

Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.

PROOF Since $a \in \langle a \rangle$, $\langle a \rangle$ is not empty. Let a^n, $a^m \in \langle a \rangle$. Then, $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$; so, by Theorem 3.1, $\langle a \rangle$ is a subgroup of G. ∎

The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a*. In the case that $G = \langle a \rangle$, we say that G is *cyclic* and a is a *generator of G*. (A cyclic group may have many generators.) Notice that although the list $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ has infinitely many entries, the set $\{a^n \mid n \in Z\}$ might have only finitely many elements. Also note that, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, every cyclic group is Abelian.

EXAMPLE 9 In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$, for $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, $3^5 = 3^4 \cdot 3 = 1 \cdot 3$, $3^6 = 3^4 \cdot 3^2 = 9, \ldots$; $3^{-1} = 7$ (since $3 \cdot 7 = 1$), $3^{-2} = 9$, $3^{-3} = 3$, $3^{-4} = 1$, $3^{-5} = 3^{-4} \cdot 3^{-1} = 1 \cdot 7$, $3^{-6} = 3^{-4} \cdot 3^{-2} = 1 \cdot 9 = 9, \ldots$. ∎

EXAMPLE 10 In Z_{10}, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$. Remember, a^n means na when the operation is addition. ∎

EXAMPLE 11 In Z, $\langle -1 \rangle = Z$. Here each entry in the list $\ldots, -2(-1), -1(-1), 0(-1), 1(-1), 2(-1), \ldots$ represents a distinct group element. ∎

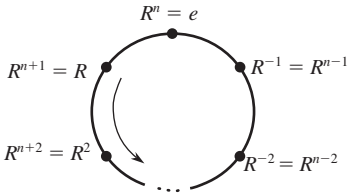
EXAMPLE 12 In D_n, the dihedral group of order $2n$, let R denote a rotation of $360/n$ degrees. Then,

$$R^n = R_{360^\circ} = e, \qquad R^{n+1} = R, \qquad R^{n+2} = R^2, \ldots.$$

Similarly, $R^{-1} = R^{n-1}$, $R^{-2} = R^{n-2}, \ldots$, so that $\langle R \rangle = \{e, R, \ldots, R^{n-1}\}$. We see, then, that the powers of R "cycle back" periodically

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

with period n. Visually, raising R to successive positive powers is the same as moving counterclockwise around the following circle one node at a time, whereas raising R to successive negative powers is the same as moving around the circle clockwise one node at a time.



In Chapter 4 we will show that $|\langle a\rangle| = |a|$; that is, the order of the subgroup generated by a is the order of a itself. (Actually, the definition of $|a|$ was chosen to ensure the validity of this equation.)

For any element a of a group G, it is useful to think of $\langle a\rangle$ as the smallest subgroup of G containing a. This notion can be extended to any collection S of elements from a group G by defining $\langle S\rangle$ as the subgroup of G with the property that $\langle S\rangle$ contains S and if H is any subgroup of G containing S, then H also contains $\langle S\rangle$ Thus, $\langle S\rangle$ is the smallest subgroup of G that contains S. The set $\langle S\rangle$ is called *the subgroup generated by S*. We illustrate this concept in the next example. The verifications are left to the reader (Exercise 40).

EXAMPLE 13 In Z_{20}, $\langle 8,14\rangle = \{0, 2, 4,\ldots, 18\} = \langle 2\rangle$; in Z, $\langle 8, 13\rangle = Z$; in D_4, $\langle H, V\rangle = \{H, H^2, V, HV\} = \{R_0, R_{180}, H, V\}$; in D_4, $\langle R_{90}, V\rangle = \{R_{90}, R_{90}{}^2, R_{90}{}^3, R_{90}{}^4, V, R_{90}V, R_{90}{}^2V, R_{90}{}^3V\} = D_4$; in **C***, the group of nonzero complex numbers under multiplication, $\langle 1, i\rangle = \{1, -1, i, -i\} = \langle i\rangle$; in **C**, the group of complex numbers under addition, $\langle 1, i\rangle = \{a + bi \mid a, b \in Z\}$ (This group is called the "Gaussian integers"); in **R,** the group of real numbers under addition, $\langle 2, \pi, \sqrt{2}\rangle = \{2a + b\pi + c\sqrt{2} \mid a, b, c \in Z\}$; in a group in which a, b, c, and d commute, $\langle a, b, c, d\rangle = \{a^q b^r c^s d^t \mid q, r, s, t \in Z\}$.

We next consider one of the most important subgroups.

Definition Center of a Group

The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}.$$

[The notation $Z(G)$ comes from the fact that the German word for center is *Zentrum.* The term was coined by J. A. de Séguier in 1904.]

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 3.5 Center Is a Subgroup

The center of a group G is a subgroup of G.

PROOF For variety, we shall use Theorem 3.2 to prove this result. Clearly, $e \in Z(G)$, so $Z(G)$ is nonempty. Now, suppose $a, b \in Z(G)$. Then $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ for all x in G; and, therefore, $ab \in Z(G)$.

Next, assume that $a \in Z(G)$. Then we have $ax = xa$ for all x in G. What we want is $a^{-1}x = xa^{-1}$ for all x in G. Informally, all we need do to obtain the second equation from the first one is simultaneously to bring the a's across the equals sign:

$$ax = xa$$

becomes $xa^{-1} = a^{-1}x$. (Be careful here; groups need not be commutative. The a on the left comes across as a^{-1} on the left, and the a on the right comes across as a^{-1} on the right.) Formally, the desired equation can be obtained from the original one by multiplying it on the left and right by a^{-1}, like so:

$$\begin{aligned} a^{-1}(ax)a^{-1} &= a^{-1}(xa)a^{-1}, \\ (a^{-1}a)xa^{-1} &= a^{-1}x(aa^{-1}), \\ exa^{-1} &= a^{-1}xe, \\ xa^{-1} &= a^{-1}x. \end{aligned}$$

This shows that $a^{-1} \in Z(G)$ whenever a is. ∎

For practice, let's determine the centers of the dihedral groups.

EXAMPLE 14 For $n \geq 3$,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & \text{when } n \text{ is even,} \\ \{R_0\} & \text{when } n \text{ is odd.} \end{cases}$$

To verify this, first observe that since every rotation in D_n is a power of $R_{360/n}$, rotations commute with rotations. We now investigate when a rotation commutes with a reflection. Let R be any rotation in D_n and let F be any reflection in D_n. Observe that since RF is a reflection we have $RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$. Thus, it follows that R and F commute if and only if $FR = RF = FR^{-1}$. By cancellation, this holds if and only if $R = R^{-1}$. But $R = R^{-1}$ only when $R = R_0$ or $R = R_{180}$, and R_{180} is in D_n only when n is even. So, we have proved that $Z(D_n) = \{R_0\}$ when n is odd and $Z(D_n) = \{R_0, R_{180}\}$ when n is even. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Although an element from a non-Abelian group does not necessarily commute with every element of the group, there are always some elements with which it will commute. For example, every element a commutes with all powers of a. This observation prompts the next definition and theorem.

Definition Centralizer of a in G

Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

EXAMPLE 15 In D_4, we have the following centralizers:

$$\begin{aligned} C(R_0) &= D_4 = C(R_{180}), \\ C(R_{90}) &= \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}), \\ C(H) &= \{R_0, H, R_{180}, V\} = C(V), \\ C(D) &= \{R_0, D, R_{180}, D'\} = C(D'). \end{aligned}$$

Notice that each of the centralizers in Example 15 is actually a subgroup of D_4. The next theorem shows that this was not a coincidence.

Theorem 3.6 $C(a)$ Is a Subgroup

For each a in a group G, the centralizer of a is a subgroup of G.

PROOF A proof similar to that of Theorem 3.5 is left to the reader to supply (Exercise 41).

Notice that for every element a of a group G, $Z(G) \subseteq C(a)$. Also, observe that G is Abelian if and only if $C(a) = G$ for all a in G.

Exercises

The purpose of proof is to understand, not to verify.

ARNOLD ROSS

1. For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

$$Z_{12}, \qquad U(10), \qquad U(12), \qquad U(20), \qquad D_4$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

2. Let Q be the group of rational numbers under addition and let Q^* be the group of nonzero rational numbers under multiplication. In Q, list the elements in $\langle \frac{1}{2} \rangle$. In Q^*, list the elements in $\langle \frac{1}{2} \rangle$.

3. Let Q and Q^* be as in Exercise 2. Find the order of each element in Q and in Q^*.

4. Prove that in any group, an element and its inverse have the same order.

5. Without actually computing the orders, explain why the two elements in each of the following pairs of elements from Z_{30} must have the same order: $\{2, 28\}$, $\{8, 22\}$. Do the same for the following pairs of elements from $U(15)$: $\{2, 8\}$, $\{7, 13\}$.

6. In the group Z_{12}, find $|a|$, $|b|$, and $|a + b|$ for each case.

a. $a = 6, b = 2$

b. $a = 3, b = 8$

c. $a = 5, b = 4$

Do you see any relationship between $|a|$, $|b|$, and $|a + b|$?

7. If a, b, and c are group elements and $|a| = 6$, $|b| = 7$, express $(a^4c^{-2}b^4)^{-1}$ without using negative exponents.

8. What can you say about a subgroup of D_3 that contains R_{240} and a reflection F? What can you say about a subgroup of D_3 that contains two reflections?

9. What can you say about a subgroup of D_4 that contains R_{270} and a reflection? What can you say about a subgroup of D_4 that contains H and D? What can you say about a subgroup of D_4 that contains H and V?

10. How many subgroups of order 4 does D_4 have?

11. Determine all elements of finite order in R^*, the group of nonzero real numbers under multiplication.

12. If a and b are group elements and $ab \neq ba$, prove that $aba \neq e$.

13. Suppose that H is a nonempty subset of a group G that is closed under the group operation and has the property that if a is not in H then a^{-1} is not in H. Is H a subgroup?

14. Let G be the group of polynomials under addition with coefficients from Z_{10}. Find the orders of $f(x) = 7x^2 + 5x + 4$, $g(x) = 4x^2 + 8x + 6$, and $f(x) + g(x) = x^2 + 3x$. If $h(x) = a_n x^n + a_n - 1x^{n-1} + \cdots + a_0$ belongs to G, determine $|h(x)|$ given that $\gcd(a_1, a_2, \ldots, a_n) = 1$; $\gcd(a_1, a_2, \ldots, a_n) = 2$; $\gcd(a_1, a_2, \ldots, a_n) = 5$; and $\gcd(a_1, a_2, \ldots, a_n) = 10$.

15. If a is an element of a group G and $|a| = 7$, show that a is the cube of some element of G.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

16. Suppose that H is a nonempty subset of a group G with the property that if a and b belong to H then $a^{-1}b^{-1}$ belongs to H. Prove or disprove that this is enough to guarantee that H is a subgroup of G.

17. Prove that if an Abelian group has more than three elements of order 2, then it has at least 7 elements of order 2. Find an example that shows this is not true for non-Abelian groups.

18. Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

19. If a is a group element and a has infinite order, prove that $a^m \neq a^n$ when $m \neq n$.

20. Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

21. Show that if a is an element of a group G, then $|a| \leq |G|$.

22. Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. [Hence, $U(14)$ is cyclic.] Is $U(14) = \langle 11 \rangle$?

23. Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]

24. Suppose n is an even positive integer and H is a subgroup of Z_n. Prove that either every member of H is even or exactly half of the members of H are even.

25. Prove that for every subgroup of D_n, either every member of the subgroup is a rotation or exactly half of the members are rotations.

26. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

27. For every even integer n, show that D_n has a subgroup of order 4.

28. Suppose that H is a proper subgroup of Z under addition and H contains 18, 30, and 40. Determine H.

29. Suppose that H is a proper subgroup of Z under addition and that H contains 12, 30, and 54. What are the possibilities for H?

30. Prove that the dihedral group of order 6 does not have a subgroup of order 4.

31. For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$. [For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.] List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$. Prove that $U_k(n)$ is a subgroup of $U(n)$. Let $H = \{x \in U(10) \mid x \bmod 3 = 1\}$. Is H a subgroup of $U(10)$? (This exercise is referred to in Chapter 8.)

32. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

33. Let G be a group. Show that $Z(G) = \cap_{a \in G} C(a)$. [This means the intersection of *all* subgroups of the form $C(a)$.]

34. Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

35. For any group element a and any integer k, show that $C(a) \subseteq C(a^k)$. Use this fact to complete the following statement: "In a group, if x commutes with a, then . . . ." Is the converse true?

36. Complete the partial Cayley group table given below.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

37. Suppose G is the group defined by the following Cayley table.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

a. Find the centralizer of each member of G.

b. Find $Z(G)$.

c. Find the order of each element of G. How are these orders arithmetically related to the order of the group?

38. If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

39. Let S be a subset of a group and let H be the intersection of all subgroups of G that contain S.

a. Prove that $\langle S \rangle = H$.

b. If S is nonempty, prove that $\langle S \rangle = \{s_1^{n_1} s_2^{n_2} \ldots s_m^{n_m} \mid m \geq 1, s_i \in S, n_i \in Z\}$. (The s_i terms need not be distinct.)

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

40. In the group Z, find

a. $\langle 8, 14\rangle$;

b. $\langle 8, 13\rangle$;

c. $\langle 6, 15\rangle$;

d. $\langle m, n\rangle$;

e. $\langle 12, 18, 45\rangle$.

In each part, find an integer k such that the subgroup is $\langle k\rangle$.

41. Prove Theorem 3.6.

42. If H is a subgroup of G, then by the *centralizer* $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

43. Must the centralizer of an element of a group be Abelian?

44. Must the center of a group be Abelian?

45. Let G be an Abelian group with identity e and let n be some fixed integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G. Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G. (This exercise is referred to in Chapter 11.)

46. Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

47. Let G be the set of all polynomials with coefficients from the set $\{0, 1, 2, 3\}$. We can make G a group under addition by adding the polynomials in the usual way, except that we use modulo 4 to combine the coefficients. With this group operation, determine the orders of the elements of G. Determine a necessary and sufficient condition for an element of G to have order 2.

48. In each case, find elements a and b from a group such that $|a| = |b| = 2$.

a. $|ab| = 3$ **b.** $|ab| = 4$ **c.** $|ab| = 5$

Can you see any relationship among $|a|$, $|b|$, and $|ab|$?

49. Suppose a group contains elements a and b such that $|a| = 4$, $|b| = 2$, and $a^3b = ba$. Find $|ab|$.

50. Suppose a and b are group elements such that $|a| = 2$, $b \neq e$, and $aba = b^2$. Determine $|b|$.

51. Let a be a group element of order n, and suppose that d is a positive divisor of n. Prove that $|a^d| = n/d$.

52. Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbf{R})$. Find |A|, |B|, and |AB|. Does your answer surprise you?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

53. Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2, \mathbf{R})$. What is the order of A? If we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of $SL(2, Z_p)$ (p is a prime), what is the order of A?

54. For any positive integer n and any angle θ, show that in the group $SL(2, \mathbf{R})$,

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}.$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos \sqrt{2}^\circ & -\sin \sqrt{2}^\circ \\ \sin \sqrt{2}^\circ & \cos \sqrt{2}^\circ \end{bmatrix}.$$

(Geometrically, $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ represents a rotation of the plane θ degrees.)

55. Let G be the symmetry group of a circle. Show that G has elements of every finite order as well as elements of infinite order.

56. Let x belong to a group and $|x| = 6$. Find $|x^2|$, $|x^3|$, $|x^4|$, and $|x^5|$. Let y belong to a group and $|y| = 9$. Find $|y^i|$ for $i = 2, 3, \ldots, 8$. Do these examples suggest any relationship between the order of the power of an element and the order of the element?

57. D_4 has seven cyclic subgroups. List them.

58. $U(15)$ has six cyclic subgroups. List them.

59. Prove that a group of even order must have an element of order 2.

60. Suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

61. Let H be a subgroup of a finite group G. Suppose that g belongs to G and n is the smallest positive integer such that $g^n \in H$. Prove that n divides $|g|$.

62. Compute the orders of the following groups.

a. $U(3)$, $U(4)$, $U(12)$

b. $U(5)$, $U(7)$, $U(35)$

c. $U(4)$, $U(5)$, $U(20)$

d. $U(3)$, $U(5)$, $U(15)$

On the basis of your answers, make a conjecture about the relationship among $|U(r)|$, $|U(s)|$, and $|U(rs)|$.

63. Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication and let $H = \{x \in \mathbf{R}^* \mid x^2 \text{ is rational}\}$. Prove that H is a subgroup of $\mathbf{R}^*$. Can the exponent 2 be replaced by any positive integer and still have H be a subgroup?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

64. Compute $|U(4)|$, $|U(10)|$, and $|U(40)|$. Do these groups provide a counterexample to your answer to Exercise 62? If so, revise your conjecture.

65. Find a cyclic subgroup of order 4 in $U(40)$.

66. Find a noncyclic subgroup of order 4 in $U(40)$.

67. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in Z \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid a + b + c + d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

68. Let $H = \{A \in GL(2, \mathbf{R}) \mid \det A \text{ is an integer power of } 2\}$. Show that H is a subgroup of $GL(2, \mathbf{R})$.

69. Let H be a subgroup of $\mathbf{R}$ under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $\mathbf{R}^*$ under multiplication.

70. Let G be a group of functions from $\mathbf{R}$ to $\mathbf{R}^*$, where the operation of G is multiplication of functions. Let $H = \{f \in G \mid f(2) = 1\}$. Prove that H is a subgroup of G. Can 2 be replaced by any real number?

71. Let $G = GL(2, \mathbf{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a \text{ and } b \text{ are nonzero integers} \right\}$ under the operation of matrix multiplication. Prove or disprove that H is a subgroup of $GL(2, \mathbf{R})$.

72. Let $H = \{a + bi \mid a, b \in \mathbf{R}, ab \geq 0\}$. Prove or disprove that H is a subgroup of $\mathbf{C}$ under addition.

73. Let $H = \{a + bi \mid a, b \in \mathbf{R}, a^2 + b^2 = 1\}$. Prove or disprove that H is a subgroup of $\mathbf{C}^*$ under multiplication. Describe the elements of H geometrically.

74. Let G be a finite Abelian group and let a and b belong to G. Prove that the set $\langle a, b \rangle = \{a^i b^j \mid i, j \in \mathrm{Z}\}$ is a subgroup of G. What can you say about $|\langle a, b \rangle|$ in terms of $|a|$ and $|b|$?

75. Let H be a subgroup of a group G. Prove that the set $HZ(G) = \{hz \mid h \in H, z \in Z(G)\}$ is a subgroup of G. This exercise is referred to in this chapter.

76. Let G be a group and H a subgroup. For any element g of G, define $gH = \{gh \mid h \in H\}$. If G is Abelian and g has order 2, show that the set $K = H \cup gH$ is a subgroup of G. Is your proof valid if we drop the assumption that G is Abelian and let $K = Z(G) \cup gZ(G)$?

77. Let a belong to a group and $|a| = m$. If n is relatively prime to m, show that a can be written as the nth power of some element in the group.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

78. Let F be a reflection in the dihedral group D_n and R a rotation in D_n. Determine $C(F)$ when n is odd. Determine $C(F)$ when n is even. Determine $C(R)$.

79. Let $G = GL(2, \mathbf{R})$.

a. Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

b. Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

c. Find $Z(G)$.

80. Let G be a finite group with more than one element. Show that G has an element of prime order.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Readings

Ruth Berger, "Hidden Group Structure," *Mathematics Magazine* 78 (2005): 45–48.

In this note, the author investigates groups obtained from $U(n)$ by multiplying each element by some k in $U(n)$. Such groups have identities that are not obvious.

J. Gallian and M. Reid, "Abelian Forcing Sets," *American Mathematical Monthly* 100 (1993): 580–582.

A set S is called *Abelian forcing* if the only groups that satisfy $(ab)^n = a^n b^n$ for all a and b in the group and all n in S are the Abelian ones. This paper characterizes the Abelian forcing sets. It can be downloaded at **http://www.d.umn.edu/~jgallian/forcing.pdf**

Gina Kolata, "Perfect Shuffles and Their Relation to Math," *Science* 216 (1982): 505–506.

This is a delightful nontechnical article that discusses how group theory and computers were used to solve a difficult problem about shuffling a deck of cards. Serious work on the problem was begun by an undergraduate student as part of a programming course.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Suggested Software

Allen Hibbard and Kenneth Levasseur, *Exploring Abstract Algebra with Mathematica*, New York: Springer-Verlag, 1999.

This book, intended as a supplement for a course in abstract algebra, consists of 14 group labs, 13 ring labs, and documentation for the *Abstract Algebra* software on which the labs are based. The software uses the Mathematica language, and only a basic familiarity with the program is required. The software can be freely downloaded at **http://www.central.edu/eaam/** and can be used independently of the book.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

4 Cyclic Groups

The notion of a "group," viewed only 30 years ago as the epitome of sophistication, is today one of the mathematical concepts most widely used in physics, chemistry, biochemistry, and mathematics itself.

ALEXEY SOSINSKY, *1991*

Properties of Cyclic Groups

Recall from Chapter 3 that a group G is called *cyclic* if there is an element a in G such that $G = \{a^n \mid n \in Z\}$. Such an element a is called a *generator* of G. In view of the notation introduced in the preceding chapter, we may indicate that G is a cyclic group generated by a by writing $G = \langle a \rangle$.

In this chapter, we examine cyclic groups in detail and determine their important characteristics. We begin with a few examples.

EXAMPLE 1 The set of integers Z under ordinary addition is cyclic. Both 1 and -1 are generators. (Recall that, when the operation is addition, 1^n is interpreted as

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

when n is positive and as

$$\underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms}}$$

when n is negative.) ∎

EXAMPLE 2 The set $Z_n = \{0, 1, \ldots, n - 1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n - 1$ are generators. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Unlike Z, which has only two generators, Z_n may have many generators (depending on which n we are given).

EXAMPLE 3 $Z_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$. To verify, for instance, that $Z_8 = \langle 3\rangle$, we note that $\langle 3\rangle = \{3, 3 + 3, 3 + 3 + 3, \ldots\}$ is the set $\{3, 6, 1, 4, 7, 2, 5, 0\} = Z_8$. Thus, 3 is a generator of Z_8. On the other hand, 2 is not a generator, since $\langle 2\rangle = \{0, 2, 4, 6\} \neq Z_8$. ∎

EXAMPLE 4 (See Example 11 in Chapter 2.)
$U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3\rangle$. Also, $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = \langle 7\rangle$. So both 3 and 7 are generators for $U(10)$. ∎

Quite often in mathematics, a "nonexample" is as helpful in understanding a concept as an example. With regard to cyclic groups, $U(8)$ serves this purpose; that is, $U(8)$ is not a cyclic group. How can we verify this? Well, note that $U(8) = \{1, 3, 5, 7\}$. But

$$\begin{aligned}\langle 1\rangle &= \{1\},\\ \langle 3\rangle &= \{3, 1\},\\ \langle 5\rangle &= \{5, 1\},\\ \langle 7\rangle &= \{7, 1\},\end{aligned}$$

so $U(8) \neq \langle a\rangle$ for any a in $U(8)$.

With these examples under our belts, we are now ready to tackle cyclic groups in an abstract way and state their key properties.

Theorem 4.1 Criterion for $a^i = a^j$

Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say, n, then $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

PROOF If a has infinite order, there is no nonzero n such that a^n is the identity. Since $a^i = a^j$ implies $a^{i-j} = e$, we must have $i - j = 0$, and the first statement of the theorem is proved.

Now assume that $|a| = n$. We will prove that $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$. Certainly, the elements $e, a, \ldots, a^{n-1}$ are in $\langle a\rangle$.

Now, suppose that a^k is an arbitrary member of $\langle a\rangle$. By the division algorithm, there exist integers q and r such that

$$k = qn + r \quad \text{with} \quad 0 \leq r < n.$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Then $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r$, so that $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$. This proves that $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Next, we assume that $a^i = a^j$ and prove that n divides $i - j$. We begin by observing that $a^i = a^j$ implies $a^{i-j} = e$. Again, by the division algorithm, there are integers q and r such that

$$i - j = qn + r \qquad \text{with} \qquad 0 \leq r < n.$$

Then $a^{i-j} = a^{qn+r}$, and therefore $e = a^{i-j} = a^{qn+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$. Since n is the least positive integer such that a^n is the identity, we must have $r = 0$, so that n divides $i - j$.

Conversely, if $i - j = nq$, then $a^{i-j} = a^{nq} = e^q = e$, so that $a^i = a^j$. ∎

Theorem 4.1 reveals the reason for the dual use of the notation and terminology for the order of an element and the order of a group.

Corollary 1 $|a| = |\langle a \rangle|$

For any group element a, $|a| = |\langle a \rangle|$.

One special case of Theorem 4.1 occurs so often that it deserves singling out.

Corollary 2 $a^k = e$ Implies That $|a|$ Divides k

Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

PROOF Since $a^k = e = a^0$, we know by Theorem 4.1 that n divides $k - 0$. ∎

Theorem 4.1 and its corollaries for the case $|a| = 6$ are illustrated in Figure 4.1.

What is important about Theorem 4.1 in the finite case is that it says that multiplication in $\langle a \rangle$ is essentially done by *addition* modulo n. That is, if $(i + j) \bmod n = k$, then $a^i a^j = a^k$. Thus, no matter what group G is, or how the element a is chosen, multiplication in $\langle a \rangle$ works the same as addition in Z_n whenever $|a| = n$. Similarly, if a has infinite order,

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

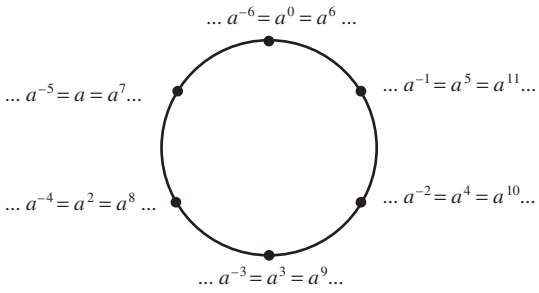


Figure 4.1

then multiplication in $\langle a \rangle$ works the same as addition in Z, since $a^i a^j = a^{i+j}$ and no modular arithmetic is done.

For these reasons, the cyclic groups Z_n and Z serve as prototypes for all cyclic groups, and algebraists say that there is essentially only one cyclic group of each order. What is meant by this is that, although there may be many different sets of the form $\{a^n \mid n \in Z\}$, there is essentially only one way to operate on these sets. Algebraists do not really care what the elements of a set are; they care only about the algebraic properties of the set—that is, the ways in which the elements of a set can be combined. We will return to this theme in the chapter on isomorphisms (Chapter 6).

The next theorem provides a simple method for computing $|a^k|$ knowing only $|a|$, and its first corollary provides a simple way to tell when $\langle a^i \rangle = \langle a^j \rangle$.

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n, k)$

Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ ***and*** $|a^k| = n/\gcd(n, k)$.

PROOF To simplify the notation, let $d = \gcd(n, k)$ and let $k = dr$. Since $a^k = (a^d)^r$, we have by closure that $\langle a^k \rangle \subseteq \langle a^d \rangle$. By Theorem 0.2 (the gcd theorem), there are integers s and t such that $d = ns + kt$. So, $a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$. This proves $\langle a^d \rangle \subseteq \langle a^k \rangle$. So, we have verified that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

We prove the second part of the theorem by showing first that $|a^d| = n/d$ for any divisor d of n. Clearly, $(a^d)^{n/d} = a^n = e$, so that $|a^d| \leq n/d$. On the other hand, if i is a positive integer less than n/d, then $(a^d)^i \neq e$ by definition of $|a|$. We now apply this fact with $d = \gcd(n, k)$ to obtain $|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = |a^{\gcd(n,k)}| = n/\gcd(n, k)$. ∎

The advantage of Theorem 4.2 is that it allows us to replace one generator of a cyclic subgroup with a more convenient one. For example,

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

if $|a| = 30$, we have $\langle a^{26}\rangle = \langle a^2\rangle$, $\langle a^{23}\rangle = \langle a\rangle$, $\langle a^{22}\rangle = \langle a^2\rangle$, $\langle a^{21}\rangle = \langle a^3\rangle$. From this we can easily see that $|a^{23}| = 30$ and $|a^{22}| = 15$. Moreover, if one wants to list the elements of, say, $\langle a^{21}\rangle$, it is easier to list the elements of $\langle a^3\rangle$ instead. (Try it doing it both ways!).

Theorem 4.2 establishes an important relationship between the order of an element in a finite cyclic group and the order of the group.

Corollary 1 Orders of Elements in Finite Cyclic Groups

In a finite cyclic group, the order of an element divides the order of the group.

Corollary 2 Criterion for $\langle a^i\rangle = \langle a^j\rangle$ and $|a^i| = |a^j|$

Let $|a| = n$. Then $\langle a^i\rangle = \langle a^j\rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$, and $|a^i| = |a^j|$ if and only if $\gcd(n, i) = \gcd(n, j)$.

PROOF Theorem 4.2 shows that $\langle a^i\rangle = \langle a^{\gcd(n,i)}\rangle$ and $\langle a^j\rangle = \langle a^{\gcd(n,j)}\rangle$, so that the proof reduces to proving that $\langle a^{\gcd(n,i)}\rangle = \langle a^{\gcd(n,j)}\rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$. Certainly, $\gcd(n, i) = \gcd(n, j)$ implies that $\langle a^{\gcd(n,i)}\rangle = \langle a^{\gcd(n,j)}\rangle$. On the other hand, $\langle a^{\gcd(n,i)}\rangle = \langle a^{\gcd(n,j)}\rangle$ implies that $|a^{\gcd(n,i)}| = |a^{\gcd(n,j)}|$, so that by the second conclusion of Theorem 4.2, we have $n/\gcd(n, i) = n/\gcd(n, j)$, and therefore $\gcd(n, i) = \gcd(n, j)$. ∎

The second part of the corollary follows from the first part and Corollary 1 of Theorem 4.1.

The next two corollaries are important special cases of the preceding corollary.

Corollary 3 Generators of Finite Cyclic Groups

Let $|a| = n$. Then $\langle a\rangle = \langle a^j\rangle$ if and only if $\gcd(n, j) = 1$, and $|a| = |\langle a^j\rangle|$ if and only if $\gcd(n, j) = 1$.

Corollary 4 Generators of Z_n

An integer k in Z_n is a generator of Z_n if and only if $\gcd(n, k) = 1$.

The value of Corollary 3 is that once one generator of a cyclic group has been found, all generators of the cyclic group can easily be determined.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

For example, consider the subgroup of all rotations in D_6. Clearly, one generator is R_{60}. And, since $|R_{60}| = 6$, we see by Corollary 3 that the only other generator is $(R_{60})^5 = R_{300}$. Of course, we could have readily deduced this information without the aid of Corollary 3 by direct calculations. So, to illustrate the real power of Corollary 3, let us use it to find all generators of the cyclic group $U(50)$. First, note that direct computations show that $|U(50)| = 20$ and that 3 is one of its generators. Thus, in view of Corollary 3, the complete list of generators for $U(50)$ is

$$\begin{aligned} 3 \bmod 50 &= 3, & 3^{11} \bmod 50 &= 47,\\ 3^3 \bmod 50 &= 27, & 3^{13} \bmod 50 &= 23,\\ 3^7 \bmod 50 &= 37, & 3^{17} \bmod 50 &= 13,\\ 3^9 \bmod 50 &= 33, & 3^{19} \bmod 50 &= 17. \end{aligned}$$

Admittedly, we had to do some arithmetic here, but it certainly entailed much less work than finding all the generators by simply determining the order of each element of $U(50)$ one by one.

The reader should keep in mind that Theorem 4.2 and its corollaries apply only to elements of finite order.

Classification of Subgroups of Cyclic Groups

The next theorem tells us how many subgroups a finite cyclic group has and how to find them.

Theorem 4.3 Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k}\rangle$.

Before we prove this theorem, let's see what it means. Understanding what a theorem means is a prerequisite to understanding its proof. Suppose $G = \langle a\rangle$ and G has order 30. The first and second parts of the theorem say that if H is any subgroup of G, then H has the form $\langle a^{30/k}\rangle$ for some k that is a divisor of 30. The third part of the theorem says that G has one subgroup of each of the orders 1, 2, 3, 5, 6, 10, 15, and 30—and no others. The proof will also show how to find these subgroups.

PROOF Let $G = \langle a\rangle$ and suppose that H is a subgroup of G. We must show that H is cyclic. If it consists of the identity alone, then clearly H is cyclic. So we may assume that $H \neq \{e\}$. We now claim that H contains

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

an element of the form a^t, where t is positive. Since $G = \langle a \rangle$, every element of H has the form a^t; and when a^t belongs to H with $t < 0$, then a^{-t} belongs to H also and $-t$ is positive. Thus, our claim is verified. Now let m be the least positive integer such that $a^m \in H$. By closure, $\langle a^m \rangle \subseteq H$. We next claim that $H = \langle a^m \rangle$. To prove this claim, it suffices to let b be an arbitrary member of H and show that b is in $\langle a^m \rangle$. Since $b \in G = \langle a \rangle$, we have $b = a^k$ for some k. Now, apply the division algorithm to k and m to obtain integers q and r such that $k = mq + r$ where $0 \leq r < m$. Then $a^k = a^{mq+r} = a^{mq}a^r$, so that $a^r = a^{-mq}a^k$. Since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q}$ is in H also, $a^r \in H$. But, m is the *least* positive integer such that $a^m \in H$, and $0 \leq r < m$, so r must be 0. Therefore, $b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$. This proves the assertion of the theorem that every subgroup of a cyclic group is cyclic.

To prove the next portion of the theorem, suppose that $|\langle a \rangle| = n$ and H is any subgroup of $\langle a \rangle$. We have already shown that $H = \langle a^m \rangle$, where m is the least positive integer such that $a^m \in H$. Using $e = b = a^n$ as in the preceding paragraph, we have $n = mq$.

Finally, let k be any positive divisor of n. We will show that $\langle a^{n/k} \rangle$ is the one and only subgroup of $\langle a \rangle$ of order k. From Theorem 4.2, we see that $\langle a^{n/k} \rangle$ has order $n/\gcd(n, n/k) = n/(n/k) = k$. Now let H be any subgroup of $\langle a \rangle$ of order k. We have already shown above that $H = \langle a^m \rangle$, where m is a divisor of n. Then $m = \gcd(n, m)$ and $k = |a^m| = |a^{\gcd(n,m)}| = n/\gcd(n, m) = n/m$. Thus, $m = n/k$ and $H = \langle a^{n/k} \rangle$.

Returning for a moment to our discussion of the cyclic group $\langle a \rangle$, where a has order 30, we may conclude from Theorem 4.3 that the subgroups of $\langle a \rangle$ are precisely those of the form $\langle a^m \rangle$, where m is a divisor of 30. Moreover, if k is a divisor of 30, the subgroup of order k is $\langle a^{30/k} \rangle$. So the list of subgroups of $\langle a \rangle$ is:

$$\begin{aligned}
\langle a \rangle &= \{e, a, a^2, \ldots, a^{29}\} && \text{order 30,}\\
\langle a^2 \rangle &= \{e, a^2, a^4, \ldots, a^{28}\} && \text{order 15,}\\
\langle a^3 \rangle &= \{e, a^3, a^6, \ldots, a^{27}\} && \text{order 10,}\\
\langle a^5 \rangle &= \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\} && \text{order 6,}\\
\langle a^6 \rangle &= \{e, a^6, a^{12}, a^{18}, a^{24}\} && \text{order 5,}\\
\langle a^{10} \rangle &= \{e, a^{10}, a^{20}\} && \text{order 3,}\\
\langle a^{15} \rangle &= \{e, a^{15}\} && \text{order 2,}\\
\langle a^{30} \rangle &= \{e\} && \text{order 1.}
\end{aligned}$$

In general, if $\langle a \rangle$ has order n and k divides n, then $\langle a^{n/k} \rangle$ is the unique subgroup of order k.

Taking the group in Theorem 4.3 to be Z_n and a to be 1, we obtain the following important special case.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Corollary Subgroups of Z_n

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.

EXAMPLE 5 The list of subgroups of Z_{30} is

$$\begin{aligned}
\langle 1 \rangle &= \{0, 1, 2, \ldots, 29\} && \text{order } 30,\\
\langle 2 \rangle &= \{0, 2, 4, \ldots, 28\} && \text{order } 15,\\
\langle 3 \rangle &= \{0, 3, 6, \ldots, 27\} && \text{order } 10,\\
\langle 5 \rangle &= \{0, 5, 10, 15, 20, 25\} && \text{order } 6,\\
\langle 6 \rangle &= \{0, 6, 12, 18, 24\} && \text{order } 5,\\
\langle 10 \rangle &= \{0, 10, 20\} && \text{order } 3,\\
\langle 15 \rangle &= \{0, 15\} && \text{order } 2,\\
\langle 30 \rangle &= \{0\} && \text{order } 1.
\end{aligned}$$

Theorems 4.2 and 4.3 provide a simple way to find all the generators of the subgroups of a finite cyclic group.

EXAMPLE 6 To find the generators of the subgroup of order 9 in Z_{36}, we observe that $36/9 = 4$ is one generator. To find the others, we have from Corollary 3 of Theorem 4.2 that they are all elements of Z_{36} of the form $4j$, where $\gcd(9, j) = 1$. Thus,

$$\langle 4 \cdot 1 \rangle = \langle 4 \cdot 2 \rangle = \langle 4 \cdot 4 \rangle = \langle 4 \cdot 5 \rangle = \langle 4 \cdot 7 \rangle = \langle 4 \cdot 8 \rangle.$$

In the generic case, to find all the subgroups of $\langle a \rangle$ of order 9 where $|a| = 36$, we have

$$\langle (a^4)^1 \rangle = \langle (a^4)^2 \rangle = \langle (a^4)^4 \rangle = \langle (a^4)^5 \rangle = \langle (a^4)^7 \rangle = \langle (a^4)^8 \rangle.$$

In particular, note that once you have the generator $a^{n/d}$ for the subgroup of order d where d is a divisor of $|a| = n$, all the generators of $\langle a^d \rangle$ have the form $(a^d)^j$ where $j \in U(d)$.

By combining Theorems 4.2 and 4.3, we can easily count the number of elements of each order in a finite cyclic group. For convenience, we introduce an important number-theoretic function called the *Euler phi function*. Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n. Notice that by definition of the group $U(n)$, $|U(n)| = \phi(n)$. The first 12 values of $\phi(n)$ are given in Table 4.1.

Table 4.1 Values of $\phi(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 4.4 Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

PROOF By Theorem 4.3, the group has exactly one subgroup of order d—call it $\langle a \rangle$. Then every element of order d also generates the subgroup $\langle a \rangle$ and, by Corollary 3 of Theorem 4.2, an element a^k generates $\langle a \rangle$ if and only if $\gcd(k, d) = 1$. The number of such elements is precisely $\phi(d)$.

Notice that for a finite cyclic group of order n, the number of elements of order d for any divisor d of n depends only on d. Thus, Z_8, Z_{640}, and Z_{80000} each have $\phi(8) = 4$ elements of order 8.

Although there is no formula for the number of elements of each order for arbitrary finite groups, we still can say something important in this regard.

Corollary Number of Elements of Order *d* in a Finite Group

In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

PROOF If a finite group has no elements of order d, the statement is true, since $\phi(d)$ divides 0. Now suppose that $a \in G$ and $|a| = d$. By Theorem 4.4, we know that $\langle a \rangle$ has $\phi(d)$ elements of order d. If all elements of order d in G are in $\langle a \rangle$, we are done. So, suppose that there is an element b in G of order d that is not in $\langle a \rangle$. Then, $\langle b \rangle$ also has $\phi(d)$ elements of order d. This means that we have found $2\phi(d)$ elements of order d in G provided that $\langle a \rangle$ and $\langle b \rangle$ have no elements of order d in common. If there is an element c of order d that belongs to both $\langle a \rangle$ and $\langle b \rangle$, then we have $\langle a \rangle = \langle c \rangle = \langle b \rangle$, so that $b \in \langle a \rangle$, which is a contradiction. Continuing in this fashion, we see that the number of elements of order d in a finite group is a multiple of $\phi(d)$.

On its face, the value of Theorem 4.4 and its corollary seem limited for large values of n, because it is tedious to determine the number of positive integers less than or equal to n and relatively prime to n by examining them one by one. However, the following properties of the ϕ function make computing $\phi(n)$ simple: For any prime p, $\phi(p^n) = p^n - p^{n-1}$ (see Exercise 85) and for relatively prime m and n, $\phi(mn) = \phi(m)\phi(n)$. Thus, $\phi(40) = \phi(8)\phi(5) = 4 \cdot 4 = 16$; $\phi(75) = \phi(5^2)\phi(3) = (25 - 5) \cdot 2 = 40$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The relationships among the various subgroups of a group can be illustrated with a *subgroup lattice* of the group. This is a diagram that includes all the subgroups of the group and connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if H is a proper subgroup of K. Although there are many ways to draw such a diagram, the connections between the subgroups must be the same. Typically, one attempts to present the diagram in an eye-pleasing fashion. The lattice diagram for Z_{30} is shown in Figure 4.2. Notice that $\langle 10 \rangle$ is a subgroup of both $\langle 2 \rangle$ and $\langle 5 \rangle$, but $\langle 6 \rangle$ is not a subgroup of $\langle 10 \rangle$.

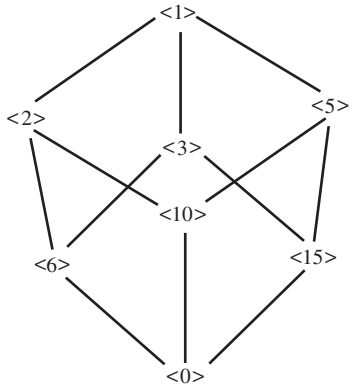


Figure 4.2 Subgroup lattice of Z_{30}.

The precision of Theorem 4.3 can be appreciated by comparing the ease with which we are able to identify the subgroups of Z_{30} with that of doing the same for, say, $U(30)$ or D_{30}. And these groups have relatively simple structures among noncyclic groups.

We will prove in Chapter 7 that a certain portion of Theorem 4.3 extends to arbitrary finite groups; namely, the order of a subgroup divides the order of the group itself. We will also see, however, that a finite group need not have exactly one subgroup corresponding to each divisor of the order of the group. For some divisors, there may be none at all, whereas for other divisors, there may be many. Indeed, D_4, the dihedral group of order 8, has five subgroups of order 2 and three of order 4.

One final remark about the importance of cyclic groups is appropriate. Although cyclic groups constitute a very narrow class of finite groups, we will see in Chapter 11 that they play the role of building blocks for all finite Abelian groups in much the same way that primes are the building blocks for the integers and that chemical elements are the building blocks for the chemical compounds.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Exercises

It is not unreasonable to use the hypothesis.

ARNOLD ROSS

1. Find all generators of Z_6, Z_8, and Z_{20}.
2. Suppose that $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are cyclic groups of orders 6, 8, and 20, respectively. Find all generators of $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$.
3. List the elements of the subgroups $\langle 20 \rangle$ and $\langle 10 \rangle$ in Z_{30}. Let a be a group element of order 30. List the elements of the subgroups $\langle a^{20} \rangle$ and $\langle a^{10} \rangle$.
4. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in Z_{18}. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3 \rangle$ and $\langle a^{15} \rangle$.
5. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 7 \rangle$ in $U(20)$.
6. What do Exercises 3, 4, and 5 have in common? Try to make a generalization that includes these three cases.
7. Find an example of a noncyclic group, all of whose proper subgroups are cyclic.
8. Let a be an element of a group and let $|a| = 15$. Compute the orders of the following elements of G.
   a. a^3, a^6, a^9, a^{12}
   b. a^5, a^{10}
   c. a^2, a^4, a^8, a^{14}
9. How many subgroups does Z_{20} have? List a generator for each of these subgroups. Suppose that $G = \langle a \rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of these subgroups.
10. In Z_{24}, list all generators for the subgroup of order 8. Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.
11. Let G be a group and let $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.
12. In Z, find all generators of the subgroup $\langle 3 \rangle$. If a has infinite order, find all generators of the subgroup $\langle a^3 \rangle$.
13. In Z_{24}, find a generator for $\langle 21 \rangle \cap \langle 10 \rangle$. Suppose that $|a| = 24$. Find a generator for $\langle a^{21} \rangle \cap \langle a^{10} \rangle$. In general, what is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?
14. Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is a prime?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

15. Let G be an Abelian group and let $H = \{g \in G \mid |g| \text{ divides } 12\}$. Prove that H is a subgroup of G. Is there anything special about 12 here? Would your proof be valid if 12 were replaced by some other positive integer? State the general result.

16. Find a collection of distinct subgroups $\langle a_1\rangle, \langle a_2\rangle, \ldots, \langle a_n\rangle$ of Z_{240} with the property that $\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle$ with n as large as possible.

17. Complete the following statement: $|a| = |a^2|$ if and only if $|a| \ldots$.

18. If a cyclic group has an element of infinite order, how many elements of finite order does it have?

19. List the cyclic subgroups of $U(30)$.

20. Suppose that G is an Abelian group of order 35 and every element of G satisfies the equation $x^{35} = e$. Prove that G is cyclic. Does your argument work if 35 is replaced with 33?

21. Let G be a group and let a be an element of G.
- **a.** If $a^{12} = e$, what can we say about the order of a?
- **b.** If $a^m = e$, what can we say about the order of a?
- **c.** Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a\rangle = G$.

22. Prove that a group of order 3 must be cyclic.

23. Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? Why? Describe all the subgroups of Z. Let a be a group element with infinite order. Describe all subgroups of $\langle a\rangle$.

24. For any element a in any group G, prove that $\langle a\rangle$ is a subgroup of $C(a)$ (the centralizer of a).

25. If d is a positive integer, $d \neq 2$, and d divides n, show that the number of elements of order d in D_n is $\phi(d)$. How many elements of order 2 does D_n have?

26. Find all generators of Z. Let a be a group element that has infinite order. Find all generators of $\langle a\rangle$.

27. Prove that C^*, the group of nonzero complex numbers under multiplication, has a cyclic subgroup of order n for every positive integer n.

28. Let a be a group element that has infinite order. Prove that $\langle a^i\rangle = \langle a^j\rangle$ if and only if $i = \pm j$.

29. List all the elements of order 8 in $Z_{8000000}$. How do you know your list is complete? Let a be a group element such that $|a| = 8000000$. List all elements of order 8 in $\langle a\rangle$. How do you know your list is complete?

30. Suppose a and b belong to a group, a has odd order, and $aba^{-1} = b^{-1}$. Show that $b^2 = e$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

31. Let G be a finite group. Show that there exists a fixed positive integer n such that $a^n = e$ for all a in G. (Note that n is independent of a.)

32. Determine the subgroup lattice for Z_{12}.

33. Determine the subgroup lattice for Z_{p^2q}, where p and q are distinct primes.

34. Determine the subgroup lattice for Z_8.

35. Determine the subgroup lattice for Z_{p^n}, where p is a prime and n is some positive integer.

36. Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

37. Show that the group of positive rational numbers under multiplication is not cyclic.

38. Consider the set $\{4, 8, 12, 16\}$. Show that this set is a group under multiplication modulo 20 by constructing its Cayley table. What is the identity element? Is the group cyclic? If so, find all of its generators.

39. Give an example of a group that has exactly 6 subgroups (including the trivial subgroup and the group itself). Generalize to exactly n subgroups for any positive integer n.

40. Let m and n be elements of the group Z. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

41. Suppose that a and b are group elements that commute and have orders m and n. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.

42. Suppose that a and b belong to a group G, a and b commute, and $|a|$ and $|b|$ are finite. What are the possibilities for $|ab|$?

43. Suppose that a and b belong to a group G, a and b commute, and $|a|$ and $|b|$ are finite. Prove that G has an element of order $\text{lcm}(|a|, |b|)$.

44. Let F and F' be distinct reflections in D_{21}. What are the possibilities for $|FF'|$?

45. Suppose that H is a subgroup of a group G and $|H| = 10$. If a belongs to G and a^6 belongs to H, what are the possibilities for $|a|$?

46. Which of the following numbers could be the exact number of elements of order 21 in a group: 21600, 21602, 21604?

47. If G is an infinite group, what can you say about the number of elements of order 8 in the group? Generalize.

48. Suppose that K is a proper subgroup of D_{35} and K contains at least two reflections. What are the possible orders of K? Explain your reasoning.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

49. For each positive integer n, prove that $\boldsymbol{C}^*$, the group of nonzero complex numbers under multiplication, has exactly $\phi(n)$ elements of order n.

50. Prove or disprove that $H = \{n \in Z \mid n \text{ is divisible by both 8 and 10}\}$ is a subgroup of Z.

51. Suppose that G is a finite group with the property that every nonidentity element has prime order (for example, D_3 and D_5). If $Z(G)$ is not trivial, prove that every nonidentity element of G has the same order.

52. Prove that an infinite group must have an infinite number of subgroups.

53. Let p be a prime. If a group has more than $p - 1$ elements of order p, why can't the group be cyclic?

54. Suppose that G is a cyclic group and that 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If a is one element of order 8, list the other elements of order 8.

55. List all the elements of Z_{40} that have order 10. Let $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.

56. Reformulate the corollary of Theorem 4.4 to include the case when the group has infinite order.

57. Determine the orders of the elements of D_{33} and how many there are of each.

58. If G is a cyclic group and 15 divides the order of G, determine the number of solutions in G of the equation $x^{15} = e$. If 20 divides the order of G, determine the number of solutions of $x^{20} = e$. Generalize.

59. If G is an Abelian group and contains cyclic subgroups of orders 4 and 5, what other sizes of cyclic subgroups must G contain? Generalize.

60. If G is an Abelian group and contains cyclic subgroups of orders 4 and 6, what other sizes of cyclic subgroups must G contain? Generalize.

61. Prove that no group can have exactly two elements of order 2.

62. Given the fact that $U(49)$ is cyclic and has 42 elements, deduce the number of generators that $U(49)$ has without actually finding any of the generators.

63. Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

64. Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

65. Let a and b belong to a group. If $|a| = 24$ and $|b| = 10$, what are the possibilities for $|\langle a\rangle \cap \langle b\rangle|$?

66. Prove that $U(2^n)$ $(n \geq 3)$ is not cyclic.

67. Suppose that G is a group of order 16 and that, by direct computation, you know that G has at least nine elements x such that $x^8 = e$. Can you conclude that G is not cyclic? What if G has at least five elements x such that $x^4 = e$? Generalize.

68. Prove that Z_n has an even number of generators if $n > 2$. What does this tell you about $\phi(n)$?

69. If $|a^5| = 12$, what are the possibilities for $|a|$? If $|a^4| = 12$, what are the possibilities for $|a|$?

70. Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r\rangle \subseteq \langle x^s\rangle$.

71. Suppose a is a group element such that $|a^{28}| = 10$ and $|a^{22}| = 20$. Determine $|a|$.

72. Let a be a group element such that $|a| = 48$. For each part, find a divisor k of 48 such that

a. $\langle a^{21}\rangle = \langle a^k\rangle$;

b. $\langle a^{14}\rangle = \langle a^k\rangle$;

c. $\langle a^{18}\rangle = \langle a^k\rangle$.

73. Let p be a prime. Show that in a cyclic group of order $p^n - 1$, every element is a pth power (that is, every element can be written in the form a^p for some a).

74. Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \;\middle|\; n \in Z \right\}$ is a cyclic subgroup of $GL(2, \mathbf{R})$.

75. Let a and b belong to a group. If $|a| = 12$, $|b| = 22$, and $\langle a\rangle \cap \langle b\rangle \neq \{e\}$, prove that $a^6 = b^{11}$.

76. (2008 GRE Practice Exam) If x is an element of a cyclic group of order 15 and exactly two of x^3, x^5, and x^9 are equal, determine $|x^{13}|$.

77. Determine the number of cyclic subgroups of order 4 in D_n.

78. If n is odd, prove that D_n has no subgroup of order 4.

79. If $n \geq 4$ and is even, show that D_n has exactly $n/2$ noncyclic subgroups of order 4.

80. If $n \geq 4$ and n is divisible by 2 but not by 4, prove that D_n has exactly $n/2$ subgroups of order 4.

81. How many subgroups of order n does D_n have?

82. Let G be the set of all polynomials of the form $ax^2 + bx + c$ with coefficients from the set $\{0, 1, 2\}$. We can make G a group under addition by adding the polynomials in the usual way, except that we use modulo 3 to combine the coefficients. With this operation, prove that G is a group of order 27 that is not cyclic.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

83. Let a and b belong to some group. Suppose that $|a| = m$, $|b| = n$, and m and n are relatively prime. If $a^k = b^k$ for some integer k, prove that mn divides k.

84. For every integer n greater than 2, prove that the group $U(n^2 - 1)$ is not cyclic.

85. Prove that for any prime p and positive integer n, $\phi(p^n) = p^n - p^{n-1}$.

86. Give an example of an infinite group that has exactly two elements of order 4.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

Suggested Reading

Deborah L. Massari, "The Probability of Generating a Cyclic Group," *Pi Mu Epsilon Journal* 7 (1979): 3–6.

In this easy-to-read paper, it is shown that the probability of a randomly chosen element from a cyclic group being a generator of the group depends only on the set of prime divisors of the order of the group, and not on the order itself. This article, written by an undergraduate student, received first prize in a Pi Mu Epsilon paper contest.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

James Joseph Sylvester

I really love my subject.

J. J. SYLVESTER

Stock Montage

JAMES JOSEPH SYLVESTER was the most influential mathematician in America in the 19th century. Sylvester was born on September 3, 1814, in London and showed his mathematical genius early. At the age of 14, he studied under De Morgan and won several prizes for his mathematics, and at the unusually young age of 25, he was elected a fellow of the Royal Society.

After receiving B.A. and M.A. degrees from Trinity College in Dublin in 1841, Sylvester began a professional life that was to include academics, law, and actuarial careers. In 1876, at the age of 62, he was appointed to a prestigious position at the newly founded Johns Hopkins University. During his seven years at Johns Hopkins, Sylvester pursued research in pure mathematics with tremendous vigor and enthusiasm. He also founded the *American Journal of Mathematics*, the first journal in America devoted to mathematical research. Sylvester returned to England in 1884 to a professorship at Oxford, a position he held until his death on March 15, 1897.

Sylvester's major contributions to mathematics were in the theory of equations, matrix theory, determinant theory, and invariant theory (which he founded with Cayley). His writings and lectures—flowery and eloquent, pervaded with poetic flights, emotional expressions, bizarre utterances, and paradoxes—reflected the personality of this sensitive, excitable, and enthusiastic man. We quote three of his students.[†] E. W. Davis commented on Sylvester's teaching methods.

> Sylvester's methods! He had none. "Three lectures will be delivered on a New Universal Algebra," he would say; then, "The course must be extended to twelve." It did last all the rest of that year. The following year the course was to be *Substitutions-Theorie*, by Netto. We all got the text. He lectured about three times, following the text closely and stopping sharp at the end of the hour. Then he began to think about matrices again. "I must give one lecture a week on those," he said. He could not confine himself to the hour, nor to the one lecture a week. Two weeks were passed, and Netto was forgotten entirely and never mentioned again. Statements like the following were not infrequent in his lectures: "I haven't proved this, but I am as sure as I can be of anything that it must be so. From this it will follow, etc." At the next lecture it turned out that what he was so sure of was false. Never mind, he kept on forever guessing and trying, and presently a wonderful discovery followed, then another and another. Afterward he would go back and work it all over again, and surprise us with all sorts of side lights. He then made another leap in the dark, more treasures were discovered, and so on forever.

[†]F. Cajori, *Teaching and History of Mathematics in the United States*, Washington: Government Printing Office, 1890, 265–266.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Sylvester's enthusiasm for teaching and his influence on his students are captured in the following passage written by Sylvester's first student at Johns Hopkins, G. B. Halsted.

> A short, broad man of tremendous vitality, . . . Sylvester's capacious head was ever lost in the highest cloud-lands of pure mathematics. Often in the dead of night he would get his favorite pupil, that he might communicate the very last product of his creative thought. Everything he saw suggested to him something new in the higher algebra. This transmutation of everything into new mathematics was a revelation to those who knew him intimately. They began to do it themselves.

Another characteristic of Sylvester, which is very unusual among mathematicians, was his apparent inability to remember mathematics! W. P. Durfee had the following to say.

> Sylvester had one remarkable peculiarity. He seldom remembered theorems, propositions, etc., but had always to deduce them when he wished to use them. In this he was the very antithesis of Cayley, who was thoroughly conversant with everything that had been done in every branch of mathematics.
>
> I remember once submitting to Sylvester some investigations that I had been engaged on, and he immediately denied my first statement, saying that such a proposition had never been heard of, let alone proved. To his astonishment, I showed him a paper of his own in which he had proved the proposition; in fact, I believe the object of his paper had been the very proof which was so strange to him.

For more information about Sylvester, visit:

http://www-groups.dcs.st-and.ac.uk/~history/

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Supplementary Exercises for Chapters 1–4

If you really want something in this life, you have to work for it. Now quiet, they're about to announce the lottery numbers!

HOMER SIMPSON

True/false questions for Chapters 1–4 are available on the Web at:

http://www.d.umn.edu/~jgallian/TF

1. Let G be a group and let H be a subgroup of G. For any fixed x in G, define $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Prove the following.
a. xHx^{-1} is a subgroup of G.
b. If H is cyclic, then xHx^{-1} is cyclic.
c. If H is Abelian, then xHx^{-1} is Abelian.
The group xHx^{-1} is called a *conjugate* of H. (Note that conjugation preserves structure.)

2. Let G be a group and let H be a subgroup of G. Define $N(H) = \{x \in G \mid xHx^{-1} = H\}$. Prove that $N(H)$ (called the *normalizer* of H) is a subgroup of G.[†]

3. Let G be a group. For each $a \in G$, define $\text{cl}(a) = \{xax^{-1} \mid x \in G\}$. Prove that these subsets of G partition G. [$\text{cl}(a)$ is called the *conjugacy class* of a.]

4. The group defined by the following table is called the *group of quaternions.* Use the table to determine each of the following.
a. The center
b. $\text{cl}(a)$
c. $\text{cl}(b)$
d. All cyclic subgroups

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

[†]This very important subgroup was first used by L. Sylow in 1872 to prove the existence of certain kinds of subgroups in a group. His work is discussed in Chapter 24.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

5. (Conjugation preserves order.) Prove that, in any group, $|xax^{-1}| = |a|$. (This exercise is referred to in Chapter 24.)

6. Prove that, in any group, $|ab| = |ba|$.

7. If a and b are group elements, prove that $|ab| = |a^{-1}b^{-1}|$.

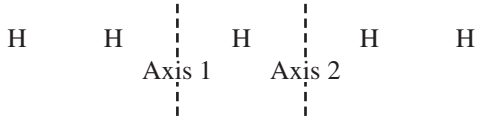
8. Prove that a group of order 4 cannot have a subgroup of order 3.

9. If a, b, and c are elements of a group, give an example to show that it need not be the case that $|abc| = |cba|$.

10. Let a and b belong to a group G. Prove that there is an element x in G such that $xax = b$ if and only if $ab = c^2$ for some element c in G.

11. Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.

12. Let G be the plane symmetry group of the infinite strip of equally spaced H's shown below.



Let x be the reflection about Axis 1 and let y be the reflection about Axis 2. Calculate $|x|$, $|y|$, and $|xy|$. Must the product of elements of finite order have finite order? (This exercise is referred to in Chapter 27.)

13. What are the orders of the elements of D_{15}? How many elements have each of these orders?

14. Prove that a group of order 4 is Abelian.

15. Prove that a group of order 5 must be cyclic.

16. Prove that an Abelian group of order 6 must be cyclic.

17. Let G be an Abelian group and let n be a fixed positive integer. Let $G^n = \{g^n \mid g \in G\}$. Prove that G^n is a subgroup of G. Give an example showing that G^n need not be a subgroup of G when G is non-Abelian. (This exercise is referred to in Chapter 11.)

18. Let $G = \{a + b\sqrt{2}\}$, where a and b are rational numbers not both 0. Prove that G is a group under ordinary multiplication.

19. (1969 Putnam Competition) Prove that no group is the union of two proper subgroups. Does the statement remain true if "two" is replaced by "three"?

20. Prove that the subset of elements of finite order in an Abelian group forms a subgroup. (This subgroup is called the *torsion subgroup.*) Is the same thing true for non-Abelian groups?

21. Let p be a prime and let G be an Abelian group. Show that the set of all elements whose orders are powers of p is a subgroup of G.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

22. Suppose that a and b are group elements. If $|b| = 2$ and $bab = a^4$, determine the possibilities for $|a|$.

23. Suppose that a finite group is generated by two elements a and b (that is, every element of the group can be expressed as some product of a's and b's). Given that $a^3 = b^2 = e$ and $ba^2 = ab$, construct the Cayley table for the group. We have already seen an example of a group that satisfies these conditions. Name it.

24. If a is an element from a group and $|a| = n$, prove that $C(a) = C(a^k)$ when k is relatively prime to n.

25. Let x and y belong to a group G. If $xy \in Z(G)$, prove that $xy = yx$.

26. Suppose that H and K are nontrivial subgroups of Q under addition. Show that $H \cap K$ is a nontrivial subgroup of Q. Is this true if Q is replaced by $\mathbf{R}$?

27. Let H be a subgroup of G and let g be an element of G. Prove that $N(gHg^{-1}) = gN(H)g^{-1}$. See Exercise 2 for the notation.

28. Let H be a subgroup of a group G and let $|g| = n$. If g^m belongs to H, and m and n are relatively prime, prove that g belongs to H.

29. Find a group that contains elements a and b such that $|a| = 2$, $|b| = 11$, and $|ab| = 2$.

30. Suppose that G is a group with exactly eight elements of order 10. How many cyclic subgroups of order 10 does G have?

31. (1989 Putnam Competition) Let S be a nonempty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a^n \mid n = 1, 2, 3, \ldots\}$ is finite. Must S be a group?

32. Let $H_1, H_2, H_3, \ldots$ be a sequence of subgroups of a group with the property that $H_1 \subseteq H_2 \subseteq H_3 \ldots$. Prove that the union of the sequence is a subgroup.

33. Let n be an integer greater than 1. Find a noncyclic subgroup of $U(4n)$ of order 4 that contains the element $2n - 1$.

34. Let G be an Abelian group and $H = \{x \in G \mid x^n = e$ for some odd integer n (n may vary with x)$\}$. Prove that H is a subgroup of G. Is H a subgroup if "odd" is replaced by "even"?

35. Let $H = \{A \in GL(2, \mathbf{R}) \mid \det A$ is rational$\}$. Prove or disprove that H is a subgroup of $GL(2, \mathbf{R})$. What if "rational" is replaced by "an integer"?

36. Suppose that G is a group that has exactly one nontrivial proper subgroup. Prove that G is cyclic and $|G| = p^2$, where p is prime.

37. Suppose that G is a group and G has exactly two nontrivial proper subgroups. Prove that G is cyclic and $|G| = pq$, where p and q are distinct primes, or that G is cyclic and $|G| = p^3$, where p is prime.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

38. If $|a^2| = |b^2|$, prove or disprove that $|a| = |b|$.

39. (1995 Putnam Competition) Let S be a set of real numbers that is closed under multiplication. Let T and U be disjoint subsets of S whose union is S. Given that the product of any three (not necessarily distinct) elements of T is in T and that the product of any three elements of U is in U, show that at least one of the two subsets T and U is closed under multiplication.

40. If p is an odd prime, prove that there is no group that has exactly p elements of order p.

41. Give an example of a group G with infinitely many distinct subgroups $H_1, H_2, H_3, \ldots$ such that $H_1 \subset H_2 \subset H_3 \ldots$.

42. Suppose a and b are group elements and $b \neq e$. If $a^{-1}ba = b^2$ and $|a| = 3$, find $|b|$. What is $|b|$, if $|a| = 5$? What can you say about $|b|$ in the case where $|a| = k$?

43. Let a and b belong to a group G. Show that there is an element g in G such that $g^{-1}abg = ba$.

44. Suppose G is a group and $x^3y^3 = y^3x^3$ for every x and y in G. Let $H = \{x \in G \mid |x| \text{ is relatively prime to } 3\}$. Prove that elements of H commute with each other and that H is a subgroup of G. Is your argument valid if 3 is replaced by an arbitrary positive integer n? Explain why or why not.

45. Let G be a finite group and let S be a subset of G that contains more than half of the elements of G. Show that every element of G can be expressed in the form s_1s_2 where s_1 and s_2 belong to S.

46. Let G be a group and let f be a function from G to some set. Show that $H = \{g \in G \mid f(xg) = f(x) \text{ for all } x \in G\}$ is a subgroup of G. In the case that G is the group of real numbers under addition and $f(x) = \sin x$, describe H.

47. Let G be a cyclic group of order n and let H be the subgroup of order d. Show that $H = \{x \in G \mid |x| \text{ divides } d\}$.

48. Let a be an element of maximum order from a finite Abelian group G. Prove that for any element b in G, $|b|$ divides $|a|$. Show by example that this need not be true for finite non-Abelian groups.

49. Define an operation $*$ on the set of integers by $a * b = a + b - 1$. Show that the set of integers under this operation is a cyclic group.

50. Let n be an integer greater than 1. Find a noncyclic subgroup of $U(4n)$ of order 4 that contains the element $2n - 1$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

5 Permutation Groups

Wigner's discovery about the electron permutation group was just the beginning. He and others found many similar applications and nowadays group theoretical methods—especially those involving characters and representations—pervade all branches of quantum mechanics.

GEORGE MACKEY, *Proceedings of the American Philosophical Society*

Definition and Notation

In this chapter, we study certain groups of functions, called permutation groups, from a set A to itself. In the early and mid-19th century, groups of permutations were the only groups investigated by mathematicians. It was not until around 1850 that the notion of an abstract group was introduced by Cayley, and it took another quarter century before the idea firmly took hold.

Definitions **Permutation of *A*, Permutation Group of *A***
A *permutation* of a set A is a function from A to A that is both one-to-one and onto. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

Although groups of permutations of any nonempty set A of objects exist, we will focus on the case where A is finite. Furthermore, it is customary, as well as convenient, to take A to be a set of the form $\{1, 2, 3, \ldots, n\}$ for some positive integer n. Unlike in calculus, where most functions are defined on infinite sets and are given by formulas, in algebra, permutations of finite sets are usually given by an explicit listing of each element of the domain and its corresponding functional value. For example, we define a permutation α of the set $\{1, 2, 3, 4\}$ by specifying

$$\alpha(1) = 2, \qquad \alpha(2) = 3, \qquad \alpha(3) = 1, \qquad \alpha(4) = 4.$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A more convenient way to express this correspondence is to write α in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Here $\alpha(j)$ is placed directly below j for each j. Similarly, the permutation β of the set $\{1, 2, 3, 4, 5, 6\}$ given by

$$\beta(1) = 5, \quad \beta(2) = 3, \quad \beta(3) = 1, \quad \beta(4) = 6, \quad \beta(5) = 2, \quad \beta(6) = 4$$

is expressed in array form as

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}.$$

Composition of permutations expressed in array notation is carried out from right to left by going from top to bottom, then again from top to bottom. For example, let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

and

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix};$$

then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

On the right we have 4 under 1, since $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$, so $\gamma\sigma$ sends 1 to 4. The remainder of the bottom row $\gamma\sigma$ is obtained in a similar fashion.

We are now ready to give some examples of permutation groups.

EXAMPLE 1 Symmetric Group S_3 Let S_3 denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself. Then S_3, under function composition, is a group with six elements. The six elements are

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \qquad \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \qquad \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \qquad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \qquad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

Note that $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta$, so that S_3 is non-Abelian. ∎

The relation $\beta\alpha = \alpha^2\beta$ can be used to compute other products in S_3 without resorting to the arrays. For example, $\beta\alpha^2 = (\beta\alpha)\alpha = (\alpha^2\beta)\alpha = \alpha^2(\beta\alpha) = \alpha^2(\alpha^2\beta) = \alpha^4\beta = \alpha\beta$.

Example 1 can be generalized as follows.

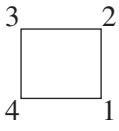
EXAMPLE 2 Symmetric Group S_n Let $A = \{1, 2, \ldots, n\}$. The set of all permutations of A is called the *symmetric group of degree n* and is denoted by S_n. Elements of S_n have the form

$$\alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}.$$

It is easy to compute the order of S_n. There are n choices of $\alpha(1)$. Once $\alpha(1)$ has been determined, there are $n - 1$ possibilities for $\alpha(2)$ [since α is one-to-one, we must have $\alpha(1) \neq \alpha(2)$]. After choosing $\alpha(2)$, there are exactly $n - 2$ possibilities for $\alpha(3)$. Continuing along in this fashion, we see that S_n has $n(n-1) \cdots 3 \cdot 2 \cdot 1 = n!$ elements. We leave it to the reader to prove that S_n is non-Abelian when $n \geq 3$ (Exercise 45). ∎

The symmetric groups are rich in subgroups. The group S_4 has 30 subgroups, and S_5 has well over 100 subgroups.

EXAMPLE 3 Symmetries of a Square As a third example, we associate each motion in D_4 with the permutation of the locations of each of the four corners of a square. For example, if we label the four corner positions as in the figure below and keep these labels fixed for reference, we may describe a 90° counterclockwise rotation by the permutation



$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix},$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

whereas a reflection across a horizontal axis yields

$$\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

These two elements generate the entire group (that is, every element is some combination of the ρ's and ϕ's).

When D_4 is represented in this way, we see that it is a subgroup of S_4. ∎

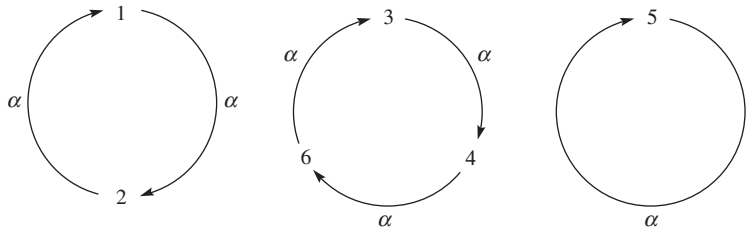
Cycle Notation

There is another notation commonly used to specify permutations. It is called *cycle notation* and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical advantages in that certain important properties of the permutation can be readily determined when cycle notation is used.

As an illustration of cycle notation, let us consider the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}.$$

This assignment of values could be presented schematically as follows.



Although mathematically satisfactory, such diagrams are cumbersome. Instead, we leave out the arrows and simply write $\alpha = (1, 2)(3, 4, 6)(5)$. As a second example, consider

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}.$$

In cycle notation, β can be written $(2, 3, 1, 5)(6, 4)$ or $(4, 6)(3, 1, 5, 2)$, since both of these unambiguously specify the function β. An expression of the form $(a_1, a_2, \ldots, a_m)$ is called a *cycle of length m* or an *m-cycle.*

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A multiplication of cycles can be introduced by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle. Thus, the cycle (4, 6) can be thought of as representing the permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{bmatrix}$. In this way, we can multiply cycles by thinking of them as permutations given in array form. Consider the following example from S_8. Let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. (When the domain consists of single-digit integers, it is common practice to omit the commas between the digits.) What is the cycle form of $\alpha\beta$? Of course, one could say that $\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$, but it is usually more desirable to express a permutation in a *disjoint* cycle form (that is, the various cycles have no number in common). Well, keeping in mind that function composition is done from right to left and that each cycle that does not contain a symbol fixes the symbol, we observe that (5) fixes 1; (648) fixes 1; (1237) sends 1 to 2; (8) fixes 2; (456) fixes 2; (27) sends 2 to 7; and (13) fixes 7. So the net effect of $\alpha\beta$ is to send 1 to 7. Thus, we begin $\alpha\beta = (17\cdots)\cdots$. Now, repeating the entire process beginning with 7, we have, cycle by cycle, right to left,

$$7 \to 7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3,$$

so that $\alpha\beta = (173\cdots)\cdots$. Ultimately, we have $\alpha\beta = (1732)(48)(56)$. The important thing to bear in mind when multiplying cycles is to "keep moving" from one cycle to the next from right to left. (*Warning:* Some authors compose cycles from left to right. When reading another text, be sure to determine which convention is being used.)

To be sure you understand how to switch from one notation to the other and how to multiply permutations, we will do one more example of each.

If array notations for α and β, respectively, are

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix},$$

then, in cycle notation, $\alpha = (12)(3)(45)$, $\beta = (153)(24)$, and $\alpha\beta = (12)(3)(45)(153)(24)$.

To put $\alpha\beta$ in disjoint cycle form, observe that (24) fixes 1; (153) sends 1 to 5; (45) sends 5 to 4; and (3) and (12) both fix 4. So, $\alpha\beta$ sends 1 to 4. Continuing in this way we obtain $\alpha\beta = (14)(253)$.

One can convert $\alpha\beta$ back to array form without converting each cycle of $\alpha\beta$ into array form by simply observing that (14) means 1 goes to 4 and 4 goes to 1; (253) means $2 \to 5$, $5 \to 3$, $3 \to 2$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

One final remark about cycle notation: Mathematicians prefer not to write cycles that have only one entry. In this case, it is understood that any missing element is mapped to itself. With this convention, the permutation α above can be written as (12)(45). Similarly,

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix}$$

can be written $\alpha = (134)$. Of course, the identity permutation consists only of cycles with one entry, so we cannot omit all of these! In this case, one usually writes just one cycle. For example,

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

can be written as $\varepsilon = (5)$ or $\varepsilon = (1)$. Just remember that missing elements are mapped to themselves.

Properties of Permutations

We are now ready to state several theorems about permutations and cycles. The proof of the first theorem is implicit in our discussion of writing permutations in cycle form.

Theorem 5.1 Products of Disjoint Cycles

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

PROOF Let α be a permutation on $A = \{1, 2, \ldots, n\}$. To write α in disjoint cycle form, we start by choosing any member of A, say a_1, and let

$$a_2 = \alpha(a_1), \qquad a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1),$$

and so on, until we arrive at $a_1 = \alpha^m(a_1)$ for some m. We know that such an m exists because the sequence $a_1, \alpha(a_1), \alpha^2(a_1), \ldots$ must be finite; so there must eventually be a repetition, say $\alpha^i(a_1) = \alpha^j(a_1)$ for some i and j with $i < j$. Then $a_1 = \alpha^m(a_1)$, where $m = j - i$. We express this relationship among $a_1, a_2, \ldots, a_m$ as

$$\alpha = (a_1, a_2, \ldots, a_m) \cdots .$$

The three dots at the end indicate the possibility that we may not have exhausted the set A in this process. In such a case, we merely choose any element b_1 of A not appearing in the first cycle and proceed to

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

create a new cycle as before. That is, we let $b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1)$, and so on, until we reach $b_1 = \alpha^k(b_1)$ for some k. This new cycle will have no elements in common with the previously constructed cycle. For, if so, then $\alpha^i(a_1) = \alpha^j(b_1)$ for some i and j. But then $\alpha^{i-j}(a_1) = b_1$, and therefore $b_1 = a_t$ for some t. This contradicts the way b_1 was chosen. Continuing this process until we run out of elements of A, our permutation will appear as

$$\alpha = (a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_k) \cdots (c_1, c_2, \ldots, c_s).$$

In this way, we see that every permutation can be written as a product of disjoint cycles. ∎

Theorem 5.2 Disjoint Cycles Commute

If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

PROOF For definiteness, let us say that α and β are permutations of the set

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\},$$

where the c's are the members of S left fixed by both α and β (there may not be any c's). To prove that $\alpha\beta = \beta\alpha$, we must show that $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all x in S. If x is one of the a elements, say a_i, then

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

since β fixes all a elements. (We interpret a_{i+1} as a_1 if $i = m$.) For the same reason,

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}.$$

Hence, the functions of $\alpha\beta$ and $\beta\alpha$ agree on the a elements. A similar argument shows that $\alpha\beta$ and $\beta\alpha$ agree on the b elements as well. Finally, suppose that x is a c element, say c_i. Then, since both α and β fix c elements, we have

$$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$$

and

$$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i.$$

This completes the proof. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In demonstrating how to multiply cycles, we showed that the product (13)(27)(456)(8)(1237)(648)(5) can be written in disjoint cycle form as (1732)(48)(56). Is economy in expression the only advantage to writing a permutation in disjoint cycle form? No. The next theorem shows that the disjoint cycle form has the enormous advantage of allowing us to "eyeball" the order of the permutation.

Theorem 5.3 Order of a Permutation (Ruffini, 1799)

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

PROOF First, observe that a cycle of length n has order n. (Verify this yourself.) Next, suppose that α and β are disjoint cycles of lengths m and n, and let k be the least common multiple of m and n. It follows from Theorem 4.1 that both α^k and β^k are the identity permutation ε and, since α and β commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus, we know by Corollary 2 to Theorem 4.1 ($a^k = e$ implies that $|a|$ divides k) that the order of $\alpha\beta$—let us call it t—must divide k. But then $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, so that $\alpha^t = \beta^{-t}$. However, it is clear that if α and β have no common symbol, the same is true for α^t and β^{-t}, since raising a cycle to a power does not introduce new symbols. But, if α^t and β^{-t} are equal and have no common symbol, they must both be the identity, because every symbol in α^t is fixed by β^{-t} and vice versa (remember that a symbol not appearing in a permutation is fixed by the permutation). It follows, then, that both m and n must divide t. This means that k, the least common multiple of m and n, divides t also. This shows that $k = t$.

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way. ∎

Theorem 5.3 is an enomously powerful tool for calculating the orders of permutations and the number of permutations of a particular order. We demonstrate this in the next two examples.

EXAMPLE 4 To determine the orders of the $7! = 5040$ elements of S_7, we need only consider the possible disjoint cycle structures of the elements of S_7. For convenience, we denote an n-cycle by $(\underline{n})$. Then, arranging all possible disjoint cycle structures of elements of S_7 according to longest cycle lengths left to right, we have

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

(7)
(6) (1)
(5) (2)
(5) (1) (1)
(4) (3)
(4) (2) (1)
(4) (1) (1) (1)
(3) (3) (1)
(3) (2) (2)
(3) (2) (1) (1)
(3) (1) (1) (1) (1)
(2) (2) (2) (1)
(2) (2) (1) (1) (1)
(2) (1) (1) (1) (1) (1)
(1) (1) (1) (1) (1) (1) (1).

Now, from Theorem 5.3 we see that the orders of the elements of S_7 are 7, 6, 10, 5, 12, 4, 3, 2, and 1. To do the same for the $10! = 3628800$ elements of S_{10} would be nearly as simple. ∎

∎ **EXAMPLE 5** We determine the number of elements of S_7 of order 3. By Theorem 5.3, we need only count the number of permutations of the forms $(a_1a_2a_3)$ and $(a_1a_2a_3)\,(a_4a_5a_6)$. In the first case consider the triple $a_1a_2a_3$. Clearly there are $7 \cdot 6 \cdot 5$ such triples. But this product counts the permutation $(a_1a_2a_3)$ three times (for example, it counts 134, 341, 413 as distinct triples whereas the cycles (134), (341), and (413) are the same group element). Thus, the number of permutations in S_7 for the form $(a_1a_2a_3)$ is $(7 \cdot 6 \cdot 5)/3 = 70$. For elements of S_7 of the form $(a_1a_2a_3)\,(a_4a_5a_6)$ there are $(7 \cdot 6 \cdot 5)/3$ ways to create the first cycle and $(4 \cdot 3 \cdot 2)/3$ to create the second cycle but the product of $(7 \cdot 6 \cdot 5)/3$ and $(4 \cdot 3 \cdot 2)/3$) counts $(a_1a_2a_3)\,(a_4a_5a_6)$ and $(a_4a_5a_6)(a_3a_2a_1)$ as distinct when they are equal group elements. Thus, the number of elements in S_7 for the form $(a_1a_2a_3)\,(a_4a_5a_6)$ is $(7 \cdot 6 \cdot 5)(4 \cdot 3 \cdot 2)/(3 \cdot 3 \cdot 2) = 280$. This gives us 350 elements of order 3 in S_7. ∎

As we will soon see, it is often greatly advantageous to write a permutation as a product of cycles of length 2—that is, as permutations of the form (ab) where $a \neq b$. Many authors call these permutations *transpositions*, since the effect of (ab) is to interchange or transpose a and b.

Example 6 and Theorem 5.4 show how this can always be done.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 6

$$(12345) = (15)(14)(13)(12)$$
$$(1632)(457) = (12)(13)(16)(47)(45)$$ ∎

Theorem 5.4 Product of 2-Cycles

Every permutation in S_n, $n > 1$, is a product of 2-cycles.

PROOF First, note that the identity can be expressed as (12)(12), and so it is a product of 2-cycles. By Theorem 5.1, we know that every permutation can be written in the form

$$(a_1a_2 \cdots a_k)(b_1b_2 \cdots b_t) \cdots (c_1c_2 \cdots c_s).$$

A direct computation shows that this is the same as

$$(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)(b_1b_t)(b_1b_{t-1}) \cdots (b_1b_2) \cdots (c_1c_s)(c_1c_{s-1}) \cdots (c_1c_2).$$

This completes the proof. ∎

The decomposition of a permutation into a product of 2-cycles given in Example 6 and in the proof of Theorem 5.4 is not the only way a permutation can be written as a product of 2-cycles. Although the next example shows that even the *number* of 2-cycles may vary from one decomposition to another, we will prove in Theorem 5.5 (first proved by Cauchy) that there is one aspect of a decomposition that never varies.

EXAMPLE 7

$$(12345) = (54)(53)(52)(51)$$
$$(12345) = (54)(52)(21)(25)(23)(13)$$ ∎

We isolate a special case of Theorem 5.5 as a lemma.

Lemma

If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where the β's are 2-cycles, then r is even.

PROOF Clearly, $r \neq 1$, since a 2-cycle is not the identity. If $r = 2$, we are done. So, we suppose that $r > 2$, and we proceed by induction.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Suppose that the rightmost 2-cycle is (ab). Then, since $(ij) = (ji)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right:

$$\begin{aligned} \varepsilon &= (ab)(ab), \\ (ab)(bc) &= (ac)(ab), \\ (ac)(cb) &= (bc)(ab), \\ (ab)(cd) &= (cd)(ab). \end{aligned}$$

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\varepsilon = \beta_1\beta_2 \cdots \beta_{r-2}$, and therefore, by the Second Principle of Mathematical Induction, $r - 2$ is even. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart on the left to obtain a new product of r 2-cycles that is still the identity, but where the rightmost occurrence of the integer a is in the second-from-the-rightmost 2-cycle of the product instead of the rightmost 2-cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r - 2)$ 2-cycles equal to the identity or a new product of r 2-cycles, where the rightmost occurrence of a is in the third 2-cycle from the right. Continuing this process, we must obtain a product of $(r - 2)$ 2-cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurrence of the integer a is in the leftmost 2-cycle, and such a product does not fix a, whereas the identity does. Hence, by the Second Principle of Mathematical Induction, $r - 2$ is even, and r is even as well. ∎

Theorem 5.5 Always Even or Always Odd

If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

$$\alpha = \beta_1\beta_2 \cdots \beta_r \qquad \textit{and} \qquad \alpha = \gamma_1\gamma_2 \cdots \gamma_s,$$

where the β's and the γ's are 2-cycles, then r and s are both even or both odd.

PROOF Observe that $\beta_1\beta_2 \cdots \beta_r = \gamma_1\gamma_2 \cdots \gamma_s$ implies

$$\begin{aligned} \varepsilon &= \gamma_1\gamma_2 \cdots \gamma_s\beta_r^{-1} \cdots \beta_2^{-1}\beta_1^{-1} \\ &= \gamma_1\gamma_2 \cdots \gamma_s\beta_r \cdots \beta_2\beta_1, \end{aligned}$$

since a 2-cycle is its own inverse. Thus, the lemma on page 108 guarantees that $s + r$ is even. It follows that r and s are both even or both odd. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Definition **Even and Odd Permutations**
A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

Theorems 5.4 and 5.5 together show that every permutation can be unambiguously classified as either even or odd. The significance of this observation is given in Theorem 5.6.

Theorem 5.6 Even Permutations Form a Group

The set of even permutations in S_n forms a subgroup of S_n.

PROOF This proof is left to the reader (Exercise 17). ∎

The subgroup of even permutations in S_n arises so often that we give it a special name and notation.

Definition **Alternating Group of Degree *n***
The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree n*.

The next result shows that exactly half of the elements of $S_n (n > 1)$ are even permutations.

Theorem 5.7

For $n > 1$, A_n has order $n!/2$.

PROOF For each odd permutation α, the permutation $(12)\alpha$ is even and, by the cancellation property in groups, $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many even permutations as there are odd ones. On the other hand, for each even permutation α, the permutation $(12)\alpha$ is odd and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many odd permutations as there are even ones. It follows that there are equal numbers of even and odd permutations. Since $|S_n| = n!$, we have $|A_n| = n!/2$. ∎

The names for the symmetric group and the alternating group of degree n come from the study of polynomials over n variables. A *symmetric* polynomial in the variables $x_1, x_2, \ldots, x_n$ is one that is unchanged under any transposition of two of the variables. An *alternating* polynomial is one that changes signs under any transposition of two of the variables. For

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

example, the polynomial $x_1x_2x_3$ is unchanged by any transposition of two of the three variables, whereas the polynomial $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ changes signs when any two of the variables are transposed. Since every member of the symmetric group is the product of transpositions, the symmetric polynomials are those that are unchanged by members of the symmetric group. Likewise, since any member of the alternating group is the product of an even number of transpositions, the alternating polynomials are those that are unchanged by members of the alternating group.

The alternating groups are among the most important examples of groups. The groups A_4 and A_5 will arise on several occasions in later chapters. In particular, A_5 has great historical significance.

A geometric interpretation of A_4 is given in Example 8, and a multiplication table for A_4 is given as Table 5.1.

EXAMPLE 8 Rotations of a Tetrahedron

The 12 rotations of a regular tetrahedron can be conveniently described with the elements of A_4. The top row of Figure 5.1 illustrates the identity and three 180° "edge" rotations about axes joining midpoints of two edges. The second row consists of 120° "face" rotations about axes joining a vertex to the center of the opposite face. The third row consists of −120° (or 240°) "face" rotations. Notice that the four rotations in the second row can be obtained from those in the first row by left-multiplying the four in the first row by the rotation (123), whereas those in the third row can be obtained from those in the first row by left-multiplying the ones in the first row by (132). ∎

Table 5.1 The Alternating Group A_4 of Even Permutations of {1, 2, 3, 4}

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3\,\alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

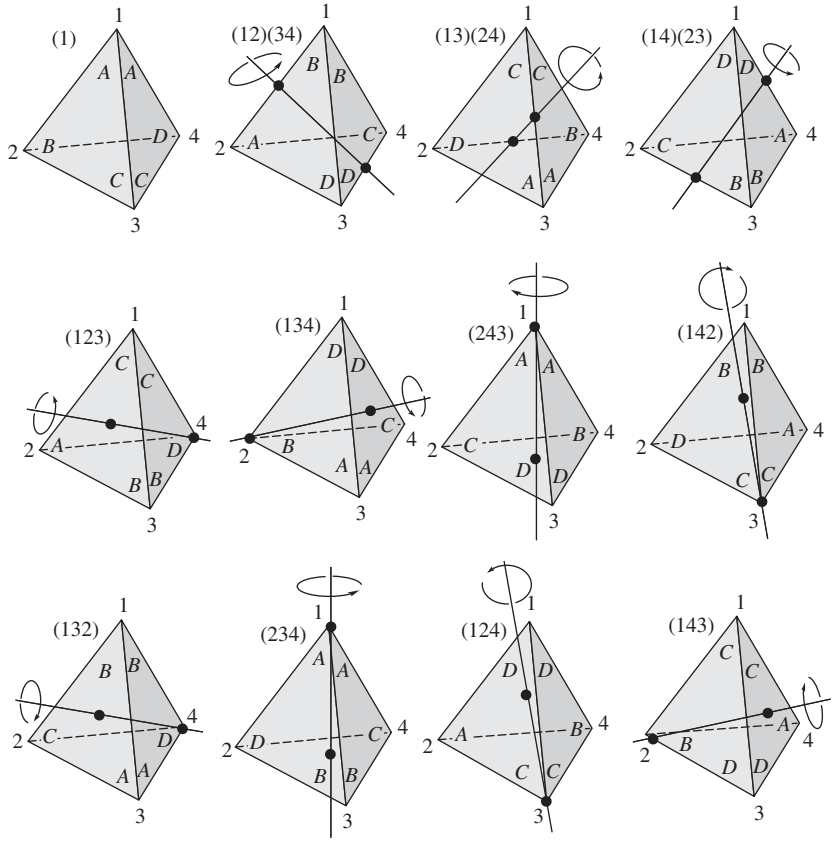


Figure 5.1 Rotations of a regular tetrahedron.

Many molecules with chemical formulas of the form AB_4, such as methane (CH_4) and carbon tetrachloride (CCl_4), have A_4 as their symmetry group. Figure 5.2 shows the form of one such molecule.

Many games and puzzles can be analyzed using permutations.

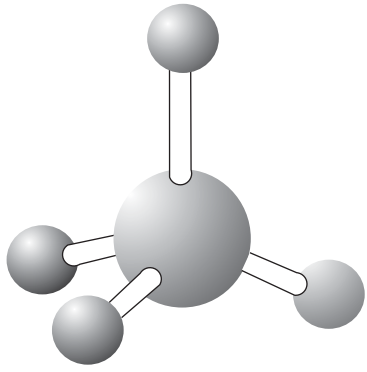
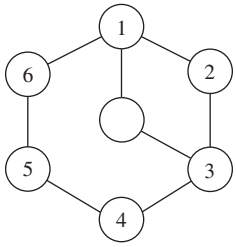


Figure 5.2 A tetrahedral AB_4 molecule.

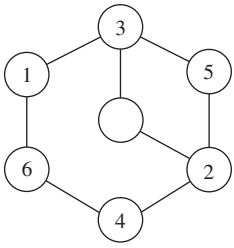
Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 9 (Loren Larson) A Sliding Disk Puzzle

Consider the puzzle shown below (the space in the middle is empty).



By sliding disks from one position to another along the lines indicated without lifting or jumping them, can we obtain the following arrangement?



To answer this question, we view the positions as numbered in the first figure above and consider two basic operations. Let r denote the following operation: Move the disk in position 1 to the center position, then move the disk in position 6 to position 1, the disk in position 5 to position 6, the disk in position 4 to position 5, the disk in position 3 to position 4, then the disk in the middle position to position 3. Let s denote the operation: Move the disk in position 1 to the center position, then move the disk in position 2 to position 1, then move the disk in position 3 to position 2, and finally move the disk in the center to position 3. In permutation notation, we have $r = (13456)$ and $s = (132)$. The permutation for the arrangement we seek is (16523). Clearly, if we can express (16523) as a string of r's and s's, we can achieve the desired arangement. Rather than attempt to find an appropriate combination of r's and s's by hand, it is easier to employ computer software that is designed for this kind of problem. One such software program is GAP (see Suggested Software at the end of this chapter). With GAP, all we need to do is use the following commands:

gap> $G :=$ SymmetricGroup(6);
gap> $r :=$ (1,3,4,5,6); $s :=$ (1, 3, 2);
gap> $K :=$ Subgroup(G,[r,s]);
gap> Factorization(K,(1,6,5,2,3));

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The first three lines inform the computer that our group is the subgroup of S_6 generated by $r = (13456)$ and $s = (132)$. The fourth line requests that (16523) be expressed in terms of r and s. If we include the command

$$\text{gap}> \text{Size } (K)$$

we would find that the order of the subgroup generated by r and s is 360. Then, observing that r and s are even permutations and that $|A_6| = 360$, we deduce that r and s can achieve any arrangement that corresponds to an even permutation. ∎

Rubik's Cube

The Rubik's Cube made from 48 cubes called "facets" is the quintessential example of a group theory puzzle. It was invented in 1974 by the Hungarian Erről Rubik. By 2009 more than 350 million Rubik's Cubes had been sold. The current record time for solving it is under 7 seconds; under 31 seconds blindfolded. Although it was proved in 1995 that there was a starting configuration that required at least 20 moves to solve, it was not until 2010 that it was determined that every cube could be solved in at most 20 moves. This computer calculation utilized about 35 CPU-years donated by Google to complete. In early discussions about the minimum number of moves to solve the cube in the worst possible case, someone called it "God's number," and the name stuck. A history of the quest to find God's number is given at the website at **http://www.cube20.org/**.

The set of all configuration of the Rubik's Cube form a group of permutations of order 43,252,003,274,489,856,00. This order can be computed using GAP by labeling the faces of the cube as shown here.

			1	2	3						
			4	top	5						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	left	13	20	front	21	28	right	29	36	rear	37
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	bottom	45						
			46	47	48						

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The group of permutations of the cube is generated by the following rotations of the six layers.

top = (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)
left = (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)
front = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)
right = (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)
rear = (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)
bottom = (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)
(16,24,32,40)

A Check-Digit Scheme Based on D_5

In Chapter 0, we presented several schemes for appending a check digit to an identification number. Among these schemes, only the International Standard Book Number method was capable of detecting all single-digit errors and all transposition errors involving adjacent digits. However, recall that this success was achieved by introducing the alphabetical character X to handle the case where 10 was required to make the dot product 0 modulo 11.

In contrast, in 1969, J. Verhoeff [2] devised a method utilizing the dihedral group of order 10 that detects all single-digit errors and all transposition errors involving adjacent digits without the necessity of avoiding certain numbers or introducing a new character. To describe this method, consider the permutation $\sigma = (01589427)(36)$ and the dihedral group of order 10 as represented in Table 5.2. (Here we use 0 through 4 for the rotations, 5 through 9 for the reflections, and $*$ for the operation of D_5.)

Table 5.2 Multiplication for D_5

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Verhoeff's idea was to view the digits 0 through 9 as the elements of the group D_5 and to replace ordinary addition with calculations done in D_5. In particular, to any string of digits $a_1a_2 \ldots a_{n-1}$, we append the check digit a_n so that $\sigma(a_1) * \sigma^2(a_2) * \cdots * \sigma^{n-2}(a_{n-2}) * \sigma^{n-1}(a_{n-1}) * \sigma^n(a_n) = 0$. [Here $\sigma^2(x) = \sigma(\sigma(x))$, $\sigma^3(x) = \sigma(\sigma^2(x))$, and so on.] Since σ has the property that $\sigma^i(a) \neq \sigma^i(b)$ if $a \neq b$, all single-digit errors are detected. Also, because

$$a * \sigma(b) \neq b * \sigma(a) \qquad \text{if } a \neq b, \tag{1}$$

as can be checked on a case-by-case basis (see Exercise 67), it follows that all transposition errors involving adjacent digits are detected [since Equation (1) implies that $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ if $a \neq b$].

From 1990 until 2002, the German government used a minor modification of Verhoeff's check-digit scheme to append a check digit to the serial numbers on German banknotes. Table 5.3 gives the values of the functions $\sigma, \sigma^2, \ldots, \sigma^{10}$ needed for the computations. [The functional value $\sigma^i(j)$ appears in the row labeled with σ^i and the column labeled j.] Since the serial numbers on the banknotes use 10 letters of the alphabet in addition to the 10 decimal digits, it is necessary to assign numerical values to the letters to compute the check digit. This assignment is shown in Table 5.4.

Table 5.3 Powers of σ

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$\boldsymbol{\sigma}$	1	5	7	6	2	8	3	0	9	4
$\boldsymbol{\sigma^2}$	5	8	0	3	7	9	6	1	4	2
$\boldsymbol{\sigma^3}$	8	9	1	6	0	4	3	5	2	7
$\boldsymbol{\sigma^4}$	9	4	5	3	1	2	6	8	7	0
$\boldsymbol{\sigma^5}$	4	2	8	6	5	7	3	9	0	1
$\boldsymbol{\sigma^6}$	2	7	9	3	8	0	6	4	1	5
$\boldsymbol{\sigma^7}$	7	0	4	6	9	1	3	2	5	8
$\boldsymbol{\sigma^8}$	0	1	2	3	4	5	6	7	8	9
$\boldsymbol{\sigma^9}$	1	5	7	6	2	8	3	0	9	4
$\boldsymbol{\sigma^{10}}$	5	8	0	3	7	9	6	1	4	2

Table 5.4 Letter Values

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

To any string of digits $a_1a_2 \ldots a_{10}$ corresponding to a banknote serial number, the check digit a_{11} is chosen such that $\sigma(a_1) * \sigma^2(a_2) * \cdots * \sigma^9(a_9) * \sigma^{10}(a_{10}) * a_{11} = 0$ [instead of $\sigma(a_1) * \sigma^2(a_2) * \cdots * \sigma^{10}(a_{10}) * \sigma^{11}(a_{11}) = 0$ as in the Verhoeff scheme].

To trace through a specific example, consider the banknote (featuring the mathematician Gauss) shown in Figure 5.3 with the number AG8536827U7. To verify that 7 is the appropriate check digit, we observe that $\sigma(0) * \sigma^2(2) * \sigma^3(8) * \sigma^4(5) * \sigma^5(3) * \sigma^6(6) * \sigma^7(8) * \sigma^8(2) * \sigma^9(7) * \sigma^{10}(7) * 7 = 1 * 0 * 2 * 2 * 6 * 6 * 5 * 2 * 0 * 1 * 7 = 0$, as it should be. [To illustrate how to use the multiplication table for D_5, we compute $1 * 0 * 2 * 2 = (1 * 0) * 2 * 2 = 1 * 2 * 2 = (1 * 2) * 2 = 3 * 2 = 0$.]

Figure 5.3 German banknote with serial number AG8536827U and check digit 7.

One shortcoming of the German banknote scheme is that it does not distinguish between a letter and its assigned numerical value. Thus, a substitution of 7 for U (or vice versa) and the transposition of 7 and U are not detected by the check digit. Moreover, the banknote scheme does not detect all transpositions of adjacent characters involving the check digit itself. For example, the transposition of D and 8 in positions 10 and 11 is not detected. Both of these defects can be avoided by using the Verhoeff method with D_{18}, the dihedral group of order 36, to assign every letter and digit a distinct value together with an appropriate function σ [1]. Using this method to append a check character, all single-position errors and all transposition errors involving adjacent digits will be detected.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Exercises

When you feel how depressingly
slowly you climb,
it's well to remember that
Things Take Time.

PIET HEIN, "T. T. T.," *Grooks (1966)*†*

1. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$

Compute each of the following.

a. α^{-1}

b. $\beta\alpha$

c. $\alpha\beta$

2. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \text{and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

Write α, β, and $\alpha\beta$ as

a. products of disjoint cycles;

b. products of 2-cycles.

3. Write each of the following permutations as a product of disjoint cycles.

a. (1235)(413)

b. (13256)(23)(46512)

c. (12)(13)(23)(142)

4. Find the order of each of the following permutations.

a. (14)

b. (147)

c. (14762)

d. $(a_1 a_2 \cdots a_k)$

5. What is the order of each of the following permutations?

a. (124)(357)

b. (124)(3567)

c. (124)(35)

d. (124)(357869)

e. (1235)(24567)

f. (345)(245)

†Hein is a Danish engineer and poet and is the inventor of the game *Hex*.

*Piet Hein, "T.T.T.," Grooks (1966) Copyright © Piet Hein Grooks. Reprinted with kind permission from Piet Hein a/s, DK-5500 Middelfart, Denmark.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

6. What is the order of each of the following permutations?

a. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$

b. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$

7. What is the order of the product of a pair of disjoint cycles of lengths 4 and 6?

8. Show that A_8 contains an element of order 15.

9. What are the possible orders for the elements of S_6 and A_6? What about A_7? (This exercise is referred to in Chapter 25.)

10. What is the maximum order of any element in A_{10}?

11. Determine whether the following permutations are even or odd.

a. (135)

b. (1356)

c. (13567)

d. (12)(134)(152)

e. (1243)(3521)

12. Show that a function from a finite set S to itself is one-to-one if and only if it is onto. Is this true when S is infinite? (This exercise is referred to in Chapter 6.)

13. Suppose that α is a mapping from a set S to itself and $\alpha(\alpha(x)) = x$ for all x in S. Prove that α is one-to-one and onto.

14. Find eight elements in S_6 that commute with (12)(34)(56). Do they form a subgroup of S_6?

15. Let n be a positive integer. If n is odd, is an n-cycle an odd or an even permutation? If n is even, is an n-cycle an odd or an even permutation?

16. If α is even, prove that α^{-1} is even. If α is odd, prove that α^{-1} is odd.

17. Prove Theorem 5.6.

18. In S_n, let α be an r-cycle, β an s-cycle, and γ a t-cycle. Complete the following statements: $\alpha\beta$ is even if and only if $r + s$ is . . . ; $\alpha\beta\gamma$ is even if and only if $r + s + t$ is . . . .

19. Let α and β belong to S_n. Prove that $\alpha\beta$ is even if and only if α and β are both even or both odd.

20. Associate an even permutation with the number $+1$ and an odd permutation with the number -1. Draw an analogy between the result of multiplying two permutations and the result of multiplying their corresponding numbers $+1$ or -1.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

21. Let σ be the permutation of the letters A through Z that takes each letter to the one directly below it in the display following. Write σ in cycle form.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
H D B G J E C M I L O N P F K R U S A W Q T V Z X Y

22. If α and β are distinct 2-cycles, what are the possibilities for $|\alpha\beta|$?

23. Show that if H is a subgroup of S_n, then either every member of H is an even permutation or exactly half of the members are even. (This exercise is referred to in Chapter 25.)

24. Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n.

25. Give two reasons why the set of odd permutations in S_n is not a subgroup.

26. Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

27. Use Table 5.1 to compute the following.
a. The centralizer of $\alpha_3 = (13)(24)$
b. The centralizer of $\alpha_{12} = (124)$

28. How many elements of order 5 are in S_7?

29. How many elements of order 4 does S_6 have? How many elements of order 2 does S_6 have?

30. Prove that (1234) is not the product of 3-cycles.

31. Let $\beta \in S_7$ and suppose $\beta^4 = (2143567)$. Find β. What are the possibilities for β if $\beta \in S_9$?

32. Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.

33. Find three elements σ in S_9 with the property that $\sigma^3 = (157)(283)(469)$.

34. What cycle is $(a_1 a_2 \cdots a_n)^{-1}$?

35. Let G be a group of permutations on a set X. Let $a \in X$ and define $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$. We call $\text{stab}(a)$ the *stabilizer of a in G* (since it consists of all members of G that leave a fixed). Prove that $\text{stab}(a)$ is a subgroup of G. (This subgroup was introduced by Galois in 1832.) This exercise is referred to in Chapter 7.

36. Let $\beta = (1,3,5,7,9,8,6)(2,4,10)$. What is the smallest positive integer n for which $\beta^n = \beta^{-5}$?

37. Let $\alpha = (1,3,5,7,9)(2,4,6)(8,10)$. If α^m is a 5-cycle, what can you say about m?

38. Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. How many elements are in H? Is your argument valid when S_5 is replaced by S_n for $n \geq 3$? How many elements are in H when S_5 is replaced by A_n for $n \geq 4$?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

39. How many elements of order 5 are there in A_6?

40. In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.

41. Suppose that β is a 10-cycle. For which integers i between 2 and 10 is β^i also a 10-cycle?

42. In S_3, find elements α and β such that $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

43. Find group elements α and β in S_5 such that $|\alpha| = 3$, $|\beta| = 3$, and $|\alpha\beta| = 5$.

44. Represent the symmetry group of an equilateral triangle as a group of permutations of its vertices (see Example 3).

45. Prove that S_n is non-Abelian for all $n \geq 3$.

46. Prove that A_n is non-Abelian for all $n \geq 4$.

47. For $n \geq 3$, let $H = \{\beta \in S_n \mid \beta(1) = 1 \text{ or } 2 \text{ and } \beta(2) = 1 \text{ or } 2\}$. Prove that H is a subgroup of S_n. Determine $|H|$.

48. Show that in S_7, the equation $x^2 = (1234)$ has no solutions but the equation $x^3 = (1234)$ has at least two.

49. If (ab) and (cd) are distinct 2-cycles in S_n, prove that (ab) and (cd) commute if and only if they are disjoint.

50. Let α be a 2-cycle and β be a t-cycle in S_n. Prove that $\alpha\beta\alpha$ is a t-cycle.

51. Use the previous exercise to prove that, if α and β belong to S_n and β is the product of k-cycles of lengths $n_1, n_2, \ldots, n_k$, then $\alpha\beta\alpha^{-1}$ is the product of k-cycles of lengths $n_1, n_2, \ldots n_k$.

52. Let α and β belong to S_n. Prove that $\beta\alpha\beta^{-1}$ and α are both even or both odd.

53. What is the smallest positive integer n such that S_n has an element of order greater than $2n$?

54. Let n be an even positive integer. Prove that A_n has an element of order greater than n if and only if $n \geq 8$.

55. Let n be an odd positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 13$.

56. Let n be an even positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 14$.

57. Viewing the members of D_4 as a group of permutations of a square labeled 1, 2, 3, 4 as described in Example 3, which geometric symmetries correspond to even permutations?

58. Viewing the members of D_5 as a group of permutations of a regular pentagon with consecutive vertices labeled 1, 2, 3, 4, 5, what geometric symmetry corresponds to the permutation (14253)? Which symmetry corresponds to the permutation (25)(34)?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

59. Let n be an odd integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled 1, 2, . . . , n, explain why the rotation subgroup of D_n is a subgroup of A_n.

60. Let n be an integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled 1, 2, . . . , n, determine for which n all the permutations corresponding to reflections in D_n are even permutations. Hint: Consider the fours cases for n mod 4.

61. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2. (This exercise is referred to in Chapter 25.)

62. Find a cyclic subgroup of A_8 that has order 4.

63. Find a noncyclic subgroup of A_8 that has order 4.

64. Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?

65. Show that every element in A_n for $n \geq 3$ can be expressed as a 3-cycle or a product of 3-cycle.

66. Show that for $n \geq 3$, $Z(S_n) = \{\varepsilon\}$.

67. Verify the statement made in the discussion of the Verhoeff check digit scheme based on D_5 that $a * \sigma(b) \neq b * \sigma(a)$ for distinct a and b. Use this to prove that $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ for all i. Prove that this implies that all transposition errors involving adjacent digits are detected.

68. Use the Verhoeff check-digit scheme based on D_5 to append a check digit to 45723.

69. Prove that every element of S_n $(n > 1)$ can be written as a product of elements of the form $(1k)$.

70. (Indiana College Mathematics Competition) A card-shuffling machine always rearranges cards in the same way relative to the order in which they were given to it. All of the hearts arranged in order from ace to king were put into the machine, and then the shuffled cards were put into the machine again to be shuffled. If the cards emerged in the order 10, 9, Q, 8, K, 3, 4, A, 5, J, 6, 2, 7, in what order were the cards after the first shuffle?

71. Show that a permutation with odd order must be an even permutation.

72. Let G be a group. Prove or disprove that $H = \{g^2 \mid g \in G\}$ is a subgroup of G. (Compare with Example 5 in Chapter 3.)

73. Let $H = \{\alpha^2 \mid \alpha \in S_4\}$ and $K = \{\alpha^2 \mid \alpha \in S_5\}$. Prove $H = A_4$ and $K = A_5$.

74. Let $H = \{\alpha^2 \mid \alpha \in S_6\}$. Prove $H \neq A_6$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

75. Determine integers n for which $H = \{\alpha \in A_n \mid \alpha^2 = \varepsilon\}$ is a subgroup of A_n.

76. Given that β and γ are in S_4 with $\beta\gamma = (1432)$, $\gamma\beta = (1243)$, and $\beta(1) = 4$, determine β and γ.

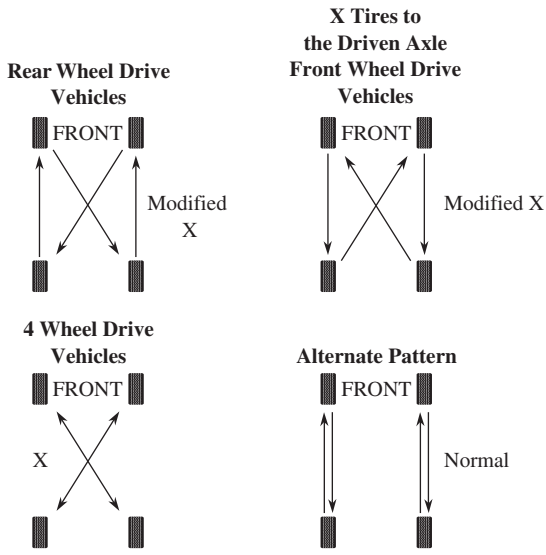
77. Why does the fact that the orders of the elements of A_4 are 1, 2, and 3 imply that $|Z(A_4)| = 1$?

78. Find five subgroups of S_5 of order 24.

79. Find six subgroups of order 60 in S_6.

80. For $n > 1$, let H be the set of all permutations in S_n that can be expressed as a product of a multiple of four transpositions. Show that $H = A_n$.

81. Shown below are four tire rotation patterns recommended by the Dunlop Tire Company. Explain how these patterns can be represented as permutations in S_4 and find the smallest subgroup of S_4 that contains these four patterns. Is the subgroup Abelian?



82. Label the four locations of tires on an automobile with the labels 1, 2, 3, and 4, clockwise. Let a represent the operation of switching the tires in positions 1 and 3 and switching the tires in positions 2 and 4. Let b represent the operation of rotating the tires in positions 2, 3, and 4 clockwise and leaving the tire in position 1 as is. Let G be the group of all possible combinations of a and b. How many elements are in G?

83. What would be wrong with using the 2-cycle notation (11) instead of the 1-cycle (1) to indicate that a cycle sends 1 to 1?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

References

1. J. A. Gallian, "The Mathematics of Identification Numbers," *The College Mathematics Journal* 22 (1991): 194–202.
2. J. Verhoeff, *Error Detecting Decimal Codes,* Amsterdam: Mathematisch Centrum, 1969.

Suggested Readings

Douglas E. Ensley, "Invariants Under Actions to Amaze Your Friends," *Mathematics Magazine,* Dec. 1999: 383–387.

This article explains some card tricks that are based on permutation groups.

Dmitry Fomin, "Getting It Together with 'Polyominoes,'" *Quantum,* Nov./Dec. 1991: 20–23.

In this article, permutation groups are used to analyze various sorts of checkerboard tiling problems.

J. A. Gallian, "Error Detection Methods," *ACM Computing Surveys* 28 (1996): 504–517.

This article gives a comprehensive survey of error-detection methods that use check digits. This article can be downloaded at **http://www.d.umn.edu/~jgallian/detection.pdf**

I. N. Herstein and I. Kaplansky, *Matters Mathematical,* New York: Chelsea, 1978.

Chapter 3 of this book discusses several interesting applications of permutations to games.

Douglas Hofstadter, "The Magic Cube's Cubies Are Twiddled by Cubists and Solved by Cubemeisters," *Scientific American* 244 (1981): 20–39.

This article, written by a Pulitzer Prize recipient, discusses the group theory involved in the solution of the Magic (Rubik's) Cube. In particular, permutation groups, subgroups, conjugates (elements of the form xyx^{-1}), commutators (elements of the form $xyx^{-1}y^{-1}$), and the "always even or always odd" theorem (Theorem 5.5) are prominently mentioned. At one point, Hofstadter says, "It is this kind of marvelously concrete illustration of an abstract notion of group theory that makes the Magic Cube one of the most amazing things ever invented for teaching mathematical ideas."

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

John O. Kiltinen, *Oval Track & Other Permutation Puzzles & Just Enough Group Theory to Solve Them*, Washington, D.C.: Mathematical Association of America, 2003.

This book and the software that comes with it present the user with an array of computerized puzzles, plus tools to vary them in thousands of ways. The book provides the background needed to use the puzzle software to its fullest potential, and also gives the reader a gentle, not-too-technical introduction to the theory of permutation groups that is a prerequisite to a full understanding of how to solve puzzles of this type. The website **http://www-instruct.nmu.edu/math_cs/kiltinen/web/mathpuzzles/** provides resources that expand upon the book. It also has news about puzzle software—modules that add functionality and fun to puzzles.

Vladimir Dubrovsky, "Portrait of Three Puzzle Graces," *Quantum,* Nov./Dec. 1991: 63–66.

The author uses permutation groups to analyze solutions to the 15 puzzle, Rubik's Cube, and Rubik's Clock.

A. White and R. Wilson, "The Hunting Group," *Mathematical Gazette* 79 (1995): 5–16.

This article explains how permutation groups are used in bell ringing.

S. Winters, "Error-Detecting Schemes Using Dihedral Groups," *UMAP Journal* 11, no. 4 (1990): 299–308.

This article discusses error-detection schemes based on D_n for odd n. Schemes for both one and two check digits are analyzed.

Suggested Software

GAP is free for downloading. Versions are available for Unix, Windows, and Macintosh at:

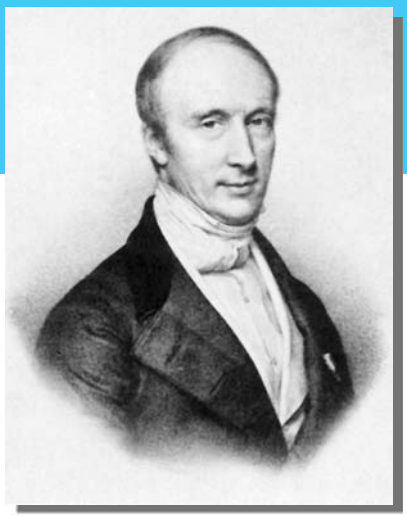
http://www.gap-system.org

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Augustin Cauchy

You see that little young man? Well! He will supplant all of us in so far as we are mathematicians.

Spoken by Lagrange to Laplace about the 11-year-old Cauchy



Stock Montage

This stamp was issued by France in Cauchy's honor.

Augustin Louis Cauchy was born on August 21, 1789, in Paris. By the time he was 11, both Laplace and Lagrange had recognized Cauchy's extraordinary talent for mathematics. In school he won prizes for Greek, Latin, and the humanities. At the age of 21, he was given a commission in Napoleon's army as a civil engineer. For the next few years, Cauchy attended to his engineering duties while carrying out brilliant mathematical research on the side.

In 1815, at the age of 26, Cauchy was made Professor of Mathematics at the École Polytechnique and was recognized as the leading mathematician in France. Cauchy and his contemporary Gauss were among the last mathematicians to know the whole of mathematics as known at their time, and both made important contributions to nearly every branch, both pure and applied, as well as to physics and astronomy.

Cauchy introduced a new level of rigor into mathematical analysis. We owe our contemporary notions of limit and continuity to him. He gave the first proof of the Fundamental Theorem of Calculus. Cauchy was the founder of complex function theory and a pioneer in the theory of permutation groups and determinants. His total written output of mathematics fills 24 large volumes. He wrote more than 500 research papers after the age of 50. Cauchy died at the age of 67 on May 23, 1857.

For more information about Cauchy, visit:

http://www–groups.dcs .st-and.ac.uk/~history/

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

6 Isomorphisms

The basis for poetry and scientific discovery is the ability to comprehend the unlike in the like and the like in the unlike.

JACOB BRONOWSKI

Motivation

Suppose an American and a German are asked to count a handful of objects. The American says, "One, two, three, four, five, . . . ," whereas the German says, "Eins, zwei, drei, vier, fünf, ..." Are the two doing different things? No. They are both counting the objects, but they are using different terminology to do so. Similarly, when one person says, "Two plus three is five" and another says, "Zwei und drei ist fünf," the two are in agreement on the *concept* they are describing, but they are using different terminology to describe the concept. An analogous situation often occurs with groups; the same group is described with different terminology. We have seen two examples of this so far. In Chapter 1, we described the symmetries of a square in geometric terms (e.g., R_{90}), whereas in Chapter 5 we described the *same* group by way of permutations of the corners. In both cases, the underlying group was the symmetries of a square. In Chapter 4, we observed that when we have a cyclic group of order n generated by a, the operation turns out to be essentially that of addition modulo n, since $a^r a^s = a^k$, where $k = (r + s) \bmod n$. For example, each of $U(43)$ and $U(49)$ is cyclic of order 42. So, each has the form $\langle a \rangle$, where $a^r a^s = a^{(r+s) \bmod 42}$.

Definition and Examples

In this chapter, we give a formal method for determining whether two groups defined in different terms are really the same. When this is the case, we say that there is an isomorphism between the two groups. This notion was first introduced by Galois about 180 years ago. The term *isomorphism* is derived from the Greek words *isos*, meaning "same" or "equal," and *morphe*, meaning "form." R. Allenby has colorfully

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

defined an algebraist as "a person who can't tell the difference between isomorphic systems."

Definition Group Isomorphism
An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \qquad \text{for all } a, b \text{ in } G.$$

If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.

This definition can be visualized as shown in Figure 6.1. The pairs of dashed arrows represent the group operations.

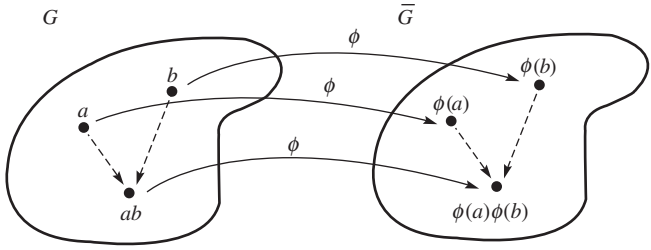


Figure 6.1

It is implicit in the definition of isomorphism that isomorphic groups have the same order. It is also implicit in the definition of isomorphism that the operation on the left side of the equal sign is that of G, whereas the operation on the right side is that of $\overline{G}$. The four cases involving $\cdot$ and $+$ are shown in Table 6.1.

Table 6.1

G Operation	$\overline{G}$ Operation	Operation Preservation
$\cdot$	$\cdot$	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
$\cdot$	$+$	$\phi(a \cdot b) = \phi(a) + \phi(b)$
$+$	$\cdot$	$\phi(a + b) = \phi(a) \cdot \phi(b)$
$+$	$+$	$\phi(a + b) = \phi(a) + \phi(b)$

There are four separate steps involved in proving that a group G is isomorphic to a group $\overline{G}$.

Step 1 "Mapping." Define a candidate for the isomorphism; that is, define a function ϕ from G to $\overline{G}$.

Step 2 "1–1." Prove that ϕ is one-to-one; that is, assume that $\phi(a) = \phi(b)$ and prove that $a = b$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Step 3 "Onto." Prove that ϕ is onto; that is, for any element $\overline{g}$ in $\overline{G}$, find an element g in G such that $\phi(g) = \overline{g}$.

Step 4 "O.P." Prove that ϕ is operation-preserving; that is, show that $\phi(ab) = \phi(a)\phi(b)$ for all a and b in G.

None of these steps is unfamiliar to you. The only one that may appear novel is the fourth one. It requires that one be able to obtain the same result by combining two elements and then mapping, or by mapping two elements and then combining them. Roughly speaking, this says that the two processes—operating and mapping—can be done in either order without affecting the result. This same concept arises in calculus when we say

$$\lim_{x \to a}(f(x) \cdot g(x)) = \lim_{x \to a} f(x) \lim_{x \to a} g(x)$$

or

$$\int_a^b (f + g)\, dx = \int_a^b f\, dx + \int_a^b g\, dx.$$

Before going any further, let's consider some examples.

EXAMPLE 1 Let G be the real numbers under addition and let $\overline{G}$ be the positive real numbers under multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\phi(x) = 2^x$. Certainly, ϕ is a function from G to $\overline{G}$. To prove that it is one-to-one, suppose that $2^x = 2^y$. Then $\log_2 2^x = \log_2 2^y$, and therefore $x = y$. For "onto," we must find for any positive real number y some real number x such that $\phi(x) = y$; that is, $2^x = y$. Well, solving for x gives $\log_2 y$. Finally,

$$\phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x)\phi(y)$$

for all x and y in G, so that ϕ is operation-preserving as well. ∎

EXAMPLE 2 Any infinite cyclic group is isomorphic to Z. Indeed, if a is a generator of the cyclic group, the mapping $a^k \to k$ is an isomorphism. Any finite cyclic group $\langle a \rangle$ of order n is isomorphic to Z_n under the mapping $a^k \to k \bmod n$. That these correspondences are functions and are one-to-one is the essence of Theorem 4.1. Obviously, the mappings are onto. That the mappings are operation-preserving follows from Exercise 9 in Chapter 0 in the finite case and from the definitions in the infinite case. ∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 3 The mapping from **R** under addition to itself given by $\phi(x) = x^3$ is *not* an isomorphism. Although ϕ is one-to-one and onto, it is not operation-preserving, since it is not true that $(x + y)^3 = x^3 + y^3$ for all x and y. ∎

EXAMPLE 4 $U(10) \approx Z_4$ and $U(5) \approx Z_4$. To verify this, one need only observe that both $U(10)$ and $U(5)$ are cyclic of order 4. Then appeal to Example 2. ∎

EXAMPLE 5 $U(10) \not\approx U(12)$. This is a bit trickier to prove. First, note that $x^2 = 1$ for all x in $U(12)$. Now, suppose that ϕ is an isomorphism from $U(10)$ onto $U(12)$. Then,

$$\phi(9) = \phi(3 \cdot 3) = \phi(3)\phi(3) = 1$$

and

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = 1.$$

Thus, $\phi(9) = \phi(1)$, but $9 \neq 1$, which contradicts the assumption that ϕ is one-to-one. ∎

EXAMPLE 6 There is no isomorphism from Q, the group of rational numbers under addition, to Q^*, the group of nonzero rational numbers under multiplication. If ϕ were such a mapping, there would be a rational number a such that $\phi(a) = -1$. But then

$$-1 = \phi(a) = \phi(\tfrac{1}{2}a + \tfrac{1}{2}a) = \phi(\tfrac{1}{2}a)\phi(\tfrac{1}{2}a) = [\phi(\tfrac{1}{2}a)]^2.$$

However, no rational number squared is -1. ∎

EXAMPLE 7 Let $G = SL(2, \mathbf{R})$, the group of 2×2 real matrices with determinant 1. Let M be any 2×2 real matrix with determinant 1. Then we can define a mapping from G to G itself by $\phi_M(A) = MAM^{-1}$ for all A in G. To verify that ϕ_M is an isomorphism, we carry out the four steps.

Step 1 ϕ_M is a function from G to G. Here, we must show that $\phi_M(A)$ is indeed an element of G whenever A is. This follows from properties of determinants:

$$\det(MAM^{-1}) = (\det M)(\det A)(\det M)^{-1} = 1 \cdot 1 \cdot 1^{-1} = 1.$$

Thus, MAM^{-1} is in G.

Step 2 ϕ_M is one-to-one. Suppose that $\phi_M(A) = \phi_M(B)$. Then $MAM^{-1} = MBM^{-1}$ and, by left and right cancellation, $A = B$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Step 3 ϕ_M is onto. Let B belong to G. We must find a matrix A in G such that $\phi_M(A) = B$. How shall we do this? If such a matrix A is to exist, it must have the property that $MAM^{-1} = B$. But this tells us exactly what A must be! For we can solve for A to obtain $A = M^{-1}BM$ and verify that $\phi_M(A) = MAM^{-1} = M(M^{-1}BM)M^{-1} = B$.

Step 4 ϕ_M is operation-preserving. Let A and B belong to G. Then,

$$\begin{aligned}\phi_M(AB) &= M(AB)M^{-1} = MA(M^{-1}M)BM^{-1} \\ &= (MAM^{-1})(MBM^{-1}) = \phi_M(A)\phi_M(B).\end{aligned}$$

The mapping ϕ_M is called *conjugation* by M. ∎

Cayley's Theorem

Our first theorem is a classic result of Cayley. An important generalization of it will be given in Chapter 25.

Theorem 6.1 Cayley's Theorem (1854)

Every group is isomorphic to a group of permutations.

PROOF To prove this, let G be any group. We must find a group $\overline{G}$ of permutations that we believe is isomorphic to G. Since G is all we have to work with, we will have to use it to construct $\overline{G}$. For any g in G, define a function T_g from G to G by

$$T_g(x) = gx \qquad \text{for all } x \text{ in } G.$$

(In words, T_g is just multiplication by g on the left.) We leave it as an exercise (Exercise 33) to prove that T_g is a permutation on the set of elements of G. Now, let $\overline{G} = \{T_g \mid g \in G\}$. Then, $\overline{G}$ is a group under the operation of function composition. To verify this, we first observe that for any g and h in G we have $T_gT_h(x) = T_g(T_h(x)) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$, so that $T_gT_h = T_{gh}$. From this it follows that T_e is the identity and $(T_g)^{-1} = T_{g^{-1}}$ (see Exercise 9). Since function composition is associative, we have verified all the conditions for $\overline{G}$ to be a group.

The isomorphism ϕ between G and $\overline{G}$ is now ready-made. For every g in G, define $\phi(g) = T_g$. If $T_g = T_h$, then $T_g(e) = T_h(e)$ or $ge = he$. Thus, $g = h$ and ϕ is one-to-one. By the way $\overline{G}$ was constructed, we see that ϕ is onto. The only condition that remains to be checked is that ϕ is operation-preserving. To this end, let a and b belong to G. Then

$$\phi(ab) = T_{ab} = T_aT_b = \phi(a)\phi(b).$$

∎

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The group $\overline{G}$ constructed previously is called the *left regular representation of G.*

EXAMPLE 8 For concreteness, let us calculate the left regular representation $\overline{U(12)}$ for $U(12) = \{1, 5, 7, 11\}$. Writing the permutations of $U(12)$ in array form, we have (remember, T_x is just multiplication by x)

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \qquad T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix},$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \qquad T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}.$$

It is instructive to compare the Cayley tables for $U(12)$ and its left regular representation $\overline{U(12)}$.

$U(12)$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\overline{U(12)}$	T_1	T_5	T_7	T_{11}
T_1	T_1	T_5	T_7	T_{11}
T_5	T_5	T_1	T_{11}	T_7
T_7	T_7	T_{11}	T_1	T_5
T_{11}	T_{11}	T_7	T_5	T_1

It should be abundantly clear from these tables that $U(12)$ and $\overline{U(12)}$ are only notationally different. ∎

Cayley's Theorem is important for two contrasting reasons. One is that it allows us to represent an abstract group in a concrete way. A second is that it shows that the present-day set of axioms we have adopted for a group is the correct abstraction of its much earlier predecessor—a group of permutations. Indeed, Cayley's Theorem tells us that abstract groups are not different from permutation groups. Rather, it is the viewpoint that is different. It is this difference of viewpoint that has stimulated the tremendous progress in group theory and many other branches of mathematics in the 20th century.

It is sometimes very difficult to prove or disprove, whichever the case may be, that two particular groups are isomorphic. For example, it requires somewhat sophisticated techniques to prove the surprising fact that the group of real numbers under addition is isomorphic to the group of complex numbers under addition. Likewise, it is not easy to prove the fact that the group of nonzero complex numbers under multiplication is isomorphic to the group of complex numbers with absolute value of 1 under multiplication. In geometric terms, this says that, as groups, the punctured plane and the unit circle are isomorphic [1].

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Properties of Isomorphisms

Our next two theorems give a catalog of properties of isomorphisms and isomorphic groups.

Theorem 6.2 Properties of Isomorphisms Acting on Elements

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. *ϕ carries the identity of G to the identity of $\overline{G}$.*
2. *For every integer n and for every group element a in G, $\phi(a^n) = [\phi(a)]^n$.*
3. *For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.*
4. *$G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.*
5. *$|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).*
6. *For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.*
7. *If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.*

PROOF We will restrict ourselves to proving only properties 1, 2, and 4, but observe that property 5 follows from properties 1 and 2, property 6 follows from property 2, and property 7 follows from property 5. For convenience, let us denote the identity in G by e and the identity in $\overline{G}$ by $\bar{e}$. Then, since $e = ee$, we have

$$\phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Also, because $\phi(e) \in \overline{G}$, we have $\phi(e) = \bar{e}\phi(e)$, as well. Thus, by cancellation, $\bar{e} = \phi(e)$. This proves property 1.

For positive integers, property 2 follows from the definition of an isomorphism and mathematical induction. If n is negative, then $-n$ is positive, and we have from property 1 and the observation about the positive integer case that $e = \phi(e) = \phi(g^n g^{-n}) = \phi(g^n)\phi(g^{-n}) = \phi(g^n)(\phi(g))^{-n}$. Thus, multiplying both sides on the right by $(\phi(g))^n$, we have $(\phi(g))^n = \phi(g^n)$. Property 1 takes care of the case $n = 0$.

To prove property 4, let $G = \langle a \rangle$ and note that, by closure, $\langle \phi(a) \rangle \subseteq \overline{G}$. Because ϕ is onto, for any element b in $\overline{G}$, there is an element a^k in G such that $\phi(a^k) = b$. Thus, $b = (\phi(a))^k$ and so $b \in \langle \phi(a) \rangle$. This proves that $\overline{G} = \langle \phi(a) \rangle$.

Now suppose that $\overline{G} = \langle \phi(a) \rangle$. Clearly, $\langle a \rangle \subseteq G$. For any element b in G, we have $\phi(b) \in \langle \phi(a) \rangle$. So, for some integer k we have

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

$\phi(b) = (\phi(a))^k = \phi(a^k)$. Because ϕ is one-to-one, $b = a^k$. This proves that $\langle a \rangle = G$. ∎

When the group operation is addition, property 2 of Theorem 6.2 is $\phi(na) = n\phi(a)$; property 4 says that an isomorphism between two cyclic groups takes a generator to a generator.

Property 6 is quite useful for showing that two groups are *not* isomorphic. Often b is picked to be the identity. For example, consider $\mathbf{C}^*$ and $\mathbf{R}^*$. Because the equation $x^4 = 1$ has four solutions in $\mathbf{C}^*$ but only two in $\mathbf{R}^*$, no matter how one attempts to define an isomorphism from $\mathbf{C}^*$ to $\mathbf{R}^*$, property 6 cannot hold.

Theorem 6.3 Properties of Isomorphisms Acting on Groups

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. *ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.*
2. *G is Abelian if and only if $\overline{G}$ is Abelian.*
3. *G is cyclic if and only if $\overline{G}$ is cyclic.*
4. *If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.*
5. *If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\}$ is a subgroup of G.*
6. *$\phi(Z(G)) = Z(\overline{G})$.*

PROOF Properties 1 and 4 are left as exercises (Exercises 31 and 32). Properties 2 and 6 are a direct consequence of property 3 of Theorem 6.2. Property 3 follows from property 4 of Theorem 6.2 and property 1 of Theorem 6.3. Property 5 follows from properties 1 and 4. ∎

Theorems 6.2 and 6.3 show that isomorphic groups have many properties in common. Actually, the definition is precisely formulated so that isomorphic groups have *all* group theoretic properties in common. By this we mean that if two groups are isomorphic, then any property that can be expressed in the language of group theory is true for one if and only if it is true for the other. This is why algebraists speak of isomorphic groups as "equal" or "the same." Admittedly, calling such groups equivalent, rather than the same, might be more appropriate, but we bow to long-standing tradition.

Automorphisms

Certain kinds of isomorphisms are referred to so often that they have been given special names.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Definition Automorphism
An isomorphism from a group G onto itself is called an *automorphism* of G.

The isomorphism in Example 7 is an automorphism of $SL(2, \mathbf{R})$. Two more examples follow.

EXAMPLE 9 The function ϕ from $\mathbf{C}$ to $\mathbf{C}$ given by $\phi(a + bi) = a - bi$ is an automorphism of the group of complex numbers under addition. The restriction of ϕ to $\mathbf{C}^*$ is also an automorphism of the group of nonzero complex numbers under multiplication. (See Exercise 35.)

EXAMPLE 10 Let $\mathbf{R}^2 = \{(a, b) \mid a, b \in \mathbf{R}\}$. Then $\phi(a, b) = (b, a)$ is an automorphism of the group $\mathbf{R}^2$ under componentwise addition. Geometrically, ϕ reflects each point in the plane across the line $y = x$. More generally, any reflection across a line passing through the origin or any rotation of the plane about the origin is an automorphism of $\mathbf{R}^2$.

The isomorphism in Example 7 is a particular instance of an automorphism that arises often enough to warrant a name and notation of its own.

Definition Inner Automorphism Induced by a
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the *inner automorphism of G induced by a.*

We leave it for the reader to show that ϕ_a is actually an automorphism of G. (Use Example 7 as a model.)

EXAMPLE 11 The action of the inner automorphism of D_4 induced by R_{90} is given in the following table.

x	$\overset{\phi_{R_{90}}}{\rightarrow}$	$R_{90}\, x\, R_{90}^{-1}$
R_0	$\rightarrow$	$R_{90}R_0R_{90}^{-1} = R_0$
R_{90}	$\rightarrow$	$R_{90}R_{90}R_{90}^{-1} = R_{90}$
R_{180}	$\rightarrow$	$R_{90}R_{180}R_{90}^{-1} = R_{180}$
R_{270}	$\rightarrow$	$R_{90}R_{270}R_{90}^{-1} = R_{270}$
H	$\rightarrow$	$R_{90}HR_{90}^{-1} = V$
V	$\rightarrow$	$R_{90}VR_{90}^{-1} = H$
D	$\rightarrow$	$R_{90}DR_{90}^{-1} = D'$
D'	$\rightarrow$	$R_{90}D'R_{90}^{-1} = D$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

When G is a group, we use $\text{Aut}(G)$ to denote the set of all automorphisms of G and $\text{Inn}(G)$ to denote the set of all inner automorphisms of G. The reason these sets are noteworthy is demonstrated by the next theorem.

Theorem 6.4 Aut(G) and Inn(G) Are Groups†

The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

PROOF The proof of Theorem 6.4 is left as an exercise (Exercise 15). ∎

The determination of $\text{Inn}(G)$ is routine. If $G = \{e, a, b, c, \ldots\}$, then $\text{Inn}(G) = \{\phi_e, \phi_a, \phi_b, \phi_c, \ldots\}$. This latter list may have duplications, however, since ϕ_a may be equal to ϕ_b even though $a \neq b$ (see Exercise 43). Thus, the only work involved in determining $\text{Inn}(G)$ is deciding which distinct elements give the distinct automorphisms. On the other hand, the determination of $\text{Aut}(G)$ is, in general, quite involved.

EXAMPLE 12 Inn(D_4)

To determine $\text{Inn}(D_4)$, we first observe that the complete list of inner automorphisms is ϕ_{R_0}, $\phi_{R_{90}}$, $\phi_{R_{180}}$, $\phi_{R_{270}}$, ϕ_H, ϕ_V, ϕ_D, and $\phi_{D'}$. Our job is to determine the repetitions in this list. Since $R_{180} \in Z(D_4)$, we have $\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x$, so that $\phi_{R_{180}} = \phi_{R_0}$. Also, $\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \phi_{R_{90}}(x)$. Similarly, since $H = R_{180}V$ and $D' = R_{180}D$, we have $\phi_H = \phi_V$ and $\phi_D = \phi_{D'}$. This proves that the previous list can be pared down to ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, and ϕ_D. We leave it to the reader to show that these are distinct (Exercise 13). ∎

EXAMPLE 13 Aut(Z_{10})

To compute $\text{Aut}(Z_{10})$, we try to discover enough information about an element α of $\text{Aut}(Z_{10})$ to determine how α must be defined. Because Z_{10} is so simple, this is not difficult to do. To begin with, observe that once we know $\alpha(1)$, we know $\alpha(k)$ for any k, because

†The group $\text{Aut}(G)$ was first studied by O. Hölder in 1893 and, independently, by E. H. Moore in 1894.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

$$\alpha(k) = \underbrace{\alpha(1 + 1 + \cdots + 1)}_{k \text{ terms}}$$
$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{k \text{ terms}} = k\alpha(1).$$

So, we need only determine the choices for $\alpha(1)$ that make α an automorphism of Z_{10}. Since property 5 of Theorem 6.2 tells us that $|\alpha(1)| = 10$, there are four candidates for $\alpha(1)$:

$$\alpha(1) = 1, \qquad \alpha(1) = 3, \qquad \alpha(1) = 7, \qquad \alpha(1) = 9.$$

To distinguish among the four possibilities, we refine our notation by denoting the mapping that sends 1 to 1 by α_1, 1 to 3 by α_3, 1 to 7 by α_7, and 1 to 9 by α_9. So the only possibilities for $\text{Aut}(Z_{10})$ are α_1, α_3, α_7, and α_9. But are all these automorphisms? Clearly, α_1 is the identity. Let us check α_3. Since $x \bmod 10 = y \bmod 10$ implies $3x \bmod 10 = 3y \bmod 10$, α_3 is well defined. Moreover, because $\alpha_3(1) = 3$ is a generator of Z_{10}, it follows that α_3 is onto (and, by Exercise 12 in Chapter 5, it is also one-to-one). Finally, since $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b)$, we see that α_3 is operation-preserving as well. Thus, $\alpha_3 \in \text{Aut}(Z_{10})$. The same argument shows that α_7 and α_9 are also automorphisms.

This gives us the elements of $\text{Aut}(Z_{10})$ but not the structure. For instance, what is $\alpha_3\alpha_3$? Well, $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$, so $\alpha_3\alpha_3 = \alpha_9$. Similar calculations show that $\alpha_3^3 = \alpha_7$ and $\alpha_3^4 = \alpha_1$, so that $|\alpha_3| = 4$. Thus, $\text{Aut}(Z_{10})$ is cyclic. Actually, the following Cayley tables reveal that $\text{Aut}(Z_{10})$ is isomorphic to $U(10)$.

$U(10)$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\text{Aut}(Z_{10})$	α_1	α_3	α_7	α_9
$\boldsymbol{\alpha_1}$	α_1	α_3	α_7	α_9
$\boldsymbol{\alpha_3}$	α_3	α_9	α_1	α_7
$\boldsymbol{\alpha_7}$	α_7	α_1	α_9	α_3
$\boldsymbol{\alpha_9}$	α_9	α_7	α_3	α_1

■

With Example 13 as a guide, we are now ready to tackle the group $\text{Aut}(Z_n)$. The result is particularly nice, since it relates the two kinds of groups we have most frequently encountered thus far—the cyclic groups Z_n and the U-groups $U(n)$.

Theorem 6.5 $\text{Aut}(Z_n) \approx U(n)$

For every positive integer n, $\text{Aut}(Z_n)$ is isomorphic to $U(n)$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PROOF As in Example 13, any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspondence from $\text{Aut}(Z_n)$ to $U(n)$ given by T: $\alpha \to \alpha(1)$. The fact that $\alpha(k) = k\alpha(1)$ (see Example 13) implies that T is a one-to-one mapping. For if α and β belong to $\text{Aut}(Z_n)$ and $\alpha(1) = \beta(1)$, then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$ for all k in Z_n, and therefore $\alpha = \beta$.

To prove that T is onto, let $r \in U(n)$ and consider the mapping α from Z_n to Z_n defined by $\alpha(s) = sr \pmod n$ for all s in Z_n. We leave it as an exercise to verify that α is an automorphism of Z_n (see Exercise 27). Then, since $T(\alpha) = \alpha(1) = r$, T is onto $U(n)$.

Finally, we establish the fact that T is operation-preserving. Let α, $\beta \in \text{Aut}(Z_n)$. We then have

$$\begin{aligned} T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) &= \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)}) \\ &= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)} = \alpha(1)\beta(1) \\ &= T(\alpha)T(\beta). \end{aligned}$$

This completes the proof. ∎

Exercises

Being a mathematician is a bit like being a manic depressive: you spend your life alternating between giddy elation and black despair.

STEVEN G. KRANTZ, *A Primer of Mathematical Writing*

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.
2. Find $\text{Aut}(Z)$.
3. Let $\mathbf{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbf{R}^+$.
4. Show that $U(8)$ is not isomorphic to $U(10)$.
5. Show that $U(8)$ is isomorphic to $U(12)$.
6. Prove that isomorphism is an equivalence relation. That is, for any groups G, H, and K, $G \approx G$, $G \approx H$ implies $H \approx G$, and $G \approx H$ and $H \approx K$ implies $G \approx K$.
7. Prove that S_4 is not isomorphic to D_{12}.
8. Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbf{R}^+$ under multiplication to $\mathbf{R}$ under addition.
9. In the notation of Theorem 6.1, prove that T_e is the identity and that $(T_g)^{-1} = T_{g^{-1}}$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

10. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

11. If g and h are elements from a group, prove that $\phi_g \phi_h = \phi_{gh}$.

12. Find two groups G and H such that $G \not\approx H$, but $\text{Aut}(G) \approx \text{Aut}(H)$.

13. Prove the assertion in Example 12 that the inner automorphisms ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, and ϕ_D of D_4 are distinct.

14. Find $\text{Aut}(Z_6)$.

15. If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups.

16. If a group G is isomorphic to H, prove that $\text{Aut}(G)$ is isomorphic to $\text{Aut}(H)$.

17. Suppose ϕ belongs to $\text{Aut}(Z_n)$ and a is relatively prime to n. If $\phi(a) = b$, determine a formula for $\phi(x)$.

18. Let H be the subgroup of all rotations in D_n and let ϕ be an automorphism of D_n. Prove that $\phi(H) = H$. (In words, an automorphism of D_n carries rotations to rotations.)

19. Let $H = \{\beta \in S_5 \mid \beta(1) = 1\}$ and $K = \{\beta \in S_5 \mid \beta(2) = 2\}$. Prove that H is isomorphic to K. Is the same true if S_5 is replaced by S_n, where $n \geq 3$?

20. Show that Z has infinitely many subgroups isomorphic to Z.

21. Let n be an even integer greater than 2 and let ϕ be an automorphism of D_n. Determine $\phi(R_{180})$.

22. Let ϕ be an automorphism of a group G. Prove that $H = \{x \in G \mid \phi(x) = x\}$ is a subgroup of G.

23. Give an example of a cyclic group of smallest order that contains a subgroup isomorphic to Z_{12} and a subgroup isomorphic to Z_{20}. No need to prove anything, but explain your reasoning.

24. Suppose that $\phi: Z_{20} \to Z_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

25. Identify a group G that has subgroups isomorphic to Z_n for all positive integers n.

26. Prove that the mapping from $U(16)$ to itself given by $x \to x^3$ is an automorphism. What about $x \to x^5$ and $x \to x^7$? Generalize.

27. Let $r \in U(n)$. Prove that the mapping $\alpha: Z_n \to Z_n$ defined by $\alpha(s) = sr \bmod n$ for all s in Z_n is an automorphism of Z_n. (This exercise is referred to in this chapter.)

28. The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in Z \right\}$ is isomorphic to what familiar group? What if Z is replaced by $\mathbf{R}$?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

29. If ϕ and γ are isomorphisms from the cyclic group $\langle a \rangle$ to some group and $\phi(a) = \gamma(a)$, prove that $\phi = \gamma$.

30. Suppose that ϕ: $Z_{50} \to Z_{50}$ is an automorphism with $\phi(11) = 13$. Determine a formula for $\phi(x)$.

31. Prove property 1 of Theorem 6.3.

32. Prove property 4 of Theorem 6.3.

33. Referring to Theorem 6.1, prove that T_g is indeed a permutation on the set G.

34. Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

35. Show that the mapping $\phi(a + bi) = a - bi$ is an automorphism of the group of complex numbers under addition. Show that ϕ preserves complex multiplication as well—that is, $\phi(xy) = \phi(x)\phi(y)$ for all x and y in $\mathbf{C}$. (This exercise is referred to in Chapter 15.)

36. Let

$$G = \{a + b\sqrt{2} \mid a, b \text{ are rational}\}$$

and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \middle| \, a, b \text{ are rational} \right\}.$$

Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition? (G and H are examples of rings—a topic we will take up in Part 3.)

37. Prove that Z under addition is not isomorphic to Q under addition.

38. Prove that the quaternion group (see Exercise 4, Supplementary Exercises for Chapters 1–4) is not isomorphic to the dihedral group D_4.

39. Let $\mathbf{C}$ be the complex numbers and

$$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \middle| \, a, b \in \mathbf{R} \right\}.$$

Prove that $\mathbf{C}$ and M are isomorphic under addition and that $\mathbf{C}^*$ and M^*, the nonzero elements of M, are isomorphic under multiplication.

40. Let $\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbf{R}\}$. Show that the mapping ϕ: $(a_1, a_2, \ldots, a_n) \to (-a_1, -a_2, \ldots, -a_n)$ is an automorphism of the group $\mathbf{R}^n$ under componentwise addition. This automorphism is called *inversion.* Describe the action of ϕ geometrically.

41. Consider the following statement: The order of a subgroup divides the order of the group. Suppose you could prove this for finite permutation groups. Would the statement then be true for all finite groups? Explain.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

42. Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that there is an infinite Abelian group for which the mapping $g \to g^2$ is one-to-one and operation-preserving but not an automorphism.

43. Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, that the mappings ϕ_g and ϕ_{zg} are equal).

44. Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbf{R}^+$ under multiplication to $\mathbf{R}$ under addition.

45. Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

46. Combine the results of Exercises 43 and 45 into a single "if and only if" theorem.

47. If x and y are elements in S_n ($n \geq 3$), prove that $\phi_x = \phi_y$ implies $x = y$. (Here, ϕ_x is the inner automorphism of S_n induced by x.)

48. Let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.

49. Suppose the ϕ and γ are isomorphisms of some group G to the same group. Prove that $H = \{g \in G \mid \phi(g) = \gamma(g)\}$ is a subgroup of G.

50. Suppose that β is an automorphism of a group G. Prove that $H = \{g \in G \mid \beta^2(g) = g\}$ is a subgroup of G. Generalize.

51. Suppose that G is an Abelian group and ϕ is an automorphism of G. Prove that $H = \{x \in G \mid \phi(x) = x^{-1}\}$ is a subgroup of G.

52. Given a group G, define a new group G^* that has the same elements as G with the operation $*$ defines by $a * b = ba$ for all a and b in G^*. Prove that the mapping from G to G^* defined by $\phi(x) = x^{-1}$ for all x in G is an isomorphism from G onto G^*.

53. Let a belong to a group G and let $|a|$ be finite. Let ϕ_a be the automorphism of G given by $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$. Exhibit an element a from a group for which $1 < |\phi_a| < |a|$.

54. Let $G = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ and $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Show that G and H are isomorphic groups under addition. Does your isomorphism preserve multiplication? Generalize to the case when $G = \langle m \rangle$ and $H = \langle n \rangle$, where m and n are integers.

55. Suppose that ϕ is an automorphism of D_4 such that $\phi(R_{90}) = R_{270}$ and $\phi(V) = V$. Determine $\phi(D)$ and $\phi(H)$.

56. In $\text{Aut}(Z_9)$, let α_i denote the automorphism that sends 1 to i where $\gcd(i, 9) = 1$. Write α_5 and α_8 as permutations of $\{0, 1, \ldots, 8\}$ in disjoint cycle form. [For example, $\alpha_2 = (0)(124875)(36)$.]

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

57. Write the permutation corresponding to R_{90} in the left regular representation of D_4 in cycle form.

58. Show that every automorphism ϕ of the rational numbers Q under addition to itself has the form $\phi(x) = x\phi(1)$.

59. Prove that Q^+, the group of positive rational numbers under multiplication, is isomorphic to a proper subgroup.

60. Prove that Q, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

61. Prove that every automorphism of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication, maps positive numbers to positive numbers and negative numbers to negative numbers.

62. Let G be a finite group. Show that in the disjoint cycle form of the right regular representation $T_g(x) = xg$ of G, each cycle has length $|g|$.

63. Give a group theoretic proof that Q under addition is not isomorphic to $\mathbf{R}^+$ under multiplication.

Reference

1. J. R. Clay, "The Punctured Plane Is Isomorphic to the Unit Circle," *Journal of Number Theory* 1 (1969): 500–501.

Computer Exercises

Software for the computer exercise in this chapter is available at the website:

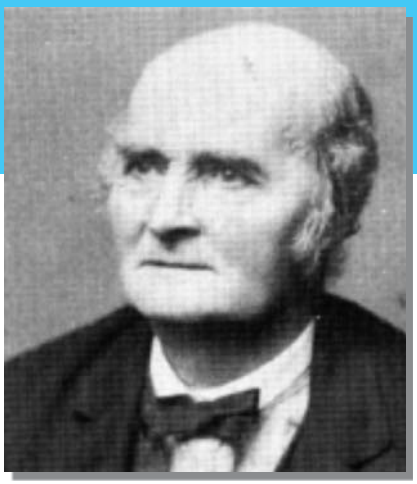
http://www.d.umn.edu/~jgallian

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Arthur Cayley

Cayley is forging the weapons for future generations of physicists.

PETER TAIT



The Granger Collection, New York

ARTHUR CAYLEY was born on August 16, 1821, in England. His genius showed itself at an early age. He published his first research paper while an undergraduate of 20, and in the next year he published eight papers. While still in his early 20s, he originated the concept of *n*-dimensional geometry.

After graduating from Trinity College, Cambridge, Cayley stayed on for three years as a tutor. At the age of 25, he began a 14-year career as a lawyer. During this period, he published approximately 200 mathematical papers, many of which are now classics.

In 1863, Cayley accepted the newly established Sadlerian professorship of mathematics at Cambridge University. He spent the rest of his life in that position. One of his notable accomplishments was his role in the successful effort to have women admitted to Cambridge.

Among Cayley's many innovations in mathematics were the notions of an abstract group and a group algebra, and the matrix concept. He made major contributions to geometry and linear algebra. Cayley and his lifelong friend and collaborator J. J. Sylvester were the founders of the theory of invariants, which was later to play an important role in the theory of relativity.

Cayley's collected works comprise 13 volumes, each about 600 pages in length. He died on January 26, 1895.

To find more information about Cayley, visit:

http://www-groups.dcs.st-and.ac.uk/~history/

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

7 Cosets and Lagrange's Theorem

It might be difficult, at this point, for students to see the extreme importance of this result [Lagrange's Theorem]. As we penetrate the subject more deeply they will become more and more aware of its basic character.

I. N. HERSTEIN, *Topics in Algebra*

Properties of Cosets

In this chapter, we will prove the single most important theorem in finite group theory—Lagrange's Theorem. In his book on abstract algebra, I. N. Herstein likened it to the ABC's for finite groups. But first we introduce a new and powerful tool for analyzing a group—the notion of a coset. This notion was invented by Galois in 1830, although the term was coined by G. A. Miller in 1910.

Definition Coset of *H* in *G*

Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a subgroup of G, the set aH is called the *left coset of H in G containing a*, whereas Ha is called the *right coset of H in G containing a*. In this case, the element a is called the *coset representative of aH* (or Ha). We use $|aH|$ to denote the number of elements in the set aH, and $|Ha|$ to denote the number of elements in Ha.

EXAMPLE 1 Let $G = S_3$ and $H = \{(1), (13)\}$. Then the left cosets of H in G are

$$\begin{aligned}(1)H &= H,\\ (12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H,\\ (13)H &= \{(13), (1)\} = H,\\ (23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.\end{aligned}$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

EXAMPLE 2 Let $\mathcal{H} = \{R_0, R_{180}\}$ in D_4, the dihedral group of order 8. Then,

$$\begin{aligned} R_0\mathcal{H} &= \mathcal{H}, \\ R_{90}\mathcal{H} &= \{R_{90}, R_{270}\} = R_{270}\mathcal{H}, \\ R_{180}\mathcal{H} &= \{R_{180}, R_0\} = \mathcal{H}, \\ V\mathcal{H} &= \{V, H\} = H\mathcal{H}, \\ D\mathcal{H} &= \{D, D'\} = D'\mathcal{H}. \end{aligned}$$

EXAMPLE 3 Let $H = \{0, 3, 6\}$ in Z_9 under addition. In the case that the group operation is addition, we use the notation $a + H$ instead of aH. Then the cosets of H in Z_9 are

$$\begin{aligned} 0 + H &= \{0, 3, 6\} = 3 + H = 6 + H, \\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H, \\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H. \end{aligned}$$

The three preceding examples illustrate a few facts about cosets that are worthy of our attention. First, cosets are usually not subgroups. Second, aH may be the same as bH, even though a is not the same as b. Third, since in Example 1 $(12)H = \{(12), (132)\}$ whereas $H(12) = \{(12), (123)\}$, aH need not be the same as Ha.

These examples and observations raise many questions. When does $aH = bH$? Do aH and bH have any elements in common? When does $aH = Ha$? Which cosets are subgroups? Why are cosets important? The next lemma and theorem answer these questions. (Analogous results hold for right cosets.)

Lemma Properties of Cosets

Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$.
2. $aH = H$ *if and only if* $a \in H$.
3. $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.
4. $aH = bH$ *if and only if* $a \in bH$.
5. $aH = bH$ *or* $aH \cap bH = \varnothing$.
6. $aH = bH$ *if and only if* $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ *if and only if* $H = aHa^{-1}$.
9. aH *is a subgroup of* G *if and only if* $a \in H$.

PROOF

1. $a = ae \in aH$.
2. To verify property 2, we first suppose that $aH = H$. Then $a = ae \in aH = H$. Next, we assume that $a \in H$ and show that $aH \subseteq H$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

and $H \subseteq aH$. The first inclusion follows directly from the closure of H. To show that $H \subseteq aH$, let $h \in H$. Then, since $a \in H$ and $h \in H$, we know that $a^{-1}h \in H$. Thus, $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$.

3. This follows directly from $(ab)h = a(bh)$ and $h(ab) = (ha)b$.

4. If $aH = bH$, then $a = ae \in aH = bH$. Conversely, if $a \in bH$ we have $a = bh$ where $h \in H$, and therefore $aH = (bh)H = b(hH) = bH$.

5. Property 5 follows directly from property 4, for if there is an element c in $aH \cap bH$, then $cH = aH$ and $cH = bH$.

6. Observe that $aH = bH$ if and only if $H = a^{-1}bH$. The result now follows from property 2.

7. To prove that $|aH| = |bH|$, it suffices to define a one-to-one mapping from aH onto bH. Obviously, the correspondence $ah \rightarrow bh$ maps aH onto bH. That it is one-to-one follows directly from the cancellation property.

8. Note that $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H$—that is, if and only if $aHa^{-1} = H$.

9. If aH is a subgroup, then it contains the identity e. Thus, $aH \cap eH \neq \varnothing$; and, by property 5, we have $aH = eH = H$. Thus, from property 2, we have $a \in H$. Conversely, if $a \in H$, then, again by property 2, $aH = H$. ∎

Although most mathematical theorems are written in symbolic form, one should also know what they say *in words.* In the preceding lemma, property 1 says simply that the left coset of H containing a does contain a. Property 2 says that the H "absorbs" an element if and only if the element belongs to H. Property 3 says that the left coset of H created by multiplying H on the left by ab is the same as the one created by multiplying H on the left by b then multiplying the resulting coset bH on the left by a (and analogously for multiplication on the right by ab). Property 4 shows that a left coset of H is uniquely determined by any one of its elements. In particular, any element of a left coset can be used to represent the coset. Property 5 says—and this is very important—that two left cosets of H are either identical or disjoint. Thus, a left coset of H is uniquely determined by any one of its elements. In particular, any element of a left coset can be used to represent the coset. Property 6 shows how we may transfer a question about equality of left cosets of H to a question about H itself and vice versa. Property 7 says that all left cosets of H have the same size. Property 8 is analogous to property 6 in that it shows how a question about the equality of the left and right cosets of H containing a is equivalent to a question about the equality of two subgroups of G. The last property of the lemma says that H itself is the only coset of H that is a subgroup of G.

Note that properties 1, 5, and 7 of the lemma guarantee that the left cosets of a subgroup H of G partition G into blocks of equal size. Indeed, we may view the cosets of H as a partitioning of G into

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

equivalence classes under the equivalence relation defined by $a \sim b$ if $aH = bH$ (see Theorem 0.7).

In practice, the subgroup H is often chosen so that the cosets partition the group in some highly desirable fashion. For example, if G is 3-space $\mathbf{R}^3$ and H is a plane through the origin, then the coset $(a, b, c) + H$ (addition is done componentwise) is the plane passing through the point (a, b, c) and parallel to H. Thus, the cosets of H constitute a partition of 3-space into planes parallel to H. If $G = GL(2, \mathbf{R})$ and $H = SL(2, \mathbf{R})$, then for any matrix A in G, the coset AH is the set of *all* 2×2 matrices with the same determinant as A. Thus,

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} H \quad \text{is the set of all } 2 \times 2 \text{ matrices of determinant } 2$$

and

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} H \quad \text{is the set of all } 2 \times 2 \text{ matrices of determinant } -3.$$

Property 5 of the lemma is useful for actually finding the distinct cosets of a subgroup. We illustrate this in the next example.

EXAMPLE 4 To find the cosets of $H = \{1, 15\}$ in $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$, we begin with $H = \{1, 15\}$. We can find a second coset by choosing any element not in H, say 3, as a coset representative. This gives the coset $3H = \{3, 13\}$. We find our next coset by choosing a representative not already appearing in the two previously chosen cosets, say 5. This gives us the coset $5H = \{5, 11\}$. We continue to form cosets by picking elements from $U(32)$ that have not yet appeared in the previous cosets as representatives of the cosets until we have accounted for every element of $U(32)$. We then have the complete list of all distinct cosets of H. ∎

Lagrange's Theorem and Consequences

We are now ready to prove a theorem that has been around for more than 200 years—longer than group theory itself! (This theorem was not originally stated in group theoretic terms.) At this stage, it should come as no surprise.

Theorem 7.1 Lagrange's Theorem†: $|H|$ Divides $|G|$

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

†Lagrange stated his version of this theorem in 1770, but the first complete proof was given by Pietro Abbati some 30 years later.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PROOF Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G. Then, for each a in G, we have $aH = a_iH$ for some i. Also, by property 1 of the lemma, $a \in aH$. Thus, each member of G belongs to one of the cosets a_iH. In symbols,

$$G = a_1H \cup \cdots \cup a_rH.$$

Now, property 5 of the lemma shows that this union is disjoint, so that

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Finally, since $|a_iH| = |H|$ for each i, we have $|G| = r|H|$. ∎

We pause to emphasize that Lagrange's Theorem is a subgroup candidate criterion; that is, it provides a list of candidates for the orders of the subgroups of a group. Thus, a group of order 12 may have subgroups of order 12, 6, 4, 3, 2, 1, but no others. *Warning!* The converse of Lagrange's Theorem is false. For example, a group of order 12 need not have a subgroup of order 6. We prove this in Example 5.

A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group. The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G:H|$. As an immediate consequence of the proof of Lagrange's Theorem, we have the following useful formula for the number of distinct left (or right) cosets of H in G.

Corollary 1 $|G:H| = |G|/|H|$

If G is a finite group and H is a subgroup of G, then $|G:H| = |G|/|H|$.

Corollary 2 $|a|$ Divides $|G|$

In a finite group, the order of each element of the group divides the order of the group.

PROOF Recall that the order of an element is the order of the subgroup generated by that element. ∎

Corollary 3 Groups of Prime Order Are Cyclic

A group of prime order is cyclic.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PROOF Suppose that G has prime order. Let $a \in G$ and $a \neq e$. Then, $|\langle a \rangle|$ divides $|G|$ and $|\langle a \rangle| \neq 1$. Thus, $|\langle a \rangle| = |G|$ and the corollary follows. ∎

Corollary 4 $a^{|G|} = e$

Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

PROOF By Corollary 2, $|G| = |a|k$ for some positive integer k. Thus, $a^{|G|} = a^{|a|k} = e^k = e$. ∎

Corollary 5 Fermat's Little Theorem

For every integer a and every prime p, $a^p \bmod p = a \bmod p$.

PROOF By the division algorithm, $a = pm + r$, where $0 \leq r < p$. Thus, $a \bmod p = r$, and it suffices to prove that $r^p \bmod p = r$. If $r = 0$, the result is trivial, so we may assume that $r \in U(p)$. [Recall that $U(p) = \{1, 2, \ldots, p - 1\}$ under multiplication modulo p.] Then, by the preceding corollary, $r^{p-1} \bmod p = 1$ and, therefore, $r^p \bmod p = r$. ∎

Fermat's Little Theorem has been used in conjunction with computers to test for primality of certain numbers. One case concerned the number $p = 2^{257} - 1$. If p is prime, then we know from Fermat's Little Theorem that $10^p \bmod p = 10 \bmod p$ and, therefore, $10^{p+1} \bmod p = 100 \bmod p$. Using multiple precision and a simple loop, a computer was able to calculate $10^{p+1} \bmod p = 10^{2^{257}} \bmod p$ in a few seconds. The result was not 100, and so p is not prime.

EXAMPLE 5 The Converse of Lagrange's Theorem Is False.[†] The group A_4 of order 12 has no subgroups of order 6. To verify this, recall that A_4 has eight elements of order 3 (α_5 through α_{12}, in the notation of Table 5.1) and suppose that H is a subgroup of order 6. Let a be any element of order 3 in A_4. If a is not in H, then $A_4 = H \cup aH$. But then a^2 is in H or a^2 is in aH. If a^2 is in H then so is $(a^2)^2 = a^4 = a$, so this case is ruled out. If a^2 is in aH, then $a^2 = ah$ for some h in H, but this also implies that a is in H. This argument shows that any subgroup of A_4 of order 6 must contain all eight elements of A_4 of order 3, which is absurd. ∎

[†]The first counterexample to the converse of Lagrange's Theorem was given by Paolo Ruffini in 1799.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Lagrange's Theorem demonstrates that the finiteness of a group imposes severe restrictions on the possible orders of subgroups. The next theorem also places powerful limits on the existence of certain subgroups in finite groups.

Theorem 7.2 $|HK| = |H||K|/|H \cap K|$

For two finite subgroups H and K of a group, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = |H||K|/|H \cap K|$.

PROOF Although the set HK has $|H||K|$ products, not all of these products need represent distinct group elements. That is, we may have $hk = h'k'$ where $h \neq h'$ and $k \neq k'$. To determine $|HK|$, we must find the extent to which this happens. For every t in $H \cap K$, the product $hk = (ht)(t^{-1}k)$, so each group element in HK is represented by at least $|H \cap K|$ products in HK. But $hk = h'k'$ implies $t = h^{-1}h' = kk'^{-1} \in H \cap K$, so that $h' = ht$ and $k' = t^{-1}k$. Thus, each element in HK is represented by exactly $|H \cap K|$ products. So, $|HK| = |H||K|/|H \cap K|$. ∎

EXAMPLE 6 A group of order 75 can have at most one subgroup of order 25. (It is shown in Chapter 24 that every group of order 75 has a subgroup of order 25). To see that a group of order 75 cannot have two subgroups of order 25, suppose H and K are two such subgroups. Since $|H \cap K|$ divides $|H| = 25$ and $|H \cap K| = 1$ or 5 results in $|HK| = |H||K|/|H \cap K| = 25 \cdot 25/|H \cap K| = 625$ or 125 elements, we have that $|H \cap K| = 25$ and therefore $H = K$. ∎

For any prime $p > 2$, we know that Z_{2p} and D_p are nonisomorphic groups of order $2p$. This naturally raises the question of whether there could be other possible groups of these orders. Remarkably, with just the simple machinery available to us at this point, we can answer this question.

Theorem 7.3 Classification of Groups of Order $2p$

Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p.

PROOF We assume that G does not have an element of order $2p$ and show that $G \approx D_p$. We begin by first showing that G must have an element of order p. By our assumption and Lagrange's Theorem, any nonidentity element of G must have order 2 or p. Thus, to verify our assertion, we may assume that every nonidentity element of G has order 2.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In this case, we have for all a and b in the group $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, so that G is Abelian. Then, for any nonidentity elements $a, b \in G$ with $a \neq b$, the set $\{e, a, b, ab\}$ is closed and therefore is a subgroup of G of order 4. Since this contradicts Lagrange's Theorem, we have proved that G must have an element of order p; call it a.

Now let b be any element not in $\langle a \rangle$. Then by Lagrange's Theorem and our assumption that G does not have an element of order $2p$, we have that $|b| = 2$ or p. Because $|\langle a \rangle \cap \langle b \rangle|$ divides $|\langle a \rangle| = p$ and $\langle a \rangle \neq \langle b \rangle$ we have that $|\langle a \rangle \cap \langle b \rangle| = 1$. But then $|b| = 2$, for otherwise, by Theorem 7.2 $|\langle a \rangle\langle b \rangle| = |\langle a \rangle||\langle b \rangle| = p^2 > 2p = |G|$, which is impossible. So, any element of G not in $\langle a \rangle$ has order 2.

Next consider ab. Since $ab \notin \langle a \rangle$, our argument above shows that $|ab| = 2$. Then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$. Moreover, this relation completely determines the multiplication table for G. [For example, $a^3(ba^4) = a^2(ab)a^4 = a^2(ba^{-1})a^4 = a(ab)a^3 = a(ba^{-1})a^3 = (ab)a^2 = (ba^{-1})a^2 = ba$.] Since the multiplication table for all noncyclic groups of order $2p$ is uniquely determined by the relation $ab = ba^{-1}$, all noncyclic groups of order $2p$ must be isomorphic to each other. But of course, D_p, the dihedral group of order $2p$, is one such group. ∎

As an immediate corollary, we have that the non-Abelian groups S_3, the symmetric group of degree 3, and GL(2, Z_2), the group of 2×2 matrices with nonzero determinants with entries from Z_2 (see Example 19 and Exercise 51 in Chapter 2) are isomorphic to D_3.

An Application of Cosets to Permutation Groups

Lagrange's Theorem and its corollaries dramatically demonstrate the fruitfulness of the coset concept. We next consider an application of cosets to permutation groups.

Definition Stabilizer of a Point
Let G be a group of permutations of a set S. For each i in S, let $\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. We call $\text{stab}_G(i)$ the *stabilizer of i in G*.

The student should verify that $\text{stab}_G(i)$ is a subgroup of G. (See Exercise 35 in Chapter 5.)

Definition Orbit of a Point
Let G be a group of permutations of a set S. For each s in S, let $\text{orb}_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $\text{orb}_G(s)$ is a subset of S called the *orbit of s under G*. We use $|\text{orb}_G(s)|$ to denote the number of elements in $\text{orb}_G(s)$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Example 7 should clarify these two definitions.

EXAMPLE 7 Let

$$G = \{(1), (132)(465)(78), (132)(465), (123)(456), (123)(456)(78), (78)\}.$$

Then,

$\text{orb}_G(1) = \{1, 3, 2\}$, $\text{stab}_G(1) = \{(1), (78)\}$,
$\text{orb}_G(2) = \{2, 1, 3\}$, $\text{stab}_G(2) = \{(1), (78)\}$,
$\text{orb}_G(4) = \{4, 6, 5\}$, $\text{stab}_G(4) = \{(1), (78)\}$,
$\text{orb}_G(7) = \{7, 8\}$, $\text{stab}_G(7) = \{(1), (132)(465), (123)(456)\}$. ∎

EXAMPLE 8 We may view D_4 as a group of permutations of a square region. Figure 7.1(a) illustrates the orbit of the point p under D_4, and Figure 7.1(b) illustrates the orbit of the point q under D_4. Observe that $\text{stab}_{D_4}(p) = \{R_0, D\}$, whereas $\text{stab}_{D_4}(q) = \{R_0\}$. ∎

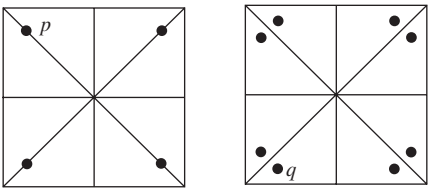


Figure 7.1

The preceding two examples also illustrate the following theorem.

Theorem 7.4 Orbit-Stabilizer Theorem

Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |\text{orb}_G(i)|\,|\text{stab}_G(i)|$.

PROOF By Lagrange's Theorem, $|G|/|\text{stab}_G(i)|$ is the number of distinct left cosets of $\text{stab}_G(i)$ in G. Thus, it suffices to establish a one-to-one correspondence between the left cosets of $\text{stab}_G(i)$ and the elements in the orbit of i. To do this, we define a correspondence T by mapping the coset $\phi\text{stab}_G(i)$ to $\phi(i)$ under T. To show that T is a well-defined function, we must show that $\alpha\text{stab}_G(i) = \beta\text{stab}_G(i)$ implies $\alpha(i) = \beta(i)$. But $\alpha\text{stab}_G(i) = \beta\text{stab}_G(i)$ implies $\alpha^{-1}\beta \in \text{stab}_G(i)$, so that $(\alpha^{-1}\beta)(i) = i$ and, therefore, $\beta(i) = \alpha(i)$. Reversing the argument from the last step to the first step shows that T is also one-to-one. We conclude

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

the proof by showing that T is onto $\text{orb}_G(i)$. Let $j \in \text{orb}_G(i)$. Then $\alpha(i) = j$ for some $\alpha \in G$ and clearly $T(\alpha \text{stab}_G(i)) = \alpha(i) = j$, so that T is onto. ∎

We leave as an exercise the proof of the important fact that the orbits of the elements of a set S under a group partition S (Exercise 43).

The Rotation Group of a Cube and a Soccer Ball

It cannot be overemphasized that Theorem 7.4 and Lagrange's Theorem (Theorem 7.1) are *counting* theorems.† They enable us to determine the numbers of elements in various sets. To see how Theorem 7.4 works, we will determine the order of the rotation group of a cube and a soccer ball. That is, we wish to find the number of essentially different ways in which we can take a cube or a soccer ball in a certain location in space, physically rotate it, and then have it still occupy its original location.

EXAMPLE 9 Let G be the rotation group of a cube. Label the six faces of the cube 1 through 6. Since any rotation of the cube must carry each face of the cube to exactly one other face of the cube and different rotations induce different permutations of the faces, G can be viewed as a group of permutations on the set $\{1, 2, 3, 4, 5, 6\}$. Clearly, there is some rotation about a central horizontal or vertical axis that carries face number 1 to any other face, so that $|\text{orb}_G(1)| = 6$. Next, we consider $\text{stab}_G(1)$. Here, we are asking for all rotations of a cube that leave face number 1 where it is. Surely, there are only four such motions—rotations of 0°, 90°, 180°, and 270°—about the line perpendicular to the face and passing through its center (see Figure 7.2). Thus, by Theorem 7.4, $|G| = |\text{orb}_G(1)|\,|\text{stab}_G(1)| = 6 \cdot 4 = 24$. ∎

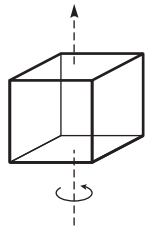


Figure 7.2 Axis of rotation of a cube.

Now that we know how many rotations a cube has, it is simple to determine the actual structure of the rotation group of a cube. Recall that S_4 is the symmetric group of degree 4.

†"People who don't count won't count" (Anatole France).

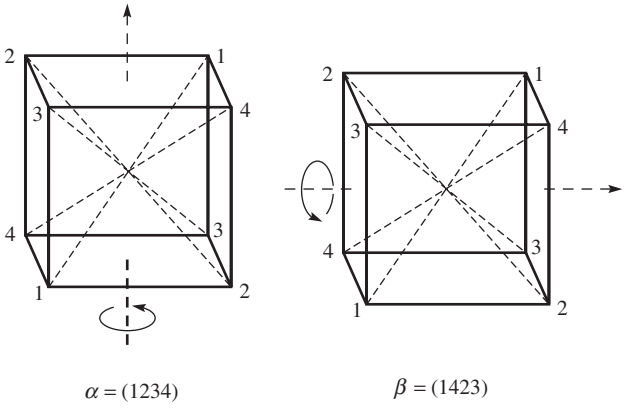
Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 7.5 The Rotation Group of a Cube

The group of rotations of a cube is isomorphic to S_4.

PROOF Since the group of rotations of a cube has the same order as S_4, we need only prove that the group of rotations is isomorphic to a subgroup of S_4. To this end, observe that a cube has four diagonals and that the rotation group induces a group of permutations on the four diagonals. But we must be careful not to assume that different rotations correspond to different permutations. To see that this is so, all we need do is show that all 24 permutations of the diagonals arise from rotations. Labeling the consecutive diagonals 1, 2, 3, and 4, it is obvious that there is a 90° rotation that yields the permutation $\alpha = (1234)$; another 90° rotation about an axis perpendicular to our first axis yields the permutation $\beta = (1423)$. See Figure 7.3. So, the group of permutations induced by the rotations contains the eight-element subgroup $\{\varepsilon, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\}$ (see Exercise 63) and $\alpha\beta$, which has order 3. Clearly, then, the rotations yield all 24 permutations, since the order of the rotation group must be divisible by both 8 and 3. ∎

EXAMPLE 10 A traditional soccer ball has 20 faces that are regular hexagons and 12 faces that are regular pentagons. (The technical term for this solid is *truncated icosahedron*.) To determine the number of rotational symmetries of a soccer ball using Theorem 7.4, we may choose our set S to be the 20 hexagons or the 12 pentagons. Let us say that S is the set of 12 pentagons. Since any pentagon can be carried to any other



$\alpha = (1234)$ $\beta = (1423)$

Figure 7.3

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

pentagon by some rotation, the orbit of any pentagon is S. Also, there are five rotations that fix (stabilize) any particular pentagon. Thus, by the Orbit-Stabilizer Theorem, there are $12 \cdot 5 = 60$ rotational symmetries. (In case you are interested, the rotation group of a soccer ball is isomorphic to A_5.) ∎

In 1985, chemists Robert Curl, Richard Smalley, and Harold Kroto caused tremendous excitement in the scientific community when they created a new form of carbon by using a laser beam to vaporize graphite. The structure of the new molecule was composed of 60 carbon atoms arranged in the shape of a soccer ball! Because the shape of the new molecule reminded them of the dome structures built by the architect R. Buckminster Fuller, Curl, Smalley, and Kroto named their discovery "buckyballs." Buckyballs are the roundest, most symmetric large molecules known. Group theory has been particularly useful in illuminating the properties of buckyballs, since the absorption spectrum of a molecule depends on its symmetries and chemists classify various molecular states according to their symmetry properties. The buckyball discovery spurred a revolution in carbon chemistry. In 1996, Curl, Smalley, and Kroto received the Nobel Prize in chemistry for their discovery.

An Application of Cosets to the Rubik's Cube

Recall from Chapter 5 that in 2010 it was proved via a computer computation, which took 35 CPU-years to complete, that every Rubik's cube could be solved in at most 20 moves. To carry out this effort, the research team of Morley Davidson, John Dethridge, Herbert Kociemba, and Tomas Rokicki applied a program of Rokicki, which built on early work of Kociemba, that checked the elements of the cosets of a subgroup H of order $(8! \cdot 8! \cdot 4!)/2 = 19{,}508{,}428{,}800$ to see if each cube in a position corresponding to the elements in a coset could be solved within 20 moves. In the rare cases where Rokicki's program did not work, an alternate method was employed. Using symmetry considerations, they were able to reduce the approximately 2 billion cosets of H

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

to about 56 million cosets for testing. Cosets played a role in this effort because Rokicki's program could handle the 19.5+ billion elements in the same coset in about 20 seconds.

Exercises

I don't know, Marge. Trying is the first step towards failure.

HOMER SIMPSON

1. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (see Table 5.1 on page 111).

2. Let H be as in Exercise 1. How many left cosets of H in S_4 are there? (Determine this without listing them.)

3. Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in Z.

4. Rewrite the condition $a^{-1}b \in H$ given in property 5 of the lemma on page 145 in additive notation. Assume that the group is Abelian.

5. Let H be as in Exercise 3. Use Exercise 4 to decide whether or not the following cosets of H are the same.
   a. $11 + H$ and $17 + H$
   b. $-1 + H$ and $5 + H$
   c. $7 + H$ and $23 + H$

6. Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in Z. How many are there?

7. Find all of the left cosets of $\{1, 11\}$ in $U(30)$.

8. Suppose that a has order 15. Find all of the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.

9. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.

10. Give an example of a group G and subgroups H and K such that $HK = \{h \in H, k \in K\}$ is not a subgroup of G.

11. If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.

12. Let a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

13. Let H be a subgroup of $\mathbf{R}^*$, the group of nonzero real numbers under multiplication. If $\mathbf{R}^+ \subseteq H \subseteq \mathbf{R}^*$, prove that $H = \mathbf{R}^+$ or $H = \mathbf{R}^*$.

14. Let $\mathbf{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbf{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

15. Let G be a group of order 60. What are the possible orders for the subgroups of G?

16. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

17. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

18. Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \bmod n = 1$.

19. Compute $5^{15} \bmod 7$ and $7^{13} \bmod 11$.

20. Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.

21. Suppose G is a finite group of order n and m is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.

22. Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.

23. Suppose that H is a subgroup of S_4 and that H contains (12) and (234). Prove that $H = S_4$.

24. Suppose that H and K are subgroups of G and there are elements a and b in G such that $aH \subseteq bK$. Prove that $H \subseteq K$.

25. Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.

26. Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

27. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.

28. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?

29. Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.

30. Let $|G| = 8$. Show that G must have an element of order 2.

31. Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.

32. Determine all finite subgroups of $\mathbf{C}^*$, the group of nonzero complex numbers under multiplication.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

33. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K|\,|K:H|$.

34. Suppose that a group contains elements of orders 1 through 10. What is the minimum possible order of the group?

35. Give an example of the dihedral group of smallest order that contains a subgroup isomorphic to Z_{12} and a subgroup isomorphic to Z_{20}. No need to prove anything, but explain your reasoning.

36. Show that in any group of order 100, either every element has order that is a power of a prime or there is an element of order 10.

37. Suppose that a finite Abelian group G has at least three elements of order 3. Prove that 9 divides $|G|$.

38. Prove that if G is a finite group, the index of $Z(G)$ cannot be prime.

39. Find an example of a subgroup H of a group G and elements a and b in G such that $aH \neq Hb$ and $aH \cap Hb \neq \phi$. (Compare with property 5 of cosets.)

40. Prove that a group of order 63 must have an element of order 3.

41. Let G be a group of order 100 that has a subgroup H of order 25. Prove that every element of G of order 5 is in H.

42. Let G be a group of order n and k be any integer relatively prime to n. Show that the mapping from G to G given by $g \to g^k$ is one-to-one. If G is also Abelian, show that the mapping given by $g \to g^k$ is an automorphism of G.

43. Let G be a group of permutations of a set S. Prove that the orbits of the members of S constitute a partition of S. (This exercise is referred to in this chapter and in Chapter 29.)

44. Prove that every subgroup of D_n of odd order is cyclic.

45. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.

- **a.** Find the stabilizer of 1 and the orbit of 1.
- **b.** Find the stabilizer of 3 and the orbit of 3.
- **c.** Find the stabilizer of 5 and the orbit of 5.

46. Prove that a group of order 12 must have an element of order 2.

47. Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all a in G.

48. Let G be a group of order pqr, where p, q, and r are distinct primes. If H and K are subgroups of G with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$.

49. Prove that a group that has more than one subgroup of order 5 must have order at least 25.

50. Prove that A_5 has a subgroup of order 12.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

51. Prove that A_5 has no subgroup of order 30.

52. Prove that A_5 has no subgroup of order 15 to 20.

53. Suppose that α is an element from a permutation group G and one of its cycles in disjoint cycle form is $(a_1a_2\cdots a_k)$. Show that $\{a_1, a_2, \ldots, a_k\} \subseteq \text{orb}_G(a_i)$ for $1 = 1, 2, \ldots, k$.

54. Let G be a group and suppose that H is a subgroup of G with the property that for any a in G we have $aH = Ha$. (That is, every element of the form ah where h is some element of H can be written in the form h_1a for some $h_1 \in H$.) If a has order 2, prove that the set $K = H \cup aH$ is a subgroup of G. Generalize to the case that $|a| = k$.

55. Prove that A_5 is the only subgroup of S_5 of order 60.

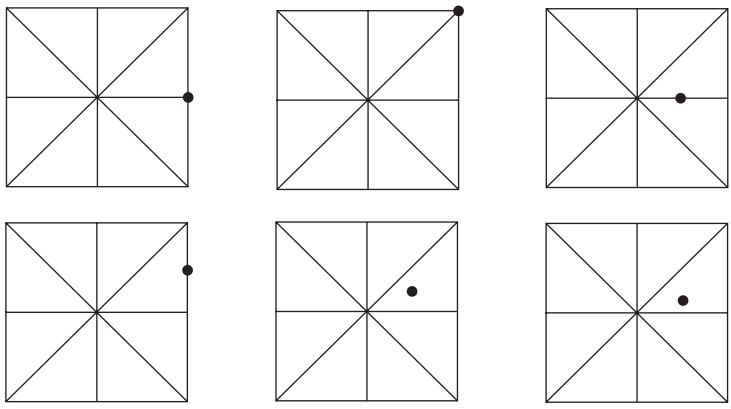
56. Why does the fact that A_4 has no subgroup of order 6 imply that $|Z(A_4)| = 1$?

57. Let $G = GL(2, \mathbf{R})$ and $H = SL(2, \mathbf{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2.

58. Let G be the group of rotations of a plane about a point P in the plane. Thinking of G as a group of permutations of the plane, describe the orbit of a point Q in the plane. (This is the motivation for the name "orbit.")

59. Let G be the rotation group of a cube. Label the faces of the cube 1 through 6, and let H be the subgroup of elements of G that carry face 1 to itself. If σ is a rotation that carries face 2 to face 1, give a physical description of the coset $H\sigma$.

60. The group D_4 acts as a group of permutations of the square regions shown below. (The axes of symmetry are drawn for reference purposes.) For each square region, locate the points in the orbit of the indicated point under D_4. In each case, determine the stabilizer of the indicated point.



Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

61. Let $G = GL(2, \mathbf{R})$, the group of 2×2 matrices over $\mathbf{R}$ with nonzero determinant. Let H be the subgroup of matrices of determinant ± 1. If $a, b \in G$ and $aH = bH$, what can be said about det (a) and det (b)? Prove or disprove the converse. [Determinants have the property that det $(xy) =$ det (x)det (y).]

62. Calculate the orders of the following (refer to Figure 27.5 for illustrations).

- **a.** The group of rotations of a regular tetrahedron (a solid with four congruent equilateral triangles as faces)
- **b.** The group of rotations of a regular octahedron (a solid with eight congruent equilateral triangles as faces)
- **c.** The group of rotations of a regular dodecahedron (a solid with 12 congruent regular pentagons as faces)
- **d.** The group of rotations of a regular icosahedron (a solid with 20 congruent equilateral triangles as faces)

63. Prove that the eight-element set in the proof of Theorem 7.5 is a group.

64. A soccer ball has 20 faces that are regular hexagons and 12 faces that are regular pentagons. Use Theorem 7.4 to explain why a soccer ball cannot have a 60° rotational symmetry about a line through the centers of two opposite hexagonal faces.

65. If G is a finite group with fewer than 100 elements and G has subgroups of orders 10 and 25, what is the order of G?

Computer Exercises

A computer exercise for this chapter is available at the website:

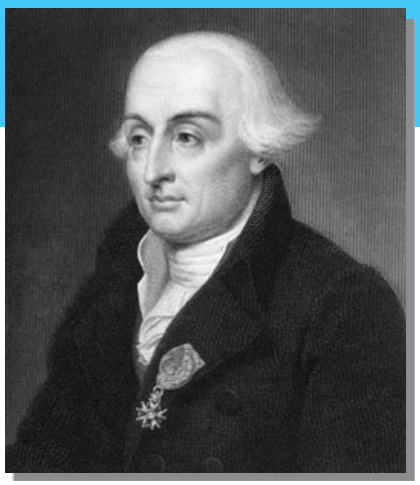
http://www.d.umn.edu/~jgallian

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Joseph Lagrange

Lagrange is the Lofty Pyramid of the Mathematical Sciences.

NAPOLEON BONAPARTE



The Granger Collection, New York

JOSEPH LOUIS LAGRANGE was born in Italy of French ancestry on January 25, 1736. He became captivated by mathematics at an early age when he read an essay by Halley on Newton's calculus. At the age of 19, he became a professor of mathematics at the Royal Artillery School in Turin. Lagrange made significant contributions to many branches of mathematics and physics, among them the theory of numbers, the theory of equations, ordinary and partial differential equations, the calculus of variations, analytic geometry, fluid dynamics, and celestial mechanics. His methods for solving third- and fourth-degree polynomial equations by radicals laid the groundwork for the group theoretic approach to solving polynomials taken by Galois. Lagrange was a very careful writer with a clear and elegant style.

At the age of 40, Lagrange was appointed head of the Berlin Academy, succeeding Euler. In offering this appointment, Frederick the Great proclaimed that the "greatest king in Europe" ought to have the "greatest mathematician in Europe" at his court. In 1787, Lagrange was invited to Paris by Louis XVI and became a good friend of the king and his wife, Marie Antoinette. In 1793, Lagrange headed a commission, which included Laplace and Lavoisier, to devise a new system of weights and measures. Out of this came the metric system. Late in his life he was made a count by Napoleon. Lagrange died on April 10, 1813.

This stamp was issued by France in Lagrange's honor in 1958.

To find more information about Lagrange, visit:

http://www-groups.dcs.st-and.ac.uk/~history/

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

8 External Direct Products

The universe is an enormous direct product of representations of symmetry groups.

STEVEN WEINBERG[†]

Definition and Examples

In this chapter, we show how to piece together groups to make larger groups. In Chapter 9, we will show that we can often start with one large group and decompose it into a product of smaller groups in much the same way as a composite positive integer can be broken down into a product of primes. These methods will later be used to give us a simple way to construct all finite Abelian groups.

Definition External Direct Product
Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

In symbols,

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\},$$

where $(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n')$ is defined to be $(g_1g_1', g_2g_2', \ldots, g_ng_n')$. It is understood that each product g_ig_i' is performed with the operation of G_i. Note that in the case that each G_i is finite, we have by properties of sets that $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1||G_2| \cdots |G_n|$. We leave it to the reader to show that the external direct product of groups is itself a group (Exercise 1).

This construction is not new to students who have had linear algebra or physics. Indeed, $\mathbf{R}^2 = \mathbf{R} \oplus \mathbf{R}$ and $\mathbf{R}^3 = \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R}$—the operation being componentwise addition. Of course, there is also scalar multiplication, but

[†]Weinberg received the 1979 Nobel Prize in physics with Sheldon Glashow and Abdus Salam for their construction of a single theory incorporating weak and electromagnetic interactions.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

we ignore this for the time being, since we are interested only in the group structure at this point.

EXAMPLE 1

$$U(8) \oplus U(10) = \{(1, 1), (1, 3), (1, 7), (1, 9), (3, 1), (3, 3), (3, 7), (3, 9), (5, 1), (5, 3), (5, 7), (5, 9), (7, 1),(7, 3), (7, 7), (7, 9)\}.$$

The product $(3, 7)(7, 9) = (5, 3)$, since the first components are combined by multiplication modulo 8, whereas the second components are combined by multiplication modulo 10. ∎

EXAMPLE 2

$$Z_2 \oplus Z_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

Clearly, this is an Abelian group of order 6. Is this group related to another Abelian group of order 6 that we know, namely, Z_6? Consider the subgroup of $Z_2 \oplus Z_3$ generated by $(1, 1)$. Since the operation in each component is addition, we have $(1, 1) = (1, 1)$, $2(1, 1) = (0, 2)$, $3(1, 1) = (1, 0)$, $4(1, 1) = (0, 1)$, $5(1, 1) = (1, 2)$, and $6(1, 1) = (0, 0)$. Hence $Z_2 \oplus Z_3$ is cyclic. It follows that $Z_2 \oplus Z_3$ is isomorphic to Z_6. ∎

In Theorem 7.3 we classified the groups of order $2p$ where p is an odd prime. Now that we have defined $Z_2 \oplus Z_2$, it is easy to classify the groups of order 4.

EXAMPLE 3 Classification of Groups of Order 4

A group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$. To verify this, let $G = \{e, a, b, ab\}$. If G is not cyclic, then it follows from Lagrange's Theorem that $|a| = |b| = |ab| = 2$. Then the mapping $e \to (0, 0)$, $a \to (1, 0)$, $b \to (0, 1)$, and $ab \to (1, 1)$ is an isomorphism from G onto $Z_2 \oplus Z_2$. ∎

We see from Examples 2 and 3 that in some cases $Z_m \oplus Z_n$ is isomorphic to Z_{mn} and in some cases it is not. Theorem 8.2 provides a simple characterization for when the isomorphism holds.

Properties of External Direct Products

Our first theorem gives a simple method for computing the order of an element in a direct product in terms of the orders of the component pieces.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Theorem 8.1 Order of an Element in a Direct Product

The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$

PROOF Denote the identity of G_i by e_i. Let $s = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$ and $t = |(g_1, g_2, \ldots, g_n)|$. Because the fact that s is a multiple of each $|g_i|$ implies that $(g_1, g_2, \ldots, g_n)^s = (g_1^s, g_2^s, \ldots, g_n^s) = (e_1, e_2, \ldots, e_n)$, we know that $t \leq s$. On the other hand, from $(g_1^t, g_2^t, \ldots, g_n^t) = (g_1, g_2, \ldots, g_n)^t = (e_1, e_2, \ldots, e_n)$ we see that t is a common multiple of $|g_1|, |g_2|, \ldots, |g_n|$. Thus, $s \leq t$. ∎

The next two examples are applications of Theorem 8.1.

EXAMPLE 4 We determine the number of elements of order 5 in $Z_{25} \oplus Z_5$. By Theorem 8.1, we may count the number of elements (a, b) in $Z_{25} \oplus Z_5$ with the property that $5 = |(a, b)| = \text{lcm}(|a|, |b|)$. Clearly this requires that either $|a| = 5$ and $|b| = 1$ or 5, or $|b| = 5$ and $|a| = 1$ or 5. We consider two mutually exclusive cases.

Case 1 $|a| = 5$ and $|b| = 1$ or 5. Here there are four choices for a (namely, 5, 10, 15, and 20) and five choices for b. This gives 20 elements of order 5.

Case 2 $|a| = 1$ and $|b| = 5$. This time there is one choice for a and four choices for b, so we obtain four more elements of order 5.

Thus, $Z_{25} \oplus Z_5$ has 24 elements of order 5. ∎

EXAMPLE 5 We determine the number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$. We begin by counting the number of elements (a, b) of order 10.

Case 1 $|a| = 10$ and $|b| = 1$ or 5. Since Z_{100} has a unique cyclic subgroup of order 10 and any cyclic group of order 10 has four generators (Theorem 4.4), there are four choices for a. Similarly, there are five choices for b. This gives 20 possibilities for (a, b).

Case 2 $|a| = 2$ and $|b| = 5$. Since any finite cyclic group of even order has a unique subgroup of order 2 (Theorem 4.4), there is only one choice for a. Obviously, there are four choices for b. So, this case yields four more possibilities for (a, b).

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Thus, $Z_{100} \oplus Z_{25}$ has 24 elements of order 10. Because each cyclic subgroup of order 10 has four elements of order 10 and no two of the cyclic subgroups can have an element of order 10 in common, there must be $24/4 = 6$ cyclic subgroups of order 10. (This method is analogous to determining the number of sheep in a flock by counting legs and dividing by 4.) ∎

The direct product notation is convenient for specifying certain subgroups of a direct product.

∎ **EXAMPLE 6** For each divisor r of m and s of n, the group $Z_m \oplus Z_n$ has a subgroup isomorphic to $Z_r \oplus Z_s$ (see Exercise 19). To find a subgroup of, say, $Z_{30} \oplus Z_{12}$ isomorphic to $Z_6 \oplus Z_4$, we observe that $\langle 5 \rangle$ is a subgroup of Z_{30} of order 6 and $\langle 3 \rangle$ is a subgroup of Z_{12} of order 4, so $\langle 5 \rangle \oplus \langle 3 \rangle$ is the desired subgroup. ∎

The next theorem and its first corollary characterize those direct products of cyclic groups that are themselves cyclic.

Theorem 8.2 Criterion for $G \oplus H$ to be Cyclic

Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

PROOF Let $|G| = m$ and $|H| = n$, so that $|G \oplus H| = mn$. To prove the first half of the theorem, we assume $G \oplus H$ is cyclic and show that m and n are relatively prime. Suppose that $\gcd(m, n) = d$ and (g, h) is a generator of $G \oplus H$. Since $(g, h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e, e)$, we have $mn = |(g, h)| \leq mn/d$. Thus, $d = 1$.

To prove the other half of the theorem, let $G = \langle g \rangle$ and $H = \langle h \rangle$ and suppose $\gcd(m, n) = 1$. Then, $|(g, h)| = \text{lcm}(m, n) = mn = |G \oplus H|$, so that (g, h) is a generator of $G \oplus H$. ∎

As a consequence of Theorem 8.2 and an induction argument, we obtain the following extension of Theorem 8.2.

Corollary 1 Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to Be Cyclic

An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Corollary 2 Criterion for $Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$

Let $m = n_1 n_2 \cdots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

By using the results above in an iterative fashion, one can express the same group (up to isomorphism) in many different forms. For example, we have

$$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5 \approx Z_2 \oplus Z_{30}.$$

Similarly,

$$\begin{aligned} Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 &\approx Z_2 \oplus Z_6 \oplus Z_5 \\ &\approx Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5 \approx Z_6 \oplus Z_{10}. \end{aligned}$$

Thus, $Z_2 \oplus Z_{30} \approx Z_6 \oplus Z_{10}$. Note, however, that $Z_2 \oplus Z_{30} \not\approx Z_{60}$.

The Group of Units Modulo *n* as an External Direct Product

The U-groups provide a convenient way to illustrate the preceding ideas. We first introduce some notation. If k is a divisor of n, let

$$U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}.$$

For example, $U_7(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}$. It can be readily shown that $U_k(n)$ is indeed a subgroup of $U(n)$. (See Exercise 31 in Chapter 3.)

Theorem 8.3 $U(n)$ as an External Direct Product

Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,

$$U(st) \approx U(s) \oplus U(t).$$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

PROOF An isomorphism from $U(st)$ to $U(s) \oplus U(t)$ is $x \to (x \bmod s, x \bmod t)$; an isomorphism from $U_s(st)$ to $U(t)$ is $x \to x \bmod t$; an isomorphism from $U_t(st)$ to $U(s)$ is $x \to x \bmod s$. We leave the verification that these mappings are operation-preserving, one-to-one, and onto to the reader. (See Exercises 9, 17, and 19 in Chapter 0; see also [1].) ∎

As a consequence of Theorem 8.3, we have the following result.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Corollary

Let $m = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

To see how these results work, let's apply them to $U(105)$. We obtain

$$\begin{aligned} U(105) &\approx U(7) \oplus U(15), \\ U(105) &\approx U(21) \oplus U(5), \\ U(105) &\approx U(3) \oplus U(5) \oplus U(7). \end{aligned}$$

Moreover,

$$\begin{aligned} U(7) &\approx U_{15}(105) = \{1, 16, 31, 46, 61, 76\}, \\ U(15) &\approx U_{7}(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}, \\ U(21) &\approx U_{5}(105) = \{1, 11, 16, 26, 31, 41, 46, 61, 71, 76, 86, 101\}, \\ U(5) &\approx U_{21}(105) = \{1, 22, 43, 64\}, \\ U(3) &\approx U_{35}(105) = \{1, 71\}. \end{aligned}$$

Among all groups, surely the cyclic groups Z_n have the simplest structures and, at the same time, are the easiest groups with which to compute. Direct products of groups of the form Z_n are only slightly more complicated in structure and computability. Because of this, algebraists endeavor to describe a finite Abelian group as such a direct product. Indeed, we shall soon see that every finite Abelian group can be so represented. With this goal in mind, let us reexamine the U-groups. Using the corollary to Theorem 8.3 and the facts (see [2, p. 93]), first proved by Carl Gauss in 1801, that

$$U(2) \approx \{0\}, \qquad U(4) \approx Z_2, \qquad U(2^n) \approx Z_2 \oplus Z_{2^{n-2}} \qquad \text{for } n \geq 3,$$

and

$$U(p^n) \approx Z_{p^n - p^{n-1}} \qquad \text{for } p \text{ an odd prime},$$

we now can write any U-group as an external direct product of cyclic groups. For example,

$$\begin{aligned} U(105) = U(3 \cdot 5 \cdot 7) &\approx U(3) \oplus U(5) \oplus U(7) \\ &\approx Z_2 \oplus Z_4 \oplus Z_6 \end{aligned}$$

and

$$\begin{aligned} U(720) = U(16 \cdot 9 \cdot 5) &\approx U(16) \oplus U(9) \oplus U(5) \\ &\approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4. \end{aligned}$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

What is the advantage of expressing a group in this form? Well, for one thing, we immediately see that the orders of the elements $U(720)$ can only be 1, 2, 3, 4, 6, and 12. This follows from the observations that an element from $Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$ has the form (a, b, c, d), where $|a| = 1$ or 2, $|b| = 1$, 2, or 4, $|c| = 1$, 2, 3, or 6, and $|d| = 1$, 2, or 4, and that $|(a, b, c, d)| = \text{lcm}(|a|, |b|, |c|, |d|)$. For another thing, we can readily determine the number of elements of order 12, say, that $U(720)$ has. Because $U(720)$ is isomorphic to $Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$, it suffices to calculate the number of elements of order 12 in $Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$. But this is easy. By Theorem 8.1, an element (a, b, c, d) has order 12 if and only if $\text{lcm}(|a|, |b|, |c|, |d|) = 12$. Since $|a| = 1$ or 2, it does not matter how a is chosen. So, how can we have $\text{lcm}(|b|, |c|, |d|) = 12$? One way is to have $|b| = 4$, $|c| = 3$ or 6, and d arbitrary. By Theorem 4.4, there are two choices for b, four choices for c, and four choices for d. So, in this case, we have $2 \cdot 4 \cdot 4 = 32$ choices. The only other way to have $\text{lcm}(|b|, |c|, |d|) = 12$ is for $|d| = 4$, $|c| = 3$ or 6, and $|b| = 1$ or 2 (we exclude $|b| = 4$, since this was already accounted for). This gives $2 \cdot 4 \cdot 2 = 16$ new choices. Finally, since a can be either of the two elements in Z_2, we have a total of $2(32 + 16) = 96$ elements of order 12.

These calculations tell us more. Since $\text{Aut}(Z_{720})$ is isomorphic to $U(720)$, we also know that there are 96 automorphisms of Z_{720} of order 12. Imagine trying to deduce this information directly from $U(720)$ or, worse yet, from $\text{Aut}(Z_{720})$! These results beautifully illustrate the advantage of being able to represent a finite Abelian group as a direct product of cyclic groups. They also show the value of our theorems about $\text{Aut}(Z_n)$ and $U(n)$. After all, theorems are labor-saving devices. If you want to convince yourself of this, try to prove directly from the definitions that $\text{Aut}(Z_{720})$ has exactly 96 elements of order 12.

Applications

We conclude this chapter with five applications of the material presented here—three to cryptography, the science of sending and deciphering secret messages, one to genetics, and one to electric circuits.

Data Security

Because computers are built from two-state electronic components, it is natural to represent information as strings of 0s and 1s called *binary strings*. A binary string of length n can naturally be thought of as an element of $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ (n copies) where the parentheses and the commas have been deleted. Thus the binary string

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

11000110 corresponds to the element (1, 1, 0, 0, 0, 1, 1, 0) in $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$. Similarly, two binary strings $a_1a_2 \cdots a_n$ and $b_1b_2 \cdots b_n$ are added componentwise modulo 2 just as their corresponding elements in $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ are. For example,

$$11000111 + 01110110 = 10110001$$

and

$$10011100 + 10011100 = 00000000.$$

The fact that the sum of two binary sequences $a_1a_2 \cdots a_n + b_1b_2 \cdots b_n = 00 \cdots 0$ if and only if the sequences are identical is the basis for a data security system used to protect Internet transactions.

Suppose that you want to purchase a compact disc from **http://www.amazon.com**. Need you be concerned that a hacker will intercept your credit-card number during the transaction? As you might expect, your credit-card number is sent to Amazon in a way that protects the data. We explain one way to send credit-card numbers over the Web securely. When you place an order with Amazon, the company sends your computer a randomly generated string of 0's and 1's called a *key*. This key has the same length as the binary string corresponding to your credit-card number and the two strings are added (think of this process as "locking" the data). The resulting sum is then transmitted to Amazon. Amazon in turn adds the same key to the received string, which then produces the original string corresponding to your credit-card number (adding the key a second time "unlocks" the data).

To illustrate the idea, say you want to send an eight-digit binary string such as $s = 10101100$ to Amazon (actual credit-card numbers have very long strings) and Amazon sends your computer the key $k = 00111101$. Your computer returns the string $s + k = 10101100 + 00111101 = 10010001$ to Amazon, and Amazon adds k to this string to get $10010001 + 00111101 = 10101100$, which is the string representing your credit-card number. If someone intercepts the number $s + k = 10010001$ during transmission it is no value without knowing k.

The method is secure because the key sent by Amazon is randomly generated and used only one time. You can tell when you are using an encryption scheme on a Web transaction by looking to see if the Web address begins with "https" rather than the customary "http." You will also see a small padlock in the status bar at the bottom of the browser window.

Public Key Cryptography

Unlike auctions such as those on eBay, where each bid is known by everyone, a silent auction is one in which each bid is secret. Suppose that you wanted to use your Twitter account to run a silent auction.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

How could a scheme be devised so that users could post their bids in such a way that the amounts are intelligible only to the account holder? In the mid-1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman devised an ingenious method that permits each person who is to receive a secret message to tell publicly how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message. The idea is based on the fact that there exist efficient methods for finding very large prime numbers (say about 100 digits long) and for multiplying large numbers, but no one knows an efficient algorithm for factoring large integers (say about 200 digits long). The person who is to receive the message chooses a pair of large primes p and q and chooses an integer e (called the *encryption exponent*) with $1 < e < m$, where $m = \text{lcm}\,(p - 1, q - 1)$, such that e is relatively prime to m (any such e will do). This person calculates $n = pq$ (n is called the *key*) and announces that a message M is to be sent to him or her publicly as $M^e \bmod n$. Although e, n, and M^e are available to everyone, only the person who knows how to factor n as pq will be able to decipher the message.

To present a simple example that nevertheless illustrates the principal features of the method, say we wish to send the messages "YES." We convert the message into a string of digits by replacing A by 01, B by 02, . . . , Z by 26, and a blank by 00. So, the message YES becomes 250519. To keep the numbers involved from becoming too unwieldy, we send the message in blocks of four digits and fill in with blanks when needed. Thus, the messages YES is represented by the two blocks 2505 and 1900. The person to whom the message is to be sent has picked two primes p and q, say $p = 37$ and $q = 73$, and a number e that has no prime divisors in common with $\text{lcm}\,(p - 1, q - 1) = 72$, say $e = 5$, and has published $n = 37 \cdot 73 = 2701$ and $e = 5$ in a public forum. We will send the "scrambled" numbers $(2505)^5 \bmod 2701$ and $(1900)^5 \bmod 2701$ rather than 2505 and 1900, and the receiver will unscramble them. We show the work involved for us and the receiver only for the block 2505. We determine $(2505)^5 \bmod 2701 = 2415$ by using a modular arithmetic calculator such as the one at **http://users.wpi.edu/~martin/mod.html**.†

†Provided that the numbers are not too large, the Google search engine at **http://www.google.com** will do modular arithmetic. For example, entering 2505^2 mod 2701 in the search box yields 602. Be careful, however: Entering 2505^5 mod 2701 does not return a value, because 2505^5 is too large. Instead, we can use Google to compute smaller powers such as 2505^2 mod 2701 and 2505^3 mod 2701 (which yields 852) and then enter $(852 \times 602) \bmod 2701$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Thus, the number 2415 is sent to the receiver. Now the receiver must take this number and convert it back to 2505. To do so, the receiver takes the two factors of 2701, $p = 37$ and $q = 73$, and calculates the least common multiple of $p - 1 = 36$ and $q - 1 = 72$, which is 72. (This is where the knowledge of p and q is necessary.) Next, the receiver must find $e^{-1} = d$ (called the *decryption exponent*) in $U(72)$—that is, solve the equation $5 \cdot d = 1 \bmod 72$. This number is 29. See **http://www.d.umn.edu/~jgallian/msproject06/chap8.html #chap8ex5** or use a Google search box to compute 5^k for each divisor k of $|U(72)| = \phi(9) \cdot \phi(8) = 24$ starting with 2 until we reach $5^k \bmod 72 = 1$. Doing so, we obtain $5^6 \bmod 72 = 1$, which implies that $5^5 \bmod 72 = 29$ is 5^{-1} in $U(72)$.

Then the receiver takes the number received, 2415, and calculates $(2415)^{29} \bmod 2701 = 2505$, the encoded number. Thus, the receiver correctly determines the code for "YE." On the other hand, without knowing how pq factors, one cannot find the modulus (in our case, 72) that is needed to determine the decryption exponent d.

The procedure just described is called the *RSA public key encryption scheme* in honor of the three people (Rivest, Shamir, and Adleman) who discovered the method. It is widely used in conjunction with web servers and browsers, e-mail programs, remote login sessions, and electronic financial transactions. The algorithm is summarized below.

Receiver

1. Pick very large primes p and q and compute $n = pq$.
2. Compute the least common multiple of $p - 1$ and $q - 1$; let us call it m.
3. Pick e relatively prime to m.
4. Find d such that $ed \bmod m = 1$.
5. Publicly announce n and e.

Sender

1. Convert the message to a string of digits.
2. Break up the message into uniform blocks of digits; call them M_1, M_2,…, M_k.
3. Check to see that the greatest common divisor of each M_i and n is 1. If not, n can be factored and our code is broken. (In practice, the primes p and q are so large that they exceed all M_i, so this step may be omitted.)
4. Calculate and send $R_i = M_i^e \bmod n$.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Receiver

1. For each received message R_i, calculate $R_i^d \bmod n$.
2. Convert the string of digits back to a string of characters.

Why does this method work? Well, we know that $U(n) \approx U(p) \oplus U(q) \approx Z_{p-1} \oplus Z_{q-1}$. Thus, an element of the form x^m in $U(n)$ corresponds under an isomorphism to one of the form (mx_1, mx_2) in $Z_{p-1} \oplus Z_{q-1}$. Since m is the least common multiple of $p - 1$ and $q - 1$, we may write $m = s(p - 1)$ and $m = t(q - 1)$ for some integers s and t. Then $(mx_1, mx_2) = (s(p - 1)x_1, t(q - 1)x_2) = (0, 0)$ in $Z_{p-1} \oplus Z_{q-1}$, and it follows that $x^m = 1$ for all x in $U(n)$. So, because each message M_i is an element of $U(n)$ and e was chosen so that $ed = 1 + km$ for some k, we have, modulo n,

$$R_i^d = (M_i^e)^d = M_i^{ed} = M_i^{\,1+km} = M_i(M_i^m)^k = M_i 1^k = M_i.$$

In 2002, Ronald Rivest, Adi Shamir, and Leonard Adleman received the Association for Computing Machinery A. M. Turing Award, which is considered the "Nobel Prize of computing," for their contribution to public key cryptography.

An RSA calculator that does all the calculations is provided at **http://www.d.umn.edu/~jgallian/msproject06/chap8.html#chap8ex5**. A list of primes can be found by searching the Web for "list of primes."

Digital Signatures

With so many financial transactions now taking place electronically, the problem of authenticity is paramount. How is a stockbroker to know that an electronic message she receives that tells her to sell one stock and buy another actually came from her client? The technique used in public key cryptography allows for digital signatures as well. Let us say that person A wants to send a secret message to person B in such a way that only B can decode the message and B will know that only A could have sent it. Abstractly, let E_A and D_A denote the algorithms that A uses for encryption and decryption, respectively, and let E_B and D_B denote the algorithms that B uses for encryption and decryption, respectively. Here we assume that E_A and E_B are available to the public, whereas D_A is known only to A and D_B is known only to B, and that $D_B E_B$ and $E_A D_A$ applied to any message leaves the message unchanged. Then A sends a message M to B as $E_B(D_A(M))$ and B decodes the received message by applying the function $E_A D_B$ to it to obtain

$$(E_A D_B)\,(E_B(D_A(M)) = E_A(D_B E_B)(D_A(M)) = E_A(D_A(M)) = M.$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Notice that only A can execute the first step (i.e., create $D_A(M)$) and only B can implement the last step (i.e., apply $E_A D_B$ to the received message).

Transactions using digital signatures became legally binding in the United States in October 2000.

Genetics†

The genetic code can be conveniently modeled using elements of $Z_4 \oplus Z_4 \oplus \cdots \oplus Z_4$, where we omit the parentheses and the commas and just use strings of 0's, 1's, 2's, and 3's and add componentwise modulo 4. A DNA molecule is composed of two long strands in the form of a double helix. Each strand is made up of strings of the four nitrogen bases adenine (A), thymine (T), guanine (G), and cytosine (C). Each base on one strand binds to a complementary base on the other strand. Adenine always is bound to thymine, and guanine always is bound to cytosine. To model this process, we identify A with 0, T with 2, G with 1, and C with 3. Thus, the DNA segment ACGTAACAGGA and its complement segment TGCATTGTCCT are denoted by 03120030110 and 21302212332. Noting that in Z_4, $0 + 2 = 2$, $2 + 2 = 0$, $1 + 2 = 3$, and $3 + 2 = 1$, we see that adding 2 to elements of Z_4 interchanges 0 and 2 and 1 and 3. So, for any DNA segment $a_1 a_2 \cdots a_n$ represented by elements of $Z_4 \oplus Z_4 \oplus \cdots \oplus Z_4$, we see that its complementary segment is represented by $a_1 a_2 \cdots a_n + 22 \cdots 2$.

Electric Circuits

Many homes have light fixtures that are operated by a pair of switches. They are wired so that when either switch is thrown, the light changes its status (from on to off or vice versa). Suppose the wiring is done so that the light is on when both switches are in the up position. We can conveniently think of the states of the two switches as being matched with the elements of $Z_2 \oplus Z_2$, with the two switches in the up position corresponding to (0, 0) and the two switches in the down position corresponding to (1, 1). Each time a switch is thrown, we add 1 to the corresponding component in the group $Z_2 \oplus Z_2$. We then see that the lights are on when the switches correspond to the elements of the subgroup $\langle (1, 1) \rangle$ and are off when the switches correspond to the elements in the coset $(1, 0) + \langle (1, 1) \rangle$. A similar analysis applies in the case of three switches, with the subgroup $\{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$ corresponding to the lights-on situation.

†This discussion is adapted from [3].

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Exercises

What's the most difficult aspect of your life as a mathematician, Diane Maclagan, an assistant professor at Rutgers, was asked. "Trying to prove theorems," she said. And the most fun? "Trying to prove theorems."

1. Prove that the external direct product of any finite number of groups is a group. (This exercise is referred to in this chapter.)

2. Show that $Z_2 \oplus Z_2 \oplus Z_2$ has seven subgroups of order 2.

3. Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.

4. Show that $G \oplus H$ is Abelian if and only if G and H are Abelian. State the general case.

5. Prove or disprove that $Z \oplus Z$ is a cyclic group.

6. Prove, by comparing orders of elements, that $Z_8 \oplus Z_2$ is not isomorphic to $Z_4 \oplus Z_4$.

7. Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$. State the general case.

8. Is $Z_3 \oplus Z_9$ isomorphic to Z_{27}? Why?

9. Is $Z_3 \oplus Z_5$ isomorphic to Z_{15}? Why?

10. How many elements of order 9 does $Z_3 \oplus Z_9$ have? (Do not do this exercise by brute force.)

11. How many elements of order 4 does $Z_4 \oplus Z_4$ have? (Do not do this by examining each element.) Explain why $Z_4 \oplus Z_4$ has the same number of elements of order 4 as does $Z_{8000000} \oplus Z_{400000}$. Generalize to the case $Z_m \oplus Z_n$.

12. Give examples of four groups of order 12, no two of which are isomorphic. Give reasons why no two are isomorphic.

13. For each integer $n > 1$, give examples of two nonisomorphic groups of order n^2.

14. The dihedral group D_n of order $2n$ ($n \geq 3$) has a subgroup of n rotations and a subgroup of order 2. Explain why D_n cannot be isomorphic to the external direct product of two such groups.

15. Prove that the group of complex numbers under addition is isomorphic to $\mathbf{R} \oplus \mathbf{R}$.

16. Suppose that $G_1 \approx G_2$ and $H_1 \approx H_2$. Prove that $G_1 \oplus H_1 \approx G_2 \oplus H_2$. State the general case.

17. If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.

18. In $Z_{40} \oplus Z_{30}$, find two subgroups of order 12.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

19. If r is a divisor of m and s is a divisor of n, find a subgroup of $Z_m \oplus Z_n$ that is isomorphic to $Z_r \oplus Z_s$.

20. Find a subgroup of $Z_{12} \oplus Z_{18}$ that is isomorphic to $Z_9 \oplus Z_4$.

21. Let G and H be finite groups and $(g, h) \in G \oplus H$. State a necessary and sufficient condition for $\langle (g, h) \rangle = \langle g \rangle \oplus \langle h \rangle$.

22. Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $Z_{30} \oplus Z_{20}$.

23. What is the order of any nonidentity element of $Z_3 \oplus Z_3 \oplus Z_3$? Generalize.

24. Let $m > 2$ be an even integer and let $n > 2$ be an odd integer. Find a formula for the number of elements of order 2 in $D_m \oplus D_n$.

25. Let M be the group of all real 2×2 matrices under addition. Let $N = \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R} \oplus \mathbf{R}$ under componentwise addition. Prove that M and N are isomorphic. What is the corresponding theorem for the group of $m \times n$ matrices under addition?

26. The group $S_3 \oplus Z_2$ is isomorphic to one of the following groups: Z_{12}, $Z_6 \oplus Z_2$, A_4, D_6. Determine which one by elimination.

27. Let G be a group, and let $H = \{(g, g) \mid g \in G\}$. Show that H is a subgroup of $G \oplus G$. (This subgroup is called the *diagonal* of $G \oplus G$.) When G is the set of real numbers under addition, describe $G \oplus G$ and H geometrically.

28. Find a subgroup of $Z_4 \oplus Z_2$ that is not of the form $H \oplus K$, where H is a subgroup of Z_4 and K is a subgroup of Z_2.

29. Find all subgroups of order 3 in $Z_9 \oplus Z_3$.

30. Find all subgroups of order 4 in $Z_4 \oplus Z_4$.

31. What is the largest order of any element in $Z_{30} \oplus Z_{20}$?

32. What is the order of the largest cyclic subgroup of $Z_6 \oplus Z_{10} \oplus Z_{15}$? What is the order of the largest cyclic subgroup of $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$?

33. Find three cyclic subgroups of maximum possible order in $Z_6 \oplus Z_{10} \oplus Z_{15}$ of the form $\langle a \rangle \oplus \langle b \rangle \oplus \langle c \rangle$, where $a \in Z_6$, $b \in Z_{10}$, and $c \in Z_{15}$.

34. How many elements of order 2 are in $Z_{2000000} \oplus Z_{4000000}$? Generalize.

35. Find a subgroup of $Z_{800} \oplus Z_{200}$ that is isomorphic to $Z_2 \oplus Z_4$.

36. Find a subgroup of $Z_{12} \oplus Z_4 \oplus Z_{15}$ that has order 9.

37. Prove that $\mathbf{R}^* \oplus \mathbf{R}^*$ is not isomorphic to $\mathbf{C}^*$. (Compare this with Exercise 15.)

38. Let

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b \in Z_3 \right\}.$$

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

(See Exercise 48 in Chapter 2 for the definition of multiplication.) Show that H is an Abelian group of order 9. Is H isomorphic to Z_9 or to $Z_3 \oplus Z_3$?

39. Let $G = \{3^m 6^n \mid m, n \in Z\}$ under multiplication. Prove that G is isomorphic to $Z \oplus Z$. Does your proof remain valid if $G = \{3^m 9^n \mid m, n \in Z\}$?

40. Let $(a_1, a_2, \ldots, a_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Give a necessary and sufficient condition for $|(a_1, a_2, \ldots, a_n)| = \infty$.

41. Prove that $D_3 \oplus D_4 \ncong D_{12} \oplus Z_2$.

42. Determine the number of cyclic subgroups of order 15 in $Z_{90} \oplus Z_{36}$. Provide a generator for each of the subgroups of order 15.

43. List the elements in the groups $U_5(35)$ and $U_7(35)$.

44. Prove or disprove that $U(40) \oplus Z_6$ is isomorphic to $U(72) \oplus Z_4$.

45. Prove or disprove that $\boldsymbol{C}^*$ has a subgroup isomorphic to $Z_2 \oplus Z_2$.

46. Let G be a group isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{nk}$. Let x be the product of all elements in G. Describe all possibilities for x.

47. If a group has exactly 24 elements of order 6, how many cyclic subgroups of order 6 does it have?

48. For any Abelian group G and any positive integer n, let $G^n = \{g^n \mid g \in G\}$ (see Exercise 17, Supplementary Exercises for Chapters 1–4). If H and K are Abelian, show that $(H \oplus K)^n = H^n \oplus K^n$.

49. Express $\mathrm{Aut}(U(25))$ in the form $Z_m \oplus Z_n$.

50. Determine $\mathrm{Aut}(Z_2 \oplus Z_2)$.

51. Suppose that $n_1, n_2, \ldots, n_k$ are positive even integers. How many elements of order 2 does $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ have ? How many are there if we drop the requirement that $n_1, n_2, \ldots, n_k$ must be even?

52. Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{60} \oplus Z_6 \oplus Z_2$?

53. Is $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_{15} \oplus Z_4 \oplus Z_{12}$?

54. Find an isomorphism from Z_{12} to $Z_4 \oplus Z_3$.

55. How many isomorphisms are there from Z_{12} to $Z_4 \oplus Z_3$?

56. Suppose that ϕ is an isomorphism from $Z_3 \oplus Z_5$ to Z_{15} and $\phi(2, 3) = 2$. Find the element in $Z_3 \oplus Z_5$ that maps to 1.

57. If ϕ is an isomorphism from $Z_4 \oplus Z_3$ to Z_{12}, what is $\phi(2, 0)$? What are the possibilities for $\phi(1, 0)$? Give reasons for your answer.

58. Prove that $Z_5 \oplus Z_5$ has exactly six subgroups of order 5.

59. Let (a, b) belong to $Z_m \oplus Z_n$. Prove that $|(a, b)|$ divides $\mathrm{lcm}(m, n)$.

60. Let $G = \{ax^2 + bx + c \mid a, b, c \in Z_3\}$. Add elements of G as you would polynomials with integer coefficients, except use modulo 3 addition. Prove that G is isomorphic to $Z_3 \oplus Z_3 \oplus Z_3$. Generalize.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

61. Determine all cyclic groups that have exactly two generators.

62. Explain a way that a string of length n of the four nitrogen bases A, T, G, and C could be modeled with the external direct product of n copies of $Z_2 \oplus Z_2$.

63. Let p be a prime. Prove that $Z_p \oplus Z_p$ has exactly $p + 1$ subgroups of order p.

64. Give an example of an infinite non-Abelian group that has exactly six elements of finite order.

65. Give an example to show that there exists a group with elements a and b such that $|a| = \infty$, $|b| = \infty$, and $|ab| = 2$.

66. Express $U(165)$ as an external direct product of cyclic groups of the form Z_n.

67. Express $U(165)$ as an external direct product of U-groups in four different ways.

68. Without doing any calculations in $\text{Aut}(Z_{20})$, determine how many elements of $\text{Aut}(Z_{20})$ have order 4. How many have order 2?

69. Without doing any calculations in $\text{Aut}(Z_{720})$, determine how many elements of $\text{Aut}(Z_{720})$ have order 6.

70. Without doing any calculations in $U(27)$, decide how many subgroups $U(27)$ has.

71. What is the largest order of any element in $U(900)$?

72. Let p and q be odd primes and let m and n be positive integers. Explain why $U(p^m) \oplus U(q^n)$ is not cyclic.

73. Use the results presented in this chapter to prove that $U(55)$ is isomorphic to $U(75)$.

74. Use the results presented in this chapter to prove that $U(144)$ is isomorphic to $U(140)$.

75. For every $n > 2$, prove that $U(n)^2 = \{x^2 \mid x \in U(n)\}$ is a proper subgroup of $U(n)$.

76. Show that $U(55)^3 = \{x^3 \mid x \in U(55)\}$ is $U(55)$.

77. Find an integer n such that $U(n)$ contains a subgroup isomorphic to $Z_5 \oplus Z_5$.

78. Find a subgroup of order 6 in $U(700)$.

79. Show that there is a U-group containing a subgroup isomorphic to $Z_3 \oplus Z_3$.

80. Find an integer n such that $U(n)$ is isomorphic to $Z_2 \oplus Z_4 \oplus Z_9$.

81. What is the smallest positive integer k such that $x^k = e$ for all x in $U(7 \cdot 17)$? Generalize to $U(pq)$ where p and q are distinct primes.

82. If k divides m and m divides n, how are $U_m(n)$ and $U_k(n)$ related?

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

83. Let $p_1, p_2, \ldots, p_k$ be distinct odd primes and $n_1, n_2, \ldots, n_k$ be positive integers. Determine the number of elements of order 2 in $U(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$. How many are there in $U(2^n p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$ where n is at least 3?

84. Show that no U-group has order 14.

85. Show that there is a U-group containing a subgroup isomorphic to Z_{14}.

86. Show that no U-group is isomorphic to $Z_4 \oplus Z_4$.

87. Show that there is a U-group containing a subgroup isomorphic to $Z_4 \oplus Z_4$.

88. Using the RSA scheme with $p = 37$, $q = 73$, and $e = 5$, what number would be sent for the message "RM"?

89. Assuming that a message has been sent via the RSA scheme with $p = 37$, $q = 73$, and $e = 5$, decode the received message "34."

Computer Exercises

Computer exercises in this chapter are available at the website:

http://www.d.umn.edu/~jgallian

References

1. J. A. Gallian and D. Rusin, "Factoring Groups of Integers Modulo n," *Mathematics Magazine* 53 (1980): 33–36.
2. D. Shanks, *Solved and Unsolved Problems in Number Theory,* 2nd ed., New York: Chelsea, 1978.
3. S. Washburn, T. Marlowe, and C. Ryan, *Discrete Mathematics,* Reading, MA: Addison-Wesley, 1999.

Suggested Readings

Y. Cheng, "Decompositions of U-Groups," *Mathematics Magazine* 62 (1989): 271–273.

This article explores the decomposition of $U(st)$, where s and t are relatively prime, in greater detail than we have provided.

David J. Devries, "The Group of Units in Z_m," *Mathematics Magazine* 62 (1989): 340–342.

This article provides a simple proof that $U(n)$ is not cyclic when n is not of the form 1, 2, 4, p^k, or $2p^k$, where p is an odd prime.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

David R. Guichard, "When Is $U(n)$ Cyclic? An Algebraic Approach," *Mathematics Magazine* 72 (1999): 139–142.

The author provides a group theoretic proof of the fact that $U(n)$ is cyclic if and only if n is 1, 2, 4, p^k, or $2p^k$, where p is an odd prime.

Markku Niemenmaa, "A Check Digit System for Hexadecimal Numbers," *Applicable Algebra in Engineering, Communication, and Computing* 22 (2011):109–112.

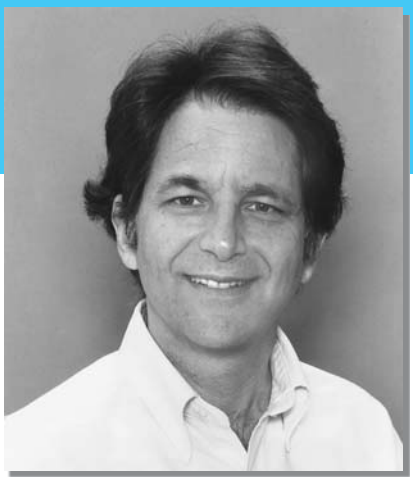
This article provides a new check-digit system for hexadecimal numbers that is based on the use of a suitable automorphism of the group $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$. It is able to detect all single errors, adjacent transpositions, twin errors, jump transpositions, and jump twin errors.

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Leonard Adleman

"For their ingenious contribution for making public-key cryptography useful in practice."

Citation for the ACM A. M. Turing Award



Leonard Aldeman

Leonard Adleman was born on December 31, 1945 in San Francisco, California. He received a B.A. degree in mathematics in 1968 and a Ph.D. degree in computer science in 1976 from the University of California, Berkeley. He spent 1976–1980 as professor of mathematics at the Massachusetts Institute of Technology where he met Ronald Rivest and Adi Shamir. Rivest and Shamir were attempting to devise a secure public key cryptosystem and asked Adleman if he could break their codes. Eventually, they invented what is now known as the RSA code that was simple to implement yet secure.

In 1983, Adleman, Shamir, and Rivest formed the RSA Data Security company to license their algorithm. Their algorithm has become the primary cryptosystem used for security on the World Wide Web. They sold their company for $200 million in 1996.

In the early 1990s, Adleman became interested in trying to find out a way to use DNA as a computer. His pioneering work on this problem lead to the field now called "DNA computing."

Among his many honors are: the Association for Computing Machinery A. M. Turing Award, the Kanallakis Award for Theory and Practice, and election to the National Academy of Engineering, the American Academy of Arts and Sciences, and the National Academy of Sciences.

Adleman's current position is the Henry Salvatori Distinguished Chair in Computer Science and Professor of Computer Science and Biological Sciences at the University of Southern California, where he has been since 1980.

For more information on Adleman, visit:

http://www.wikipedia.com

and

http://www.nytimes.com/1994/12/13/science/scientist-at-work-leonard-adleman-hitting-the-high-spots-of-computer-theory.html?pagewanted=all&src=pm

Copyright 2012 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.