

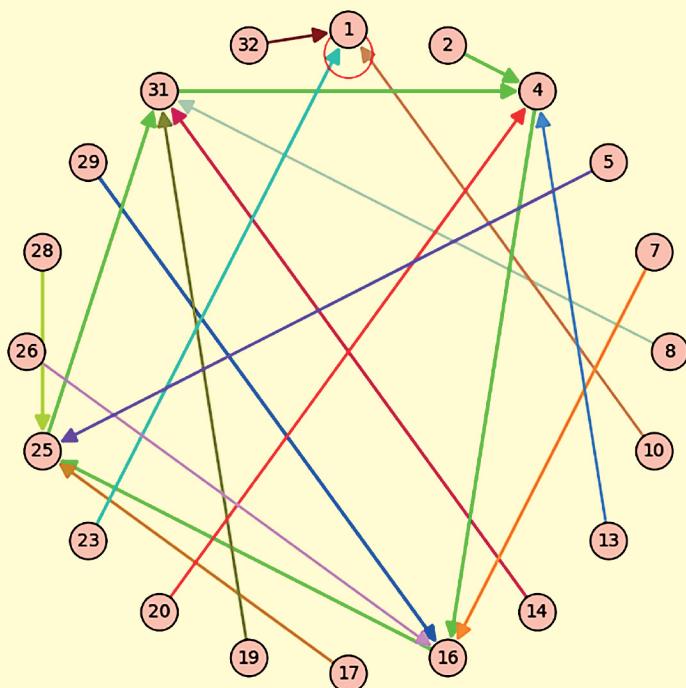
# TEXTBOOKS IN MATHEMATICS

# ABSTRACT ALGEBRA

# An Interactive Approach

# THIRD EDITION

# William Paulsen



A Chapman & Hall Book



CRC Press  
Taylor & Francis Group

# Abstract Algebra

*Abstract Algebra: An Interactive Approach, Third Edition* is a new concept in learning modern algebra. Although all the expected topics are covered thoroughly and in the most popular order, the text offers much flexibility. Perhaps more significantly, the book gives professors and students the option of including technology in their courses. Each chapter in the textbook has a corresponding interactive Mathematica notebook and an interactive SageMath workbook that can be used in either the classroom or outside the classroom.

Students will be able to visualize the important abstract concepts, such as groups and rings (by displaying multiplication tables), homomorphisms (by showing a line graph between two groups), and permutations. This, in turn, allows the students to learn these difficult concepts much more quickly and obtain a firmer grasp than with a traditional textbook. Thus, the colorful diagrams produced by Mathematica give added value to the students.

Teachers can run the Mathematica or SageMath notebooks in the classroom in order to have their students visualize the dynamics of groups and rings. Students have the option of running the notebooks at home, and experiment with different groups or rings. Some of the exercises require technology, but most are of the standard type with various difficulty levels.

The third edition is meant to be used in an undergraduate, single-semester course, reducing the breadth of coverage, size, and cost of the previous editions. Additional changes include:

- Binary operators are now in an independent section.
- The extended Euclidean algorithm is included.
- Many more homework problems are added to some sections.
- Mathematical induction is moved to [Section 1.2](#).

Despite the emphasis on additional software, the text is not short on rigor. All of the classical proofs are included, although some of the harder proofs can be shortened by using technology.

**William Paulsen** is a professor of mathematics at Arkansas State University. He is the author of *Abstract Algebra: An Interactive Approach* (CRC Press, 2009) and has published over 15 papers in applied mathematics, one of which proves that Penrose tiles can be three-colored, thus resolving a 30-year-old open problem posed by John H. Conway. Dr. Paulsen has also programmed several new games and puzzles in Javascript and C++, including Duelling Dimensions, which was syndicated through Knight Features. He received a PhD in mathematics from Washington University, St. Louis, MO.

## **Textbooks in Mathematics**

Series editors:

Al Boggess, Kenneth H. Rosen

### **A Bridge to Higher Mathematics**

*James R. Kirkwood and Raina S. Robeva*

### **Advanced Linear Algebra, Second Edition**

*Nicholas Loehr*

### **Mathematical Biology: Discrete and Differential Equations**

*Christina Alvey and Daniel Alvey*

### **Numerical Methods and Analysis with Mathematical Modelling**

*William P. Fox and Richard D. West*

### **Business Process Analytics**

Modeling, Simulation, and Design

*Manuel Laguna and Johan Marklund*

### **Quantitative Literacy Through Games and Gambling**

*Mark Hunacek*

### **Measure and Integral**

Theory and Practice

*John Srdjan Petrovic*

### **Contemporary Abstract Algebra, Eleventh Edition**

*Joseph A. Gallian*

### **Student Solutions Manual for Gallian's Contemporary Abstract Algebra, Eleventh Edition**

*Joseph A. Gallian*

### **Algebra, Second Edition**

Groups, Rings, and Fields

*Louis Halle Rowen and Uzi Vishne*

### **Functional Analysis for the Applied Mathematician**

*Todd Arbogast and Jerry L. Bona*

### **Exploring Linear Algebra, Second Edition**

Labs and Projects with Mathematica®

*Crista Arangala*

### **Measure Theory and Fine Properties of Functions, Second Edition**

*Lawrence Craig Evans and Ronald R. Gariepy*

### **Set Theory**

An Introduction to Axiomatic Reasoning

*Robert André*

### **Introduction to Differential and Difference Equations Through Modeling**

*William P. Fox and Robert E. Burks*

### **Abstract Algebra, Third Edition**

An Interactive Approach

*William Paulsen*

### **Elements of Algebraic Topology, Second Edition**

*James R. Munkres, Steven G. Krantz, and Harold R. Parks*

<https://www.routledge.com/Textbooks-in-Mathematics/book-series/CANDHTEXBOOMTH>

# Abstract Algebra

## An Interactive Approach

Third Edition

William Paulsen



CRC Press

Taylor & Francis Group

Boca Raton London New York

---

CRC Press is an imprint of the  
Taylor & Francis Group, an **informa** business  
A CHAPMAN & HALL BOOK

MATLAB® is a trademark of The MathWorks, Inc. and is used with permission. The MathWorks does not warrant the accuracy of the text or exercises in this book. This book's use or discussion of MATLAB® software or related products does not constitute endorsement or sponsorship by The MathWorks of a particular pedagogical approach or particular use of the MATLAB® software.

Third edition published 2025  
by CRC Press  
2385 Executive Center Drive, Suite 320, Boca Raton, FL 33431, U.S.A.

and by CRC Press  
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

*CRC Press is an imprint of Taylor & Francis Group, LLC*

© 2025 William Paulsen

First edition CRC Press 2009  
Second edition CRC Press 2016

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access [www.copyright.com](http://www.copyright.com) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact [mpkbookspermissions@tandf.co.uk](mailto:mpkbookspermissions@tandf.co.uk)

*Trademark notice:* Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-1-032-98540-4 (hbk)  
ISBN: 978-1-032-98646-3 (pbk)  
ISBN: 978-1-003-59976-0 (ebk)

DOI: [10.1201/9781003599760](https://doi.org/10.1201/9781003599760)

Typeset in CMR10 font  
by KnowledgeWorks Global Ltd.

Publisher's note: This book has been prepared from camera-ready copy provided by the authors.

Access support material at <https://www.routledge.com/9781032985404>

---

# Contents

<b>List of Figures</b>	vii
<b>List of Tables</b>	ix
<b>Preface for Students</b>	xi
<b>Preface for Instructors</b>	xiii
<b>Acknowledgments</b>	xvii
<b>About the Author</b>	xix
<b>Symbol Description</b>	xxi
<b>Installing the Notebooks</b>	xxiii
<b>1 Preliminaries</b>	1
1.1 Integer Factorization . . . . .	1
1.2 Functions . . . . .	12
1.3 Binary Operators . . . . .	21
1.4 Modular Arithmetic . . . . .	27
1.5 Rational and Real Numbers . . . . .	34
<b>2 Understanding the Group Concept</b>	43
2.1 Introduction to Groups . . . . .	43
2.2 Modular Congruence . . . . .	49
2.3 The Definition of a Group . . . . .	59
<b>3 The Structure within a Group</b>	68
3.1 Generators of Groups . . . . .	68
3.2 Defining Finite Groups in <i>SageMath</i> . . . . .	75
3.3 Subgroups . . . . .	83
<b>4 Patterns within the Cosets of Groups</b>	96
4.1 Left and Right Cosets . . . . .	96
4.2 Writing Secret Messages . . . . .	105
4.3 Normal Subgroups . . . . .	116
4.4 Quotient Groups . . . . .	122

<b>5 Mappings between Groups</b>	<b>127</b>
5.1 Isomorphisms . . . . .	127
5.2 Homomorphisms . . . . .	136
5.3 The Three Isomorphism Theorems . . . . .	145
<b>6 Permutation Groups</b>	<b>157</b>
6.1 Symmetric Groups . . . . .	157
6.2 Cycles . . . . .	164
6.3 Cayley's Theorem . . . . .	173
6.4 Numbering the Permutations . . . . .	184
<b>7 Building Larger Groups from Smaller Groups</b>	<b>190</b>
7.1 The Direct Product . . . . .	190
7.2 The Fundamental Theorem of Finite Abelian Groups . . . . .	198
7.3 Automorphisms . . . . .	210
7.4 Semi-Direct Products . . . . .	222
<b>8 The Search for Normal Subgroups</b>	<b>233</b>
8.1 The Center of a Group . . . . .	233
8.2 The Normalizer and Normal Closure Subgroups . . . . .	239
8.3 Conjugacy Classes and Simple Groups . . . . .	243
8.4 Subnormal Series and the Jordan-Hölder Theorem . . . . .	255
8.5 Solving the Pyraminx <sup>TM</sup> . . . . .	264
<b>9 Introduction to Rings</b>	<b>274</b>
9.1 The Definition of a Ring . . . . .	274
9.2 Entering Finite Rings into <i>SageMath</i> . . . . .	283
9.3 Some Properties of Rings . . . . .	293
<b>10 The Structure within Rings</b>	<b>300</b>
10.1 Subrings . . . . .	300
10.2 Quotient Rings and Ideals . . . . .	306
10.3 Ring Isomorphisms . . . . .	316
10.4 Homomorphisms and Kernels . . . . .	326
<b>11 Integral Domains and Fields</b>	<b>336</b>
11.1 Polynomial Rings . . . . .	336
11.2 The Field of Quotients . . . . .	346
11.3 Complex Numbers . . . . .	355
<b>Answers to Odd-Numbered Problems</b>	<b>371</b>
<b>Bibliography</b>	<b>399</b>
<b>Index</b>	<b>401</b>

---

# List of Figures

1.1	Plot depicting the rational numbers . . . . .	35
1.2	Sample path going through every rational . . . . .	36
2.1	Terry's animated dance steps . . . . .	44
2.2	Circle graphs for modulo 10 operations . . . . .	54
3.1	Circle graph of adding 3 <b>mod</b> 10 . . . . .	69
3.2	Visualizing arrangements of three books . . . . .	78
3.3	Rotations of the octahedron . . . . .	80
3.4	Pyraminx <sup>TM</sup> puzzle . . . . .	92
4.1	Circle graph of adding 4 <b>mod</b> 10 . . . . .	97
4.2	Circle graphs revealing cosets of Terry's group . . . . .	97
4.3	Circle graph for squaring in $Z_{33}^*$ . . . . .	105
4.4	Circle graph for cubing in $Z_{33}^*$ . . . . .	106
4.5	Circle graph for cubing modulo 33 . . . . .	107
4.6	Cayley table for the quotient group . . . . .	125
5.1	Diagram of a typical homomorphism . . . . .	140
5.2	Commuting diagram for first isomorphism theorem . . . . .	147
5.3	Commuting diagram for second isomorphism theorem . . . . .	151
5.4	Commuting diagram for third isomorphism theorem . . . . .	155
6.1	Circle graph for a typical permutations . . . . .	162
6.2	Circle graph of a typical cycle . . . . .	165
6.3	Circle graphs for multiplying elements of $Q$ by $i$ . . . . .	174
6.4	Multiplying cosets of $D_4$ by elements . . . . .	178
7.1	Circle graph for $x \rightarrow x^3$ in $Z_8$ . . . . .	211
7.2	Proof without words that $\text{Aut}(Q) \approx S_4$ . . . . .	217
8.1	Example of two subnormal series of different lengths . . . . .	258
8.2	Diagram showing the strategy of the refinement theorem . . . . .	259
8.3	Pyraminx <sup>TM</sup> without corners . . . . .	266
8.4	Pyraminx <sup>TM</sup> with numbered faces . . . . .	268
8.5	Sam Loyd's 14-15 puzzle . . . . .	271
8.6	Track puzzle with surprising group . . . . .	272

8.7 Simple puzzle with two wheels . . . . .	273
10.1 Commuting diagram for first ring isomorphism theorem . . . . .	332
11.1 Polar coordinates for a complex number . . . . .	361
11.2 The eight roots of unity . . . . .	364
11.3 Imaginary portion of complex logarithm . . . . .	367

---

# List of Tables

1.1	Extended Euclidean algorithm . . . . .	7
1.2	A non-commutative but associative binary operation . . . . .	23
2.1	Terry the triangle's dance steps . . . . .	44
2.2	Cayley table for Terry's dance steps . . . . .	45
2.3	Addition modulo 10 . . . . .	53
2.4	Multiplication modulo 7 . . . . .	55
2.5	Multiplication modulo 10 . . . . .	56
2.6	Multiplication modulo 15 . . . . .	56
3.1	Euler's totient function . . . . .	71
3.2	Cayley table of $Z_5$ . . . . .	76
3.3	Cayley table for $S_3$ . . . . .	79
4.1	Standard alpha-numeric code . . . . .	109
4.2	Another Cayley table for $S_3$ . . . . .	125
5.1	Multiplication table for $Z_{24}^*$ . . . . .	131
5.2	Multiplication table for $D_4$ . . . . .	132
5.3	Multiplication table for $Q$ . . . . .	133
5.4	Number of groups of order $n$ for composite $n$ . . . . .	134
5.5	Multiplication table for $D_5$ . . . . .	135
6.1	Table of factorials . . . . .	160
6.2	Two ways to assign permutations to the elements of $Q$ . . . . .	175
6.3	Multiplication table for $Q$ using integer representation . . . . .	186
7.1	Cayley table of $Z_4 \times Z_2$ . . . . .	191
7.2	Table of partitions . . . . .	207
7.3	Cayley table of $Z_3 \rtimes_{\phi} Z_2$ . . . . .	224
7.4	Multiplication table for $Z_5 \rtimes Z_2 \approx D_5$ . . . . .	228
8.1	<i>SageMath</i> 's Cayley table for $D_4$ . . . . .	233
8.2	Orders of the elements for the group $E$ . . . . .	268
8.3	Moves for solving the Pyraminx <sup>TM</sup> . . . . .	270
9.1	Multiplication table for the ring $Z_6$ . . . . .	275
9.2	Checklist to show which rings have which properties . . . . .	277

9.3	Addition table for a particular ring $R$	286
9.4	Multiplication table for a particular ring $R$	288
9.5	Multiplication for a non-commutative unity ring	291
9.6	$T_4$ , one of the smallest non-commutative rings	296
9.7	$T_8$ , the smallest non-commutative unity ring	297
9.8	Examples for each of the 11 possible types of ring	297
10.1	Addition and multiplication tables for a particular subring . . . . .	302
10.2	Addition table for cosets of the subring . . . . .	307
10.3	Multiplication table for the cosets of the subring . . . . .	308
10.4	Tables for a ring of order 10 . . . . .	318
10.5	Similar ring of order 10 . . . . .	318
10.6	Multiplication for the ring $2\mathbb{Z}_{20}$ . . . . .	319
10.7	Number of rings of order $n$ for $n < 32$ . . . . .	323
10.8	Ring number 51 of order 8 . . . . .	324
11.1	Addition table for “complex numbers modulo 3” . . . . .	343
11.2	Multiplication table for “complex numbers modulo 3” . . . . .	344

---

## Preface for Students

Today’s technology is full of applications of abstract algebra. As we go through the checkout line at the grocery store, we scan our items using UPS codes. We used to listen to our music from CDs encrypted with error-correcting codes that could compensate for scratches. We do financial transactions online using an encryption scheme that will foil the attempt of any eavesdroppers from gaining personal information. Economists use group theory to analyze market trends and predict financial movements, allowing more informed investment decisions. As more and more of our everyday lives are influenced by abstract algebra, the need arises for students to learn these concepts.

This book teaches these concepts of abstract algebra in a unique way: each chapter of the book has a corresponding interactive notebook that will allow students to experiment with groups and rings in a way no other textbook can. The notebooks will work with either *Mathematica*® or *SageMath*, and not only do these notebooks go through the examples mentioned in the textbook, they allow students to try out other examples, to see what tables or graphs are produced by other groups or rings. Although *Mathematica*® costs money, *SageMath* is free, and in fact can be accessed on the cloud using CoCalc (Collaborative Calculation and Data Science) at [www.cocalc.com](http://www.cocalc.com). See the section “Installing the Notebooks” for a comparison of the two programs, as well as instructions for how to install the notebooks into your computer.

Often this course will be the first course in which students will have to write proofs. Proofs can be very intimidating for students, but this book starts out with very easy proofs in §1.1, which use only the concept of integer divisors. It also helps if the students read the proofs that are included in the textbook. In the notebooks, the proofs start out as hidden, so the students can first imagine how they would proceed with the proof before revealing the actual proof. Each exercise set has a mixture of calculation problems and proof problems, both easy and more challenging. By starting out with the very easy proofs first, students can gain the courage to tackle the harder problems.

This text has many tools that will aid students. There is a symbols table, so if a student sees an unfamiliar symbol, he can look up the description in this table, and see where this symbol is first defined. The text is sprinkled with “Historical Diversions,” which are one page biographies of famous algebraic mathematicians and their contributions to abstract algebra. The answers to the odd-numbered problems are in the back, although the proofs are often abbreviated. There is an extensive index that not only lists the relevant pages for a particular terminology but also highlights the page where the term is

first defined. Lists of tables and figures allow students to find tables for a particular group or ring.

This textbook assumes that the student is familiar with only basic mathematics. There is no calculus required, in fact, most calculations are done with only integers. The book is completely self-contained, so there is no need to look at other sources for definitions. However, the book is rigorous, using the theorem-proof format which makes the important results easy to find. By familiarizing the student with the techniques of abstract algebra, the student is prepared for higher-level mathematics courses.

---

## Preface for Instructors

This textbook uses a new approach to teaching an introductory course in abstract algebra. Unlike the previous editions, this edition is streamlined for a one-semester undergraduate course, covering group theory, rings, and fields. The third edition contains over 200 new homework problems to give the instructor more options for assigning problems to students.

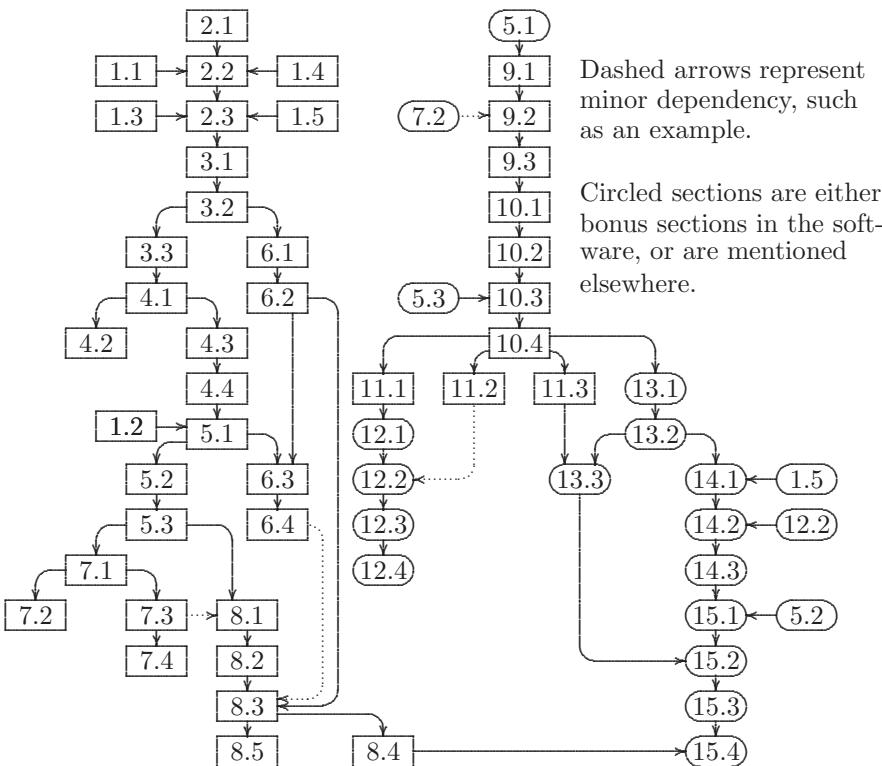
What makes this book unique is the incorporation of technology into a modern algebra course. Often the book will focus on an example or two, and guide the reader into finding patterns in these examples. As the student looks into why these patterns appear, a proof is formulated. This interaction is made possible by the use of either *SageMath* or *Mathematica* notebooks. It is recommended that the instructor use at least one of these in the classroom to allow students to visualize the group and ring concepts. (*SageMath* is totally free. See the section “Installing the Notebooks” for more information about both of these programs.) Every section includes many non-software exercises, so the students are not forced into using software. However, each section also has several interactive problems, so students can choose to use these programs to explore groups and rings. By doing these experiments, students can get a better grasp of the topic.

But despite the additional technology, this text is not short on rigor. There are still all of the classical proofs, although some of the harder proofs can be shortened with the added technology. For example, Abel’s theorem is much easier to prove if we first assume that the groups  $A_5$  and  $A_6$  are simple, which *Mathematica* or *SageMath* can verify in the classroom in a few seconds. In fact, the added technology allows students to study larger groups, such as some of the Chevalley groups.

Another feature in this book are sequences of homework problems that together formulate new results not found in the text. For example, there is a sequence that outlines a proof of Fermat’s two-square theorem, and another that finds recursively defined sequence containing every positive rational number. These sequences of problems are ideal for use as special projects for students taking the course with an honors option.

This textbook is also designed to work with a variety of different syllabi. A dependency diagram for the different sections is given below. To clarify this chart, here is a summary of each chapter with an explanation of some of the dependencies.

## Dependency Diagram for the Textbook



**Chapter 1: Preliminaries.** This chapter can be considered as a primer of the mathematics required to study abstract algebra. Undergraduate students should go over this material, although many sections will be familiar.

**Chapter 2: Understanding the Group Concept.** This chapter defines the group abstractly by first looking at several key examples, and observing the properties in common between the examples. The cyclic groups  $Z_n$  and the group of units  $Z_n^*$  are defined in terms of modular arithmetic. The non-abelian group  $D_3$  is also introduced using the featured software.

**Chapter 3: The Structure within a Group.** The basic properties of groups are developed in this chapter, including subgroups and generators. Also included in this section is a way to describe a group using generators and relations, giving us many more key examples of groups.

**Chapter 4: Patterns within the Cosets of Groups.** In this chapter, the notations of left and right cosets, normal groups, and quotient groups are developed. [Section 4.2](#), which covers RSA encryption, is optional, but with the enhancement of the software packages it is a fun section to teach.

**Chapter 5: Mappings between Groups.** This chapter discusses group isomorphisms, and then generalizes the mappings to form group homomorphisms. This in turn leads to the three isomorphism theorems.

**Chapter 6: Permutation Groups.** This chapter introduces another important class of groups, the symmetric groups  $S_n$ . The first two sections only require knowledge of §3.2, so these sections could in fact be taught earlier. But Cayley's theorem requires the concept of isomorphisms, requiring §5.1. The last section is optional, but introduces a notation for large subgroups of  $S_n$ , which comes in very handy for a number of examples.

**Chapter 7: Building Larger Groups from Smaller Groups.** As the name suggests, this chapter focuses on new ways to form groups, such as the direct product and the automorphism group. Section 6.2, on the fundamental theorem of finite abelian groups, is not needed in the remaining sections on groups, but is referred to in a key exercise in §9.2 as we consider the additive group structure of a finite ring. The final section explains how we can form even more examples of groups.

**Chapter 8: The Search for Normal Subgroups.** This chapter explores the center of a group, the normalizer, and the conjugacy classes of a group. In this chapter we prove that the alternating groups  $A_n$  from §6.2 are simple when  $n \geq 5$ , along with the group  $L_2(3)$  with 168 elements, using the notation from §6.4. We then show that the simple groups act as the building blocks for all other groups, using subnormal series. The last section is optional, but introduces a special feature of *SageMath*, not in *Mathematica*, which finds a way to express any element of a group in terms of a set of elements that generate the group. With this feature, we can solve Rubik's Cube<sup>TM</sup>-like puzzles, giving an entertaining application of group theory.

**Chapter 9: Introduction to Rings.** This chapter introducing rings only requires §5.1, so one has the option of jumping to this chapter after covering §5.1. One exercise uses the fundamental theorem of finite abelian groups, but this can be avoided if that section was not covered.

**Chapter 10: The Structure within Rings.** This chapter focuses on the parallels between groups and rings, namely the similarities between normal subgroups and ideals. The chapter culminates with the first isomorphism theorem for rings, requiring only the counterpart in §5.3 from group theory.

**Chapter 11: Integral Domains and Fields.** The book culminates with applications of abstract algebra. The first section on polynomial rings shows how we can generate larger rings from an integral domain, and sets up the problem of factorization. The next section on the field of quotients shows how we can produce a field from any integral domain. Finally, Section 11.3 gives an overview of complex numbers, using the concepts of abstract algebra.



Taylor & Francis  
Taylor & Francis Group  
<http://taylorandfrancis.com>

---

## Acknowledgments

I am very grateful to Alexander Hulpke from Colorado State University for developing the GAP package “newrings.g” specifically for the first edition of my book. This package is currently incorporated into GAP, which in turn is included in *SageMath*. Without this package, *SageMath* would not be able to work with the examples that grace [Chapters 9–11](#). Other suggestions of his have proved to be invaluable.

I also must express my thanks to Shashi Kumar at the L<sup>A</sup>T<sub>E</sub>X help desk, who helped me with several different formatting issues throughout the text.



Taylor & Francis  
Taylor & Francis Group  
<http://taylorandfrancis.com>

---

## About the Author

**William Paulsen** is a professor of mathematics at Arkansas State University. He has taught abstract algebra at both the undergraduate and graduate levels since 1997. He earned his BS (summa cum laude), MS, and PhD in mathematics at Washington University in St. Louis. He was on the winning team for the 45th William Lowell Putnam Mathematical Competition.

Dr. Paulsen has authored over 25 papers in abstract algebra and applied mathematics. Most of these papers make use of *Mathematica*®, including one which solves the tetration problem, that is, finds a unique complex function satisfying natural conditions for which  $f(z + 1) = b^{f(z)}$ . He has also authored an applied mathematics textbook, *Asymptotic Analysis and Perturbation Theory*, also published by CRC press.

Dr. Paulsen has also programmed several new games and puzzles in Javascript and C++. One of these puzzles, Duelling Dimensions, has been syndicated through Knight Features. Other puzzles and games are available on the Internet.

Dr. Paulsen lives in Harrisburg, Arkansas with his wife Cynthia, and their three dogs.



Taylor & Francis  
Taylor & Francis Group  
<http://taylorandfrancis.com>

---

# Symbol Description

$\mathbb{Z}$	The set of integers	1
$\lfloor x \rfloor$	Greatest integer less than or equal to $x$	3
$\gcd(m, n)$	The greatest common divisor of $m$ and $n$	5
$\operatorname{lcm}(m, n)$	The least common multiple of $m$ and $n$	11
$ G $	Number of elements in a set or group	15, 61
$A - \{a\}$	The set $A$ with the element $a$ removed	16
$f \circ g$	Composition of functions	16
$x * y$	Binary operation	21
$x \pmod n$	Modular arithmetic in base $n$	27
$x^{-1}$	The inverse of the element $x$	46
$(\bmod n)$	Modular equivalence in base $n$	49
$x \equiv y$	$x$ and $y$ are in the same equivalence class	49, 123
$x \cdot y$	Group multiplication	59
$e$	Identity element of a group	59
$x \in G$	$x$ is a member of the set or group $G$	60
$\mathbb{Z}_n$	The group $\{0, 1, 2, \dots, n-1\}$ using addition modulo $n$ , or the ring of the same elements	60 293
$\mathbb{Z}_n^*$	Numbers $< n$ coprime to $n$ , with multiplication mod $n$	60
$\mathbb{Q}$	The group or field of rational numbers (fractions)	61
$\mathbb{Q}^*$	Non-zero rational numbers using multiplication	61
$\mathbb{R}$	The group or field of real numbers	61
$\mathbb{R}^*$	Non-zero real numbers using multiplication	137
$x^n$	$x$ operated on itself $n$ times	62
$\phi(n)$	Euler totient function	71
$\{\dots   \dots\}$	The set of elements ... such that ...	89
$H \cap K$	The intersection of $H$ and $K$	84
$\bigcap_{H \in L} H$	The intersection of all sets in the collection $L$	84
$[S]$	Smallest subgroup containing the set $S$	85
$[x]$	Smallest subgroup containing the element $x$	86
$R_k(G)$	Number of solutions to $x^k = e$ in the group $G$	92
$xH$	A left coset of the subgroup $H$	98
$Hx$	A right coset of the subgroup $H$	98
$H \backslash G$	The collection of right cosets of $H$ in the group $G$	98
$G/H$	The collection of left cosets of $H$ in the group $G$ , or the quotient group of $G$ with respect to $H$	98 122
$G \approx M$	The group $G$ is isomorphic to $M$	128

$D_4$	The group of symmetries of a square	48, 132
$D_5$	The group of symmetries of a pentagon	228
$Q$	The quaternion group	132
$D_n$	The dihedral group with $2n$ elements	133, 228
$f : G \rightarrow M$	The function $f$ maps elements of $G$ to elements of $M$	136
$\text{Im}(f)$	The image (range) of the function $f$	140
$f^{-1}(x)$	The set of elements that map to $x$	141
$f^{-1}(H)$	The set of elements that map to an element of $H$	141
$\text{Ker}(f)$	The kernel of the homomorphism $f$ , which is $f^{-1}(e)$	141
$S_n$	The symmetric group on $n$ objects	159
$(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix})$	Permutation notation	158
$n!$	$n$ factorial = $1 \cdot 2 \cdot 3 \cdots n$	160
$(1 \ 2 \ 4 \ 6 \ 3)$	Cycle notation	165
$()$	The 0-cycle, the identity element of $S_n$	167
$\sigma(x)$	The signature function of the permutation $x$	169
$A_n$	The alternating group of permutations on $n$ objects	170
$H \times K$	The direct product of the groups $H$ and $K$	190
$P(n)$	The number of partitions of $m$	206
$\text{Aut}(G)$	The group of automorphisms of the group $G$	212
$\text{Inn}(G)$	The inner automorphisms of the group $G$	215
$\text{Out}(G)$	The outer automorphisms of the group $G$	218
$Z(G)$	The center of the group $G$	234
$N_G(H)$	The normalizer of the subset $H$ by the group $G$	239
$\mathbb{H}$	The skew field of quaternions $a + bi + cj + dk$	276
$-x$	The additive inverse of $x$	278
$nx$	$x + x + \cdots + x$ , $n$ times	283
$T_4$	The smallest non-commutative ring	296
$T_8$	The smallest non-commutative unity ring	297
$\overline{x}$	The conjugate of $x$	282, 360
$R/I$	The quotient ring of the ring $R$ by the ideal $I$	309
$X * Y$	The product of two cosets in $R/I$	309
$\langle S \rangle$	The smallest ideal containing the set $S$	312
$\langle a \rangle$	The smallest ideal containing the element $a$	312
$n\mathbb{Z}$	Multiples of $n$ (also written as $\langle n \rangle$ )	313
$kZ_{kn}$	Multiples of $k$ in the ring $Z_{kn}$	319
$\mathbb{C}$	The field of complex numbers	333, 355
$\mathbb{Z}[x]$	The polynomials with integer coefficients	337
$K[x]$	The polynomials with coefficients in the ring $K$	336
$(\frac{x}{y})$	The equivalence class of ordered pairs containing $(x, y)$	348
$ z $	The absolute value of the complex number $z$	360
$\theta$	Polar angle of a complex number	360
$e^z$	Complex exponential function	365
$\log(z)$	Complex logarithm function	366
$x^z$	Complex exponents	366
$\omega_n$	Principle $n$ -th root of unity	363

---

## *Installing the Notebooks*

This textbook incorporates either *SageMath* or *Mathematica* to help students visualize the important concepts of abstract algebra. It is recommended that one of the two programs be used with the book, but it is not necessary to have both. This section compares the two programs, and gives instructions for how to use these programs with the files that can be downloaded from websites that are mentioned below.

*Mathematica* is a symbolic manipulator package published by Wolfram Research, Inc. That is, it is a general purpose mathematical program used by scientists, engineers, and analysts. Its main feature that sets it apart from other symbolic manipulators is the graphics capabilities. In *Mathematica*, one can plot a 3-dimensional object, then use the mouse to rotate the object in three dimensions to see it from all possible angles.

*SageMath* is also a symbolic manipulator, but has the advantage of being open source. This means that it is totally free. It has slightly less graphic capabilities than *Mathematica*, but it can still graph three-dimensional objects, and rotate them. *SageMath* is also capable of interfacing with GAP, which stands for “Groups, Algorithms, and Programming.” Hence *SageMath* is particularly suited for abstract algebra. *Mathematica*, however, was never designed to work problems involving abstract algebra. The reason why *Mathematica* is able to do the abstract algebra calculations is because of the supporting software provided with the textbook.

IMPORTANT: In order to use either *SageMath* or *Mathematica* for this textbook, you will also need to either install the supporting files onto your computer, or run *SageMath* on a cloud using *CoCalc*. To install the files, download the .zip files found at either:

[myweb.astate.edu/wpaulsen/algebra.html](http://myweb.astate.edu/wpaulsen/algebra.html)

or the Github repository

<https://github.com/wpaulsen1/absalg/>

Note that this only downloads the supporting files, so you will also have to install *Mathematica* or *SageMath* programs as well.

On the other hand, you can forego downloading the files and run *SageMath* using *CoCalc*: Collaborative Calculation and Data Science. One can create a free account at [cocalc.com](http://cocalc.com) using any email address. Since this is perhaps the easiest way to get started with the text’s notebooks, we will begin explaining how to set this up.

## Using CoCalc

Go to [cocalc.com](https://cocalc.com) and sign up for a new account. You can use any email address, which CoCalc will verify by emailing you a link that you must click on. Once your email has been verified, you can sign in to your account.

The first step will be to create a new project. All notebooks, files, and directories must be placed in a *project*, which is an isolated computational workspace. Click on the “Create New Project...” button to open up the form for creating a project. You can use any name for the project, but using your own name is recommended, since this facilitates sharing your project with other users. Click on the “Create Project” button to create the project.

This should automatically take you into the project, but if not, click on the “Projects” tab, to see the project you just created, and click on the project name. At this point you should see a button labeled “Library.” (If the project is stopped, you will have to start the project to see the button.) This button allows you to download many different sets of notebooks for different topics. CoCalc has graciously agreed to include the *SageMath* notebooks for this text in their library. Scroll down to find “Abstract Algebra: An Interactive Approach,” or use the search bar. First, select this item, then click on the box labelled “Get a Copy.”

This will install a folder named “paulsen-abstract-algebra” into your project. You will start out within this folder, but you can click on the house icon to see this folder, then click on the folder to get back in. There is a Jupyter notebook (with the extension .ipynb) for each chapter of the textbook. (Jupyter notebooks used to be called Interactive Python Notebooks, hence the strange extension name.) The first 8 chapters deal with groups, so the files are “group01.ipynb” through “group08.ipynb.” The later chapters deal with rings, so for example [Chapter 9](#) would have the corresponding notebook “ring09.ipynb”. Note that there is bonus material in the folder that is not in the textbook.

If you click on one of these Jupyter notebooks, such as “group02.ipynb,” it will most likely not be in its proper format, because the notebook is not trusted. Click on the red “Not Trusted” button, and then click on “Trust” to get the notebook’s HTML code to properly function. Note that executing any input will also make it trusted.

Next to the “Trusted/Not Trusted” in the toolbar is an indicator which shows which kernel is selected. It should be set to the most recent version of *SageMath*. If some other kernel is appearing, such as Python 3 or R, click on the button and select the *SageMath* option.

Before we start working with any notebook, it must be *initialized*. The very first command after the title is the initialization cell, with the command

```
load('absalgtex2.sage')
```

Click on this cell, so that it is highlighted. Then hold down the **Shift** key and press **Enter** at the same time. This is how we execute a command in both *SageMath* and *Mathematica*. It will take a while for this to execute,

but eventually the message “Initialization Done” will appear. Notice a green circle appears next to the command to show it is being evaluated. The file “absalgtex2.sage” contains about 4000 lines of Python code that allows the commands we see in the textbook, along with the graphics capabilities.

You can see that this code uses up quite a bit of memory, since there is a “Memory” indicator in the toolbar. CoCalc puts a limit on how much memory is allocated to a project. Even with a project without upgrades, you should be able to execute most of the commands in *SageMath*, even the two-dimensional graphics. However, the animations, such as in Terry’s dance steps at the beginning of [Chapter 2](#), will likely use up the allocated memory, and cause the kernel to stop. (Being inactive for too long can also cause the kernel to stop.) For a nominal monthly fee, one can apply an upgrade to the project that will double the allocated memory, which is more than enough for the animations.

## Using Mathematica

First, you will have to download the “MathFiles.zip” file from one of the websites,

[myweb.astate.edu/wpaulsen/algebra.html](http://myweb.astate.edu/wpaulsen/algebra.html)

<https://github.com/wpaulsen1/absalg/>

and unzip it to get the files in the `math` folder. Then you will have to make sure that *Mathematica* is installed on your machine.

*Mathematica* is not free, but price information can be obtained from

<http://www.wolfram.com>

However, one can obtain a 30-day *Mathematica* product trial.

To load one of the supporting files in *Mathematica*, click on “File” and then slide down to “Open.” One can locate one of the 15 notebooks with the .nb extension in the `math` folder that you unzipped. Included in the supporting files are two *Mathematica* packages “group.m” and “ring.m.” The first of these is used for [Chapters 1-8](#) of the text, while the other is used in the remaining chapters. These two files allow *Mathematica* to work with groups as fluently as *SageMath*. There are, however, a few things that *SageMath* can do that *Mathematica* cannot, due to the algorithms.

Also in the folder are *Mathematica* files for each chapter of the textbook. The file names are “group01.nb” through “group08.nb,” and “ring09.nb” through “ring15.nb” in the `math` directory. These notebooks allow a student to walk through the examples in the book, along with other similar examples. Included in these notebooks are all the theorems and proofs in the textbook.

Once the supporting files have been installed, then one of the packages can be loaded into *Mathematica* with either of the two commands:

```
<< math\group.m
```

```
<< math\ring.m
```

This will only have to be done once in each *Mathematica* session. These are in the *initialization cells* of the notebook. Note that if you execute any command in the notebook, it will ask you whether you want to first execute the initialization cells in the notebook. Clicking “Yes” will do the initialization step for you.

Because of the similarities of the two systems, this book only shows the input and output for *SageMath*. The main reason for this is that switching back and forth between two systems proved to be distracting, as seen in the first edition of this book. Those using *Mathematica* can open the notebooks to see the corresponding *Mathematica* commands, and still follow along closely with the book.

### **Installing SageMath**

Although *SageMath* is a totally free program, it takes some effort to install. This is because it runs on Linux, not Windows. As a result, one has three options.

1. Enable Windows Subsystem for Linux (WSL), which allows one to run Linux as a program running inside of Windows. Then install a Linux operating system, such as Ubuntu, into the subsystem. You will then be able to start Ubuntu from the Windows start menu.
2. Create a hard drive partition that can boot to a Linux operating system, such as Ubuntu. The computer will then be able to boot to either Windows or Linux. This is actually the preferred method and is easier than it might first appear. However, it uses up more of your hard drive space.
3. *SageMath* is available on macOS, even though it is not available for Windows. The signed and notarized app will work for macOS 10.12 and newer.

Each of the three options requires some instructions to set up. The details are also available at

[www.sagemath.org](http://www.sagemath.org)

by clicking on the “Install” icon.

### **Using Windows Subsystem**

You must be using Windows 10 version 2004 and higher, or Windows 11 for these commands to work.

Click on the Start Menu, and find the Command Prompt. If it is not already one of the main options, it will be under “Windows System.” Another option is to type “Command Prompt” in the search box.

Right click on the Command Prompt, to see more options. There will be a “More” selection, and then click on “Run as Administrator.” It will prompt

you whether you want to allow the app to make changes to your device, so click “Yes”.

In this command prompt, type

```
wsl --install
```

This will install the Ubuntu distribution of Linux as a subsystem. (One can change the distribution, but there is no need for it.) It also defaults to using WSL 2, which is what we need.

You may have to reboot the computer before the installation is complete. If so, when the computer reboots, click on the Search icon and type “Ubuntu” to find the newly formed app. You will probably want to pin this to your desktop or taskbar to make it easier to find in the future. If the computer does not need rebooting, this app will automatically open, but it is a good idea to put the “Ubuntu” app where you can find it later.

The first time this app is launched, it will take several minutes for the files to decompress and be stored on your machine. It will ask for a new UNIX username, which will become the name of the Linux home directory. It will also ask for a new password, which we will need later on, so make it easy to remember (it doesn’t have to be secure). You will have to retype the password, since it does not display what you type.

Even though this launch took a while, future launches of the app will take less than a second.

One issue with using WSL is understanding how the directory system in Linux is linked to the directory system in Windows. After unzipping the notebooks from the above website, there will be a folder named “jupyter” somewhere in a Windows directory, probably something like

```
C:\Users\...\jupyter\
```

where the dots would be replaced with your Windows user name and the directory you put the files. Within the Linux subsystem, the C: drive is mounted into a special folder called `mnt`. So your folder, from the viewpoint of Linux, is at

```
/mnt/c/Users/.../jupyter/
```

Note that in Linux, the slashes go the other way. However, whenever you launch a Ubuntu terminal, by default you are in the home folder `~` (notice the `~$` prompt), which is an abbreviation for the home directory

```
/home/username
```

where `username` is replaced by the name you entered earlier. In order for *SageMath* to access the files in the C: drive, we will add a new folder which is linked to the `/mnt/c` folder. At the Ubuntu terminal, enter the command

```
sudo ln -s /mnt/c cdrive
```

You will have to enter your password that you set up above. You will have to enter your password for every **sudo** command, since this stands for “super-user do.” After this linked folder is set up, you can find your files at

```
~/cdrive/Users/.../jupyter/
```

Next, we have to install a web browser within Linux for *SageMath* to interact with. The simplest browser to install is Google Chrome. First, update the package index to make sure the system is up to date by entering the following command at the Ubuntu terminal:

```
sudo apt update
```

We can then upgrade the packages to the new version with the command:

```
sudo apt upgrade
```

At the “[Y/n]” prompt, answer ‘Y’ to begin the upgrade. (Actually, any response starting with ‘y’ or ‘Y’ will do.) Throughout this installation, we will answer ‘Y’ to any “[Y/n]” prompts.

We will use GNU wget to retrieve the content from the web servers. This should already be installed at this point, but we can double check by entering the command

```
wget --version
```

which will displace the current version of the program, if it is installed. If it turns out to not be installed, we can install GNU wget with the command

```
sudo apt install wget
```

Now can use GNU wget to download the latest version of Google Chrome:

```
wget https://dl.google.com/linux/direct/  
google-chrome-stable_current_amd64.deb
```

Note that this must be entered on a single line. This command will put the downloaded file into your Linux home folder. We can then use the *dpkg* tool to install Google Chrome from this file.

```
sudo dpkg -i google-chrome-stable_current_amd64.deb
```

If there are any errors in the installation process (which there probably will be), we can fix them by running the command:

```
sudo apt-get install -f
```

That should install Google Chrome! We can launch the Linux web browser with the command:

```
google-chrome
```

This will open up a welcoming message window, asking if you want to make Google Chrome your default browser. Since we want this to be the default within the Linux subsystem, hit OK. (It will not affect your default browser in Windows.) Then press the big “Get Started” button. It will then ask if you want to import bookmarks, or set a background, and so forth, which can all be skipped. Finally the Chrome browser will open up, and you could surf the web from here. However, we will only need this browser for interacting with *SageMath*, so you can go ahead and close this window for now.

Since we successfully installed Chrome, we no longer need the file that we downloaded. To remove this file, enter the command

```
rm google-chrome-stable_current_amd64.deb
```

At this point we are ready to install *SageMath* using the command

```
sudo apt-get install sagemath sagemath-jupyter
```

which will take several minutes to run. Once this is finally done, we can launch *SageMath* from the Ubuntu terminal by typing

```
sage -n
```

This will launch the Chrome browser inside of Linux, and the program will run within this browser. We can now select the **cdrive** folder, and select other folders to get to the **jupyter** folder. You can then open up one of the *SageMath* notebooks, such as **group01.ipynb**.

To *politely* get out of *SageMath*, first we have to save and close the notebook we are working on. Select the “File” tab, and then select “Close and Halt.” Once the notebook is closed, click on the “Quit” button in the Chrome browser.

If one exits the browser without hitting “Quit,” *SageMath* will still be running, but will have no way to interact with the user. The only way to quit *SageMath* would be to hold the Ctrl key down while pressing C, and then hit Y for yes when it asks if you want to quit. Closing the Ubuntu window will also quit the program.

There will not be a *SageMath* icon as with other installations. Every time you want to run *SageMath*, open the Ubuntu window and type

```
sage -n
```

## Using Linux

This assumes that you have already installed a Debian Linux system such as Ubuntu or Linux Mint. To install *Sage*, open a terminal application, and type

```
sudo apt-add-repository -y ppa:aims/sagemath
sudo apt-get update
sudo apt-get install sagemath-upstream-binary
```

For other Linux distributions, a tarball can be downloaded from the main website [www.sagemath.org](http://www.sagemath.org).

There are also a database file to be installed, that allows GAP to perform advanced group operations, which are only needed for the **GaloisType** and **StructureDescription** commands.

```
sudo sage -i database_gap
```

In order to view animations in *SageMath*, you will also have to install either *ImageMagick* or *FFmpeg*. The following installs *ImageMagick*, along with other recommended programs.

```
sudo apt-get install gfortran  
sudo apt-get install imagemagick texlive dvipng
```

You will have to manually copy the *SageMath* notebooks to a directory named `jupyter` in your home directory. You can now exit the terminal window with **exit**. It is important at this point to run the Software Update on the computer. This final step links the *SageMath* and *ImageMagick* programs, so they can interact.

At this point the big blue *SageMath* button should appear in the Applications menu. Clicking on this will cause *SageMath* to appear in a web browser. Click on “Upload,” and on the menu select “Browse.” One can either navigate through “Filesystem” to find the “jupyter” folder you created earlier. Select one of the notebooks, such as “group01.ipynb.” Finally, click on “Open.”

## Installing on macOS

There are binary releases of *SageMath* available for macOS 10.12 and newer. It will work for either Intel CPUs (x86) or for Apple’s new Arm CPU (i.e., M1, M1X or M2). Make sure you download the correct files. The downloads are available at

[https://github.com/3-manifolds/Sage\\_macOS/releases](https://github.com/3-manifolds/Sage_macOS/releases)

The complete instructions are in this webpage.

## Once the Notebook is Loaded

The first cell of every *Mathematica* notebook or *SageMath* worksheet is the Initialization cell. This must be executed first before any other commands in the notebook will work, since it loads either the “group.m,” “ring.m,” or “absalgttext2.sage” file.

Click on this cell, and hit Shift and Enter at the same time. When done, the message

Initialization Done

will appear. In *Mathematica*, it will always prompt you if you want to run the initialization cell first. The very first time that the initialization is done in *SageMath*, there may be additional databases that are automatically downloaded from the internet.

Both of the programs are interactive systems. Every expression that one types into the computer is immediately evaluated, and the result is shown. This is known as a read-evaluate-print loop. To create a new cell in *SageMath*, move the cursor to a point between two cells, and a long blue strip will appear. Clicking on this strip inserts a new input cell. In *Mathematica*, click between two cells and start typing, and a new cell will be created.

In either system, try computing  $3^{90}$ , using the Shift-Enter combination.

**3<sup>90</sup>**

```
8727963568087712425891397479476727340041449
```

*Mathematica* adds `In[]` and `Out[]` numbers.

`In[2] := 390`

```
Out[2]:= 8 727 963 568 087 712 425 891 397 479 476 727 340 041 449
```

*Mathematica* will number all of the input and output statements, but the prompt does not appear until *after* some expression is entered. Note that the numbers correspond to the cells evaluated in the current *session*, not the current notebook. So when the notebooks are first opened, none of the “`In[n] :=`” or “`Out[n] :=`” will be present. Likewise, if a second notebook is opened and a cell is evaluated, it might start with a value other than “`In[1]`. It is suggested that the cells be evaluated in the order that they appear, but there is nothing to prevent executing the statements in any order, or executing a statement more than once. The “`In[n] :=`” and “`Out[n] :=`” will show which commands have been run and in what order. Any cell that does not have an “`In[n] :=`” has not been evaluated yet, even though it appears to have a corresponding output.

Had we put a semi-colon before pressing the Shift-Enter, we would get a different effect. It computes the expression, but does not display the answer. For example, entering

**a = 3<sup>300</sup>;**

will assign the variable a 144 digit number, but will not display this number. Actually, *SageMath* would not display the number even without the semi-colon, because the value is assigned to the variable. To see the value of *a*, one can enter

**a**

```
1368914790585883759913260273820883159664636956253374364 \
7148019007836899717749907659380020615568894138825048444 \
0597994042813512732765695774566001
```

Note that both *SageMath* and *Mathematica* use the backslash to show that the number is continued on the next line.

In both programs, a variable is a sequence of letters and or digits, but must begin with a letter. Variables are case sensitive, so *a* is a different variable than *A*. Keywords, such as **if** or **quit**, are not allowed as variables, but the list of keywords is too long to give here. None of the lower case letters are keywords, so we can safely use the 26 variables *a* through *z*.

*Mathematica* does not automatically expand an expression, although it might rearrange the factors and terms.

$$(y^2 + 3y - 1)(y^2 - 2y + 4)$$

$$(4 - 2y + y^2)(-1 + 3y + y^2)$$

Because we have not yet assigned a value to *y*, *Mathematica* assumes that it is an indeterminate, so that it expresses the answer in terms of *y*. Also note that *Mathematica* assumes that a number and letter next to each other are to be multiplied together. In *SageMath*, we must explicitly use the **\*** for every multiplication.

```
(y^2 + 3*y - 1)*(y^2 - 2*y + 4)
Traceback (click to the left of this block for traceback)
...
NameError: name 'y' is not defined
```

This time, we get an error message, since *SageMath* has not been told what *y* is. Unlike *Mathematica*, we must declare *y* to be a variable in *SageMath* before we can use it as a variable. The simplest way to do this is with the command:

```
var("y")
y
```

We can try the expression again.

```
(y^2 + 3*y - 1)*(y^2 - 2*y + 4)
(y^2 + 3*y - 1)*(y^2 - 2*y + 4)
```

If we want to expand this, we can use the **expand** function.

```
expand(_)
y^4 + y^3 - 3*y^2 + 14*y - 4
factor(_)
(y^2 + 3*y - 1)*(y^2 - 2*y + 4)
```

Note that the underscore (\_) is a *SageMath* abbreviation for the last output. The corresponding symbol in *Mathematica* is the percent sign (%).

**Expand[%]**

$$-4 + 14y - 3y^2 + y^3 + y^4$$

**Factor[%]**

$$(4 - 2y + y^2)(-1 + 3y + y^2)$$

There are other syntax differences between *SageMath* and *Mathematica*: *SageMath* uses parentheses for functions, as the standard notation, but *Mathematica* uses square brackets for functions. Also, every function name in *Mathematica* is capitalized.

Most calculations in *Mathematica* and *SageMath* are also exact, but you do have the option of finding a decimal approximation using the **N** function. For example, the first 50 digits of  $\sqrt{2}$  are computed in *Mathematica* as

**N[Sqrt[2], 50]**

$$1.4142135623730950488016887242096980785696718753769$$

The same command in *SageMath* requires a bit more syntax.

**N(sqrt(2), digits=50)**

$$1.4142135623730950488016887242096980785696718753769$$

Both *SageMath* and *Mathematica* will point out any mistakes in the input line. For example, if one types

**(4 = 3)\*2**

Traceback (click to the left of this block for traceback)

...

SyntaxError: invalid syntax

To find out more information, click on the left side of the error message, and it will expand. The last few lines are as follows:

**(4 = 3)\*2**

$(\text{sage\_const\_4} = \text{sage\_const\_3}) * \text{sage\_const\_2}$

SyntaxError: invalid syntax

*SageMath* points to the error with an arrow (^). The same typo also produces an error in *Mathematica*, but for a different reason.

**(4 = 3)\*2**

6

*Mathematica* returns an answer but also displays a strange message,

“Set: Cannot assign to raw object 4.”

Because the equal sign in *Mathematica* is used to assign a value to a variable, *Mathematica* thinks we are trying to assign the value 3 to the number 4, which

of course cannot be done. But besides this, this value of 3 is multiplied by 2 to get the answer displayed.

Ironically, had we used a double equal sign, neither the *Mathematica* nor *SageMath* command would have produced an error.

```
(4 == 3)*2
```

```
2 False
```

The double equal sign is used to test if two expressions are equal. *Mathematica* sees no problem in symbolically multiplying **False** with an integer. *SageMath* produces a different answer.

```
(4 == 3)*2
```

```
0
```

*SageMath* converts **False** to 0, and **True** to 1 if needed. Other features of *SageMath* will be introduced in the textbook as the need arises. With a little practice, you will find both programs are relatively easy to use.

# Chapter 1

---

## Preliminaries

This chapter gives the background material for studying abstract algebra. It introduces the concepts of sets and mappings, which are the foundations of all of modern mathematics. It also introduces some important strategies for writing proofs, such as induction and *reductio ad absurdum*. It is preferable to introduce this material here since introducing this information at the point where it is needed interrupts the flow of the text. Undergraduate students and those using the book for self-study are encouraged to go through this chapter since it introduces concepts and notations that are used throughout the book.

---

### 1.1 Integer Factorization

Even in prehistoric times, there is evidence that societies developed a terminology for the counting numbers 1, 2, 3, etc. In fact, the Ishango bone suggests that prime numbers were contemplated as early as twenty thousand years ago. It is known that the early Egyptians understood prime numbers, but the Greeks of the fifth century B.C. get the credit for being the first to explore prime numbers for their own sake.

In this section, we will explore the basic properties of integers stemming from the prime factorizations. We will denote the set of all integers,

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

by the stylized letter  $\mathbb{Z}$ . This notation comes from the German word for number, *Zahl*. Many of the properties of factorizations refer only to positive integers, which are denoted  $\mathbb{Z}^+$ . Thus, we can write  $n \in \mathbb{Z}^+$  to say that  $n$  is a positive integer.

We begin by defining a divisor of a number.

**DEFINITION 1.1** We say that an integer  $a$  is a *divisor* of an integer  $b$ , denoted by  $a|b$ , if there is some integer  $c$  such that  $b = ac$ . Other ways of saying this is that  $a$  *divides*  $b$ , or  $a$  is a *factor* of  $b$ , or  $b$  is a *multiple* of  $a$ .

**Example 1.1**

Find the divisors of 30.

SOLUTION: Note that the definition allows for both negative and positive integers. Clearly, if  $30 = ac$  for integers  $a$  and  $c$ ,  $|a| \leq 30$ . With a little trial and error, we find the divisors to be

$$\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \text{ and } \pm 30.$$

□

We can extend the idea of integer divisors to that of finding the quotient  $q$  and remainder  $r$  of integer division.

**THEOREM 1.1: The Division Algorithm**

Given any  $x \in \mathbb{Z}$ , and any  $y \in \mathbb{Z}^+$ , there are unique integers  $q$  and  $r$  such that

$$x = qy + r \quad \text{and} \quad 0 \leq r < y.$$

PROOF: Since  $y > 0$ , we can consider the rational number  $x/y$ . Let  $q$  be the largest integer that is less than or equal to  $x/y$ . That is, we will pick the integer  $q$  so that

$$q \leq \frac{x}{y} < q + 1.$$

Multiplying by  $y$ , we have

$$yq \leq x < yq + y.$$

If we let  $r = x - yq$ , we have  $0 \leq r < y$ , and also  $x = yq + r$ , so we have found integers  $q$  and  $r$  that satisfy the required properties.

In order to show that  $q$  and  $r$  are unique, let us suppose that  $q_2$  and  $r_2$  are two other integers that satisfy the required conditions. Then  $qy + r = q_2y + r_2$ , so

$$(q - q_2)y = r_2 - r.$$

Since both  $r$  and  $r_2$  are between 0 and  $y - 1$ , the right-hand side is less than  $y$  in absolute value. But the left-hand side is at least  $y$  in absolute value unless  $q = q_2$ . This in turn will force  $r = r_2$ , so we see that the solution is unique. □

This is a constructive proof since it gives an algorithm for finding  $q$  and  $r$ . This proof also demonstrates how to prove that a solution is *unique*. We assume there is another solution and prove that the two solutions are in fact the same.

**Example 1.2**

Find integers  $q$  and  $r$  such that  $849 = 31q + r$ , with  $0 \leq r < 31$ .

SOLUTION: We can use *SageMath* as a calculator. To find the numerical approximation of  $849/31$ , enter

**N(849/31)**

27.3870967741935

Note that the function **N( )** gives the numerical approximation. The largest integer less than this value is  $q = 27$ . Then we can compute  $r$  to be

**849 - 27\*31**

12

□

The notation for finding the greatest integer function used in this algorithm is

$$\lfloor x \rfloor = \text{the greatest integer less than or equal to } x.$$

Using this notation, we have

$$q = \left\lfloor \frac{x}{y} \right\rfloor, \quad r = \left( \frac{x}{y} - \left\lfloor \frac{x}{y} \right\rfloor \right) \cdot y. \quad (1.1)$$

### **Example 1.3**

Find integers  $q$  and  $r$  such that  $-925 = 28q + r$ , with  $0 \leq r < 28$ .

SOLUTION: Note that  $-925/28 \approx -33.0357142857143$ . But to find an integer less than this, we round *down*, so in the case of a negative number, it will increase in magnitude. Thus,  $q = -34$ , and  $r = -925 - (-34)28 = 27$ . □

We define a *prime* as an integer that has exactly two positive factors. This definition actually allows negative numbers, such as  $-5$ , to be prime. Although this may seem to be a non-standard definition, it agrees with the generalized definition of primes defined in [Chapter 10](#). The numbers  $1$  and  $-1$  are not considered to be prime, for they have only one positive factor. The goal of this section is to prove that any integer greater than  $1$  can be uniquely factored into a product of positive primes.

We will begin by proving that every large number has at least one prime factor. This requires an assumption about the set of positive numbers, known as the *Well-Ordering Axiom*.

#### **The Well-Ordering Axiom:**

Every non-empty subset of  $\mathbb{Z}^+$  contains a smallest element.

The reason why this is considered to be an axiom is that it cannot be proven using only arithmetic operations. (Note that this statement is *not* true for rational numbers, which have the same arithmetic operations.) So this self-evident statement is assumed to be true and is used to prove other properties of the integers.

#### **LEMMA 1.1**

*Every number greater than 1 has a prime factor.*

**PROOF:** Suppose that some number greater than 1 does not have a prime factor. Then we consider the set of all integers greater than 1 which do not have a prime factor, and using the well-ordering axiom, we find the smallest such number, called  $n$ .

Then  $n$  is not prime, otherwise  $n$  would have a prime factor. Then by definition,  $n$  must have a positive divisor besides 1 and  $n$ , say  $m$ . Since  $1 < m < n$ , and  $n$  was the smallest number greater than 1 without a prime factor,  $m$  must have a prime factor, say  $p$ . Then  $p$  is also a prime factor of  $n$ , so we have a contradiction. Therefore, every number greater than 1 has a prime factor.  $\square$

This proof introduces an important strategy in proofs. Notice that to prove that every number greater than 1 had a prime factor, we assumed just the opposite. It was as if we admitted defeat from the very beginning! Yet from this we were able to reach a conclusion that was absurd—a number without a prime factor that did have a prime factor. This strategy is known as *reductio ad absurdum*, which is Latin for “reduce to the absurd.” We assume what we are trying to prove is actually false, and proceed logically until we reach a contradiction. The only explanation would be that the assumption was wrong, which proves the original statement.

This proof also combined *reductio ad absurdum* with the well-ordering principle. Since we are assuming there is some positive integer that makes our statement false, there must be a smallest such integer. This combination is known as the *least criminal method*, where the least criminal refers to the smallest integer that would make the statement false. In fact, the first paragraph of Lemma 1.1 can be abbreviated to “Let  $n$  be the least criminal.” Here is another example of the least criminal method.

### **LEMMA 1.2**

*Every integer  $n \geq 2$  can be written as a product of one or more positive primes.*

**PROOF:** Let  $n$  be the least criminal. This allows us to assume the statement is true for all integers  $2 \leq k < n$ , and that  $n$  is not the product of one or more primes. If  $n$  is prime, we have  $n$  as the product of one prime, which gives us a contradiction. If  $n$  is not prime, then we can express  $n = ab$ , where both  $a$  and  $b$  are between 1 and  $n$ . By our assumption,  $a$  and  $b$  can both be expressed as a product of positive primes, and so  $n$  can also be expressed as a product of primes, again giving us a contradiction. In either case we have a contradiction, so we have proven the lemma.  $\square$

This lemma illustrates another technique of proofs, known as *divide and conquer*. We considered two different cases, either  $n$  was prime, or  $n$  was not prime. Each case then became much easier to handle. As long as both possibilities lead to the same conclusion, we can proceed with the proof.

In order to prove that the prime factorization is *unique*, we will first have to develop the concept of the greatest common divisor.

**DEFINITION 1.2** We define the *greatest common divisor (GCD)* of two numbers to be the largest integer that divides both of the numbers. If the greatest common divisor is 1, this means that there are no prime factors in common. We say the numbers are *coprime* in this case. We denote the greatest common divisor of  $x$  and  $y$  by  $\gcd(x, y)$ .

We can use *SageMath*'s **gcd** function to quickly test whether two numbers are coprime without having to factor them.

```
gcd(153809229555633320199029, 573040781012789119612213)
1
```

There is an important property of the greatest common divisor, given in the following theorem.

**LEMMA 1.3: Bézout's Lemma**

Given two non-zero integers  $x$  and  $y$ , the greatest common divisor of  $x$  and  $y$  is the smallest positive integer which can be expressed in the form

$$ux + vy$$

with  $u$  and  $v$  being integers.

**PROOF:** Let  $A$  denote the set of all positive numbers that can be expressed in the form  $ux + vy$ . Note that both  $|x|$  and  $|y|$  can be written in the form  $ux + vy$ , so by the well-ordering axiom, we can consider the smallest positive number  $n$  in  $A$ . Note that  $\gcd(x, y)$  is a factor of both  $x$  and  $y$ , so  $\gcd(x, y)$  must be a factor of  $n$ .

By the division algorithm (Theorem 1.1), we can find  $q$  and  $r$ , with  $0 \leq r < n$ , such that  $x = qn + r$ . Then

$$r = x - qn = x - q(ux + vy) = (1 - qu)x + (-v)y.$$

If  $r \neq 0$ , then  $r$  would be a smaller positive number in  $A$  than  $n$ , which contradicts the way we chose  $n$ . Thus,  $r = 0$ , and  $n|x$ . By similar reasoning,  $n$  is also a divisor of  $y$ . Thus,  $n$  is a common divisor of  $x$  and  $y$ , and since the  $\gcd(x, y)$  is in turn a divisor of  $n$ ,  $n$  must be equal to  $\gcd(x, y)$ .  $\blacksquare$

Unfortunately, this is a *non-constructive proof*. Although this lemma proves the existence of the integers  $u$  and  $v$ , it does not explain how to compute them. Fortunately, there is an algorithm, known as the *Euclidean Algorithm*, which does compute  $u$  and  $v$ . (See the Historical Diversion on page 10.)

We start by assuming that  $x > y > 0$ , since we can consider absolute values if  $x$  or  $y$  are negative. We then repeatedly use the division algorithm to find  $q_i$  and  $r_i$  such that

$$\begin{aligned}x &= q_1y + r_1, & 0 \leq r_1 < y, \\y &= q_2r_1 + r_2, & 0 \leq r_2 < r_1, \\r_1 &= q_3r_2 + r_3, & 0 \leq r_3 < r_2, \\r_2 &= q_4r_3 + r_4, & 0 \leq r_4 < r_3, \dots\end{aligned}$$

Because the integer sequence  $\{r_1, r_2, r_3, \dots\}$  is decreasing, this will reach 0 in a finite number of steps, say  $r_m = 0$ . Then  $r_{m-1}$  will be  $\gcd(x, y)$ . We can find the values for  $u$  and  $v$  by solving the second to the last equation for  $r_{m-1}$  in terms of the previous two remainders  $r_{m-2}$  and  $r_{m-3}$ , and then using the previous equations recursively to express  $r_{m-1}$  in terms of the previous remainders. This will eventually lead to  $r_{m-1}$  expressed in terms of  $x$  and  $y$ , which is what we want. It helps to put the remainders  $r_i$  in parenthesis, as well as  $x$  and  $y$ , since these numbers are treated as variables.

### Example 1.4

Find integers  $u$  and  $v$  such that  $144u + 100v = \gcd(144, 100)$ .

SOLUTION: Using the division algorithm repeatedly, we have

$$\begin{aligned}(144) &= 1 \cdot (100) + (44) \\(100) &= 2 \cdot (44) + (12) \\(44) &= 3 \cdot (12) + (8) \\(12) &= 1 \cdot (8) + (4) \\(8) &= 2 \cdot (4) + (0).\end{aligned}$$

Thus, we see that  $\gcd(144, 100) = 4$ . Starting from the second to the last equation, we have

$$\begin{aligned}(4) &= (12) - (8) \\&= (12) - [(44) - 3 \cdot (12)] = 4 \cdot (12) - (44) \\&= 4 \cdot [(100) - 2 \cdot (44)] - (44) = 4 \cdot (100) - 9 \cdot (44) \\&= 4 \cdot (100) - 9 \cdot [(144) - (100)] = 13 \cdot (100) - 9 \cdot (144).\end{aligned}$$

Thus, we have  $u = -9$  and  $v = 13$ . □

There is also a tabular way of computing  $u$  and  $v$ , called the *extended Euclidean algorithm*. Table 1.1 shows the computations of  $u$  and  $v$  from Example 1.4. At the top of the table, we always put the two rows  $(1, 0)$  and  $(0, 1)$ . Then, to the left, we write the negatives of the divisors  $q$  from the standard Euclidean algorithm. However, we do not include the last quotient that leads to a remainder of 0.

**TABLE 1.1:** Extended Euclidean algorithm

	1	0	} always the same
	0	1	
Negative of the $q$ values, except for the one leading to a remainder of 0.	-1 -2 -3 -1	1 -2 7 -9 $\uparrow$ $u$	Take the number at the far left, times the number above, and then add the number which is above that one. $v$

Now we fill in the main part of the table. For each space in the table, starting with the top and working our way down, we multiply the negative number on the far left with the number immediately above the space, and then add the number which is above that one. For example, the  $-9$  in the table was computed by taking  $-1$  on the left times the  $7$  above it, and adding the  $-2$  which is above the  $7$ . When we complete the table, the bottom row gives us the values of  $u$  and  $v$ . Note that this algorithm assumes that  $x > y$ , so if  $x < y$ , we have to switch the  $u$  and  $v$  values.

### Computational Example 1.5

Use *SageMath* to find the numbers  $u$  and  $v$  such that

$$153809229555633320199029u + 573040781012789119612213v = 1.$$

SOLUTION: The command **xgcd** uses the extended Euclidean algorithm to find not only the gcd of the numbers but also the values of  $u$  and  $v$ .

```
xgcd(153809229555633320199029, 573040781012789119612213)
(1, -204484278360602880676488, 54885394465812121129381)
```

So the gcd is 1, and also

$$u = -204484278360602880676488 \quad \text{and}$$

$$v = 54885394465812121129381.$$

Note that these values were computed very quickly using the algorithm. □

We can now start to prove some familiar properties of prime numbers.

### LEMMA 1.4: Euclid's Lemma

If a prime  $p$  divides a product  $ab$ , then either  $p|a$  or  $p|b$ .

PROOF: Suppose that  $p$  does not divide  $a$  so that  $p$  and  $a$  are coprime. By Bézout's Lemma (1.3), there exist integers  $u$  and  $v$  such that  $ua + vp = 1$ . Then

$$uab + vpb = b.$$

Since  $p$  divides both terms on the left-hand side, we see that  $p|b$ . Thus,  $p$  must divide either  $a$  or  $b$ .  $\square$

This lemma quickly generalizes using the least criminal method.

### LEMMA 1.5

*If a prime  $p$  divides a product  $a_1a_2a_3 \cdots a_n$ , where  $n \geq 2$ , then  $p$  divides  $a_i$  for some  $i$ .*

PROOF: We will use the least criminal method on  $n$ . That is, we will assume that  $n$  is the smallest number for which the statement is false, and reach a contradiction. Because of Euclid's Lemma (1.4), we know that  $n$  is not 2. Since  $n$  is the smallest number for which the statement is false, we know that the statement is true for the case  $n - 1$ . That is, if  $p$  divides  $a_1a_2a_3 \cdots a_{n-1}$ , then  $p$  divides  $a_i$  for some  $i$ . If we let  $b = a_1a_2a_3 \cdots a_{n-1}$ , then  $a_1a_2a_3 \cdots a_n = ban$ . By Euclid's Lemma (1.4), if  $p$  divides  $ban$ , then  $p$  divides either  $b$  or  $a_n$ . But if  $p$  divides  $b$ , then  $p$  divides  $a_i$  for some  $1 \leq i \leq n - 1$ . So in either case,  $p$  divides  $a_i$  for some  $1 \leq i \leq n$ . This means that  $n$  is not the smallest number for which the statement is false, so we have reached the contradiction.  $\square$

Note that in this application of the least criminal method, we only used the fact that the *previous case* had to be true. When this happens, the method is known as *mathematical induction*. We will discuss more on mathematical induction in the next section. For now, we can finally prove that integer factorization is unique.

### THEOREM 1.2: The Fundamental Theorem of Arithmetic

*Every integer greater than 1 can be factored into a product of one or more positive primes. Furthermore, this factorization is unique up to the rearrangement of the factors.*

PROOF: Lemma 1.2 shows that all integers greater than 1 can be expressed as a product of positive primes. So we only have to show uniqueness. We will use the least criminal method. That is, we will let  $s$  be the smallest positive integer that has two factorizations

$$s = p_1p_2p_3 \cdots p_n = q_1q_2q_3 \cdots q_m,$$

where  $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$  are all positive primes. Note that if  $s$  were prime, then  $s$  would clearly have only one prime factorization,  $s$ . So we can assume  $s$  is composite.

By Lemma 1.5, since  $p_n|q_1q_2q_3 \cdots q_m$ ,  $p_n$  must divide one of the  $q_i$ 's. Since  $p_n$  and  $q_i$  are both positive primes, we find that  $p_n = q_i$ . By rearranging the remaining  $q$ 's, we can write

$$p_1p_2p_3 \cdots p_n = q_1q_2q_3 \cdots q_{m-1}p_n.$$

Thus,

$$s/p_n = p_1p_2p_3 \cdots p_{n-1} = q_1q_2q_3 \cdots q_{m-1}.$$

Since  $s$  is the least criminal,  $s/p_n$  has a unique prime factorization, up to rearrangement of the prime factors. So  $n = m$ , and the  $p$ 's are a rearrangement of the  $q$ 's. Thus,  $s$  also has a unique prime factorization, contradicting the least criminal statement.  $\square$

The *SageMath* command for finding the prime factorization of an integer is

**factor(420)**

```
2^2 * 3 * 5 * 7
```

Note that *SageMath* puts the primes in increasing order, and repeated prime factors are expressed using exponents. This is known as the *standard form* of the factorization. As long as the integers are less than about 40 digits long, *SageMath* should have no trouble factoring them. However, for larger integers, factorization is a difficult problem even with modern technology. The amount of time required is proportional to the square root of the second largest prime in the factorization. [14, p. 133]

On the other hand, determining whether or not a number is prime can be done quickly in *SageMath*, even if the number has over 200 digits!

**is\_prime(10^200 + 357)**

```
True
```

How can *SageMath* know for certain that this number is prime when it cannot begin to test for all possible factors? The answer lies in abstract algebra. Using the properties we will discover in this book, it is possible to prove whether or not a number is prime without knowing the factorization. This in turn will have many applications in internet security and cryptology.

## Problems for §1.1

For Problems 1 through 9: Find integers  $q$  and  $r$  that satisfy  $x = qy + r$  with  $0 \leq r < y$ .

1  $x = 53, y = 7$

4  $x = -534, y = 31$

7  $x = 37, y = 235$

2  $x = 637, y = 41$

5  $x = 5628, y = 29$

8  $x = -33, y = 251$

3  $x = -417, y = 23$

6  $x = 9825, y = 107$

9  $x = 0, y = 9$

10 Use Definition 1.1 to prove that if  $a|b$  and  $n$  is an integer, then  $a|nb$ .

## Historical Diversion

# Euclid of Alexandria (c. 300 BC)

---

Euclid of Alexandria is known as the “Father of Geometry,” because of one great work that he wrote, *The Elements*. Euclid lived during the time of Ptolemy I. (323–283 B.C.) Alexandria was the intellectual hub of its day, not only with the Great Library but also the *Museum* (meaning seat of the muses), which was their equivalent to a university. Although little is known about the life of Euclid, we can infer from his writings that he was a brilliant mathematician, being able to compile all known mathematical knowledge into a sequence of small steps, each proposition building on the previous in a well-defined order.



Although the *Elements* is primarily a treatise on geometry, books VII, VIII, and IX deal with number theory. Euclid was particularly interested in primes and divisibility. He proved that there were an infinite number of primes and proved what is known as Euclid’s lemma, that if a prime divides the product of two numbers, it must divide at least one of those numbers. This lemma then leads to the fundamental theorem of arithmetic, which says that any number greater than 1 can be uniquely factored into a product of primes. Euclid also considered the greatest common divisor of two numbers and gave a constructive algorithm for finding the gcd of two numbers.

Euclid also defined a perfect number as a number equal to the sum of its divisors other than itself. He then went on to say that if  $2^p - 1$  is prime, then  $2^{p-1}(2^p - 1)$  will be perfect.

In book X Euclid worked with irrational numbers, or *incommensurables* proving that  $\sqrt{2}$  is irrational. This result was known to the school of Pythagoras, but was a closely guarded secret. The distinction between rational numbers and real numbers will play a vital role in future mathematics.

Euclid would have been aware of the three great construction problems of antiquity: trisecting an angle, duplicating the cube, and squaring the circle. The first problem is to divide any angle into 3 equal parts. The duplication of the cube involved constructing a line segment  $\sqrt[3]{2}$  times another line segment. Finally, squaring the circle required constructing a square with the same area as a given circle. Euclid’s *Elements* laid down the ground rules for a valid straight edge and compass constructions. Previous “solutions” done over a century earlier violated these rules. Although these seem like geometry problems, they were only proven to be impossible using algebraic methods in the 19th century. The first two were proven to be impossible using Galois theory. The last construction was proven impossible by Ferdinand von Lindemann in 1882 when he proved  $\pi$  is transcendental.

- 11** Use Definition 1.1 to prove that if  $a|b$  and  $b|c$ , then  $a|c$ .
- 12** Use Definition 1.1 to prove that if  $a|b$  and  $a|c$ , then  $a|(b + c)$ .
- 13** Use Definition 1.1 to prove that if  $a|b$  and  $a|c$ , then  $a|(b - c)$ .
- 14** Use Definition 1.1 to prove that if  $a|b$  and  $a|c$ , and  $n$  and  $m$  are integers, then  $a|(nb + mc)$ .
- 15** Use Definition 1.1 to prove that if  $a|b$  and  $b|a$ , then either  $a = b$ , or  $a = -b$ .
- 16** Use Problem 14 to prove that if  $a|b$  and  $a|c$ , then  $a|\gcd(b, c)$ .
- 17** Show that if  $a|bc$  and  $\gcd(a, b) = 1$ , then  $a|c$ .  
Hint: Use the trick from Euclid's Lemma (1.4).
- 18** Prove that there are an infinite number of primes. This is known as Euclid's prime number theorem.  
Hint: Suppose the positive primes are finite:  $2, 3, 5, 7, \dots, p_n$ . Apply Lemma 1.1 to

$$m = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n) + 1$$

to reach a contradiction.

For Problems **19** through **27**: Find integers  $u$  and  $v$  that satisfy  $ux + vy = \gcd(x, y)$ . Note that there could be more than one solution.

- 19**  $x = 84, y = 48$     **22**  $x = 285, y = 105$     **25**  $x = -602, y = 238$   
**20**  $x = 100, y = 64$     **23**  $x = 827, y = 103$     **26**  $x = 485, y = -119$   
**21**  $x = 84, y = 66$     **24**  $x = 249, y = 481$     **27**  $x = 0, y = 9$

- 28** Show that if  $d$  is a positive integer, then  $\gcd(da, db) = d \cdot \gcd(a, b)$ .

- 29** Define the *least common multiple* of two positive integers  $x$  and  $y$ , denoted by  $\text{lcm}(x, y)$ , to be the smallest positive integer which is a multiple of both  $x$  and  $y$ . Prove that the least common multiple will exist, and that  $\text{lcm}(x, y)|x \cdot y$

- 30** Prove that  $\text{lcm}(x, y) = (x \cdot y)/\gcd(x, y)$ . See Problem 29.

- 31** Show that if  $\gcd(x, y, z) = 1$ , then there exist integers  $u, v$ , and  $w$  such that  $ux + vy + wz = 1$ .  
Hint: Use the fact that  $\gcd(x, y, z) = \gcd(\gcd(x, y), z)$ .

For Problems **32** through **37**: Find the prime factorizations of the following numbers, and put the factorization into standard form.

- 32** 64000                  **34** 5100                  **36** 31213  
**33** 4002                  **35** 9889                  **37** 87567

## Interactive Problems

**38** Use *SageMath* to find integers  $u$  and  $v$  such that

$$876543212345678u + 123456787654321v = 1.$$

**39** Use *SageMath* to find integers  $u$  and  $v$  such that

$$98765432123456789u + 12345678987654321v = 1.$$

**40** Use *SageMath* to find the factorization of 987654321.

**41** Use *SageMath* to find the factorization of 12345678987654321.

**42** Use *SageMath* to find the factorization of 98765432123456789.

## 1.2 Functions

The concept of a function is central to virtually every branch of mathematics. There are in fact various ways to define a function, but the concept remains the same. Standard functions in calculus map real numbers to real numbers, but we want to consider a more abstract definition for which the input and output can come from any set.

**DEFINITION 1.3** Let  $A$  and  $B$  be two non-empty sets. A *function*, or *mapping*, from  $A$  to  $B$  is a rule that assigns to every element of  $A$  exactly one element of  $B$ . The set  $A$  is called the *domain* of the function, and the set  $B$  is called the *target*. If a function  $f$  assigns to  $a$  the element  $b$ , we write  $f(a) = b$ , and say that  $b$  is the *image* of  $a$  under  $f$ .

We will use the notation  $f : A \rightarrow B$  to indicate that  $f$  is a function from the set  $A$  to the set  $B$ . The *range* of  $f$ , or the *image* of  $f$ , is the set

$$\{y \mid y = f(x) \text{ for some } x \in A\}.$$

This set is denoted by either  $f(A)$  or  $\text{Im}(f)$  and is a subset of  $B$ .

### Example 1.6

Let  $A$  be the set of integers from 0 to 99, and let  $B$  be the set of English letters from  $a$  to  $z$ . Let  $\phi$  map each integer to the first letter of the English word for that number. For example,  $\phi(4) = f$ . Then the range of  $\phi$  is the set

$$\{e, f, n, o, s, t, z\}.$$

□

There is often different ways to denote the same element of the set  $A$ , so we must be careful that the rule for the function does not depend on the way the element is expressed. Had we extended the last example to include 100, this could be called either “a hundred” or “one hundred.” Another example of an ambiguous definition is if we assign to each rational number  $a/b$  the value  $1/b$ . But by this rule,  $f(1/2) \neq f(2/4)$ , even though  $1/2 = 2/4$ . In order to show that a function is *well-defined*, we must show that if  $x_1 = x_2$ , then  $f(x_1) = f(x_2)$ .

### Example 1.7

Consider the function from the set of rational functions (denoted by  $\mathbb{Q}$ ) to itself, given by

$$f\left(\frac{a}{b}\right) = \frac{\gcd(a, b)}{|b|}.$$

Show that this function is well-defined.

**SOLUTION:** We need to show that if  $x_1 = x_2$ , then  $f(x_1) = f(x_2)$ . That is, if we have two ways of expressing the rational function  $a/b = c/d$ , then we must show that

$$\frac{\gcd(a, b)}{|b|} = \frac{\gcd(c, d)}{|d|}.$$

This is equivalent to showing  $|d| \cdot \gcd(a, b) = |b| \cdot \gcd(c, d)$ . Using the result of Problem 28 from §1.1, this is equivalent to  $\gcd(ad, bd) = \gcd(bc, bd)$ . But since  $a/b = c/d$ , we have  $ad = bc$ , so this function is well-defined.  $\blacksquare$

Many functions possess special properties that we want to explore.

**DEFINITION 1.4** We say that a function  $f : A \rightarrow B$  is *injective*, or *one-to-one*, if the only way in which  $f(x) = f(y)$  is if  $x = y$ .

The function in Example 1.7 is not one-to-one, since  $f(1/3) = f(2/3)$ . In order to prove that a function is one-to-one, we assume that  $f(x) = f(y)$ , and try to prove that  $x = y$ .

### Example 1.8

Consider the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by

$$f(x) = \begin{cases} x + 3 & \text{if } x \text{ is even,} \\ 2x & \text{if } x \text{ is odd.} \end{cases}$$

Show that  $f(x)$  is one-to-one.

**SOLUTION:** We assume that  $f(x) = f(y)$ , and work to show that  $x = y$ . Because of the way that  $f(x)$  is defined, there are several cases to consider, so we will use the divide and conquer strategy.

Case 1) Both  $x$  and  $y$  are even. Then since  $f(x) = f(y)$ ,  $x + 3 = y + 3$ , which implies that  $x = y$ .

Case 2) Both  $x$  and  $y$  are odd. Then since  $f(x) = f(y)$ ,  $2x = 2y$ , so again  $x = y$ .

Case 3)  $x$  is even, and  $y$  is odd. Then  $f(x) = f(y)$  implies that  $x + 3 = 2y$ , or  $x = 2y - 3$ . But this implies that  $x$  is odd, and we started out assuming that  $x$  is even, so we have a contradiction, and this case can never happen.

Case 4)  $x$  is odd, and  $y$  is even. This is a mirror image of case 3, so we find that this case also can never happen.

In all cases, we either showed  $x = y$ , or reached a contradiction. Thus, we have shown in all cases for which  $f(x)$  could equal  $f(y)$ , then  $x = y$ . Hence  $f$  is one-to-one.  $\square$

We can also ask whether the range and the target of a given function are the same set.

**DEFINITION 1.5** We say that a function  $f : A \rightarrow B$  is *surjective*, or *onto*, if for every  $b \in B$  there is at least one  $a \in A$  such that  $f(a) = b$ . If a function is both one-to-one and onto, it is called a *bijection*.

### Example 1.9

Determine whether the function in Example 1.8 is onto.

SOLUTION: Listing the first few values of  $f(x)$ ,

$$f(0) = 3, \quad f(1) = 2, \quad f(2) = 5, \quad f(3) = 6, \quad f(4) = 7, \quad f(5) = 10, \dots,$$

it seems that  $f(x)$  is never 4. Let us suppose that  $f(x) = 4$  and reach a contradiction.

Case 1)  $x$  is even. Then  $x + 3 = 4$ , so  $x = 1$ . But this contradicts that  $x$  is even.

Case 2)  $x$  is odd. Then  $2x = 4$ , so  $x = 2$ . But this contradicts that  $x$  is odd.

Since all cases reach a contradiction, we see that  $f(x) \neq 4$ , and so the function is not onto.  $\square$

Note that one counterexample is sufficient to prove that the function is not onto. The standard strategy for proving that a function  $f : A \rightarrow B$  is onto is to show that for an arbitrary  $y \in B$ , there is some kind of formula for an element  $x \in A$  such that  $f(x) = y$ .

### Example 1.10

Let  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  be defined by  $f(x) = 3x + 5$ . Show that  $f$  is onto.

SOLUTION: If  $f(x) = y$ , we can solve for  $x$  to get  $x = (y - 5)/3$ . Note that this is defined for all rational numbers  $y$ , and produces a rational number. Then  $f((y - 5)/3) = y$  for any  $y \in \mathbb{Q}$ , so  $f$  is onto.  $\square$

Often our functions will be defined on finite sets. In these cases, it is easy to determine whether or not a function is onto if we have already proven that it is one-to-one.

**DEFINITION 1.6** For a finite set  $A$ , we denote the number of elements in the set by  $|A|$ . If  $A$  is infinite, we write  $|A| = \infty$ .

In the last section, we introduced the least criminal method, where we assumed that  $n$  was the smallest integer that caused a statement to be false. This allowed us to assume that the statement is true for all previous  $n$ . Often, we only need to utilize the fact that the statement is true for the case  $n - 1$ . In which case, there is a shortcut to the least criminal method called the *method of mathematical induction*.

### **THEOREM 1.3: Principle of Mathematical Induction**

Let  $S(n)$  be any statement about an integer  $n$ . Suppose that  $S(a)$  is true for a starting value of  $a$ , and if by assuming that  $S(n - 1)$  is true, we can prove that  $S(n)$  is true. Then  $S(n)$  is true for all integers greater than or equal to  $a$ .

**PROOF:** Suppose that there was some  $n$  greater than or equal to  $a$  for which the statement  $S(n)$  was false. Let  $n$  be the least criminal, that is, the smallest  $n$  for which  $S(n)$  is false. Since we know  $S(a)$  is true,  $n \neq a$ . Then  $S(n - 1)$  would be true, since  $n - 1$  is smaller than  $n$ , and still greater to or equal to  $a$ . But by assuming that  $S(n - 1)$  is true, we can prove that  $S(n)$  is also true. Thus, we have a contradiction, and  $S(n)$  is true for all integers greater than or equal to  $a$ .  $\square$

Here are the steps for proving a statement using mathematical induction:

1. The base case: Prove the statement for the starting value  $a$ , usually  $a = 1$ .
2. Assume the statement is true for the previous case, by replacing every  $n$  with  $n - 1$ .
3. Use this assumption to prove the statement for the case  $n$ .

We can see an example of mathematical induction in the following lemma.

### **LEMMA 1.6**

Let  $f : A \rightarrow B$  be a function that is both one-to-one and onto, and suppose that  $A$  is a finite set. Then  $|A| = |B|$ .

**PROOF:** We will use induction on the size  $n = |A|$ . If  $A$  has only one element,  $a_1$ , then  $f(a_1) = b_1$ , and  $B = \{b_1\}$ . By induction, we can suppose that the statement is true for  $n - 1$ .

If  $A = \{a_1, a_2, a_3, \dots, a_n\}$ , then  $f(a_n) = b$  for some  $b \in B$ . First we let  $C = \{a_1, a_2, a_3, \dots, a_{n-1}\} = A - \{a_n\}$ , that is, we remove the element  $a_n$  from the set  $A$ . We can also let  $D = B - \{b\}$  by removing the element  $b$  from  $B$ . Finally, we can define the function  $g : C \rightarrow D$  by  $g(x) = f(x)$  for  $x \in C$ . Since  $f$  is a bijection, so is  $g$ , since no other element of  $A$  could map to  $b$ . By induction, we see that  $|C| = |D|$ , and since  $|A| = |C| + 1$  and  $|B| = |D| + 1$ , then  $|A| = |B|$ .  $\blacksquare$

We can now prove an important principle that will help us to show whether a function is onto.

#### **THEOREM 1.4: The Pigeonhole Principle**

*Let  $f : A \rightarrow B$  be a function from a finite set  $A$  to a finite set  $B$ . If  $|A| = |B|$  and  $f$  is one-to-one, then it is also onto.*

**PROOF:** Let  $R$  be the range of  $f$ , which would be a subset of  $B$ . Then the function  $f : A \rightarrow R$  would be both one-to-one and onto, so by Lemma 1.6 we have  $|A| = |R|$ . Since we also have that  $|A| = |B|$ , then  $B = R$ , so the function is onto.  $\blacksquare$

We will often need to apply two functions in succession, creating a new function.

**DEFINITION 1.7** Let  $f : B \rightarrow C$  and  $g : A \rightarrow B$  be two functions. Then the mapping  $(f \circ g) : A \rightarrow C$  is defined by

$$(f \circ g)(x) = f(g(x)) \quad \text{for all } x \in A.$$

Note that in  $f \circ g$ , we apply the  $g$  function first, and then  $f$ . Some textbooks have  $f \circ g = g(f(x))$ , so care must be taken when referring to other texts.

#### **Example 1.11**

Let

$$f(x) = \begin{cases} x + 3 & \text{if } x \text{ is even,} \\ 2x & \text{if } x \text{ is odd,} \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 3x & \text{if } x \text{ is even,} \\ x - 1 & \text{if } x \text{ is odd.} \end{cases}$$

Compute  $f \circ g$  and  $g \circ f$ .

**SOLUTION:** For each computation, we need to consider the case  $x$  even and  $x$  odd separately. To find  $(f \circ g)(x) = f(g(x))$ :

Case 1)  $x$  is even. Then  $g(x) = 3x$ , which will also be even. Thus,  $f(g(x)) = 3x + 3$ .

Case 2)  $x$  is odd. Then  $g(x) = x - 1$ , which will be even, so  $f(g(x)) = x + 2$ . Thus,

$$f \circ g = \begin{cases} 3x + 3 & \text{if } x \text{ is even,} \\ x + 2 & \text{if } x \text{ is odd.} \end{cases}$$

To compute  $(g \circ f)(x) = g(f(x))$ , we also have to consider two cases.

Case 1)  $x$  is even. Then  $f(x) = x + 3$ , which will be odd. So  $g(f(x)) = x + 2$ .

Case 2)  $x$  is odd. Then  $f(x) = 2x$ , which will be even. So  $g(f(x)) = 6x$ . Thus,

$$g \circ f = \begin{cases} x + 2 & \text{if } x \text{ is even,} \\ 6x & \text{if } x \text{ is odd.} \end{cases}$$
□

Note that in this case,  $f \circ g \neq g \circ f$ . However, if we have three functions, with  $f : C \rightarrow D$ ,  $g : B \rightarrow C$ , and  $h : A \rightarrow B$ , then  $(f \circ g) \circ h = f \circ (g \circ h)$ , since both of these expressions represent  $f(g(h(x)))$ .

If  $f(x)$  is both one-to-one and onto, then we will be able to define the *inverse function* of  $f$ .

### PROPOSITION 1.1

*Let  $f : A \rightarrow B$  be both one-to-one and onto. Then there exists a unique function  $g : B \rightarrow A$  such that  $g(f(x)) = x$  for all  $x$  in  $A$ , and  $f(g(y)) = y$  for all  $y \in B$ .*

**PROOF:** Because  $f$  is both one-to-one and onto, for every  $y \in B$  there is a unique  $x \in A$  such that  $f(x) = y$ . Thus, we can define  $g(y)$  to be that value  $x$  such that  $f(x) = y$ . By the way  $g(y)$  is defined, we see that  $f(g(y)) = y$  for all  $y \in B$ . If we apply the function  $g$  to both sides of this equation, we have  $g(f(g(y))) = g(y)$ . Since every element  $x \in A$  can be written as  $g(y)$  for some  $y \in B$ , we can replace  $g(y)$  with  $x$  to get  $g(f(x)) = x$  for all  $x \in A$ .

To show that the function is unique, suppose there is another such function  $h(x) : B \rightarrow A$ . Then

$$h(y) = h(f(g(y))) = (h \circ f)(g(y)) = g(y) \quad \text{for all } y \in B.$$

Thus,  $h = g$ , showing that the function is unique.

□

**DEFINITION 1.8** The unique function in Proposition 1.1 is called the *inverse function* of  $f(x)$  and is denoted by  $f^{-1}(y)$ .

### Example 1.12

Consider the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  given by

$$f(x) = \begin{cases} x + 3 & \text{if } x \text{ is even,} \\ x - 1 & \text{if } x \text{ is odd.} \end{cases}$$

Show that this is both one-to-one and onto, and find  $f^{-1}(y)$ .

**SOLUTION:** If  $f(x) = f(y)$ , the only interesting case is if  $x$  is even, and  $y$  is odd. Then  $x+3 = y-1$ , or  $y = x+4$ , which would be even, not odd. Likewise, case where  $x$  is odd and  $y$  is even leads to a contradiction. Thus,  $x = y$ , and  $f$  is one-to-one.

To show that  $f$  is onto, we must show that for every  $y$ , there is an  $x$  so that  $f(x) = y$ . We break this into two cases.

Case 1)  $y$  is even. Then  $y+1$  will be odd, so  $f(y+1) = (y+1)-1 = y$ .

Case 2)  $y$  is odd. Then  $y-3$  is even, so  $f(y-3) = (y-3)+3 = y$ .

In both cases, we found an  $x$  so that  $f(x) = y$ . In the process of determining that  $f$  is onto, we computed the inverse.

$$f^{-1}(y) = \begin{cases} y+1 & \text{if } y \text{ is even,} \\ y-3 & \text{if } y \text{ is odd.} \end{cases}$$

□

## Problems for §1.2

- 1** Let  $\phi$  be the mapping that sends every number from 0 to 99 to the *last* letter of the English word for that number. What would be the range of  $\phi$ ?
- 2** Show that the function  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  given by  $f(a/b) = ab/(a^2 + b^2)$  is well-defined.

For Problems **3** through **8**: Part a) For the given  $f : \mathbb{R} \rightarrow \mathbb{R}$ , determine if the function is one-to-one. Part b) Determine if the function is onto. In both cases, prove your answer is correct.

<b>3</b> $f(x) =  x $	<b>5</b> $f(x) = x^3$	<b>7</b> $x^2 - 2x$
<b>4</b> $f(x) = 5x + 3$	<b>6</b> $f(x) = x/3 - 2/3$	<b>8</b> $f(x) = 2x +  x $

For Problems **9** through **14**: Part a) For the given  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ , determine if the function is one-to-one. Part b) Determine if the function is onto. In both cases, prove your answer is correct.

<b>9</b> $f(x) = \begin{cases} 2x+1 & \text{if } x \text{ is even,} \\ 2x & \text{if } x \text{ is odd.} \end{cases}$	<b>12</b> $f(x) = \begin{cases} 2x+4 & \text{if } x \text{ is even,} \\ x-2 & \text{if } x \text{ is odd.} \end{cases}$
<b>10</b> $f(x) = \begin{cases} x-1 & \text{if } x \text{ is even,} \\ (x+1)/2 & \text{if } x \text{ is odd.} \end{cases}$	<b>13</b> $f(x) = \begin{cases} (x+2)/2 & \text{if } x \text{ is even,} \\ (x-1)/2 & \text{if } x \text{ is odd.} \end{cases}$
<b>11</b> $f(x) = \begin{cases} x+1 & \text{if } x \text{ is even} \\ 2x & \text{if } x \text{ is odd.} \end{cases}$	<b>14</b> $f(x) = \begin{cases} 3x & \text{if } x \text{ is even,} \\ 5x-1 & \text{if } x \text{ is odd.} \end{cases}$

- 15** Show that the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $f(x) = 2x^2 + x$  is one-to-one.  
Hint: Use the quadratic equation to solve  $2x^2 + x = c$ , and show that the two solutions cannot both be integers.

- 16** Use mathematical induction to show that  $1 + n < n^2$  for all integers  $n \geq 2$ .

- 17** Use mathematical induction to show that  $2^n < n!$  for all integers  $n \geq 4$ . (Recall that  $n! = 1 \cdot 2 \cdot 3 \cdots n$ .)
- 18** Use mathematical induction to show that  $n^2 + 3n + 4$  is a multiple of 2 for all  $n \geq 1$ .
- 19** Use mathematical induction to show that  $n^3 + 2n$  is a multiple of 3 for all  $n \geq 1$ .
- 20** Use mathematical induction to show that  $4^n - 1$  is a multiple of 3 for all  $n \geq 1$ .
- 21** Use mathematical induction to show that  $6^n + 4$  is a multiple of 20 for all  $n \geq 2$ .
- 22** Use mathematical induction to show that  $x$  is a positive real number, then  $(1+x)^n \geq 1 + xn$  for all positive integers  $n$ .
- 23** Use mathematical induction to prove that for all positive integers  $n$ ,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

- 24** Use mathematical induction to prove that for all positive integers  $n$ ,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

- 25** Use mathematical induction to prove that for all positive integers  $n$ ,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

- 26** Use mathematical induction to prove that for all positive integers  $n$ ,

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

- 27** Use mathematical induction to prove that for all positive integers  $n$ ,

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

- 28** Use mathematical induction to prove that for all positive integers  $n$ ,

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

- 29** Let  $f : A \rightarrow B$  be a function from a finite set  $A$  to a finite set  $B$ . If  $|B| < |A|$ , use Lemma 1.6 to show that  $f$  cannot be one-to-one.

- 30** Let  $f : A \rightarrow B$  be a function from a finite set  $A$  to a finite set  $B$ . If  $|B| > |A|$ , show that  $f$  cannot be onto.
- 31** Let  $f : A \rightarrow B$  be a function from a finite set  $A$  to a finite set  $B$ . If  $|B| = |A|$ , and  $f$  is onto, use Problem 30 to show that  $f$  is also one-to-one. Note that Problems 29 through 31 are three alternative ways to state the pigeonhole principle.
- 32** Use Problem 29 to show that there are two people in London with exactly the same number of hairs on their head. (Since the average number of hairs is about 150,000, assume no one can have more than 1,000,000 hairs.)

For Problems **33** through **38**: For the given  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  and  $g : \mathbb{Z} \rightarrow \mathbb{Z}$ , determine  $(f \circ g)(x)$ .

**33**  $f(x) = x^2 - 1$

$$g(x) = x^2 + 1$$

**34**  $f(x) = x^2$

$$g(x) = x + |x|$$

**35**  $f(x) = x^3 + 2x^2$

$$g(x) = x - 1$$

**36**  $f(x) = \begin{cases} 2x + 5 & \text{if } x \text{ is even,} \\ x + 2 & \text{if } x \text{ is odd.} \end{cases}$

$$g(x) = \begin{cases} 2x + 1 & \text{if } x \text{ is even,} \\ x - 1 & \text{if } x \text{ is odd.} \end{cases}$$

**37**  $f(x) = \begin{cases} 3x + 2 & \text{if } x \text{ is even,} \\ x + |x| & \text{if } x \text{ is odd.} \end{cases}$

$$g(x) = \begin{cases} x + 4 & \text{if } x \text{ is even,} \\ 2x & \text{if } x \text{ is odd.} \end{cases}$$

**38**  $f(x) = \begin{cases} x + 3 & \text{if } x \text{ is even,} \\ (x - 1)/2 & \text{if } x \text{ is odd.} \end{cases}$

$$g(x) = \begin{cases} 2x - 1 & \text{if } x \text{ is even,} \\ x + 4 & \text{if } x \text{ is odd.} \end{cases}$$

**39** Let  $f : B \rightarrow C$  and  $g : A \rightarrow B$  be both one-to-one functions. Show that  $f \circ g : A \rightarrow C$  is one-to-one.

**40** Let  $f : B \rightarrow C$  and  $g : A \rightarrow B$  be both onto functions. Show that  $f \circ g : A \rightarrow C$  is onto.

**41** Let  $f : B \rightarrow C$  and  $g : A \rightarrow B$  be functions, and suppose that  $f$  is *not* onto. Show that  $f \circ g : A \rightarrow C$  is not onto.

**42** Let  $f : B \rightarrow C$  and  $g : A \rightarrow B$  be functions, and suppose that  $g$  is *not* one-to-one. Show that  $f \circ g : A \rightarrow C$  is not one-to-one.

**43** Show that the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(x) = \begin{cases} x + 5 & \text{if } x \text{ is even,} \\ x - 3 & \text{if } x \text{ is odd.} \end{cases}$  is a bijection, and find  $f^{-1}(x)$ .

**44** Show that the function  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = \begin{cases} x^2 & \text{if } x \geq 0, \\ x & \text{if } x < 0. \end{cases}$  is a bijection, and find  $f^{-1}(x)$ .

## Interactive Problems

**45** Consider the function

$$f(x) = 2\lfloor x \rfloor - x.$$

*SageMath* uses the function **floor** to denote  $\lfloor x \rfloor$ . Thus, we can have *SageMath* plot this function with the commands

```
f(x) = 2*floor(x) - x
plot(f(x), [x, 0, 5])
```

Judging by the graph, is this function one-to-one? Is it onto? (Ignore the vertical lines in the graph.)

**46** Define a function  $g(x)$  in *SageMath* such that  $f(g(x)) = x$  for all  $x$ , using the function from Problem 45. Note that the formula must work for both integers and non-integers. Is  $g(f(x))$  always equal to  $x$ ?

### 1.3 Binary Operators

So far we have only considered functions with one input variable. But we could also consider functions with two input variables,  $f(x, y)$ . For simplicity we will only consider the cases where  $x$  and  $y$  come from the same set, which is also the target set.

**DEFINITION 1.9** Let  $A$  be a non-empty set. A *binary operation* is a function that assigns to every  $x$  and  $y$  in  $A$  an element  $z$  in  $A$ .

Although we could denote a binary operation as  $z = f(x, y)$ , we will typically denote the operation by the infix notation  $z = x * y$ . The binary operators that we are familiar with are addition, subtraction, and multiplication, but the  $*$  could represent *any* function with two input values. Often we will use a dot ( $\cdot$ ) instead of the asterisk, depending on the context.

#### Example 1.13

Suppose that we define the binary operation  $x * y$  on the set of integers by

$$x * y = x + y + xy.$$

Show that  $a * b = b * a$ .

**SOLUTION:** To find  $a * b$ , we replace every  $x$  with  $a$  and every  $y$  with  $b$  in the definition, to get  $a * b = a + b + ab$ . Likewise, to find  $b * a$ , we replace every  $x$

with  $b$  and every  $y$  with  $a$  to get  $b * a = b + a + ba$ . But  $a + b + ab = b + a + ba$ , so  $a * b = b * a$ .  $\square$

**DEFINITION 1.10** If a binary operation  $*$  has the property that  $a * b = b * a$  for all  $a$  and  $b$  in the set, we say that the binary operation is *commutative*. If a binary operation has the property that  $(a * b) * c = a * (b * c)$  for all  $a$ ,  $b$ , and  $c$  in the set, we say the binary operation is *associative*.

We saw in the last example that the binary operation  $x * y = x + y + xy$  is commutative. But because the binary operation is a *function*, to test if a binary operation is associative, we have to plug a function into *itself*.

### Example 1.14

Determine whether the binary operation of Example 1.13 is associative. That is, determine if  $(a * b) * c = a * (b * c)$ .

SOLUTION: To compute  $(a * b) * c$ , we replace every  $x$  with  $(a * b)$  and every  $y$  with  $c$  in the definition.

$$(a * b) * c = (a * b) + c + (a * b)c.$$

Now we can replace  $a * b$  with  $a + b + ab$ , again using the definition of  $*$ .

$$\begin{aligned} (a * b) * c &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc. \end{aligned}$$

To compute  $a * (b * c)$ , we replace every  $x$  with  $a$  and every  $y$  with  $(b * c)$  in the definition.

$$a * (b * c) = a + (b * c) + a(b * c).$$

Now we can replace  $b * c$  with  $b + c + bc$  according to the definition of  $*$ .

$$\begin{aligned} a * (b * c) &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + ab + ac + bc + abc. \end{aligned}$$

Thus, we see that  $(a * b) * c = a * (b * c)$  for all  $a$ ,  $b$ , and  $c$ , so the binary operation is associative.  $\square$

### Example 1.15

Define the binary operation on the set of real numbers by

$$x * y = \min(x, y),$$

where  $\min(x, y)$  denotes the smaller of  $x$  or  $y$ . Show that this binary operation is both commutative and associative.

**TABLE 1.2:**  
Binary operator for  
Example 1.16

*	a	b	c	d
a	a	a	a	a
b	a	b	b	a
c	a	c	c	a
d	a	d	d	a

SOLUTION: We have  $a * b = \min(a, b)$  and  $b * a = \min(b, a)$ . But finding the smaller of two numbers does not depend on the order of the numbers, so  $a * b = b * a$ , and the binary operator is commutative.

To show that the binary operator is associative, we need to compute  $(a * b) * c$ . Using the definition of  $*$  twice, this becomes  $\min(\min(a, b), c)$ . But if we take the smaller of two numbers, and then in turn take the smaller of this with a third number, we will get the smallest of the three numbers. Thus,  $(a * b) * c = \min(a, b, c)$ . Likewise,  $a * (b * c) = \min(a, \min(b, c)) = \min(a, b, c)$ , so the binary operation is associative.  $\blacksquare$

Although a binary operation is usually defined by a formula, if the set  $A$  on which the binary operation is defined is finite, we can also define the binary operation by making a table of all combinations of  $x * y$ . Such a table is called a *Cayley table*. To find  $x * y$  using a Cayley table, the first value  $x$  is always on the *left*, and the second value  $y$  is always on the *top*.

### Example 1.16

Let the set  $A$  consist of the four letters  $\{a, b, c, d\}$ . Define a binary operation on this set using the Cayley table in [Table 1.2](#). Show that this binary operator is associative, even though it is not commutative.

SOLUTION: It is easy to tell from the Cayley table whether or not the binary operator is commutative. If the binary operator is commutative, the table will be symmetric about the line going from the top left to the bottom right. However, this table is not symmetric, since  $b * c = b$ , but  $c * b = c$ . Thus, this binary operator is not commutative.

Determining whether a binary operator is associative or not from the Cayley table is harder. We must determine whether  $(x * y) * z = x * (y * z)$  for every combination of  $x$ ,  $y$ , and  $z$ . In this case, it would mean testing  $4^3 = 64$  combinations. However, we can shorten this list by observing patterns in the Cayley table. By looking at the columns of the table, we find that

$$x * a = a, \quad x * b = x, \quad x * c = x, \quad \text{and} \quad x * d = a \quad \text{for all } x.$$

Thus, for any  $x$  and  $y$ ,

$$\begin{aligned}(x * y) * a &= a, \text{ and } x * (y * a) = x * a = a, \\ (x * y) * b &= x * y \text{ and } x * (y * b) = x * y, \\ (x * y) * c &= x * y \text{ and } x * (y * c) = x * y, \\ (x * y) * d &= a, \text{ and } x * (y * d) = x * a = a.\end{aligned}$$

Thus we have shown that  $(x * y) * z = x * (y * z)$  for every combination of  $x$ ,  $y$ , and  $z$ , so the binary operation is associative.  $\square$

**DEFINITION 1.11** Let  $*$  be a binary operation defined on a set  $A$ . We say that a subset  $B$  of  $A$  is *closed with respect to  $*$*  if whenever both  $x$  and  $y$  are in  $B$ , then  $x * y$  is in  $B$ .

### Example 1.17

Let  $*$  be the binary operation of Example 1.13. Show that the subset of odd integers is closed with respect to  $*$ .

SOLUTION: Let  $x$  and  $y$  be odd integers. Then we can express  $x = 2m + 1$  and  $y = 2n + 1$  for some integers  $m$  and  $n$ . Then

$$\begin{aligned}x * y &= (2m + 1) * (2n + 1) \\ &= (2m + 1) + (2n + 1) + (2m + 1)(2n + 1) \\ &= 2m + 1 + 2n + 1 + 4mn + 2m + 2n + 1 \\ &= 4m + 4n + 4mn + 3 \\ &= 2(2m + 2n + 2mn + 1) + 1.\end{aligned}$$

Thus, we see that  $x * y$  is an odd integer, so the set is closed.  $\square$

## Problems for §1.3

For Problems 1 through 8:

Determine if the binary operation defined on the set  $\mathbb{R}$  is (Part a) commutative, (Part b) associative.

- |                       |                              |
|-----------------------|------------------------------|
| 1 $x * y = x + y - 1$ | 5 $x * y = x - y$            |
| 2 $x * y = 2x + y$    | 6 $x * y = x + y - xy$       |
| 3 $x * y = y$         | 7 $x * y = 2x + 2y + 2 + xy$ |
| 4 $x * y = 2x + 2y$   | 8 $x * y = 2 - x - y + xy$   |

- 9 Let  $\mathbb{Z}^+$  be the set of positive integers. Define the binary operator on  $\mathbb{Z}^+$  by  $x * y = \gcd(x, y)$ . Show that this binary operator is associative. See Problem 31 of §1.1.

- 10** Define the following binary operator on the set of integers:

$$x * y = \begin{cases} xy & \text{if } x \neq \pm 1 \text{ and } y \neq \pm 1 \\ 1 & \text{otherwise.} \end{cases}$$

Show that this binary operator is associative. Note that you will have to consider 2 cases, one for which none of the numbers are  $\pm 1$ , and one for which at least one of the numbers is  $\pm 1$ .

- 11** Define the following binary operator on the set of integers:

$$x * y = \begin{cases} x + y & \text{if } x \neq 0 \text{ and } y \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Is this binary operator associative?

For Problems **12** through **16**: Form the Cayley table for the binary operator defined on the set  $A$ .

- |                                        |                           |
|----------------------------------------|---------------------------|
| <b>12</b> $A = \{0, 1, 2, 3, 4, 5\}$   | $x * y =  x - y .$        |
| <b>13</b> $A = \{0, 1, 2, 3, 4\}$      | $x * y = y.$              |
| <b>14</b> $A = \{1, 2, 3, 4, 5\}$      | $x * y = \min(x, y).$     |
| <b>15</b> $A = \{1, 2, 3, 4, 5\}$      | $x * y = \max(x, y).$     |
| <b>16</b> $A = \{0, 1, 2, 3, 4\}$      | $x * y = \min(x + y, 4).$ |
| <b>17</b> $A = \{1, 2, 3, 4, 5, 6\}$   | $x * y = \gcd(x, y).$     |
| <b>18</b> $A = \{1, 2, 4, 8, 16, 32\}$ | $x * y = \gcd(x, y).$     |
| <b>19</b> $A = \{0, 1, 2, 3, 4, 5\}$   | $x * y = \max(x - y, 0).$ |

- 20** Let  $n > 0$  be an integer, and let  $A = \{0, 1, 2, \dots, n\}$ . Show that the binary operator  $x * y = \min(x + y, n)$  is associative.

- 21** Let  $A$  be the set of all *functions* from  $\mathbb{R}$  to  $\mathbb{R}$ , and for two functions  $f(x)$  and  $g(x)$ , define  $f * g = f \circ g$ , the function composition. Show that this binary operator is associative.

- 22** Given a binary operation on a set  $A$ , an element  $l$  is called a *left identity* if  $l * x = x$  for all  $x$  in  $A$ . Likewise,  $r$  is called a right identity if  $x * r = x$  for all  $x$  in  $A$ . Show that the binary operation of Example 1.16 has two right identities, but no left identity.

- 23** Show that if a binary operation on a set  $A$  has both a left identity and a right identity, then these are the same. See Problem 22.

- 24** Given a binary operation on a set  $A$ , an element  $e$  is called a *two-sided identity* if it is both a left identity and a right identity. That is,  $x * e = e * x = x$  for all  $x$  in  $A$ . Find a two-sided identity for the binary operation of Example 1.13.

- 25** Show that the binary operation of Example 1.15 does *not* have a two-sided identity. See Problem 24.

For Problems **26** through **31**: Determine if the subset  $S$  is closed with respect to the binary operation.

- 26**  $x * y = x - y$        $S = \text{set of even integers.}$
- 27**  $x * y = x - y$        $S = \text{set of odd integers.}$
- 28**  $x * y = xy$        $S = \text{set of even integers.}$
- 29**  $x * y = xy$        $S = \text{set of odd integers.}$
- 30**  $f * g = f \circ g$        $S = \text{set of all polynomial functions.}$
- 31**  $x * y = x/y$        $S = \text{non-zero integers.}$
- 32**  $x * y = x/y$        $S = \text{non-zero rational numbers.}$

### Interactive Problems

- 33** Consider the binary operator on the set of integers:

$$x * y = \begin{cases} x & \text{if } x \text{ is even,} \\ y & \text{if } x \text{ is odd.} \end{cases}$$

Defining a piecewise defined binary operator is a little tricky in *SageMath*, but we can define it as a function  $f(x, y)$  as follows:

```
def f(x,y): return x + (y-x)*(x % 2)
```

Since the binary operator is defined as a function,  $(x * y) * z$  must be entered as **f(f(x, y), z)**, and  $x * (y * z)$  is entered as **f(x, f(y, z))**. Try computing these for different integers  $x$ ,  $y$ , and  $z$ . Show this binary operator is not commutative. Does this binary operator seem to be associative?

- 34** Consider the binary operator on the set of integers:

$$x * y = \begin{cases} x & \text{if } x + y \text{ is even,} \\ y & \text{if } x + y \text{ is odd.} \end{cases}$$

This can be defined in *SageMath* as

```
def g(x,y): return x + (y-x)*((x+y) % 2)
```

Try computing  $(x * y) * z$  and  $x * (y * z)$  for different integers  $x$ ,  $y$ , and  $z$ . Show this binary operator is not commutative. Does this binary operator seem to be associative? See Problem 33.

- 35** *SageMath* can work with tables of numbers, called *matrices*. For example, a  $2 \times 2$  matrix can be entered by

```
var("a11 a12 a21 a22")  
A = matrix([[a11, a12], [a21, a22]]); A  
[a11 a12]  
[a21 a22]
```

The first command defines a set of variables for us to use. If we define two such matrices, we can use `*` to multiply them together.

```
var("b11 b12 b21 b22")
B = matrix([[b11, b12], [b21, b22]])
A*B
[a11*b11 + a12*b21 a11*b12 + a12*b22]
[a21*b11 + a22*b21 a21*b12 + a22*b22]
```

The result is another  $2 \times 2$  matrix, showing that `*` is a binary operator on  $2 \times 2$  matrices. Is this operator commutative?

**36** Extend Problem 35 by defining a third  $2 \times 2$  matrix.

```
var("c11 c12 c21 c22")
C = matrix([[c11, c12], [c21, c22]]); C
```

Is the binary operator `*` associative?

## 1.4 Modular Arithmetic

There is an important operation on the set of integers  $\mathbb{Z}$  that we will use throughout the book, based on the division algorithm. It is an abstraction of a counting method often used in everyday life. For example, using standard 12 hour time, if it is 7:00 now, what time will it be 8 hours from now? The answer is not 15:00, since clock time “wraps around” every 12 hours, so the correct answer is 3:00. This type of arithmetic that “wraps around” is called modular arithmetic. We formally define modular arithmetic as follows:

**DEFINITION 1.12** Let  $x, y \in \mathbb{Z}$ , with  $y > 0$ . We define the operator

$$x \text{ mod } y,$$

pronounced “ $x$  modulo  $y$ ,” to be the unique value  $r$  from the division algorithm, which selects  $q$  and  $0 \leq r < y$  such that  $x = qy + r$ . The number  $y$  is called the *modulus*.

The `mod` operation is almost, but not quite, a binary operation on  $\mathbb{Z}$ , since it is not defined if  $y = 0$ . Since there is a difference of opinion as to how the operator should be defined for  $y < 0$ , we will only use the operator for  $y > 0$ .

### Example 1.18

Compute  $8348 \text{ mod } 43$ .

SOLUTION: Since  $8342 = 194 \cdot 43 + 6$ , we see that  $8348 \bmod 43 = 6$ . □

### Computational Example 1.19

Compute  $743532645703453453463 \bmod 257275073624623$ .

SOLUTION: For numbers this large, we will use *SageMath* to help. We use the `%` symbol for the **mod** operator.

**743532645703453453463 % 257275073624623**  
221951157869396 □

Sometimes the modulo operation is very easy to compute. For any positive  $x$ ,  $x \bmod 10$  will be the last digit in the decimal representation of the number. There are other tricks for small values of  $y$ . See Problem 13.

A familiar property of standard arithmetic is that the last digit of the sum and product of two positive numbers  $x$  and  $y$  can be computed using only the last digits of  $x$  and  $y$ . This can be generalized in the following proposition.

### PROPOSITION 1.2

If  $x$ ,  $y$ , and  $n$  are integers with  $n > 0$ , then

$$(x + y) \bmod n = ((x \bmod n) + (y \bmod n)) \bmod n, \quad (1.2)$$

and

$$(xy) \bmod n = ((x \bmod n) \cdot (y \bmod n)) \bmod n. \quad (1.3)$$

PROOF: In both equations, the two sides are between 0 and  $n - 1$ , so it is sufficient to show that the difference of the two sides is a multiple of  $n$ . Let  $a = x \bmod n$ ,  $b = y \bmod n$ ,  $c = (x + y) \bmod n$ , and  $d = (xy) \bmod n$ . Then there are integers  $q_1, q_2, q_3$ , and  $q_4$  such that

$$x = q_1n + a, \quad y = q_2n + b, \quad x + y = q_3n + c, \quad xy = q_4n + d.$$

For the equation 1.2, we note that

$$\begin{aligned} c - (a + b) &= (x + y - q_3n) - ((x - q_1n) + (y - q_2n)) \\ &= q_1n + q_2n - q_3n = (q_1 + q_2 - q_3)n. \end{aligned}$$

Thus, the two sides of equation 1.2 differ by a multiple of  $n$ . Likewise, for equation 1.3, we see

$$\begin{aligned} d - ab &= (xy - q_4n) - (x - q_1n) \cdot (y - q_2n) \\ &= yq_1n + xq_2n - q_4n - q_1q_2n^2 = (yq_1 + xq_2 - q_4 - q_1q_2n)n. \end{aligned}$$

So again, the two sides of equation 1.3 differ by a multiple of  $n$ . □

We can use Proposition 1.2 to compute powers modulo  $n$ . Since raising a number to an integer power is equivalent to repeated multiplication, we see that

$$(x^y) \bmod n = (x \bmod n)^y \bmod n.$$

**Example 1.20**

Compute  $234^5 \bmod 29$ .

SOLUTION: Since  $234 \bmod 29 = 2$ , the answer is the same as  $2^5 \bmod 29$ , and  $32 \bmod 29 = 3$ . □

WARNING: It is not true that

$$(x^y) \bmod n = (x \bmod n)^{(y \bmod n)} \bmod n.$$

That is, we cannot apply the modulus to an exponent. However, there is a trick for simplifying a power in the case that the exponent is large—using the binary representation of the exponent  $y$ . The procedure is known as the *repeated squaring algorithm* and is best explained by an example.

**Example 1.21**

Compute  $25^{35} \bmod 29$ .

SOLUTION: The number  $25^{35}$  is 49 digits long, and the base is already smaller than the modulus, so there is no obvious way of simplifying the expression. By looking at the binary representation of 35, we find that  $35 = 32 + 2 + 1$ . Thus,

$$25^{35} = 25^{32} \cdot 25^2 \cdot 25.$$

In order to compute  $25^{32} \bmod 29$ , we can *square* the number 5 times, reducing modulo 29 at each stage.

$$\begin{aligned} 25^2 \bmod 29 &= 625 \bmod 29 = 16, \\ 25^4 \bmod 29 &= 16^2 \bmod 29 = 256 \bmod 29 = 24, \\ 25^8 \bmod 29 &= 24^2 \bmod 29 = 576 \bmod 29 = 25, \\ 25^{16} \bmod 29 &= 25^2 \bmod 29 = 625 \bmod 29 = 16, \\ 25^{32} \bmod 29 &= 16^2 \bmod 29 = 256 \bmod 29 = 24. \end{aligned}$$

Finally, we see that

$$25^{35} \bmod 29 = 25^{32} \cdot 25^2 \cdot 25^1 \bmod 29 = 24 \cdot 16 \cdot 25 \bmod 29 = 9600 \bmod 29 = 1.$$

Note that we never had to deal with numbers more than 4 digits long. □

The *SageMath* command **PowerMod(x, y, n)** uses the repeated squaring algorithm to compute  $x^y \bmod n$ .

**Computational Example 1.22**

Use *SageMath* to find

$$743532645703453453463^{42364872163462467234} \pmod{2572750736246233264872}.$$

SOLUTION:

```
PowerMod(743532645703453453463, 42364872163462467234,
2572750736246233264872)
1270976212484154802393
```

Note that *SageMath* was able to do this computation fast. We will see that the ability for computers to quickly compute large powers modulo  $n$  has applications in internet security.  $\square$

There is another property of modular arithmetic involving coprime numbers that will be used often throughout the book, known to the ancient Chinese since before 240 C.E.

**THEOREM 1.5: The Chinese Remainder Theorem**

If  $x$  and  $y$  in  $\mathbb{Z}^+$  are coprime, then given any  $a$  and  $b$  in  $\mathbb{Z}$ , there is a unique  $k$  in  $\mathbb{Z}$  such that

$$0 \leq k < xy,$$

$$k \pmod{x} = a \pmod{x},$$

and

$$k \pmod{y} = b \pmod{y}.$$

PROOF: We will begin by showing that there cannot be more than one such number. Suppose we have two different numbers,  $k$  and  $m$ , which satisfy the above conditions. Then

$$(k - m) \pmod{x} = 0 \quad \text{and} \quad (k - m) \pmod{y} = 0.$$

Thus,  $k - m$  must be a multiple of both  $x$  and  $y$ . But since  $x$  and  $y$  are coprime, the least common multiple of  $x$  and  $y$  is  $xy$ . (See Problem 30 from §1.1.) Thus,  $k - m$  is a multiple of  $xy$ .

However, both  $k$  and  $m$  are less than  $xy$ . So the only way this is possible is for  $k - m = 0$ , which contradicts our assumption that  $k$  and  $m$  were distinct solutions.

To show that there is a solution, we first note that since  $x$  and  $y$  are coprime, by Bézout's lemma (1.3), there are integers  $u$  and  $v$  such that  $ux + vy = 1$ . Then we can consider the number

$$k = (avy + bux) \pmod{(xy)}.$$

Clearly  $0 \leq k < xy$ , so we only have to show that  $k \bmod x = a \bmod x$  and  $k \bmod y = b \bmod y$ . Since  $vy = 1 - ux$ ,

$$\begin{aligned} k \bmod x &= (avy + bux) \bmod x \\ &= (a(1 - ux) + bux) \bmod x \\ &= (a + ux(b - a)) \bmod x = a \bmod x. \end{aligned}$$

Likewise, since  $ux = 1 - vy$ ,

$$\begin{aligned} k \bmod y &= (avy + bux) \bmod y \\ &= (avy + b(1 - vy)) \bmod y \\ &= (b + vy(a - b)) \bmod y = b \bmod y. \quad \square \end{aligned}$$

This is a constructive proof, since it gives us a formula for finding the value of  $k$ .

### Example 1.23

Find a non-negative number  $k$  less than 210 such that

$$\begin{aligned} k \bmod 14 &= 3, \quad \text{and} \\ k \bmod 15 &= 7. \end{aligned}$$

SOLUTION: Since 14 and 15 are coprime, we begin by finding  $u$  and  $v$  such that  $14u + 15v = 1$ . But there is the obvious solution

$$14(-1) + 15(1) = 1.$$

Then we compute  $k$  to be  $avy + bux = 3 \cdot 15 + 7 \cdot (-14) = -53$ . But since this is negative, we can add  $14 \cdot 15$  to get another solution, 157.  $\square$

There is a *SageMath* command `crt(a, b, x, y)` that finds  $k$  given the 2 sets  $\{a, b\}$  and  $\{x, y\}$ .

### Computational Example 1.24

Use *SageMath* to find a number  $k$  such that

$$\begin{aligned} k \bmod 77123471239874233 &= 57345720357234529 \quad \text{and} \\ k \bmod 64237468234862362 &= 56813465823592454. \end{aligned}$$

SOLUTION:

```
crt(57345720357234529, 56813465823592454,
77123471239874233, 64237468234862362)
1959998626378684249237399917749988
```

We can verify that this solution is correct.

**1959998626378684249237399917749988 % 77123471239874233**

57345720357234529

**1959998626378684249237399917749988 % 64237468234862362**

56813465823592454

□

The Chinese remainder theorem has many applications. One of these is in the distribution of classified information among two or more people in such a way so that no one person can see the information. Each would receive one of the two (or more) modulus conditions, which is not enough information to determine the number  $k$ . Only when all of the pieces of the problem are assembled can  $k$  be determined, which can be decoded.

Another application is in solving linear congruence equations of the form

$$(mx) \text{ mod } n = a.$$

This can be solved by letting  $k = mx$ . Then

$$\begin{aligned} k \text{ mod } n &= a, && \text{and} \\ k \text{ mod } m &= 0. \end{aligned}$$

Since we can solve for  $k$ , we can find  $x$ .

### Example 1.25

Solve the linear congruence equation

$$12x \text{ mod } 19 = 3.$$

**SOLUTION:** We need to solve  $k \text{ mod } 19 = 3$  and  $k \text{ mod } 12 = 0$ . Thus, we must first find a  $u$  and  $v$  such that  $19u + 12v = 1$ . Using the Euclidean algorithm, we find that

$$(-5) \cdot 19 + 8 \cdot 12 = 1.$$

Using these values of  $u$  and  $v$ , we have that

$$k = avy + bux = 3 \cdot 8 \cdot 12 + 0 \cdot (-5) \cdot 19 = 288.$$

Finally,  $k = 12x$ , so  $x = 24$ . Note that we can add or subtract multiples of 19 to get other solutions, so  $x = 5$  also works. □

### Problems for §1.4

For Problems 1 through 12: Evaluate the following modular arithmetic problems.

<b>1</b>	$7243 \pmod{31}$	<b>5</b>	$297^7 \pmod{23}$	<b>9</b>	$728^{57} \pmod{23}$
<b>2</b>	$729645 \pmod{127}$	<b>6</b>	$473^6 \pmod{37}$	<b>10</b>	$984^{29} \pmod{47}$
<b>3</b>	$987654 \cdot 876543 \pmod{101}$	<b>7</b>	$21^{28} \pmod{31}$	<b>11</b>	$6395^{31} \pmod{103}$
<b>4</b>	$83627 \cdot 74234 \cdot 92658 \pmod{47}$	<b>8</b>	$33^{43} \pmod{41}$	<b>12</b>	$5837^{61} \pmod{113}$

- 13** A trick for computing  $x \pmod{9}$  for any positive  $x$  is to add the digits of the number  $x$ . If this number is greater than 9, add the digits of the new number. Eventually the number will be between 1 and 9. If the result is 9,  $x \pmod{9} = 0$ , otherwise  $x \pmod{9}$  is the final number produced. Prove that this method will always work.

For Problems **14** through **25**: Use the Chinese remainder theorem to find the smallest non-negative number that satisfies the system of modular equations.

<b>14</b>	$\begin{cases} k \pmod{13} = 5, \\ k \pmod{12} = 7. \end{cases}$	<b>18</b>	$\begin{cases} k \pmod{21} = 7, \\ k \pmod{16} = 10. \end{cases}$	<b>22</b>	$\begin{cases} k \pmod{79} = 48, \\ k \pmod{83} = 65. \end{cases}$
<b>15</b>	$\begin{cases} k \pmod{17} = 5, \\ k \pmod{11} = 8. \end{cases}$	<b>19</b>	$\begin{cases} k \pmod{34} = 19, \\ k \pmod{27} = 10. \end{cases}$	<b>23</b>	$\begin{cases} k \pmod{103} = 78, \\ k \pmod{97} = 49. \end{cases}$
<b>16</b>	$\begin{cases} k \pmod{18} = 7, \\ k \pmod{13} = 3. \end{cases}$	<b>20</b>	$\begin{cases} k \pmod{51} = 17, \\ k \pmod{49} = 26. \end{cases}$	<b>24</b>	$\begin{cases} k \pmod{107} = 43, \\ k \pmod{128} = 35. \end{cases}$
<b>17</b>	$\begin{cases} k \pmod{23} = 3, \\ k \pmod{12} = 7. \end{cases}$	<b>21</b>	$\begin{cases} k \pmod{61} = 47, \\ k \pmod{73} = 58. \end{cases}$	<b>25</b>	$\begin{cases} k \pmod{142} = 47, \\ k \pmod{113} = 74. \end{cases}$

- 26** Let  $u$ ,  $v$ , and  $w$  be three positive integers that are *mutually coprime*. That is, each is coprime to the other two. Given any  $x$ ,  $y$ , and  $z$  in  $\mathbb{Z}$ , prove that there is a unique number  $k$  such that

$$0 \leq k < u \cdot v \cdot w,$$

$$k \equiv x \pmod{u},$$

$$k \equiv y \pmod{v},$$

and

$$k \equiv z \pmod{w}.$$

Hint: Use the Chinese remainder theorem (1.5) twice.

For Problems **27** through **38**: Solve the following linear congruence equations.

<b>27</b>	$8x \pmod{11} = 9$	<b>31</b>	$7x \pmod{31} = 19$	<b>35</b>	$32x + 19 \pmod{51} = 17$
<b>28</b>	$6x \pmod{13} = 9$	<b>32</b>	$12x \pmod{37} = 17$	<b>36</b>	$16x + 35 \pmod{61} = 29$
<b>29</b>	$7x \pmod{18} = 13$	<b>33</b>	$18x \pmod{41} = 7$	<b>37</b>	$17x + 71 \pmod{83} = 48$
<b>30</b>	$9x \pmod{23} = 11$	<b>34</b>	$27x \pmod{43} = 8$	<b>38</b>	$23x + 47 \pmod{91} = 37$

**39** Use *SageMath*'s **PowerMod** function to compute

$$123456789^{123454321} \bmod 987654321.$$

**40** Use *SageMath*'s **PowerMod** function to compute

$$12345678987654321^{56789876543212345} \bmod 98765432123456789.$$

**41** Use *SageMath*'s **crt** function to find the solution to the system

$$\begin{aligned} k \bmod 953703810582341 &= 638523792756361 \quad \text{and} \\ k \bmod 2526928697126346 &= 1638525978351423. \end{aligned}$$

**42** Use *SageMath*'s **crt** function to find the solution to the system

$$\begin{aligned} k \bmod 8675612376265160933543 &= 152352352346254753545, \quad \text{and} \\ k \bmod 6226345262345235236201 &= 526352346234573523462. \end{aligned}$$

**43** Use *SageMath* to solve the linear congruence equation

$$289475362034522153x \bmod 915156238625161124 = 210982524590982446.$$

**44** Use *SageMath* to solve the linear congruence equation

$$9357298518686215025x \bmod 1965156273498612517 = 1871551633523628256.$$

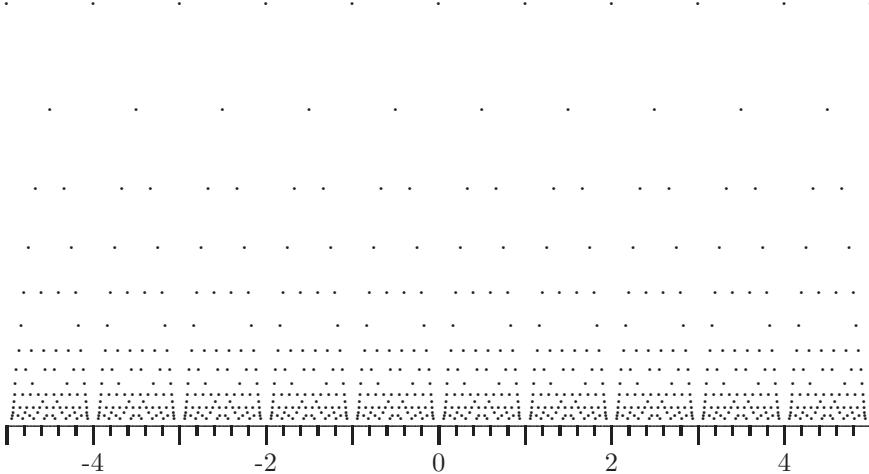
## 1.5 Rational and Real Numbers

Having studied the properties of integers, let us turn our attention to rational numbers and real numbers. The set of rational numbers  $\mathbb{Q}$  can be described as the numbers of the form  $p/q$ , where  $p$  is an integer and  $q$  is a positive integer.

Although the set of rationals  $\mathbb{Q}$  is easy to define, it is often hard to visualize. One way to illustrate the rationals graphically can be seen by the *SageMath* command

**ShowRationals (-5, 5)**

which draws [Figure 1.1](#). This figure helps to visualize the rational numbers from  $-5$  to  $5$  using a sequence of rows. The  $n^{\text{th}}$  row represents the rational numbers with denominator  $n$  when expressed in simplest form. In principle



**FIGURE 1.1:** Plot depicting the rational numbers

there would be an infinite number of rows, getting closer and closer to each other as they get close to the axis.

Figure 1.1 suggests the following.

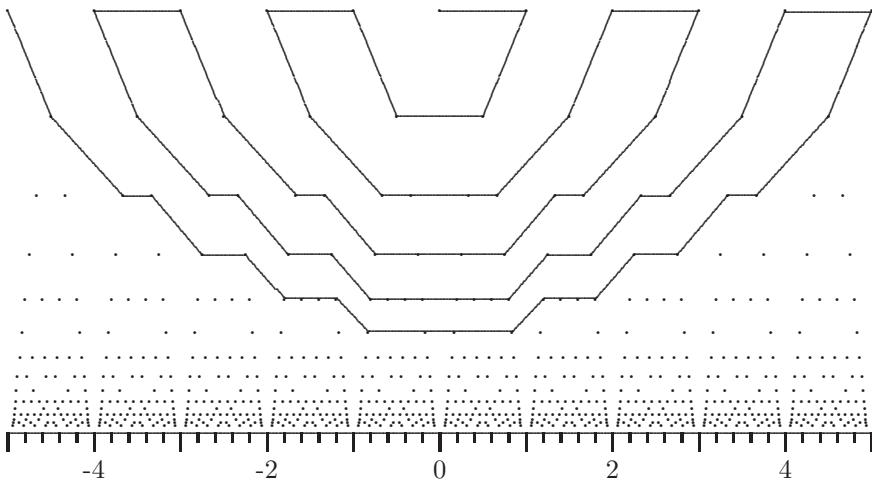
### PROPOSITION 1.3

If  $a$  and  $b$  are any two different real numbers, then there is a rational number between  $a$  and  $b$ .

**PROOF:** Let  $x = |a - b|$ . Since  $x$  is not zero, we let  $q$  be any integer that is greater than  $1/x$ . Then  $|a \cdot q - b \cdot q| = q \cdot x > 1$ , so there must be an integer between  $a \cdot q$  and  $b \cdot q$ , which we will call  $p$ . But then  $p/q$  will be between  $a$  and  $b$ , and the proposition is proved.  $\square$

From this proposition, we can keep dividing the interval up into smaller and smaller pieces to show that there are in fact an infinite number of rational numbers between any two real numbers. This would make it seem that the number of rational numbers is “doubly infinite,” since there are an infinite number of integers, and an infinite number of rational numbers between each pair of integers. But surprisingly, the set of rational numbers is no larger than the set of the integers. To understand what is meant by this statement, let us first show how we can compare the sizes of two infinite sets.

**DEFINITION 1.13** A set  $S$  is called *countable* if there is an infinite sequence of elements from the set that includes every member of the set.



**FIGURE 1.2:** Beginning of a path that will hit every rational number

What do sequences have to do with comparing the sizes of two sets? A sequence can be considered as a function between the set of positive integers and the set  $S$ . If a sequence manages to include every member of the set  $S$ , then it stands to reason that there are at least as “many” positive integers as there are elements of  $S$ . The shocking fact is that even though it would first appear that there must be infinitely many more rational numbers than integers, in fact the two sets have the same size.

#### PROPOSITION 1.4

*The set of rationals forms a countable set.*

PROOF: In order to show that the rationals are countable, we need a sequence that will eventually contain every rational somewhere in the sequence. Equivalently, we can connect the dots of Figure 1.1 using a pattern that would, in principle, reach every dot of Figure 1.1 extended to infinity. There are of course many ways to do this, but one way is given in Figure 1.2. This path starts at 0, and swings back and forth, each time hitting the rationals on the next row. Since there are an infinite number of rows, we can extend this pattern indefinitely, and every rational number will eventually be hit by this path. This path gives rise to the sequence

$$\{0, 1, \frac{1}{2}, \frac{-1}{2}, -1, -2, \frac{-3}{2}, \frac{-2}{3}, \frac{-1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, 2, 3, \dots\}$$

which contains every rational number, so we have shown that the rationals form a countable set.  $\square$

There of course are many other ways of creating a sequence of rational numbers that includes every rational. Problems 1 through 8 explore the Calkin-Wilf sequence, which is a recursively defined sequence that contains all of the positive rational numbers.

Even though we have shown that there are an infinite number of rational numbers between any two numbers, the natural question to ask is whether there are numbers that are not rational. The first number that was discovered not to be rational was  $\sqrt{2}$ , proven by the Greeks. [12, p. 82]

### **PROPOSITION 1.5**

*There is no rational number  $p/q$  such that  $(p/q)^2 = 2$ .*

PROOF: Suppose that there was such a rational number,  $p/q$ . Let us further suppose that  $p/q$  is in simplest form, so that  $p$  and  $q$  are integers with no common factors. We could rewrite the equation  $(p/q)^2 = 2$  as

$$p^2 = 2q^2.$$

This would indicate that  $p^2$  is a multiple of 2, which by Euclid's Lemma (1.4) implies that  $p$  is a multiple of 2.

Next, we make the substitution  $p = 2r$ , where  $r$  is an integer. This produces the equation

$$(2r)^2 = 2q^2, \quad \text{or} \quad 2r^2 = q^2.$$

This would indicate that  $q^2$ , and hence  $q$ , is even by the same reasoning. But this contradicts the fact that  $p/q$  was written in simplest form. Thus, there is no rational number whose square is 2.  $\square$

The real numbers that are not rational are called *irrational* numbers. Irrational numbers are characterized by the fact that their decimal representation never repeats. See Problems 9 and 10.

We will denote the set of real numbers, both rational and irrational, by  $\mathbb{R}$ . We have already proven that there is, in essence, the same number of rational numbers as integers. This may not come as too much of a shock, since both sets are infinite, so logically two infinite sets ought to be the same size. But the set of real numbers is also infinite, so one might be tempted to think that there is the same number of real numbers as integers. However, the number of reals is “more infinite” than the number of integers. In other words, we cannot construct a sequence of real numbers that contains every real number, as we did for rational numbers. This surprising fact was proved by Georg Cantor using a classic argument. [11, p. 670] (See the Historical Diversion on page 39.)

### **THEOREM 1.6: Cantor's Diagonalization Theorem**

*The set of all real numbers between 0 and 1 is uncountable. That is, there*

cannot be a sequence of numbers that contains every real number between 0 and 1.

PROOF: We begin by assuming that we can form such a sequence

$$\{a_1, a_2, a_3, \dots\}$$

and work to find a contradiction. The plan is to find a number  $b$  that cannot be in this list. We can do this by forcing  $b$  to have a different first digit than  $a_1$ , a different second digit than  $a_2$ , a different third digit than  $a_3$ , and so on. The only technical problem with this is that some numbers have two decimal representations, such as

$$0.3486000000000000\dots = 0.3485999999999999\dots$$

For these numbers, all we need to do is require that *both* representations are in the list. (That is, some rational numbers will appear twice on the list with different decimal representations.)

We now can find a number  $b$  using any number of procedures, such as letting the  $n^{\text{th}}$  digit of  $b$  be one more than the  $n^{\text{th}}$  digit of  $a_n$ , **mod** 10. For example, if the list of numbers is

$$\begin{aligned} a_1 &= 0.94837490123798570\dots \\ a_2 &= 0.8384000000000000\dots \\ a_3 &= 0.8383999999999999\dots \\ a_4 &= 0.3428165534342444\dots \end{aligned}$$

then  $b = 0.0499\dots$ . Certainly  $b$  is missing from the list, since it differs from each member of the list by at least one digit. This contradiction proves the theorem.  $\square$

We will use the sets  $\mathbb{Q}$  and  $\mathbb{R}$  throughout this book, so knowing the properties of these two sets will be important in many of the examples.

## Problems for §1.5

- 1 Although we exhibited a sequence that contains every element of  $\mathbb{Q}$ , there are other ways to accomplish this. One way is to consider the Calkin-Wilf sequence, defined recursively by

$$a_0 = 0, \quad \text{and} \quad a_{n+1} = \frac{1}{1 + 2\lfloor a_n \rfloor - a_n} \quad \text{for } n \geq 1.$$

(Recall  $\lfloor a_n \rfloor$  means the largest integer which is less than or equal to  $a_n$ .) Write out the first 16 terms of this sequence,  $a_0$  through  $a_{15}$ . (Problems 2 through 7 show this sequence contains all of the non-negative elements of  $\mathbb{Q}$ .)

## Historical Diversion

# Georg Cantor (1845–1918)

Georg Cantor was born in St. Petersburg, Russia. When he was eleven, his father became ill, so his family moved to Germany to escape the cold climate. He graduated with distinction in 1860 from the Realschule in Darmstadt, with exceptional skills in trigonometry. In 1862, he entered the University of Zürich, but shifted his studies to the University of Berlin after the death of his father. Cantor attended lectures by Leopold Kronecker, Karl Weierstrass and Ernst Kummer.

Cantor completed his dissertation on number theory in 1867, and took up a position at the University of Halle. He began his work on set theory in 1874, being the first mathematician to consider infinite sets. He was able to prove that the set of real numbers is “more numerous” than the set of integers, which shows that there exist infinite sets of different sizes. He was also the first mathematician to appreciate the importance of a one-to-one mapping.

However, his work was met with opposition, particularly from Kronecker. Cantor often proved the existence of sets which had certain properties, without giving any examples of such sets. He assumed that one is allowed to make an infinite number of decisions in the construction of a set, an assumption we currently call the Axiom of Choice. Kronecker, a well-established mathematician, had a constructive viewpoint of mathematics, and called Cantor a “scientific charlatan,” and a “renegade.” While Cantor tried to publish one of his papers in *Acta Mathematica*, the publisher Mittag-Leffler asked Cantor to withdraw the paper, since it was “about one hundred years too soon.”

In 1884, Cantor suffered his first bout with depression, and spent some time in a sanitarium. Cantor soon recovered, and returned to his research, producing his famous diagonal argument and Cantor’s theorem. Cantor also tried to prove, in vain, the Continuum Hypothesis, which states that there is no set that is both strictly larger than the set of integers, but strictly smaller than the set of reals. Today we know that the Continuum Hypothesis, like the Axiom of Choice, is undecidable, that is, it can be neither proven or disproven.

In 1899, Cantor returned to the sanatorium. Soon afterwards, Cantor’s youngest son died suddenly. Cantor’s passion for mathematics was completely drained, and he suffered from chronic depression for the rest of his life, going in and out of sanatoriums. Although he still made mathematical lectures, he retired in 1913, and died in poverty on January 6, 1918 in a sanatorium.



- 2** Show that in the sequence defined by Problem 1, the numerator of  $a_{n+1}$  is the denominator of  $a_n$ , when the fractions are expressed in lowest terms. (Assume integers have a denominator of 1.)
- 3** Define the integer sequence  $b_n$  to be the numerator of  $a_n$  in Problem 1. Show that this sequence satisfies

$$b_0 = 0, \quad b_1 = 1, \quad \text{and} \quad b_{n+2} = b_n + b_{n+1} - 2(b_n \bmod b_{n+1}) \quad \text{for } n \geq 0.$$

This sequence is known as *Stern's diatomic sequence*. (Hint: by Problem 2,  $a_n = b_n/b_{n+1}$ .)

- 4** Use induction to show that the sequence in Problem 3 satisfies

$$b_{2n} = b_n, \quad \text{and} \quad b_{2n+1} = b_n + b_{n+1}$$

for all integers  $n > 0$ .

Hint: Assume *both* statements are true for the case  $n - 1$ , and use Problem 3 to prove both statements for the case  $n$ .

- 5** Use Problem 4 to show that the sequence in Problem 1 satisfies

$$a_{2n} = \frac{a_n}{1 + a_n}$$

for integers  $n > 0$ . Note that  $a_n = b_n/b_{n+1}$ .

- 6** Use Problem 4 to show that the sequence in Problem 1 satisfies

$$a_{2n+1} = a_n + 1$$

for integers  $n > 0$ . Note that  $a_n = b_n/b_{n+1}$ .

- 7** Use Problems 5 and 6 to show that the sequence in Problem 1 contains every non-negative rational number.

Hint: If  $x = p/q$ , let  $n = p + q$ , and assume true for previous  $n$ . Either  $x - 1$  or  $x/(1 - x)$  will have a smaller  $n$ .

- 8** Use Problem 7 to show that no rational number is mentioned twice in the sequence given by Problem 1.

Hint: if  $a_i = a_j$  for  $i > j$ , what is  $a_{2i-j}$ ?

- 9** For a given rational number  $p/q$ , consider the sequence that begins  $a_0 = p$ , and

$$a_{n+1} = (10a_n) \bmod q.$$

Show that this sequence will eventually repeat. See the hint for Problem 8.

- 10** Use Problem 9 to show that the decimal expansion of a rational number  $p/q$  will eventually repeat. ( $1/2$  can be considered as  $.500000000000\cdots$ )

- 11** Show that if the decimal expansion of a number eventually repeats,

$$x = n.d_1d_2d_3 \dots d_i\overline{d_{i+1}d_{i+2} \dots d_{i+j}}$$

the number is rational. Here,  $d_1, d_2, \dots$  and the digits, and the overlined digits will repeat.

Hint: Sum a geometric series.

For Problems **12** through **19**: Prove that the following numbers are irrational.

**12**  $\sqrt{3}$

**13**  $\sqrt[3]{2}$

**14**  $\sqrt{5}$

**15**  $\sqrt{6}$

**16**  $\sqrt{10}$

**17**  $\sqrt{15}$

**18**  $\sqrt[3]{3}$

**19**  $\sqrt[3]{4}$

- 20** Prove that if  $a$  is irrational, then  $1/a$  is irrational.

- 21** Prove that if  $a$  is rational and  $b$  is irrational, then  $a + b$  is irrational.

- 22** Prove that between any two distinct real numbers, there is an irrational number.

Hint: Use Problem 21 along with Proposition 1.3.

- 23** Prove that if  $a$  is rational and nonzero, and  $b$  is irrational, then  $a \cdot b$  is irrational.

- 24** Prove that  $y = \sqrt{2} + \sqrt{3}$  is irrational.

Hint: First show that  $y^2$  is irrational.

- 25** Prove that  $\log_2(3)$  is irrational.

Hint:  $2^{\log_2(3)} = 3$ .

- 26** The number  $e \approx 2.718281828 \dots$  can be expressed by the series

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \dots$$

Show that  $e$  is irrational.

Hint: If  $e = p/q$ , put an upper bound on the sum of the non-integral terms of  $q! \cdot e$ .

- 27** Is the sum of two irrational numbers always irrational? If not, find a counter-example.

### Interactive Problems

- 28** If we begin the sequence in Problem 1 with an irrational number, all terms of the sequence will be irrational. Explore what happens if we consider the same formula, but start with  $a_0 = \sqrt{2}$ .

```
a = sqrt(2); a
sqrt(2)
a = Together(1/(1 + 2*floor(a) - a)); a
1/7*sqrt(2) + 3/7
```

Here, **floor(a)** calculates  $\lfloor a \rfloor$ , and **Together** rationalizes the denominator. By repeatedly evaluating the last statement, we can compute the sequence  $\{a_0, a_1, a_2, a_3, \dots\}$ . Note that  $a_6$  is  $\sqrt{2}$  plus an integer. When is the next time in the sequence that  $a_n$  is an integer plus  $\sqrt{2}$ ?

- 29** Repeat Problem 28, only start with  $a_0 = \sqrt{3}$ . When is the first time  $a_n$  is an integer plus  $\sqrt{3}$ ? When is the next time in the sequence that  $a_n$  is an integer plus  $\sqrt{3}$ ? Can you find a third instance? For an explanation, see [17].

# *Chapter 2*

---

## *Understanding the Group Concept*

The goal of this chapter is to formulate the definition of a group. This is done by first exploring many different examples for which there is a binary operator defined on a set, for which some interesting patterns seem to persist. By observing the minimum requirements for these patterns to appear, we can create the simplest definition of a group that will apply to all of the examples we encountered, plus many other new examples. This will produce an abstract definition of a group.

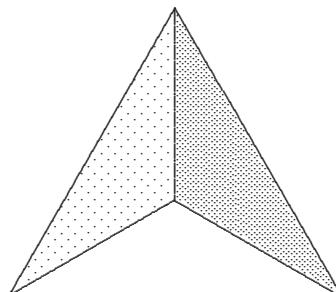
---

### **2.1 Introduction to Groups**

This section focuses on one particular group, and then explores this group to find different patterns within the structure of the group. As we strive to determine why these patterns exist, we begin to find proofs that will later be valid for all groups. This particular example is *non-commutative*, since  $x * y$  is not always equal to  $y * x$ . For students not exposed to linear algebra, non-commutativity takes some time to get used to, hence it is important to introduce it early.

To help introduce us to the concept of groups, let us meet a triangle whose dance steps give us an unusual kind of arithmetic. Terry the triangle is a simple looking three-colored triangle that appears by the *SageMath* command

```
ShowTerry()
```

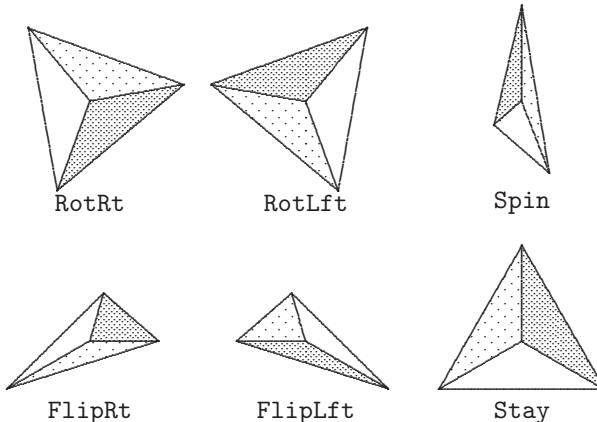


**TABLE 2.1:** Terry's dance steps

---

RotRt	rotate clockwise 120 degrees.
RotLft	rotate counterclockwise 120 degrees.
Spin	spins in three dimensions, keeping the top fixed.
FlipRt	flips over the right shoulder, keeping the left point fixed.
FlipLft	flips over the left shoulder, keeping the right point fixed.
Stay	does nothing.

---

**FIGURE 2.1:** Scenes from Terry's animated dance steps

Terry can perform the dance steps listed in [Table 2.1](#). Although *SageMath* animates these dance steps, one can understand the six steps without *SageMath* by observing scenes in [Figure 2.1](#), taken from the animation close to the completion of each step.

Terry can combine these dance steps to form a dance routine. But in any routine, the ending position of the triangle is the same as that of performing just one dance step. Thus, when the triangle gets “lazy,” it can perform just one dance step instead of several. The *SageMath* command

```
InitTerry()
{Stay, FlipRt, RotRt, FlipLft, RotLft, Spin}
```

allows these dance steps to be combined, using a **\*** between the dance steps. So we find that:

```
FlipRt * Spin
RotLft
```

That is, a flip over the left shoulder followed by a spin puts the triangle in the same orientation as a counter-clockwise rotation.

**TABLE 2.2:** Cayley table for Terry’s dance steps

*	Stay	FlipRt	RotRt	FlipLft	RotLft	Spin
Stay	Stay	FlipRt	RotRt	FlipLft	RotLft	Spin
FlipRt	FlipRt	Stay	FlipLft	RotRt	Spin	RotLft
RotRt	RotRt	Spin	RotLft	FlipRt	Stay	FlipLft
FlipLft	FlipLft	RotLft	Spin	Stay	FlipRt	RotRt
RotLft	RotLft	FlipLft	Stay	Spin	RotRt	FlipRt
Spin	Spin	RotRt	FlipRt	RotLft	FlipLft	Stay

In order to keep track of the way these dance steps are multiplied together, we can form a “multiplication table” of the dance steps, known as the *Cayley table*. The *SageMath* command

**CayleyTable([Stay, FlipRt, RotRt, FlipLft, RotLft, Spin])**

forms the table shown in [Table 2.2](#).

To read this table, the first of the dance steps is located on the left side of the table, and the second dance step is found on the top. Thus, one can use the Cayley table to see that **FlipRt \* Spin = RotLft**. This table allows us to combine dance steps without the help of *SageMath*.

We can notice several things from the Cayley table of the dance steps:

1. The combination of any two dance steps is equivalent to one of the six dance steps. In other words, there are no “holes” in [Table 2.2](#).
2. The *order* in which the dance steps are performed are important. For example, **Spin \* FlipRt ≠ FlipRt \* Spin**.
3. The order in which a dance routine is simplified does not matter. That is,

$$x * (y * z) = (x * y) * z$$

where  $x$ ,  $y$ , and  $z$  represent three dance steps.

4. Any dance step combined with **Stay** yields the same dance step. This is apparent by looking at the row and column corresponding to **Stay** in [Table 2.2](#).
5. Every dance step has another dance step that “undoes” it. That is, for every  $x$  there is a  $y$  such that  $x * y = \text{Stay}$ . For example, the step that undoes **RotRt** is **RotLft**.

We will introduce the following mathematical terminology to express each of these properties:

1. The dance steps are *closed* under the operation  $*$ . Another way of saying this is that  $*$  is a *binary operator*.

2. The dance steps are not *commutative*.
3. The dance steps are *associative*.
4. There is an *identity* dance step.
5. Every dance step has an *inverse*.

With just these properties, we are able to prove the following.

### **PROPOSITION 2.1**

*If  $y$  is an inverse of  $x$ , then  $x$  is an inverse of  $y$ . Furthermore,  $x$  will be the only inverse of  $y$ .*

PROOF: Let  $z$  be *any* inverse of  $y$ . Our job is the show that  $z$  is in fact equal to  $x$ . Consider the product  $x * y * z$ . According to the associative property,

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

On the left side, we see that  $y * z$  is an identity element, so  $x * (y * z) = x$ . But on the right side, we find that  $x * y$  is an identity element, so  $(x * y) * z = z$ . Thus,  $x = z$ , and so  $x$  is an inverse of  $y$ . Therefore, the inverse of an inverse gives us back the original element.

But as a bonus, we see that inverses are unique! We let  $z$  be any inverse of  $y$ , and found that it had to equal  $x$ . Thus,  $y$  has only one inverse, namely  $x$ . But if we apply the argument again, reversing the roles of  $x$  and  $y$ , we see that  $x$  has only one inverse, namely  $y$ . Thus, all inverses are unique.  $\square$

Notice that we did not yet assume that there is only one identity element. However, this fact immediately follows from Proposition 2.1. (See Problems 3 and 4.)

**DEFINITION 2.1** We use the notation  $x^{-1}$  for the unique inverse of the element  $x$ .

Proposition 2.1 can now be expressed simply as  $(x^{-1})^{-1} = x$ . This raises the question as to whether other familiar exponential properties hold. For example, does  $(x * y)^{-1}$  always equal  $x^{-1} * y^{-1}$ ?

```
(Spin * RotRt)^{-1}
  FlipRt
Spin^{-1} * RotRt^{-1}
  FlipLft
```

These results can be verified by looking at [Table 2.2](#). Apparently  $(x * y)^{-1}$  is not always equal to  $x^{-1} * y^{-1}$ . Yet it is not hard to determine the correct way to simplify  $(x * y)^{-1}$ .

**PROPOSITION 2.2**

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

PROOF: Since the inverse  $(x * y)^{-1}$  is the unique dance step  $z$  such that

$$(x * y) * z = \mathbf{Stay},$$

it suffices to show that  $y^{-1} * x^{-1}$  has this property. We see that

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * \mathbf{Stay} * x^{-1} = x * x^{-1} = \mathbf{Stay}.$$

So  $(x * y)^{-1} = y^{-1} * x^{-1}$ . □

Another pattern of the Cayley table of the dance steps is that each row and each column in the interior part of the table contain all six dance steps. For example, **RotRt** appears only once in the row beginning with **Spin**. That is, there is only one solution to  $\mathbf{Spin} * x = \mathbf{RotRt}$ . We can use inverses to show why this pattern holds in general.

**PROPOSITION 2.3**

If  $a$  and  $b$  are given, then there exists a unique  $x$  such that

$$a * x = b.$$

PROOF: Suppose that there is an  $x$  such that  $a * x = b$ . We can multiply both sides of the equation on the *left* by  $a^{-1}$  to give us

$$a^{-1} * (a * x) = a^{-1} * b.$$

Then

$$(a^{-1} * a) * x = a^{-1} * b.$$

$$\mathbf{Stay} * x = a^{-1} * b.$$

So

$$x = a^{-1} * b.$$

Thus, if there is a solution, this must be the unique solution  $x = a^{-1} * b$ . Let us check that this is indeed a solution.

$$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = \mathbf{Stay} * b = b.$$

Thus, there is only one solution to the equation, namely  $a^{-1} * b$ . □

This last proposition, when combined with Problem 6, shows that the interior of the Cayley table forms a *Latin square*. A Latin square is a formation

in which every row and every column contain each item once and only once. The Latin square property is easy to check visually.

Even though there are very few of Terry's dance steps, we already can see some of the patterns that can appear when we consider the "multiplication" of these dance steps. In the next section, we will consider another operation that has many of the same patterns.

## Problems for §2.1

- 1** Suppose that Terry the Triangle has a friend who is a square. (Most of us have had such a friend from time to time.) How many dance steps would the square have? Construct a Cayley table of all of the square's dance steps. This group is referred to as  $D_4$ .
- 2** Suppose that Terry has a friend who is a regular tetrahedron. (A tetrahedron is a triangular pyramid.) How many dance steps would this tetrahedron have?
- 3** Using only the four basic properties of Terry's dance steps, prove that there can be only one identity element. That is, there cannot be two elements  $e$  and  $e'$  for which  $x * e = e * x = x$  and  $x * e' = e' * x = x$  for all  $x \in G$ .
- 4** Using only the four basic properties of Terry's dance steps, prove that an element cannot have two different inverses. That is, show that there cannot be two elements  $y$  and  $y'$  such that both  $x * y = e$  and  $x * y' = e$ .
- 5** Prove the cancellation law holds for Terry's dance steps. That is, if  $a * b = a * c$  for dance steps  $a$ ,  $b$ , and  $c$ , then  $b = c$ .
- 6** Prove that if  $a$  and  $b$  are two of Terry's dance steps, then there is a unique dance step  $x$  such that

$$x * a = b.$$

This shows that every column in the Cayley table contains one and only one of each element.

- 7** If two of Terry's dance steps are chosen at random, what are the chances that these two dance steps will commute?

Hint: There are 36 ways of choosing two dance steps. Count the number of combinations that satisfy the equation  $x * y = y * x$ .

- 8** Three of Terry's dance steps are types of flips, **FlipRt**, **FlipLft**, and **Spin**. Is the product of two different flips always produce a rotation? Explain why this is so.

- 9** Is the product of a flip and a rotation always a flip? Explain why this is so. See Problem 8.
- 10** Find three of Terry's dance steps  $a$ ,  $b$ , and  $c$  such that  $a * b = b * c$ , but  $a \neq c$ .
- 11** Find two of Terry's dance steps  $a$  and  $b$  such that  $(a * b)^{-1} \neq a^{-1} * b^{-1}$ .
- 12** Find two of Terry's dance steps  $a$  and  $b$  such that  $(a * b)^2 \neq a^2 * b^2$ .

### Interactive Problems

- 13** If Terry was only allowed to do the dance steps **FlipRt** or **FlipLft**, could it get itself into all six possible positions? If possible, express the other four dance steps in terms of these two. The command

**InitTerry()**

reloads Terry's group.

- 14** Repeat Problem 13, only allow Terry to do only the steps **RotRt** and **RotLft**.
- 15** Can you find a dance routine which includes each of Terry's 6 dance steps once, and only once, that puts Terry back into the initial position?
- 

## 2.2 Modular Congruence

We have already seen that one operation, namely the combination of Terry's dance steps, produces some interesting properties such as the Latin square property. In this section, we will find some other operations that have many of the same properties, using ordinary integers and modulo arithmetic.

We have already introduced modular arithmetic in §1.4. We defined  $x \bmod n$  as the remainder  $r$  when  $x$  is divided by  $n$ , using the division algorithm. But we can also say that two integers  $x$  and  $y$  are *equivalent* if

$$x \bmod n = y \bmod n.$$

We will introduce another notation for this relation.

**DEFINITION 2.2** Let  $x$ ,  $y$ , and  $n$  be integers. We say  $x$  and  $y$  are *equivalent modulo  $n$* , written

$$x \equiv y \pmod{n}$$

if, and only if, there is an integer  $k$  such that

$$(x - y) = k \cdot n.$$

Note the slight difference in notation between the operator **mod** (expressed in boldface) and the above notation (where mod is not in boldface). The two notations are clearly related, since  $x \equiv y \pmod{n}$  means that  $x \text{ mod } n = y \text{ mod } n$ .

The new notation also satisfies three very important properties for equivalence ( $\pmod{n}$ ).

1. (Reflexive) Every integer  $x$  is equivalent to itself.
2. (Symmetric) If  $x$  is equivalent to  $y$ , then  $y$  is equivalent to  $x$ .
3. (Transitive) If  $x$  is equivalent to  $y$ , and  $y$  in turn is equivalent to  $z$ , then  $x$  is equivalent to  $z$ .

**DEFINITION 2.3** Any relation that satisfies these three properties is called an *equivalence relation*. We will use the notation  $x \sim y$  to say that  $x$  is equivalent to  $y$  for a generic equivalence relation.

Let us prove that equivalence ( $\pmod{n}$ ) forms an equivalence relation.

#### PROPOSITION 2.4

Let  $n$  be a positive integer. Then the definition of

$$x \equiv y \pmod{n}$$

forms an equivalence relation on the set of integers.

PROOF: To show that this definition is reflexive, we need to show that  $x \equiv x \pmod{n}$ , which is clear since  $x - x = 0 \cdot n$ .

To show that this definition is symmetric, suppose that  $x \equiv y \pmod{n}$ . Then  $x - y = kn$  for some integer  $k$ , hence  $y - x = -kn$  for the integer  $-k$ . Thus,  $y \equiv x \pmod{n}$ .

Finally, to show that this definition is transitive, suppose both  $x \equiv y \pmod{n}$  and  $y \equiv z \pmod{n}$ . Then  $x - y = k_1n$  and  $y - z = k_2n$ , so

$$x - z = (x - y) + (y - z) = k_1n + k_2n = (k_1 + k_2)n.$$

Hence, we find that  $x \equiv z \pmod{n}$ . □

Whenever an equivalence relation is defined on a set, the set can be broken up into disjoint *equivalence classes*, where each equivalence class is the set of elements related to one element in the class.

**DEFINITION 2.4** Let  $x \sim y$  be an equivalence relation defined on a set  $S$ . Then the equivalence class  $[a]$  is the set of elements of  $S$  related to  $a$ . That is,

$$[a] = \{s \in S \mid s \sim a\}.$$

**Example 2.1**

In the relation  $x \equiv y \pmod{10}$ , the set  $[3]$  will be the set of integers equivalent to 3 (mod 10), giving the set

$$[3] = \{\dots - 37, -27, -17, -7, 3, 13, 23, 33, 43, \dots\}$$

Other equivalence classes in this relation are similar. □

It is not hard to show that the set of integers can be broken up into disjoint sets using the equivalence classes.

**PROPOSITION 2.5**

If  $x \sim y$  is an equivalence relation on a set  $S$ , then  $S$  is the disjoint union of equivalence classes.

PROOF: For any  $a \in S$ , we have by the reflexive property that  $a \in [a]$ , so  $[a]$  is non-empty, and the union of all equivalence classes will be all of  $S$ . Next, let us show that if there is an element  $c$  in common with two equivalence classes  $[a]$  and  $[b]$ , then these classes are the same. Since  $c \sim a$  and  $c \sim b$ , we have by the symmetric and transitive properties that  $a \sim b$ . Hence, for every  $x \in [a]$ ,  $x \sim a$ , so  $x \in [b]$  as well, indicating  $[a] \subseteq [b]$ . By similar logic,  $[b] \subseteq [a]$ , so  $[a] = [b]$ . □

Many of the properties of modular arithmetic found in §1.4 can be translated in terms of equivalence relations. For example, Proposition 1.2 can be restated by saying that if

$$x \equiv a \pmod{n} \quad \text{and} \quad y \equiv b \pmod{n},$$

then  $x + y \equiv a + b \pmod{n}$  and  $xy \equiv ab \pmod{n}$ .

These statements make it clear that to add or multiply two numbers modulo  $n$ , we can choose any representative element from the equivalence class.

One common exercise with modulo arithmetic is solving the linear congruence equation  $(mx) \pmod{n} = a$ , where  $m$  is coprime to  $n$ . In the new notation this becomes

$$mx \equiv a \pmod{n}.$$

Although this can be converted to a Chinese remainder problem, there is another way to solve this if  $m$  happens to have only small prime factors. The method relies on the following proposition.

**PROPOSITION 2.6**

If  $ab \equiv ac \pmod{n}$ , and if  $a$  is coprime to  $n$ , then  $b \equiv c \pmod{n}$ .

PROOF: We are essentially given that  $ab - ac = kn$  for some integer  $k$ . Since  $a$  and  $n$  are coprime, by Bézout's lemma (1.3), there exist integers  $u$  and  $v$  such that  $ua + vn = 1$ . Multiplying the original equation by  $u$ , we have  $ua(b - c) = kun$ . Replacing  $ua$  with  $1 - vn$ , we get that  $b - c = kun + vn(b - c)$ , which is a multiple of  $n$ . So  $b \equiv c \pmod{n}$ .  $\square$

This proposition essentially says we can cancel any factors coprime to  $n$  from both sides of the equation  $mx \equiv a \pmod{n}$ . If there are no common factors, we can keep adding (or subtracting)  $n$  to the right-hand side until we get a common factor.

**Example 2.2**

Solve the linear congruence equation  $12x \equiv 7 \pmod{19}$ .

SOLUTION: We keep adding 19 to the right-hand side, canceling out any common factors we find.

$$\begin{aligned} 12x &\equiv 7 \pmod{19} \\ 12x &\equiv 26 \pmod{19} \\ 6x &\equiv 13 \pmod{19} \\ 6x &\equiv 32 \pmod{19} \\ 3x &\equiv 16 \pmod{19} \\ 3x &\equiv 35 \pmod{19} \\ 3x &\equiv 54 \pmod{19} \\ x &\equiv 18 \pmod{19} \end{aligned}$$

 $\square$ 

It should be noted that if  $m$  is large, converting to a Chinese remainder problem is much more efficient, since this method does not rely on the prime factorization of  $m$ .

**Computational Example 2.3**

Consider the set of numbers from 0 to 9, with the binary operation being  $x * y = (x + y) \bmod 10$ . We can have *SageMath* define this binary operation with the command

```
Z = AddMod(10); Z
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
```

**TABLE 2.3:** Addition (mod 10)

	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	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Although the elements of **z** are displayed as integers, we will soon see that they have different properties than ordinary integers. We will continue to use the star to indicate the operation, as we did for Terry's dance steps. In order to access the elements in the set **z**, we will put a number in brackets to indicate the location of the element in the set. So here is how we can combine the fourth and seventh elements in **z**:

**z[4] \* z[7]**

1

So with the star meaning “addition modulo 10,” we find that  $4 * 7 = 1$ . Although it seems strange to use the star instead of the plus sign, we will always use either a star or a dot for the binary operation, whatever that operator is. So the one thing we must remember is that *the star or dot does not always mean multiplication*. Rather, the star represents the operation in the current context. For Terry's group, the star represented combining two dance steps. Here, it represents addition modulo 10.

We will still use the command **CayleyTable** to give the Cayley table of the set. Thus the command

**CayleyTable(z)**

produces Table 2.3. □

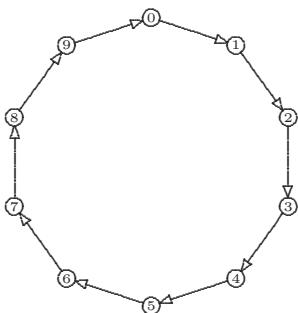
By looking at the table for addition modulo 10, we are able to establish the following properties:

1. For any two numbers  $x$  and  $y$  in  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ,  $x * y$  is in the set. (Recall that we are using the star to indicate the operation, regardless of what that operation is. In this example, the operation is addition modulo 10.)

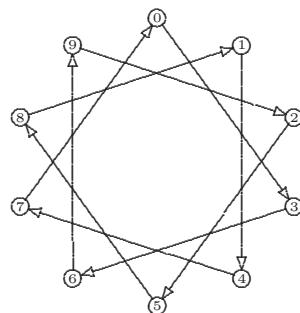
2.  $(x * y) * z = x * (y * z)$  for any  $x, y$ , and  $z$ .
3.  $x * 0 = x$  and  $0 * x = x$  for all  $x$ .
4. For any  $x$ , there is a  $y$  such that  $x * y = 0$ .
5. For any  $x$  and  $y$ ,  $x * y = y * x$ .

This operation can also be pictured by means of circular graphs. The *SageMath* command

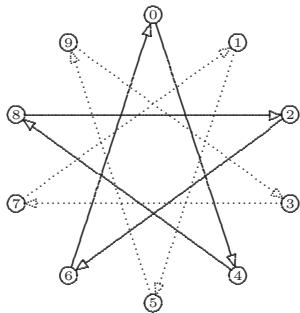
```
CircleGraph(Z, Add(1))
```



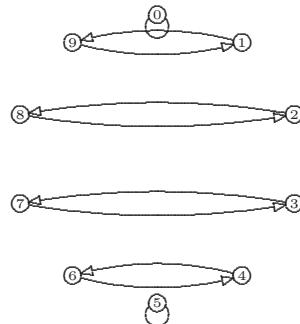
**CircleGraph(Z, Add(1))**



**CircleGraph(Z, Add(3))**



**CircleGraph(Z, Add(4))**



**CircleGraph(Z, Inv)**

**FIGURE 2.2:** Circle graphs for  $(\text{mod } 10)$  arithmetic

gives us the first picture in [Figure 2.2](#), which draws an arrow from each point to the point given by “adding 1 modulo 10.” [Figure 2.2](#) also shows what happens if we replace the 1 with 3 or 4. We get different looking graphs, but all with the same amount of symmetry. The *SageMath* command

**TABLE 2.4:**  $x * y = xy \bmod 7$ 

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

```
CircleGraph(Z, Add(1), Add(2), Add(3), Add(4), Add(5))
```

combines several of these circular graphs together, each drawn in a different color. The last picture in [Figure 2.2](#) shows the additive inverse of each digit. This graph was created with the command

```
CircleGraph(Z, Inv)
```

Of course, we could do these same experiments by considering addition modulo  $n$  with any other base as well as  $n = 10$ . The patterns formed by the circular graphs are very similar. But we can also consider the operation of *multiplying* modulo  $n$ .

### Example 2.4

Consider the set of elements  $\{0, 1, 2, 3, 4, 5, 6\}$ , with the binary operation  $x * y = xy \bmod 7$ . Form a Cayley table of this operator. Does this the table have the Latin square properties that we have been observing?

SOLUTION: This set is small enough so we can compute the table by hand, producing [Table 2.4](#). Although the first row and first column are all zeros, we notice that if we removed the 0 and only considered the digits  $\{1, 2, 3, 4, 5, 6\}$ , we would get a Latin square. The identity element is 1, and each of the numbers has an inverse. □

If we try Example 2.4 with a different base, we get a surprise. To display the Cayley table for  $(\bmod 10)$  arithmetic, we can use the *SageMath* command

```
Z = MultMod(10)
CayleyTable(Z)
```

to produce a table similar to [Table 2.5](#). We find several rows that do not contain any 1's. These rows indicate the numbers without inverses modulo 10. Only 1, 3, 7, and 9 have inverses. If we try this using 15 instead of 10, we find only 1, 2, 4, 7, 8, 11, 13, and 14 have inverses.

**TABLE 2.5:** Multiplication (mod 10)

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

**Computational Example 2.5**

What if we consider the Cayley table of just those numbers that have inverses modulo 15? We can use the *SageMath* commands

```
Z = MultMod(15)
L = [Z[1], Z[2], Z[4], Z[7], Z[8], Z[11], Z[13]]
CayleyTable(L)
```

to produce Table 2.6. Once again, many of the same patterns are found that

**TABLE 2.6:** Invertible elements (mod 15)

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

were in for Terry's multiplication, namely:

- For any two numbers  $x$  and  $y$  in  $\{1, 2, 4, 7, 8, 11, 13, 14\}$ ,  $x * y$  is in that set.
- $(x * y) * z = x * (y * z)$  for any  $x, y$ , and  $z$ .

3.  $x * 1 = x$  and  $1 * x = x$  for all  $x$ .
4. For any  $x$ , there is a  $y$  such that  $x * y = 1$ .
5. For any  $x$  and  $y$ ,  $x * y = y * x$ . □

We can generalize these patterns to multiplication modulo  $n$  for any  $n$ .

### **PROPOSITION 2.7**

For  $n$  an integer greater than 1, let  $G$  be the set of all positive numbers less than  $n$  that have multiplicative inverses modulo  $n$ . Let the operation  $(*)$  denote multiplication modulo  $n$ . Then the set  $G$  has the following properties:

1. For any two numbers  $x$  and  $y$  in  $G$ ,  $x * y$  is in  $G$ .
2.  $(x * y) * z = x * (y * z)$  for any  $x$ ,  $y$ , and  $z$ .
3.  $x * 1 = 1 * x = x$  for all  $x$ .
4. For any  $x$  that is in  $G$ , there is a  $y$  in  $G$  such that  $x * y = 1$ .
5. For any  $x$  and  $y$ ,  $x * y = y * x$ .

PROOF: Properties 2, 3, and 5 come from the properties of standard multiplication.

Property 1 comes from Proposition 2.2. If  $x$  and  $y$  are both invertible, then  $y^{-1} * x^{-1}$  is an inverse of  $x * y$ , and so  $x * y$  is invertible modulo  $n$ .

Property 4 seems obvious, since if  $x$  is invertible modulo  $n$ , we let  $y = x^{-1}$  making  $x * y = 1$ . But we must check that  $y$  is also invertible, which it is since  $y^{-1} = x$ . □

Of course, this does not tell us *which* of the numbers less than  $n$  have inverses modulo  $n$ . The following proposition will help us out.

### **PROPOSITION 2.8**

Let  $n$  be in  $\mathbb{Z}^+$ . Then for  $x$  between 0 and  $n - 1$ ,  $x$  has a multiplicative inverse modulo  $n$  if, and only if,  $x$  is coprime to  $n$ .

PROOF: If  $x$  and  $n$  are not coprime, then there is a common prime factor  $p$ . In order for  $x$  to have a multiplicative inverse, there must be a  $y$  such that

$$xy \equiv 1 \pmod{n}.$$

But this means that  $xy = 1 + wn$  for some  $w$ . This is impossible, since  $xy$  is a multiple of  $p$ , but  $1 + wn$  is one more than a multiple of  $p$ .

Now suppose that  $n$  and  $x$  are coprime. By Bézout's lemma (1.3), there are  $u$  and  $v$  in  $\mathbb{Z}$  such that

$$un + vx = \gcd(n, x) = 1.$$

But then

$$vx = 1 + (-u)n,$$

and so  $vx \equiv 1 \pmod{n}$ . Hence,  $v$  is a multiplicative inverse of  $x$ . □

We now have seen several binary operations, such as Terry's dance steps, addition modulo  $n$ , and multiplication modulo  $n$ , which have many properties in common. In the next section we will generalize these examples to produce many more interesting examples, but in such a way that they will all have the important properties that we have seen.

## Problems for §2.2

For Problems 1 through 8: Solve the following linear congruence problems.

- |                                    |                                    |
|------------------------------------|------------------------------------|
| <b>1</b> $8x \equiv 5 \pmod{9}$    | <b>5</b> $20x \equiv 13 \pmod{31}$ |
| <b>2</b> $16x \equiv 7 \pmod{19}$  | <b>6</b> $30x \equiv 11 \pmod{47}$ |
| <b>3</b> $12x \equiv 21 \pmod{23}$ | <b>7</b> $31x \equiv 15 \pmod{49}$ |
| <b>4</b> $12x \equiv 21 \pmod{29}$ | <b>8</b> $37x \equiv 13 \pmod{51}$ |

For Problems 9 through 14: Construct a Cayley table for the set of numbers using addition modulo  $n$ .

- |                                               |                                                    |
|-----------------------------------------------|----------------------------------------------------|
| <b>9</b> $\{0, 1, 2, 3, 4\}, n = 5$           | <b>12</b> $\{0, 2, 4, 6\}, n = 8$                  |
| <b>10</b> $\{0, 1, 2, 3, 4, 5\}, n = 6$       | <b>13</b> $\{0, 2, 4, 6, 8, 10\}, n = 12$          |
| <b>11</b> $\{0, 1, 2, 3, 4, 5, 6, 7\}, n = 8$ | <b>14</b> $\{0, 3, 6, 9, 12, 15, 18, 21\}, n = 24$ |

For Problems 15 through 20: Construct a Cayley table for the set of numbers using multiplication modulo  $n$ .

Hint: Since these are the numbers that are coprime to  $n$ , Propositions 2.7 and 2.8 show that the Cayley table has the same properties as Terry's dance steps, in particular, the Latin square property.

- |                                         |                                                     |
|-----------------------------------------|-----------------------------------------------------|
| <b>15</b> $\{1, 3, 5, 7\}, n = 8$       | <b>18</b> $\{1, 3, 5, 9, 11, 13\}, n = 14$          |
| <b>16</b> $\{1, 2, 4, 5, 7, 8\}, n = 9$ | <b>19</b> $\{1, 5, 7, 11, 13, 17\}, n = 18$         |
| <b>17</b> $\{1, 5, 7, 11\}, n = 12$     | <b>20</b> $\{1, 5, 7, 11, 13, 17, 19, 23\}, n = 24$ |

- 21** Let  $S$  be a set, and suppose  $S$  can be described as the union of a collection of non-empty, disjoint subsets. Show that there is an equivalence relation such that the equivalence classes is precisely the given collection of disjoint subsets.

- 22** Let  $f : S \rightarrow T$  be a function defined on a set  $S$ . Define  $x \sim y$  if  $f(x) = f(y)$ . Show that this defines an equivalence relation on  $S$ .

For Problems **23** through **28**: Find the multiplicative inverse modulo  $n$  for the following numbers. That is, find a  $y$  such that  $xy \pmod n = 1$ .

Hint: Look at the proof of Proposition 2.8.

**23**  $7 \pmod{16}$

**26**  $5 \pmod{18}$

**24**  $8 \pmod{17}$

**27**  $7 \pmod{20}$

**25**  $10 \pmod{21}$

**28**  $9 \pmod{22}$

### Interactive Problems

For Problems **29** through **34**: Proposition 2.8 explains how to use `xgcd` to find the multiplicative inverse modulo  $n$ . Use *SageMath* to find the multiplicative inverse of  $a$  modulo  $n$ .

**29**  $a = 3, n = 1000$

**32**  $a = 11, n = 9000$

**30**  $a = 5, n = 1221$

**33**  $a = 13, n = 12000$

**31**  $a = 7, n = 3600$

**34**  $a = 17, n = 15000$

- 35** We saw that there were exactly four numbers less than 10 which were invertible modulo 10. For what other values of  $n$  are there exactly four numbers less than  $n$  which are invertible modulo  $n$ ? Use *SageMath*'s circle graph to graph the inverse functions.
- 

## 2.3 The Definition of a Group

In this chapter, we have seen several different ways of combining numbers or dance steps. Yet, all of the different “products” had many properties in common. We are now ready to try to generalize these examples. Our strategy is to define a *group* abstractly by requiring the same patterns we observed to continue. Thus, we make the following definition based upon the first four properties we saw in all of our examples.

**DEFINITION 2.5** A *group* is a set  $G$  together with a binary operation (represented by either a star  $*$ , or more commonly, a dot  $\cdot$ ) such that the following four properties hold:

1. (closure) For any  $x$  and  $y$  in  $G$ ,  $x \cdot y$  is in  $G$ .
2. (identity) There exists a member denoted by  $e$  in  $G$  which has the property that, for all  $x$  in  $G$ ,  $e \cdot x = x \cdot e = x$ .
3. (inverse) For every  $x$  in  $G$ , there exists a  $y$  in  $G$ , called the *inverse* of  $x$ , such that  $x \cdot y = e$ .
4. (associative law) For any  $x$ ,  $y$ , and  $z$  in  $G$ , then  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

Terry's dance steps give us the first example of a group, more commonly referred to as the group of symmetries of a triangle,  $D_3$ .

The members of the group, whether they are numbers, dance steps, or even ordered pairs, are called the *elements* of the group. The element  $e$  that satisfies property 2 is called the *identity element* of the group.

The mathematical notation for an element  $x$  to be in a group  $G$  is

$$x \in G.$$

Since Propositions 2.1, 2.2, and 2.3 used only these four properties, the proofs are valid for all groups, using the identity element  $e$  in place of the dance step **Stay**.

Other examples of groups come from modular arithmetic. For  $n$  in  $\mathbb{Z}^+$ , we considered the elements

$$\{0, 1, 2, \dots, n - 1\},$$

with the operator  $(\cdot)$  being the sum modulo  $n$ . This group will be denoted  $Z_n$ . In fact, the *SageMath* command **ZGroup** will load the group  $Z_n$ .

**G = ZGroup(10); G**

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

We also considered having the binary operator denote the product modulo  $n$ , and considered only the set of numbers less than  $n$  that are coprime to  $n$ . Proposition 2.7 shows that this set also has the four properties of groups. We will refer to this group by  $Z_n^*$ . This group can be loaded in *SageMath* by the command **ZStar**.

**G = ZStar(15); G**

$$\{1, 2, 4, 7, 8, 11, 13, 14\}$$

The groups  $Z_n$  and  $Z_n^*$  had a fifth property—the Cayley tables were symmetric about the northwest to southeast diagonal. Not all groups have this property, but those that do are important enough to give a special name.

**DEFINITION 2.6** A group  $G$  is *abelian* (or *commutative*) if  $x \cdot y = y \cdot x$  for all  $x, y \in G$ .

Although these definitions appear to be ad hoc, in fact the four properties of groups have been carefully chosen so that they will apply to many different aspects of mathematics. Here are some important examples of groups that appear on other contexts besides group theory:

### Example 2.6

The set of integers  $\mathbb{Z}$ , with the binary operation being the sum of two numbers. The identity element is 0, and  $-x$  is the inverse of  $x$ . This forms an abelian group. □

**Example 2.7**

Consider the set of rational numbers, denoted by  $\mathbb{Q}$ . We will still use addition for our binary operation. This is also an abelian group.  $\square$

**Example 2.8**

Consider the set of all rational numbers except for 0. This time we will use multiplication instead of addition for our group operation. The identity element is now 1, and the inverse of an element is the reciprocal. This abelian group will be denoted by  $\mathbb{Q}^*$ .  $\square$

**Example 2.9**

Consider the set of all *linear* functions of the form  $f(x) = mx + b$ , with  $m, b \in \mathbb{R}$ ,  $m \neq 0$ . (The  $\mathbb{R}$  represents the real numbers.) We combine two linear functions together by function composition. That is, if  $f(x) = mx + b$  and  $g(x) = nx + c$ , then

$$f \cdot g = f(g(x)) = m(nx + c) + b = (mn)x + (mc + b).$$

Note that in  $f \cdot g$ , we do  $g$  first, then  $f$ , so we apply the functions from right to left. We can find the inverse of  $f(x)$  as well:

$$f^{-1}(x) = \frac{1}{m}x - \frac{b}{m},$$

which is also a linear function. This group satisfies all of the group properties, but is not abelian. For example, if  $f(x) = 2x + 3$  and  $g(x) = 3x + 2$ , then  $f \cdot g = f(g(x)) = 6x + 7$ , whereas  $g \cdot f = g(f(x)) = 6x + 11$ .  $\square$

**DEFINITION 2.7** The number of elements in a group  $G$  is called the *order* of the group and is denoted  $|G|$ . If  $G$  has an infinite number of elements, we say that  $|G| = \infty$ .

Examples 2.6 through 2.9 have infinite order, and hence we cannot form Cayley tables for these groups. On the other hand, the *smallest* possible group is given by the following example.

**Example 2.10**

Consider the group containing just the identity element,  $\{e\}$ . We can have *SageMath* give a Cayley table of this group by the following commands:

```
InitGroup("e")
CayleyTable([e])
```

	·	$e$
	$e$	$e$
	$e$	$e$

We call this group the *trivial group*. The first of these *SageMath* commands introduces a new command—**InitGroup**. This command designates the new identity element, and sets the stage for entering a new group. □

Note that sometimes the operator  $(\cdot)$  means addition, sometimes it means multiplication, and sometimes it means neither. Nonetheless, we can define  $x^n$  to mean  $x$  operated on itself  $n$  times. Thus,

$$x = x^1,$$

$$x \cdot x = x^2,$$

$$x \cdot x \cdot x = x^3,$$

etc.

We want to formally define  $x^n$  for any integer  $n$ . We let  $x^0 = e$ , the identity element. We then define, for  $n > 0$ ,

$$x^n = x^{n-1} \cdot x.$$

By defining the  $n$ th power in terms of the previous power, we have defined  $x^n$  whenever  $n$  is a positive integer.

Finally, we can define negative powers by letting

$$x^{-n} = (x^n)^{-1} \quad \text{if } n > 0.$$

This is a *recursive* definition, since it defines each power in terms of a previous power. This type of definition works well for proving simple propositions about  $x^n$ .

### **PROPOSITION 2.9**

If  $x$  is an element in a group  $G$ , and  $m$  and  $n$  are integers, then

$$x^{m+n} = x^m \cdot x^n.$$

PROOF: If  $m$  or  $n$  are 0, this proposition is very easy to verify:

$$x^{m+0} = x^m = x^m \cdot e = x^m \cdot x^0, \quad x^{0+n} = x^n = e \cdot x^n = x^0 \cdot x^n.$$

We will now prove the statement when  $m$  and  $n$  are positive integers. If  $n$  is 1, then we have

$$x^{m+1} = x^{(m+1)-1} \cdot x = x^m \cdot x^1,$$

using the recursive definition of the power of  $x$ .

We will now proceed by means of *mathematical induction*. That is, we will assume that the statement is true for the case  $n - 1$ , and then prove that it is then true for the case  $n$ .

Thus, we will assume that

$$x^{m+(n-1)} = x^m \cdot x^{n-1}.$$

But then

$$x^{m+n} = x^{m+n-1} \cdot x = x^m \cdot x^{n-1} \cdot x = x^m \cdot x^n.$$

By induction, this proves that  $x^{m+n} = x^m \cdot x^n$  for all positive  $n$ .

Once we have the statement true for positive  $m$  and  $n$ , we can take the inverse of both sides to give us

$$(x^{m+n})^{-1} = (x^n)^{-1} \cdot (x^m)^{-1}.$$

But by the definition of negative exponents, this is

$$x^{(-n)+(-m)} = x^{-n} \cdot x^{-m}$$

which, by letting  $M = -n$  and  $N = -m$ , proves the proposition for the case of both exponents being negative.

Finally, if  $m$  and  $n$  have different signs, then  $(m+n)$  will either have the same sign as  $-n$ , or the same sign as  $-m$ . If  $(m+n)$  has the same sign as  $-n$ , then we have already shown that

$$x^m = x^{(m+n)+(-n)} = x^{m+n} \cdot x^{-n}.$$

So we have  $x^m \cdot (x^{-n})^{-1} = x^{m+n} \cdot x^{-n} \cdot (x^{-n})^{-1}$ , and hence  $x^{m+n} = x^m \cdot x^n$ .

If  $(m+n)$  has the same sign as  $-m$ , then we have already shown that

$$x^n = x^{(-m)+(m+n)} = x^{-m} \cdot x^{m+n}.$$

So we have  $(x^{-m})^{-1} \cdot x^n = (x^{-m}) \cdot x^{-m} \cdot x^{m+n}$ , and hence  $x^{m+n} = x^m \cdot x^n$ .

Thus we have proven the proposition for all integers  $m$  and  $n$ .  $\square$

This last proof utilizes an important method of proving theorems called *mathematical induction*, which was introduced in §1.2. Induction is based on the well-ordering axiom, which states that any non-empty subset of positive integers contains a smallest element. Here is another example of mathematical induction.

### **PROPOSITION 2.10**

*If  $x$  is an element in a group  $G$ , and  $m$  and  $n$  are in  $\mathbb{Z}$ , then*

$$(x^m)^n = x^{(mn)}.$$

PROOF: Notice that this statement is trivial if  $n = 0$  and  $n = 1$ :

$$(x^m)^0 = e = x^{m \cdot 0}, \quad (x^m)^1 = x^m = x^{(m \cdot 1)}.$$

We will again proceed by means of induction, which means we can assume that the statement is true for the previous case, with  $n$  replaced by  $n - 1$ . That is, we can assume that

$$(x^m)^{n-1} = x^{m \cdot (n-1)}.$$

Note that

$$(x^m)^n = (x^m)^{n-1} \cdot x^m = x^{m \cdot (n-1)} \cdot x^m$$

By Proposition 2.9, this is equal to  $x^{m \cdot (n-1) + m} = x^{mn}$ .

So by induction, the proposition holds for positive  $n$ . To see that it holds for negative  $n$  as well, simply note that

$$(x^m)^n = ((x^m)^{-n})^{-1} = (x^{-mn})^{-1} = x^{mn}.$$

If  $n$  is negative, then  $-n$  is positive, so the second step is valid. □

Propositions 2.9 and 2.10 show that the common laws of exponents hold for elements of a group. In the next chapter, we will use the powers of elements to explore the properties of a group.

## Problems for §2.3

- 1** Consider the following Cayley table:

.	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Notice that this Cayley table satisfies the “Latin square” property, hence this binary operation satisfies Proposition 2.3. Does this set form a group? Why or why not?

- 2** Consider the following Cayley table:

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Notice that this multiplication table satisfies the “Latin square” property, hence this binary operation satisfies Proposition 2.3. Does this set form a group? Why or why not?

For Problems 3 through 14: Decide whether each set forms a group using the given binary operation. If it is not a group, state which part of Definition 2.5 fails to hold.

- |           |                                           |                      |
|-----------|-------------------------------------------|----------------------|
| <b>3</b>  | $G = \text{rational numbers},$            | $x * y = x + y.$     |
| <b>4</b>  | $G = \text{irrational numbers},$          | $x * y = x + y.$     |
| <b>5</b>  | $G = \text{non-negative real numbers},$   | $x * y = xy.$        |
| <b>6</b>  | $G = \text{positive rational numbers},$   | $x * y = xy.$        |
| <b>7</b>  | $G = \text{positive irrational numbers},$ | $x * y = xy.$        |
| <b>8</b>  | $G = \text{non-negative integers},$       | $x * y = x + y.$     |
| <b>9</b>  | $G = \text{even integers},$               | $x * y = x + y.$     |
| <b>10</b> | $G = \text{odd integers},$                | $x * y = x + y.$     |
| <b>11</b> | $G = \text{odd integers},$                | $x * y = xy.$        |
| <b>12</b> | $G = \text{all integers},$                | $x * y = xy.$        |
| <b>13</b> | $G = \{1, -1\},$                          | $x * y = xy.$        |
| <b>14</b> | $G = \text{all integers},$                | $x * y = x + y + 3.$ |

**15** Note that in Definition 2.5, we only required the inverse of  $x$  to have the property that  $x \cdot y = e$ . Show that this element will also satisfy  $y \cdot x = e$ .

**16** Show that a group can have at most one identity element.

**17** Show that the inverse of an element must be unique.

**18** Show that in any group,  $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ ,

**19** Show that if  $a \cdot x = a \cdot y$  in a group, then  $x = y$ .

**20** Suppose that  $S$  is a finite set (not necessarily a group) which is closed under the operator  $(\cdot)$ . Suppose also that the equation

$$a \cdot x = a \cdot y$$

holds if, and only if,  $x = y$ . Prove Proposition 2.3 holds for the set  $S$ , even if  $S$  is not a group.

Hint: Use the pigeonhole principle.

**21** Let  $G$  be a group. Show that  $G$  is abelian if, and only if,  $(a \cdot b)^2 = a^2 \cdot b^2$  for all  $a$  and  $b$  in  $G$ .

**22** If  $G$  is a group such that  $x^2 = e$  for all elements  $x$  in  $G$ , prove that  $G$  is abelian.

**23** If  $G$  is a group and  $a$  and  $b$  are two elements of  $G$ , use mathematical induction to show that for all positive  $n$ ,

$$(a \cdot b)^n = a \cdot (b \cdot a)^{n-1} \cdot b.$$

- 24** If  $G$  is a group and  $a$  and  $b$  are two elements of  $G$ , use mathematical induction to show that for all positive  $n$ ,

$$(a \cdot b)^n = a \cdot (b \cdot a)^{n-1} \cdot a^{-1}.$$

- 25** If  $G$  is a group and  $a$  and  $b$  are two elements of  $G$ , use mathematical induction to show that for all positive  $n$ ,

$$(a \cdot b \cdot a^{-1})^n = a \cdot b^n \cdot a^{-1}.$$

- 26** Let  $G$  be a finite group that contains an even number of elements. Show that there is at least one element besides the identity such that  $a^2 = e$ . Hint: Show that there are an even number of elements for which  $a^2 \neq e$ .

- 27** Let  $G$  be a finite group. Show that there are an odd number of elements that satisfy the equation  $a^3 = e$ .

For Problems **28** through **31**: Fill in the remaining spaces in this Cayley table so that the resulting set forms a group.

Hint: Determine what the identity element must be. Once the row and column of the identity element are filled in, the remaining table can be finished using only the Latin square property.

Problem 28

·	a	b	c	d
a	b			
b				
c		b		
d				

Problem 29

·	a	b	c	d
a				
b				
c		d		
d			b	

Problem 30

·	u	v	w	x	y	z
u				y		
v	w				x	
w				u		y
x						
y	z					w
z				v		

Problem 31

·	a	b	c	d	e	f	g	h
a	b							c
b	g	e						
c						e	d	g
d		h		b			f	
e			c					
f			e			b		a
g	e	a			g		b	
h			a				c	

## Interactive Problems

- 32** Use *SageMath*'s **ZStar** command to find the size of  $Z_n^*$  for  $n = 9, 27, 81, 243, 5, 25, 125$ . Make a conjecture about the size of  $Z_n^*$  when  $n$  is a power of an odd prime  $p$ . Note use can use the **len(\_)** command to have *SageMath* count the elements for you.
- 33** Use *SageMath*'s **ZStar** command to find the size of  $Z_n^*$  for  $n = 18, 54, 162, 486, 50, 250, 98, 686$ . Make a conjecture about the size of  $Z_n^*$  when  $n$  is twice the power of an odd prime  $p$ .
- 34** Use *SageMath*'s **ZStar** command to make a conjecture about the size of  $Z_{mn}^*$ , where  $m$  and  $n$  are coprime, in terms of the sizes of  $Z_m^*$  and  $Z_n^*$ .

# Chapter 3

---

## The Structure within a Group

We have already seen some patterns within a group, such as the Latin square property. However, in order to determine more patterns, we need to consider the possibility of a smaller group sitting inside of a larger group. For example, the group of integers is inside the group of real numbers. Whenever this happens, we say the smaller group is a *subgroup* of the larger group. Subgroups will lead to even more important properties of groups. But before we determine the subgroups of a given group, we need to understand the generators of a group.

---

### 3.1 Generators of Groups

In this section, we will explore the set of elements within the group. We will find that some elements may possess an important property, allowing every element to be expressible in terms of that one element. We can then define a group as *cyclic* if it possesses such an element.

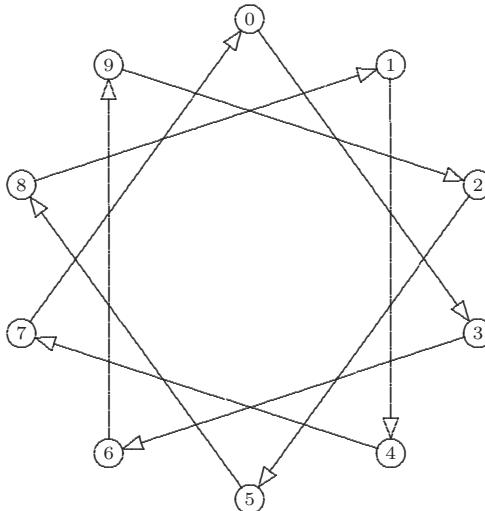
Cyclic groups turn out to be very important in the study of groups. In fact, we will discover that every finite abelian group can be expressed using the cyclic groups as building blocks.

Knowing about cyclic groups will also help us to define other groups in programs such as *SageMath*. Many of these groups will be fairly large, and so rather than giving *SageMath* the entire group, we will define a group using a very small number of elements. From these few elements, *SageMath* will be able to reconstruct the entire group.

We begin by studying *finite* groups, that is, groups with a finite number of elements, such as Terry's group,  $Z_n$ , and  $Z_n^*$ . By observing the properties of a single element within such a group, we gain insight on how to program *SageMath* to work with finite groups.

#### **Computational Example 3.1**

Study the powers of the elements 3 and 4 in the group  $Z_{10}$ .



**FIGURE 3.1:** Circle graph of **Add(3)**

This group is loaded into *SageMath* with the command

```
G = ZGroup(10); G
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
```

We can map each element  $x$  to the element  $x \cdot 3$  with a circle graph

```
CircleGraph(G, Add(3))
```

which produces [Figure 3.1](#)

This graph allows us to visualize powers of 3 in the group  $Z_{10}$ . If we follow the arrows starting with 0, we have the sequence  $\{0, 3, 6, 9, 2, 5, 8, 1, 4, 7, 0, \dots\}$ . This tells us that

$$3^0 = 0, \quad 3^1 = 3, \quad 3^2 = 6, \quad 3^3 = 9, \quad 3^4 = 2, \quad \text{etc.}$$

Recall that for this group the dot represents addition, so an exponent would represent repeated addition. Note that every element in the group can be expressed as a power of 3.

This property does not hold for all elements, since the powers of 4 are seen to be  $\{0, 4, 8, 2, 6, 0, 4, 8, \dots\}$ , which does *not* include all of the elements.  $\square$

**DEFINITION 3.1** We say that the element  $g \in G$  is a *generator* of the group  $G$  if every element of  $G$  can be expressed as a power of  $g$ .

We can have *SageMath* list all of the generators of a group for us. In the case of  $G = Z_{10}$ , the generators are:

**Generators (G)**

[1, 3, 7, 9]

So there are 4 generators to the group  $Z_{10}$ .

**Example 3.2**

Find all of the generators of the group  $Z_7^*$ .

SOLUTION: This group is small enough to do by hand. For each of the elements in  $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ , we raise the element to different powers until we reach the identity.

$$1^1 = 1.$$

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1.$$

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

$$4^1 = 4, \quad 4^2 = 2, \quad 4^3 = 1.$$

$$5^1 = 5, \quad 5^2 = 4, \quad 5^3 = 6, \quad 5^4 = 2, \quad 5^5 = 3, \quad 5^6 = 1.$$

$$6^1 = 6, \quad 6^2 = 1.$$

Thus we see that 3 and 5 are generators. □

This process of searching for generators leads us to the following definition.

**DEFINITION 3.2** Let  $x$  be an element of a group  $G$  with identity  $e$ . We define the *order* of the element  $x$  to be the smallest positive integer  $n$  for which  $x^n = e$ . If no such positive integer exists, we say the order of  $x$  is *infinite*.

In Example 3.2, we see that the element 1 has order 1, element 6 has order 2, elements 2 and 4 have order 3, and the generators 3 and 5 have order 6. We can make the following observations about the order of an element:

- The order of the identity element is always 1.
- If the group is finite, then its generators are the elements whose order is the size of the group.
- The order can be infinite if the size of the group is infinite. For example, in the group  $\mathbb{Z}$ , the element 2 has infinite order, since  $2^n$  is never 0 for  $n \geq 1$ .

The only way to find the generators in a  $Z_n^*$  group is by trial and error, as was done in Example 3.2. However, there is a shortcut for finding the generators for the group  $Z_n$ .

**PROPOSITION 3.1**

The generators of  $Z_n$  are precisely the integers between 0 and  $n$  that are coprime to  $n$ .

PROOF: Suppose that  $g$  is a generator of  $Z_n$ . Then 1 is able to be expressed as a power of  $g$ , so we have that

$$g^v = 1 \text{ in } Z_n$$

for some  $v$ . Since the group action of  $Z_n$  is addition, raising to a power is equivalent to repeated addition, or standard multiplication. Thus, we have that

$$gv \equiv 1 \pmod{n}.$$

By Proposition 2.8, there is such a  $v$  if, and only if,  $g$  is coprime to  $n$ .

Now suppose that  $g$  is coprime to  $n$ . By Proposition 2.8, there is a  $v$  such that

$$gv \equiv 1 \pmod{n}, \text{ hence } g^v = 1 \text{ in } Z_n.$$

So 1 can be expressed as a power of  $g$ . But 1 is a generator of  $Z_n$ , and so every element of  $Z_n$  can be expressed as a power of 1, say  $1^w$ . Then that element can be written as  $g^{(vw)} = (g^v)^w = 1^w$ . So every element can be expressed as a power of  $g$ , hence  $g$  is a generator of  $Z_n$ .  $\square$

The count of positive numbers less than  $n$  that are coprime to  $n$  is called the *Euler totient function* of  $n$  and is denoted  $\phi(n)$ . Thus, the number of generators of  $Z_n$  is precisely  $\phi(n)$ . A small table of this function up to  $n = 36$  is given in [Table 3.1](#).

**TABLE 3.1:** Table of  $\phi(n)$

$n$	$\phi(n)$	$n$	$\phi(n)$	$n$	$\phi(n)$	$n$	$\phi(n)$
1	1	10	4	19	18	28	12
2	1	11	10	20	8	29	28
3	2	12	4	21	12	30	8
4	2	13	12	22	10	31	30
5	4	14	6	23	22	32	16
6	2	15	8	24	8	33	20
7	6	16	8	25	20	34	16
8	4	17	16	26	12	35	24
9	6	18	6	27	18	36	12

For larger values of  $n$ , we can use the *SageMath* command **EulerPhi**.

**EulerPhi(60)**

16

Hence, there are 16 generators of  $Z_{60}$ . *SageMath* uses the following formula for the totient function based on the prime factorization of the number.

**THEOREM 3.1: The Totient Function Theorem**

If the prime factorization of  $n$  is given by

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k},$$

where  $p_1, p_2, p_3, \dots, p_k$  are distinct primes, and  $r_1, r_2, r_3, \dots, r_k$  are positive integers, then the count of numbers less than  $n$  which are coprime to  $n$  is

$$\phi(n) = (p_1 - 1) \cdot p_1^{(r_1-1)} \cdot (p_2 - 1) \cdot p_2^{(r_2-1)} \cdots \cdots (p_k - 1) \cdot p_k^{(r_k-1)}.$$

**PROOF:** To begin, let us show that if  $p$  is a prime, then  $\phi(p^r) = (p - 1)p^{r-1}$ .

Note that the only numbers that are *not* coprime to  $p^r$  will be multiples of  $p$ . So of the numbers between 1 and  $p^r$ , exactly  $1/p$  of them will be multiples of  $p$ . The remaining  $(1 - 1/p) \cdot p^r$  will be coprime, and this can be simplified to  $(p - 1)p^{r-1}$ .

Next we want to show that if  $m$  and  $n$  are coprime, then  $\phi(mn) = \phi(m)\phi(n)$ . Let  $A$  denote the set of numbers that are less than  $m$ , but coprime to  $m$ . Let  $B$  denote the set of numbers that are less than  $n$ , but coprime to  $n$ .

Then for any number  $x$  coprime to  $mn$ ,  $x \bmod m$  must be in the set  $A$ , while  $x \bmod n$  must be in  $B$ . Yet for every  $a$  in  $A$  and  $b$  in  $B$ , there is, by the Chinese remainder theorem (1.5), a unique number less than  $mn$  that is equivalent to  $a \pmod{m}$  and  $b \pmod{n}$ . This number will be coprime to both  $m$  and  $n$ , and hence will be coprime to  $mn$ .

Therefore, we have a one-to-one correspondence between ordered pairs  $(a, b)$ , where  $a$  is in  $A$ , and  $b$  is in  $B$ , and numbers coprime to  $nm$ . Thus, we have

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m).$$

Finally, we can combine these results together. By simply noting that if

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k},$$

then  $p_1^{r_1}, p_2^{r_2}, p_3^{r_3}, \dots, p_k^{r_k}$  will all be coprime. Hence, we can find  $\phi$  for each of these terms, and multiply them together, giving us our formula.  $\square$

We can also consider finding generators for the groups of the form  $Z_n^*$ , which, unfortunately, can only be done by trying each element.

**Example 3.3**

The group  $Z_{10}^*$  has four elements,  $\{1, 3, 7, 9\}$ , and looking at the powers of the elements, we see that

$$1^1 = 1.$$

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 7, \quad 3^4 = 1.$$

$$7^1 = 7, \quad 7^2 = 9, \quad 7^3 = 3, \quad 7^4 = 1.$$

$$9^1 = 9, \quad 9^2 = 1.$$

so 3 and 7 are generators.  $\square$

**Example 3.4**

$Z_8^*$  also has four elements,  $\{1, 3, 5, 7\}$ , but

$$\begin{aligned}1^1 &= 1. \\3^1 &= 3, \quad 3^2 = 1. \\5^1 &= 5, \quad 5^2 = 1. \\7^1 &= 7, \quad 7^2 = 1.\end{aligned}$$

so *none* of these elements are generators of the group! This becomes apparent as we look at the Cayley table for  $Z_8^*$ .

```
G = ZStar(8)
CayleyTable(G)
```

.	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Notice that the square of every element is equal to 1. Thus, all elements besides the identity have order 2. Hence no element of  $Z_8^*$  can generate the whole group. We can see this by asking *SageMath* to list all of the generators.

```
Generators(G)
[ ]
```

□

From these examples, we see that some groups have generators, while others do not. This leads us to the following definition.

**DEFINITION 3.3** We say a group is *cyclic* if there is one element that can generate the entire group.

Although we have seen an example of a finite group that is not cyclic, we will later see that the structure of *any* finite abelian group can be expressed in terms of the cyclic groups.

Even when a group is not cyclic, we sometimes can find *two* elements by which every element of the group can be expressed. For example, consider the two elements 3 and 5 from the group  $Z_8^*$ . Since  $1 = 3 \cdot 3$  and  $7 = 3 \cdot 5$ , we find that all four elements of the group can be written as some *combination* of 3 and 5. We say that the *set*  $\{3, 5\}$  generates the group.

Finally, consider the group of the dancing triangle, whose Cayley table is given in [Table 2.2](#). By experimenting, we find that no single element can

generate the entire group. However, there are many ways in which we can have *two* elements generating the entire group. For example, if we pick the two elements **RotRt** and **Spin**, we find that the other four elements can be expressed in terms of these two:

$$\begin{aligned}\mathbf{Stay} &= \mathbf{Spin} \cdot \mathbf{Spin}, \\ \mathbf{FlipRt} &= \mathbf{Spin} \cdot \mathbf{RotRt}, \\ \mathbf{FlipLft} &= \mathbf{RotRt} \cdot \mathbf{Spin}, \text{ and} \\ \mathbf{RotLft} &= \mathbf{RotRt} \cdot \mathbf{RotRt}.\end{aligned}$$

One of the keys for entering a group into *SageMath* is finding one or two elements (or sometimes even three are needed) that will generate the entire group. This information begins to reveal the structure of the group itself.

### Problems for §3.1

For Problems 1 through 12: Find all of the generators of the following groups. How many generators are there? (Note some groups will not have generators.)

<b>1</b>	$Z_{12}$	<b>4</b>	$Z_{24}$	<b>7</b>	$Z_{12}^*$	<b>10</b>	$Z_{16}^*$
<b>2</b>	$Z_{14}$	<b>5</b>	$Z_9^*$	<b>8</b>	$Z_{14}^*$	<b>11</b>	$Z_{18}^*$
<b>3</b>	$Z_{16}$	<b>6</b>	$Z_{11}^*$	<b>9</b>	$Z_{15}^*$	<b>12</b>	$Z_{20}^*$

For Problems 13 through 20: Use the totient function theorem (3.1) to find the size of the following groups:

<b>13</b>	$Z_{120}^*$	<b>15</b>	$Z_{525}^*$	<b>17</b>	$Z_{1155}^*$	<b>19</b>	$Z_{2695}^*$
<b>14</b>	$Z_{300}^*$	<b>16</b>	$Z_{1500}^*$	<b>18</b>	$Z_{2401}^*$	<b>20</b>	$Z_{7350}^*$

- 21** Prove that  $\phi(n)$  is even for  $n > 2$ .
- 22** Using the totient function theorem (3.1), prove that there is no value of  $n$  for which  $\phi(n) = 14$ .
- 23** Show that any cyclic group must be abelian.
- 24** Show that if  $G$  is a group, and  $a \in G$ , then  $a$  and  $a^{-1}$  have the same order.
- 25** Let  $G$  be an arbitrary group, with  $a$  and  $b$  two elements of  $G$ . Show that  $a \cdot b$  and  $b \cdot a$  have the same order.  
Hint: You can use the result of Problem 24 from §2.3.
- 26** Let  $G$  be an arbitrary group, with  $a$  and  $b$  two elements of  $G$ . Show that  $a \cdot b \cdot a^{-1}$  has the same order as  $b$ .  
Hint: You can use the result of Problem 25 from §2.3.
- 27** Suppose that  $G$  is a group with exactly one element of order 2, say  $x$ . Prove that  $x \cdot y = y \cdot x$  for all  $y$  in  $G$ .

## Interactive Problems

- 28** Use *SageMath*'s circle graph to find all of the generators of the group  $Z_{21}$ .
- 29** Use *SageMath*'s circle graph to see if there is an element of  $Z_{25}^*$  that generates  $Z_{25}^*$ . If so, how many such elements are there?
- 30** By using *SageMath*'s **Generators()** command, determine whether  $Z_n^*$  is cyclic for  $n = 9, 27, 81, 243, 5, 25, 125$ . Make a conjecture about when  $Z_n^*$  is cyclic if  $n$  is a power of an odd prime.
- 31** By using *SageMath*'s **Generators()** command, determine whether  $Z_n^*$  is cyclic for  $n = 18, 54, 162, 486, 50, 250, 98, 686$ . Make a conjecture about when  $Z_n^*$  is cyclic if  $n$  is twice the power of an odd prime.
- 32** By using *SageMath*'s **Generators()** command, see if you can find an  $n$  for which  $Z_n^*$  is cyclic, and  $n$  doesn't fit into the categories of Problems 30 or 31.
- 

### 3.2 Defining Finite Groups in *SageMath*

For some groups there is a single element that generates the entire group, whereas in other groups two or more elements are required. In this section, we will show how a finite group can be entered into *SageMath* using a set of elements that generates the group. We will begin with a cyclic group  $Z_n$  which has a single generator which we will call  $x$ . From the circle graphs of  $Z_n$ , we could see that the sequence of  $n$  elements

$$\begin{aligned} e &= x^0, \\ x &= x^1, \\ x \cdot x &= x^2, \\ x \cdot x \cdot x &= x^3, \\ &\dots \quad \dots \\ x \cdot x \cdot x \cdots \cdots x &= x^{(n-1)}, \end{aligned}$$

must mention every element of  $Z_n$  exactly once. This gives us a way to label the elements of  $Z_n$  in terms of the generator  $x$ . We also find that  $x^n = e$ . Thus, we can define the group  $Z_n$  merely by saying “ $x$  is a generator of the group, and the order of  $x$  is  $n$ .”

#### Computational Example 3.5

Define the group  $Z_5$  in *SageMath*.

**TABLE 3.2:** Table of  $Z_5$ 

.	$e$	$x$	$x^2$	$x^3$	$x^4$
$e$	$e$	$x$	$x^2$	$x^3$	$x^4$
$x$	$x$	$x^2$	$x^3$	$x^4$	$e$
$x^2$	$x^2$	$x^3$	$x^4$	$e$	$x$
$x^3$	$x^3$	$x^4$	$e$	$x$	$x^2$
$x^4$	$x^4$	$e$	$x$	$x^2$	$x^3$

This group is cyclic, so we can use a single generator  $\mathbf{x}$  to describe the group. First we define  $\mathbf{e}$  to be the identity element with the command

```
InitGroup("e")
```

Next, we define the symbol  $\mathbf{x}$  to be the group variable.

```
AddGroupVar("x")
```

Finally, we note that  $x$  has order 5, so we define  $x^5$  to be  $e$ .

```
Define(x^5, e)
```

This is all we need to define the group  $Z_5$ . □

To view this group, we use the command

```
Z5 = Group(); Z5
{e, x, x^2, x^3, x^4}
```

which gives a list of all of the elements in the group, and assigns this list to the identifier **Z5**. The Cayley table for this group produced by the **CayleyTable** command is shown in [Table 3.2](#).

Although the notation  $\{0, 1, 2, 3, 4\}$  is more concise for this particular example, the use of generators is more versatile, since almost all finite groups can be expressed easily using generators.

### Computational Example 3.6

Define the group  $Z_8^*$  in *SageMath*.

This is not cyclic, but the group can be generated by  $a = 3$  and  $b = 5$ . Since these elements both have order 2, we define  $a^2$  and  $b^2$  to be  $e$ . This group can be entered into *SageMath* with the commands:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^2, e)
Define(b*a, a*b)
```

Note that we needed an extra **Define** statement to let *SageMath* know that  $a$  and  $b$  commute with each other. To list the elements of the group, we could either use the **Group()** command as we did for  $Z_5$ , or we can include the generators  $a$  and  $b$  in the **Group** command.

```
G = Group(a, b); G
{e, a, b, a*b}
```

We still need to check that the associative law holds. This can be done with the command

**CheckGroup(G)**

This set of elements is a group. □

We can define several groups in *SageMath* at the same time (using the same identity element, and different letters for the generators) and by listing the generators with the **Group** command, *SageMath* will know which group we are referring to. However, the **InitGroup** command will clear all previously defined groups.

We can now display the Cayley table for this group.

**CayleyTable(G)**

.	e	a	b	$a^*b$
e	e	a	b	$a^*b$
a	a	e	$a^*b$	b
b	b	$a^*b$	e	a
$a^*b$	$a^*b$	b	a	e

### Computational Example 3.7

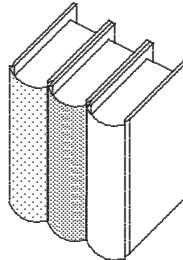
Suppose we have three different books on a shelf, and we consider rearrangements of the books. Enter this group into *SageMath*.

Such a group of arrangements can be illustrated with the command

**InitBooks(3)**

which begins by showing three differently colored books, as in [Figure 3.2](#). Two ways we could rearrange the books are to swap the first two books, or move the first book to the other end, sliding the other two books to the left. These two operations can be animated in *SageMath* by

```
MoveBooks(First)
MoveBooks(Left)
```



**FIGURE 3.2:** Three books that can be rearranged

By letting  $e$  be the identity element,  $a$  be the rearrangement swapping the first two books, and  $b$  be the rearrangement moving the books to the left, we find that all possible permutations of the books are generated by  $a$  and  $b$ . We will begin by noting the order of these two elements. Since we clearly have  $a^2 = e$  and  $b^3 = e$ , we can use this to help define the group. As in  $Z_8^*$ , the plan is to express  $b \cdot a$  in terms of a combination of elements in alphabetical order. Since  $b \cdot a$  essentially switches the first and last books, we see that  $(b \cdot a)^2 = e$ , or

$$b \cdot a = (b \cdot a)^{-1} = a^{-1} \cdot b^{-1} = a \cdot b^2.$$

Thus, we can define this group by

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^3, e)
Define(b*a, a*b^2)
```

□

If we use the **Group** command to find the list of elements,

```
G = Group(); G
{e, a, b, a*b, b^2, a*b^2}
```

we find that there are six elements. The output of

**CayleyTable(G)**

is shown in [Table 3.3](#).

Is this really a group? We can tell from the Cayley table that  $G$  is closed with respect to multiplication, and that there is an identity element,  $e$ . We also recognize the familiar Latin square property that we have seen in all of the other Cayley tables. Since every row and every column contains exactly one  $e$ , every element has a unique inverse. The only property that we cannot check directly using the Cayley table is the associativity property. *SageMath* can check this with the command

**TABLE 3.3:** Cayley table for  $S_3$ 

.	$e$	$a$	$b$	$a^*b$	$b^2$	$a^*b^2$
$e$	$e$	$a$	$b$	$a^*b$	$b^2$	$a^*b^2$
$a$	$a$	$e$	$a^*b$	$b$	$a^*b^2$	$b^2$
$b$	$b$	$a^*b^2$	$b^2$	$a$	$e$	$a^*b$
$a^*b$	$a^*b$	$b^2$	$a^*b^2$	$e$	$a$	$b$
$b^2$	$b^2$	$a^*b$	$e$	$a^*b^2$	$b$	$a$
$a^*b^2$	$a^*b^2$	$b$	$a$	$b^2$	$a^*b$	$e$

**CheckGroup (G)**

This set of elements is a group.

This group is called  $S_3$ , the permutation group on three objects. (Obviously it makes no difference what the three objects are. Books are just one possibility.)

Can *SageMath* determine the inverse of an element?

```
(a*b)^-1
a*b
```

Since *SageMath* knows that  $a$  has order 2, and  $b$  has order 3, it can deduce that  $a^{-1} = a$  and  $b^{-1} = b^2$ . Then using Proposition 2.2,  $(u \cdot v)^{-1} = v^{-1} \cdot u^{-1}$ , it can take the inverse of any element.

The Cayley tables for Terry's group and  $S_3$  are very similar. By color coding the elements in the table, we see that the color patterns of the two Cayley tables are identical. Thus, these two groups behave in exactly the same way, even though the elements have different names. We say that these groups are *isomorphic*. We will cover isomorphic groups in [Chapter 5](#).

Groups have many applications. For example, the shape of an uncut diamond, as well as many other gemstones, is shown in [Figure 3.3](#). This figure is reproduced by the *SageMath* command

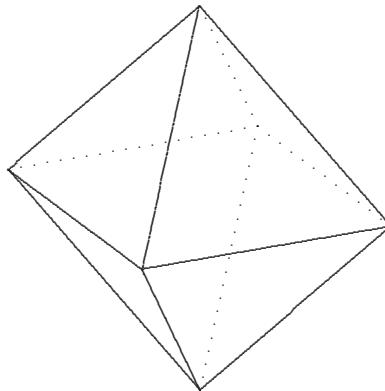
**InitOctahedron()**

One problem a gem cutter often faces is determining the orientation he should put the gemstone before he starts to cut. In which case, he needs to know all of the possible ways the octahedron can be rotated. The set of rotations would form a group, similar to Terry's dance steps.

**Computational Example 3.8**

Consider the group of rotations on the octahedron, and enter this group into *SageMath*.

There are eight triangles forming this solid. Three ways of rotating this figure are given by



**FIGURE 3.3:** Octahedron with eight equilateral triangles

```
RotateOctahedron (a)
RotateOctahedron (b)
RotateOctahedron (c)
```

The first of these flips along the side horizontal edges, turning it upside down. The second rotates the closest face counter-clockwise, while the third rotates the closest vertex clockwise. If we let  $e$  be the identity element of this group, it is easy to see that  $a$  has order 2,  $b$  has order 3, and  $c$  has order 4. Thus we have

$$a^2 = e, \quad b^3 = e, \quad c^4 = e.$$

After some experimenting, we find that  $b \cdot a \cdot b \cdot a = e$ ,  $c \cdot b \cdot c \cdot c \cdot a = e$ , and  $c \cdot a \cdot c^3 \cdot a \cdot b = e$ . From these identities, we can come up with the identities

$$b \cdot a = (b \cdot a)^{-1} = a^{-1} \cdot b^{-1} = a \cdot b^2.$$

$$c \cdot b = (c \cdot c \cdot a)^{-1} = a^{-1} \cdot c^{-1} \cdot c^{-1} = a \cdot c^3 \cdot c^3 = a \cdot c^2 \cdot c^4 = a \cdot c^2.$$

$$c \cdot a = (c^{-1} \cdot a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \cdot c = b^2 \cdot a \cdot c = b \cdot a \cdot b^2 \cdot c = a \cdot b^4 \cdot c = a \cdot b \cdot c.$$

This allows us to define the three products out of alphabetical order,  $b \cdot a$ ,  $c \cdot a$ , and  $c \cdot b$ , in terms of a product of elements that *are* in alphabetical order. Although this is not mandatory, it is a good strategy to ensure each element will have a natural representation.

```
InitGroup ("e")
AddGroupVar ("a", "b", "c")
Define (a^2, e)
Define (b^3, e)
Define (c^4, e)
Define (b*a, a*b^2)
Define (c*a, a*b*c)
```

```
Define(c*b, a*c^2)
G = Group(); G
{e, a, b, a*b, b^2, a*b^2, c, a*c, b*c, a*b*c, b^2*c,
 a*b^2*c, c^2, a*c^2, b*c^2, a*b*c^2, b^2*c^2, a*b^2*c^2,
 c^3, a*c^3, b*c^3, a*b*c^3, b^2*c^3, a*b^2*c^3}
```

**CheckGroup(G)**

This set of elements is a group.

By expressing the product of any two generators in terms of a combination in alphabetical order, *SageMath* can express all elements as a combination of generators in alphabetical order.  $\square$

We call this group the *octahedral* group, which will be an important example later on. The command

**len(G)**

24

shows this group has 24 elements. This group is too large to print a complete Cayley table, but *SageMath* is able to produce a color-coded table for groups of up to 27 elements.

We can use *SageMath*'s **ElementOrder** command to find the order of an element. For example, the order of the element  $a \cdot c$  can be found by typing

**ElementOrder(a\*c)**

3

to see that the order of this element is 3. There is a trick for finding the orders of all of the elements of the group at the same time.

[ **ElementOrder(x) for x in G** ]

```
[1, 2, 3, 2, 3, 2, 4, 3, 4, 3, 2, 2, 2, 4, 3, 4, 3, 2, 4, 3, 2,
 3, 4, 2]
```

We find that every element of this group besides the identity has order 2, 3, or 4. There is a geometrical reason for this: every element represents a rotation of either  $\pm 90^\circ$ ,  $\pm 120^\circ$ , or  $180^\circ$ . In fact, there are 9 elements of order 2, 8 elements of order 3, and 6 elements of order 4. In Problem 4, you are asked to derive these values purely by considering the geometry of the octahedron.

With *SageMath*, we are able to create new groups to study. These examples help us to find patterns in the structure of all groups. In the next section we will study the substructure of a group, by finding smaller groups within a group.

## Problems for §3.2

- 1 Show that if  $a^2 = b^2 = e$ , then saying that  $b \cdot a = a \cdot b$  is equivalent to saying that  $a \cdot b \cdot a \cdot b = e$ .

- 2** In defining  $S_3$ , we used three facts about the group:  $a^2 = e$ ,  $b^3 = e$ , and  $b \cdot a = a \cdot b^2$ . Using just these facts without *SageMath*, prove that  $b^2 \cdot a = a \cdot b$ .
- 3** The group defined in Problem 18 has elements  $a$  and  $b$  such that  $a^5 = e$ ,  $b^4 = e$ , and  $b \cdot a = a^2 \cdot b$ . Using just these facts without *SageMath*, prove that  $b^3 \cdot a = a^3 \cdot b^3$ .
- 4** Use geometry to figure out how many elements of the octahedral group are of order 4 (Rotations by 90 degrees). How many elements are of order 3? Of order 2? Check these figures by adding up these numbers, and adding one for the identity element, and show that this gives 24.  
Hint: The octahedron has 8 faces, 6 corners, and 12 edges.

For Problems **5** through **16**: Recall the octahedral group was defined with 3 generators such that  $a^2 = b^3 = c^4 = e$ ,  $b \cdot a = a \cdot b^2$ ,  $c \cdot a = a \cdot b \cdot c$ , and  $c \cdot b = a \cdot c^2$ . Using just these facts without *SageMath*, simplify the following expressions into a product that is in the form  $a^i \cdot b^j \cdot c^k$ , with  $0 \leq i < 2$ ,  $0 \leq j < 3$ , and  $0 \leq k < 4$ .

<b>5</b>	$c^2 \cdot b$	<b>8</b>	$c \cdot b^2$	<b>11</b>	$b \cdot c^2 \cdot b$	<b>14</b>	$c^2 \cdot b \cdot a$
<b>6</b>	$b \cdot c \cdot b$	<b>9</b>	$c^2 \cdot a$	<b>12</b>	$b \cdot c^2 \cdot a$	<b>15</b>	$c \cdot b \cdot a \cdot b$
<b>7</b>	$b^2 \cdot a$	<b>10</b>	$c \cdot b \cdot a$	<b>13</b>	$c^2 \cdot b^2$	<b>16</b>	$c \cdot b^2 \cdot a$

- 17** Suppose we considered rearranging four books on a shelf instead of three. How many ways could we rearrange the books?

#### Interactive Problems

- 18** Use *SageMath* to define a group that has two elements,  $a$  and  $b$ , such that  $a^5 = b^4 = e$ , and  $b \cdot a = a^2 \cdot b$ . How many elements does this group have?
- 19** Consider the rotations of a regular *tetrahedron* (triangular pyramid) oriented with its base in the  $xy$ -plane, and another face towards the front. If  $a$  represents flipping the left slanted edge, and  $b$  represents flipping the right slanted edge, then  $a \cdot b$  and  $b \cdot a$  both end up flipping the back edge. (Try it!) Let  $c$  be a  $120^\circ$  rotation of the base clockwise when viewed from the top. Then  $c \cdot a \cdot c^{-1} = b$ , since  $c$  turns the right edge to the left edge. Likewise,  $c \cdot b \cdot c^{-1} = a \cdot b$ , since the back edge is turned to the right edge. From this information, enter the rotation group into *SageMath*. You will need to find expressions for  $c \cdot a$  and  $c \cdot b$  that are in alphabetical order.
- 20** Consider extending the octahedral group by adding another generator  $d$ , which of order 5, such that  $d \cdot a = a \cdot b \cdot d$ ,  $d \cdot b = a \cdot c \cdot d$ , and  $d \cdot c = a \cdot d^2$ . Enter this larger group into *SageMath*. How many elements does it have? (Do not try to do a **CheckGroup** on this group.)

### 3.3 Subgroups

A natural question to ask is whether we can have a smaller group inside of a particular group. We begin by saying that  $H$  is a *subset* of a group  $G$ , denoted  $H \subseteq G$ , if  $H$  consists only of the elements of  $G$ . The empty set  $\{ \}$  is always considered to be a subset, but we will restrict our attention to non-empty subsets.

**DEFINITION 3.4** We say that  $H$  is a *subgroup* of  $G$  if  $H$  is a non-empty subset of  $G$  and  $H$  is a group with respect to the operation  $(\cdot)$  of  $G$ .

It should be noted that all non-trivial groups have at least two subgroups. One subgroup contains just the identity element  $\{e\}$ , while another contains all of the elements of  $G$ . These two subgroups are called the *trivial subgroups*.

To see if a subset  $H$  is a group, we must test all four of the group properties. But the associative property of  $H$  is guaranteed because the original group  $G$  is associative. The remaining three properties,

1.  $H$  is closed under multiplication. That is,  $x \cdot y \in H$  whenever  $x$  and  $y \in H$ .
2. The identity element of  $G$  is in  $H$ .
3. Every element of  $H$  has its inverse in  $H$ . That is,  $x^{-1} \in H$  whenever  $x \in H$ .

can be combined into one simple test.

#### PROPOSITION 3.2

Let  $H \subseteq G$  and  $H \neq \{ \}$ . Then  $H$  is a subgroup of  $G$  if, and only if, we have

$$x \cdot y^{-1} \in H \quad \text{for all } x, y \in H.$$

**PROOF:** First of all, we need to see that if  $H$  is a subgroup, then  $x \cdot y^{-1}$  is in  $H$  whenever  $x$  and  $y$  are in  $H$ . By property (3),  $y^{-1}$  is in  $H$ , and so by property (1),  $x \cdot y^{-1}$  is in  $H$ .

Conversely, let us suppose that  $H \subseteq G$ ,  $H \neq \{ \}$ , and whenever  $x, y \in H$ , then  $x \cdot y^{-1} \in H$ . We need to see that properties (1) through (3) are satisfied.

Since  $H$  is not the empty set, there is an element  $x$  in  $H$ , and so  $x \cdot x^{-1} = e$  is in  $H$ . Thus, property (2) holds.

Next, we have that if  $y$  is in  $H$ , then  $e \cdot y^{-1} = y^{-1}$  is in  $H$ , and so property (3) holds.

Finally, if  $x$  and  $y$  are in  $H$ , then  $y^{-1}$  is in  $H$ , and so  $x \cdot (y^{-1})^{-1} = x \cdot y$  is in  $H$ . Thus, property (1) also holds.  $\square$

**Example 3.9**

Let us find a subgroup of  $S_3$ , defined in *SageMath* by the commands:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^3, e)
Define(b*a, a*b^2)
G = Group(); G
{e, a, b, a*b, b^2, a*b^2}
```

We can find smaller groups within this one, such as

$$H = \{e, b, b^2\}.$$

It is easy to see that if  $x$  and  $y$  are in  $H$ , then  $x \cdot y^{-1}$  is in  $H$ . Therefore, this is a subgroup. There are other subgroups within this group, such as  $\{e, a\}$ .  $\square$

One of the main tools we will use to find subgroups of a group is the *intersection*. Given two subsets  $H$  and  $K$  of  $G$ , the *SageMath* command **Intersection** finds the set of elements that are in both subsets, denoted  $H \cap K$ .

```
H = [e, b, b^2]
K = [e, a]
Intersection(H, K)
[e]
```

Note that sets are *entered* in *SageMath* using square brackets, even though they are often displayed using curly braces. (Technically, using square brackets produce a list of elements, which acts similar to a set. But the *SageMath* routines know to treat a list as if it were a set.) Moreover, we can consider taking the intersection of a collection of many sets. If we let

```
L = [[e, a, b], [e, a*b, b], [e, a, b, b^2]]
```

then  $L$  represents a “set of sets.” We can take the intersection of all of the sets in this collection with the command

```
Intersection(L)
[e, b]
```

The mathematical notation for this intersection is

$$\bigcap_{H \in L} H.$$

We could ask whether the intersection of two *subgroups* of  $G$  forms a subgroup of  $G$ . The next proposition shows us that indeed, the intersection of subgroups forms a new subgroup.

### PROPOSITION 3.3

*Given a group  $G$  and a non-empty collection of subgroups, denoted by  $L$ , then the intersection of all of the subgroups in the collection*

$$H^* = \bigcap_{H \in L} H$$

*is a subgroup of  $G$ .*

PROOF: First of all, note that  $H^*$  is not the empty set, since the identity element is in each  $H$  in the collection. We now can apply Proposition 3.2. Let  $x$  and  $y$  be two elements in  $H^*$ . Then, for every  $H \in L$  we have  $x, y \in H$ . Since each  $H$  is a subgroup of  $G$ , we have

$$x \cdot y^{-1} \in H.$$

Therefore,  $x \cdot y^{-1}$  is in  $H^*$ , and so  $H^*$  is a subgroup of  $G$ . □

This proposition allows us to generate a subgroup of  $G$  from any subset of  $G$ .

**DEFINITION 3.5** Given a subset  $S$  of a group  $G$ , we define the *subgroup generated by  $S$*  to be

$$[S] = \bigcap_{H \in L} H$$

where  $L$  denotes the collection of subgroups of  $G$  that contain the set  $S$ .

By Proposition 3.3, this is a subgroup of  $G$ . (The collection  $L$  is non-empty since it contains  $G$ .) By the way that the collection was defined,  $[S]$  contains  $S$ . Actually,  $[S]$  is the *smallest* subgroup of  $G$  that contains  $S$ . For if  $H$  is a subgroup of  $G$  containing  $S$ , then  $H \in L$ , so that  $[S] \subseteq H$ .

We can determine  $[S]$  another way. It is clear that  $[S]$  contains all of the products of the form

$$x_1 \cdot x_2 \cdot x_3 \cdot \dots \cdot x_n,$$

where either

$$x_k \in S \quad \text{or} \quad x_k^{-1} \in S \quad (1 \leq k \leq n).$$

But the set of all such products forms a subgroup  $H$  of  $G$  that contains  $S$ . Thus,  $H = [S]$ .

The command **Group** finds  $[S]$  for any set  $S$ . Thus, we can find the subgroup of  $S_3$  generated by the element  $b$  by the *SageMath* command

**Group (b)**

$$\{e, b, b^2\}$$

This produces the same subgroup  $\{e, b, b^2\}$  we observed before.

The subgroup generated by the set  $\{b, a \cdot b\}$  is

**Group (b, a\*b)**

$$\{e, a, b, a*b, b^2, a*b^2\}$$

which produces the entire group.

In order to find all of the subgroups of a given group  $G$ , we will begin by finding all of the *cyclic* subgroups. Notice that if we pick any element  $x$  of  $G$ , then  $\{[x]\}$  will always be a cyclic subgroup of  $G$ , since  $x$  is the generator. This subgroup is usually denoted by  $[x]$ .

**Example 3.10**

Find all of the cyclic subgroups of  $S_3$ .

**SOLUTION:** The process of finding all of the cyclic subgroups is similar to finding the generators of a group. For each element, we consider raising that element to higher and higher powers until we produce the identity element. By referring to [Table 3.3](#), we see that:

$$\begin{aligned} (e)^1 &= e. \\ (a)^1 &= a, & (a)^2 &= e. \\ (b)^1 &= b, & (b)^2 &= b^2, & (b)^3 &= e. \\ (a \cdot b)^1 &= a \cdot b, & (a \cdot b)^2 &= e. \\ (b^2)^1 &= b^2, & (b^2)^2 &= b, & (b^2)^3 &= e. \\ (a \cdot b^2)^1 &= a \cdot b^2, & (a \cdot b^2)^2 &= e. \end{aligned}$$

Thus, there are 5 cyclic subgroups,  $\{e\}$ ,  $\{e, a\}$ ,  $\{e, b, b^2\}$ ,  $\{e, a \cdot b\}$ , and  $\{e, a \cdot b^2\}$ . Notice that none of the elements were generators, so the group itself is not cyclic.  $\square$

For each element in Example 3.10, we have observed that the power of the element eventually reaches the identity element, indicating that we have finished finding the cyclic subgroup. Here is a proof that shows this will always happen for a finite subgroup.

**PROPOSITION 3.4**

Let  $G$  be a finite group, and  $x \in G$ . Then  $x$  will have finite order  $n$  and  $|[x]| = n$ . Furthermore,

$$[x] = \{e, x, x^2, x^3, \dots, x^{n-1}\}.$$

PROOF: Consider the sequence of elements  $\{x^1, x^2, x^3, x^4, \dots\}$ . Since  $G$  is a finite group, not all of these elements can be distinct, so  $x^a = x^b$  for two integers  $a$  and  $b$ , with  $a < b$ . Then  $x^{(b-a)} = e$  and  $b - a > 0$ , so the order of  $x$  is finite. Recall from Definition 3.2 that the order is the smallest positive integer  $n$  such that  $x^n = e$ . We want to show that indeed the elements of

$$\{e = x^0, x^1, x^2, x^3, \dots, x^{n-1}\}$$

are all distinct. Indeed, if  $x^a = x^b$  with  $0 \leq a < b \leq n - 1$ , then  $x^{(b-a)} = e$  and  $0 < b - a < n$ , which contradicts the order of  $x$ . Therefore, the elements in

$$\{e = x^0, x^1, x^2, x^3, \dots, x^{n-1}\}$$

are all distinct.

Finally, we need to show that if  $y$  is in  $[x]$ , then there exists an  $r$  such that  $x^r = y$ , with  $0 \leq r \leq n - 1$ . But  $y = x^k$  for some  $k \in \mathbb{Z}$ . We can define  $r = k \bmod n$ . Then  $0 \leq r \leq n - 1$  and furthermore, there is an integer  $q$  such that  $k - r = nq$ . Thus,

$$y = x^k = x^{(nq+r)} = (x^n)^q \cdot x^r = e^q \cdot x^r = x^r.$$

So every element of  $[x]$  is of the form  $x^r$ , with  $0 \leq r \leq n - 1$ , and  $|[x]| = n$ .  $\square$

### Example 3.11

Find the cyclic subgroups of the group  $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ , showing the orders of the elements.

SOLUTION: We compute powers of each element until we reach the identity.

$$\begin{aligned} 1^1 &= 1. \\ 2^1 &= 2, & 2^2 &= 4, & 2^3 &= 8, & 2^4 &= 1. \\ 4^1 &= 4, & 4^2 &= 1. \\ 7^1 &= 7, & 7^2 &= 4, & 7^3 &= 13, & 7^4 &= 1. \\ 8^1 &= 8, & 8^2 &= 4, & 8^3 &= 2, & 8^4 &= 1. \\ 11^1 &= 11, & 11^2 &= 1. \\ 13^1 &= 13, & 13^2 &= 4, & 13^3 &= 7, & 13^4 &= 1. \\ 14^1 &= 14, & 14^2 &= 1. \end{aligned}$$

Thus, we see that the cyclic subgroups are  $[1] = \{1\}$ ,  $[2] = [8] = \{1, 2, 4, 8\}$ ,  $[4] = \{1, 4\}$ ,  $[7] = [13] = \{1, 4, 7, 13\}$ ,  $[11] = \{1, 11\}$ ,  $[14] = \{1, 14\}$ . We also see that 1 has order 1, the elements 4, 11, and 14 have order 2, and the elements 2, 7, 8, and 13 have order 4. Note this group lacks a generator.  $\square$

We can make a similar observation if we have an *infinite* cyclic subgroup.

**PROPOSITION 3.5**

Suppose that  $x$  has infinite order. Then

$$[x] = \{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, x^3, \dots\},$$

where the powers of  $x$  are all distinct.

**PROOF:** From Definition 3.2, if  $x$  has infinite order, then  $x^n \neq e$  for all  $n \geq 1$ . Suppose  $x^a = x^b$  with  $a < b$ . Then  $x^{(b-a)} = e$  with  $b - a > 0$ , contradicting the fact that the order of  $x$  is infinite. Thus, the powers of  $x$  are distinct. Since all powers of  $x$  are clearly in  $[x]$ , we have that

$$[x] = \{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, x^3, \dots\}.$$

□

Even though the group in Proposition 3.5 is infinite, we can still define it in *SageMath*. In fact, we defined an infinite group in the process of defining all of the other groups. If we have  $x$  as the generator of an infinite group, then the group is defined by the following:

```
InitGroup("e")
AddGroupVar("x")
```

At this point, we have an infinite group defined.

```
x^4 * x^-7
x^-3
```

Granted, we cannot display all of the elements as we did for the other groups (**Group**(**x**) would require interrupting *SageMath*), but we can still multiply elements of this group.

Because of Propositions 3.4 and 3.5, we know that any cyclic group  $G$  is either a finite group

$$G = \{e, x, x^2, x^3, \dots, x^{n-1}\}$$

which resembles the group  $Z_n$ , or is an infinite group

$$G = \{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, x^3, \dots\},$$

which resembles the group  $\mathbb{Z}$ . From this, we can quickly determine the nature of a subgroup of a cyclic group.

**PROPOSITION 3.6**

A subgroup of a cyclic group must be cyclic.

**PROOF:** Let  $g$  be a generator of the cyclic group  $G$ . The trivial subgroup  $\{e\}$

is considered cyclic, so let  $H$  be a non-trivial subgroup. Then every element of  $H$  can be written as  $g^i$  for some  $i$ . Since both  $g^i$  and  $g^{-i}$  would then be in  $H$ , we see that  $g^i$  is in  $H$  for some positive  $i$ . Let  $k$  be the smallest positive integer such that  $g^k$  is in  $H$ . Then  $g^{mk}$  is in  $H$  for all integers  $m$ .

If there were some other element in  $H$  not in  $[g^k]$ , then this element is  $g^y$  for some integer  $y$ . Then  $y = qk+r$  for some  $0 < r < k$ . Then  $g^r = g^y \cdot (g^k)^{-q} \in H$ , but we chose  $k$  to be the smallest positive integer for which  $g^k \in H$ . Thus,  $H = [g^k]$ , and so  $H$  is cyclic.  $\square$

### Example 3.12

Find *all* the subgroups of the group  $\mathbb{Z}$ .

SOLUTION: Since  $\mathbb{Z}$  is cyclic, we know that all subgroups are cyclic, hence can be expresses as  $[k]$  for some integer  $k$ . But  $[k]$  would be the multiples of  $k$ ,

$$[k] = \{k \cdot x \mid x \in \mathbb{Z}\}.$$

We will denote the subgroup of the multiples of  $k$  by  $k\mathbb{Z}$ . Note that  $0\mathbb{Z} = \{0\}$ , and  $1\mathbb{Z} = \mathbb{Z}$ , so even the trivial subgroups are of this form.  $\square$

Finding all of the subgroups of a *non-cyclic* group is trickier, since we have to consider subgroups generated by two or more elements. *SageMath* can speed up the process.

### Computational Example 3.13

Find all of the subgroups of the group  $S_3$ .

SOLUTION: We found all of the cyclic subgroups in Example 3.10:  $\{e\}$ ,  $\{e, a\}$ ,  $\{e, b, b^2\}$ ,  $\{e, a \cdot b\}$ , and  $\{e, a \cdot b^2\}$ . Note that any subgroup containing  $b$  must also contain  $b^2$ , and vice-versa. Also all subgroups will contain  $e$ . So to find subgroups that require two elements, we have 6 combinations to try:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^3, e)
Define(b*a, a*b^2)
Group(a, b)
    {e, a, b, a*b, b^2, a*b^2}
Group(a, a*b)
    {e, a, b, a*b, b^2, a*b^2}
Group(a, a*b^2)
    {e, a, b, a*b, b^2, a*b^2}
Group(b, a*b)
    {e, a, b, a*b, b^2, a*b^2}
Group(b, a*b^2)
    {e, a, b, a*b, b^2, a*b^2}
```

```
Group(a*b, a*b^2)
{e, a, b, a*b, b^2, a*b^2}
```

In each case, we produced the entire group. This shows that the only non-cyclic subgroup of  $S_3$  is  $S_3$  itself. Thus, we have found a total of 6 subgroups of  $S_3$ .  $\square$

Let us now consider the orders of the elements of a cyclic group, such as  $Z_{12}$ .

```
G = ZGroup(12); G
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
[ x^2 for x in G ]
[0, 2, 4, 6, 8, 10, 0, 2, 4, 6, 8, 10]
[ x^3 for x in G ]
[0, 3, 6, 9, 0, 3, 6, 9, 0, 3, 6, 9]
[ x^4 for x in G ]
[0, 4, 8, 0, 4, 8, 0, 4, 8, 0, 4, 8]
[ x^6 for x in G ]
[0, 6, 0, 6, 0, 6, 0, 6, 0, 6, 0, 6]
```

To find the number of elements of order  $n$ , we can look at the number of solutions to  $x^n = e$ , but we have to subtract off the number of elements of smaller order that divides  $n$ . There are four solutions to  $x^4 = 0$ , but two of these also solve  $x^2 = 0$ , so there are two elements of order 4. We see that there is only one element of order 2, two elements each of order 3, 4, and 6, and four elements of order 12.

It is apparent that finding the number of elements of order  $k$  involves finding the number of solutions to the equation  $x^k = e$ . To help us find the number of solutions for a cyclic group, let us first prove the following proposition about modular multiplication.

### PROPOSITION 3.7

Let  $n$  and  $k$  be two positive integers. Then

$$x \cdot k \equiv 0 \pmod{n}$$

if, and only if,

$$x = \frac{a \cdot n}{\gcd(n, k)}$$

for some integer  $a$ .

PROOF: First of all, notice that if

$$x = \frac{a \cdot n}{\gcd(n, k)},$$

then

$$x \cdot k = \frac{a \cdot n \cdot k}{\gcd(n, k)} = a \cdot n \cdot \frac{k}{\gcd(n, k)}.$$

and since  $\gcd(n, k)$  is a divisor of  $k$ , we see that  $x \cdot k$  is a multiple of  $n$ . Thus,

$$x \cdot k \equiv 0 \pmod{n}.$$

Now suppose that  $x \cdot k$  is a multiple of  $n$ . We want to show that

$$a = \frac{x \cdot \gcd(n, k)}{n}$$

is in fact an integer. By Bézout's lemma (1.3), there exist integers  $u$  and  $v$  such that  $\gcd(n, k) = u \cdot n + v \cdot k$ . Then

$$a = \frac{x \cdot (u \cdot n + v \cdot k)}{n} = x \cdot u + \frac{x \cdot k \cdot v}{n}.$$

Since  $x \cdot k$  is a multiple of  $n$ , we see that  $a$  is an integer. Thus,

$$x = \frac{a \cdot n}{\gcd(n, k)}$$

for some integer  $a$ . □

We can now find the number of elements in a cyclic group that satisfies the equation  $x^k = e$ .

### COROLLARY 3.1

*Let  $G$  be a cyclic group of order  $n$ . Then there are precisely  $\gcd(n, k)$  elements of  $G$  such that  $x^k = e$ .*

PROOF: Let  $g$  be a generator of  $G$ , and let  $x = g^y$  be an element of  $G$ . Then  $x^k = (g^y)^k = g^{y \cdot k}$ , which is equal to the identity if and only if

$$y \cdot k \equiv 0 \pmod{n}.$$

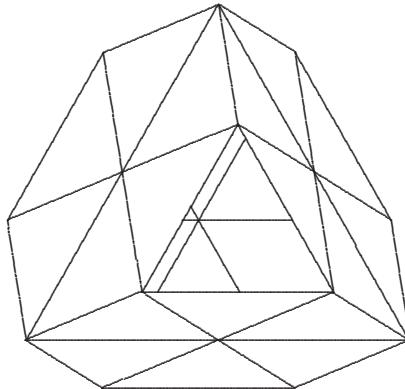
By Proposition 3.7, this is true if and only if

$$y = \frac{a \cdot n}{\gcd(n, k)}$$

for some integer  $a$ . Hence, the number of possible values of  $y$  between 0 and  $n - 1$  for which  $g^{y \cdot k} = e$  is

$$\frac{n}{\gcd(n, k)} = \gcd(n, k).$$

Each such value of  $y$  between 0 and  $n - 1$  produces a different solution  $x = g^y$ , so there are exactly  $\gcd(n, k)$  solutions. □



**FIGURE 3.4:** The Pyraminx<sup>TM</sup> puzzle without tips

Finding the number of solutions to the equation  $x^k = e$  in a group will become important as we classify the different groups. We will give a notation to this count.

**DEFINITION 3.6** Let  $G$  be a group, and  $k$  a positive integer. Then the number of elements of  $G$  for which  $x^k = e$  is called the  $k^{\text{th}}$  root count of  $G$  and is denoted by

$$R_k(G) = |\{x \in G \mid x^k = e\}|.$$

Corollary 3.1 can now be expressed in the new notation. If  $G$  is a cyclic group, then

$$R_k(G) = \gcd(|G|, k).$$

*SageMath* has a command **RootCount (G, k)** that will compute  $R_k(G)$ . For example, to find the number of solutions to the equation  $x^8 = e$  in  $Z_{12}$ , we can enter:

```
G = ZGroup(12)
RootCount(G, 8)
4
```

We are now ready to consider a more complicated group. One of the puzzles that is related to the Rubik's Cube<sup>®</sup> is called the Pyraminx<sup>TM</sup>. The Pyraminx<sup>TM</sup> consists of a triangular pyramid, with each of the four triangular sides partitioned into nine smaller triangles. The four “tips” can rotate, but this does not affect the puzzle. The command

```
InitPuzzle()
```

shows a simplified puzzle with the four tips chopped off, as in Figure 3.4. In fact, removing the four tips gives us the advantage of being able to see the

colors on the back side of the puzzle through the hole created. Now the four corners of this puzzle can rotate clockwise, using the commands

```
RotatePuzzle(f)
RotatePuzzle(b)
RotatePuzzle(l)
RotatePuzzle(r)
```

We can always put the puzzle back into its original form with the command

```
InitPuzzle()
```

The set of all actions on the puzzle forms a group, called the Pyraminx<sup>TM</sup> group. This group is generated by the elements  $\{f, b, l, r\}$ , and has over 900,000 elements! We can animate a sequence of moves as we did for the octahedron:

```
RotatePuzzle(b, f)
```

We can find the order of this element by repeatedly executing this command until the puzzle is back in order. In this particular case, the order of the element  $b \cdot f$  is 15, meaning that we have to execute this procedure 15 times before we are back where we started.

Throughout this course, we will develop tools to work with groups that will help us to solve this puzzle, and others like it. The solution to the Pyraminx<sup>TM</sup>, for example, is covered in §8.5.

### Problems for §3.3

For Problems 1 through 6: Find all of the cyclic subgroups of the following groups.

- |                   |                   |                                                                |
|-------------------|-------------------|----------------------------------------------------------------|
| <b>1</b> $Z_{12}$ | <b>3</b> $Z_{21}$ | <b>5</b> $Z_8^*$                                               |
| <b>2</b> $Z_{20}$ | <b>4</b> $Z_9^*$  | <b>6</b> $Z_{15}^*$ (see <a href="#">Table 2.6</a> on page 56) |

- 7** Using either the result of Problem 4 of §3.2, or the results of Example 3.8, find  $R_2(G)$ ,  $R_3(G)$ ,  $R_4(G)$ , and  $R_6(G)$  for the octahedral group. Is  $R_k(G)$  always a multiple of  $k$ ?
- 8** Prove that no element of the Pyraminx<sup>TM</sup> group can have order greater than 30.  
Hint: Consider corners and edges separately. See the hint for Problem 25.
- 9** Use Corollary 3.1 to find the number of solutions to the equation  $x^9 = e$  in the group  $Z_{18}$ . How many solutions are there to the equation  $x^3 = e$  in this group? How many elements of order 9 are in this group?  
Hint: For an element to be of order 9, it must solve  $x^9 = e$ , and *not* solve  $x^n = e$  for any lower value of  $n$ .

- 10** Using only Corollary 3.1, determine the number of elements of  $Z_{42}$  that are of order 6. (See the hint for Problem 9.)

- 11** Prove that if  $k$  is a divisor of  $n$ , then there are exactly  $\phi(k)$  elements of the group  $Z_n$  that are of order  $k$ .

Hint: First do the case when  $n = k$ . Then use Corollary 3.1 to show that the number of elements of order  $k$  for the groups  $Z_n$  and  $Z_k$  is the same.

- 12** Use Problem 11 to show that

$$n = \sum_{k|n} \phi(k)$$

where the sum has one term for each positive divisor  $k$  of  $n$ .

- 13** If a cyclic group has an element of infinite order, how many elements of finite order does it have? Prove your answer.

- 14** Let  $p$  be a prime number. If a group  $G$  has more than  $p - 1$  elements of order  $p$ , prove that  $G$  cannot be a cyclic group.

- 15** Let  $G$  be an abelian group. Show that the set of elements of  $G$  that have finite order forms a subgroup of  $G$ . This subgroup is called the *torsion subgroup* of  $G$ .

- 16** Let  $G$  be an abelian group, and  $k$  an integer. Let  $H$  be the set of elements  $x \in G$  such that  $x^k = e$ . Note that  $|H| = R_k(G)$ . Show that  $H$  is a subgroup of  $G$ .

- 17** Let  $G$  be an abelian group, and  $n$  an integer. Let  $H$  be the set of elements of the form  $a^n$ , with  $a \in G$ . Show that  $H$  is a subgroup of  $G$ .

- 18** Let  $p$  be an odd prime number, and  $G = Z_p^*$ . Show that there are exactly two solutions to the equation  $x^2 = 1$ , namely 1 and  $p - 1$ . Note that this is a special case of the subgroup from Problem 16.

Hint: Use Euclid's lemma (1.4) on the equation

$$x^2 - 1 \equiv 0 \pmod{p}.$$

- 19** Let  $p$  be an odd prime number, and let  $G = Z_p^*$ . Show that the set

$$H = \{x^2 \mid x \in Z_p^*\}$$

forms a subgroup of  $G$  of order  $(p - 1)/2$ . Note this is a special case of Problem 17. This subgroup  $H$  is called the group of *quadratic residues modulo p*.

Hint: Use the result of Problem 18 to show that every element of  $H$  is derived from exactly two elements of  $Z_p^*$ .

- 20** Find the quadratic residues of 17. See Problem 19.
- 21** Find the quadratic residues of 23. See Problem 19.
- 22** Let  $G$  be a group with an even number of elements. Prove that  $R_2(G)$  is even. See the hint for Problem 26 in §2.3.

### Interactive Problems

- 23** Use Problem 18 from §3.2 to find the subgroup generated by the set  $\{a, b^2\}$ . How many elements does this subgroup have?
- 24** Use *SageMath* to find the order of the elements  $b \cdot f$ ,  $b \cdot f \cdot r \cdot f \cdot f$ , and  $f \cdot b \cdot r$  in the Pyraminx<sup>TM</sup> group.
- 25** Can you use *SageMath* to find an element of the Pyraminx<sup>TM</sup> group that has order 30?  
Hint: Exactly five of the six edges must be moved out of place. The sixth edge must flip as well.

# Chapter 4

---

## Patterns within the Cosets of Groups

We introduced subgroups in the last chapter, but left many questions unanswered. For example, is there any relationship between the size of the group and the size of one of its subgroups?

In this chapter, we will introduce the tool of *cosets* to determine many of the properties of subgroups, including what possible sizes the subgroups could be. This in turn will allow us to create an encryption scheme that is virtually impossible to crack. The cosets will also reveal that some subgroups have a special property, which we will call *normal subgroups*. Normal subgroups will become an important tool for many important theorems, such as proving that a fifth-degree polynomial cannot be solved in terms of radicals.

---

### 4.1 Left and Right Cosets

In this section, we will use cosets to prove Lagrange's theorem, which states that the order of the subgroup must divide the order of the group. This has some important ramifications in many fields such as internet security.

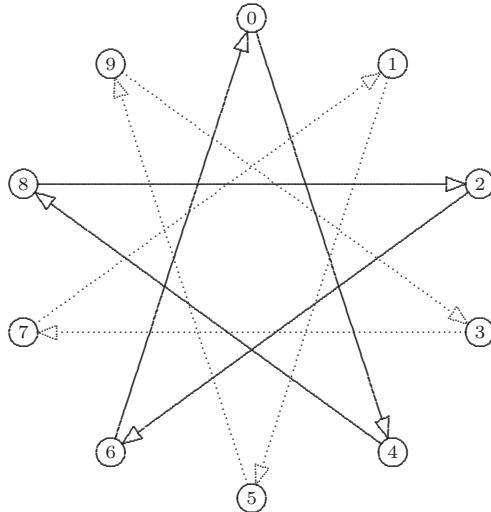
To understand cosets, let us begin by looking at some cases where an element does *not* generate the group, in hopes of finding some patterns in the circle graphs. For example, consider the element 4 from the group  $Z_{10}$ . This element does not generate the entire group, as evident from the two types of arrows in the circle graph.

```
Z = ZGroup(10)
CircleGraph(Z, Add(4))
```

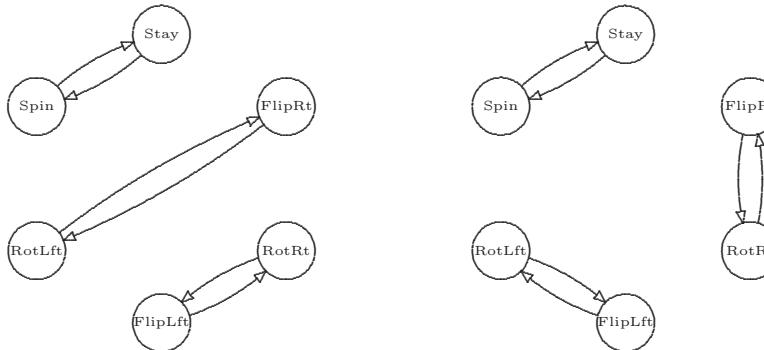
which produces [Figure 4.1](#)

The solid arrows connect the points  $\{0, 2, 4, 6, 8\}$ , while the dotted arrows connect the points  $\{1, 3, 5, 7, 9\}$ . Thus, the group is partitioned into two sets, and no arrow connects these two.

One of the two sets is actually a subgroup of  $Z_{10}$ , the subgroup generated by the element 4. The other set is obtained by adding 1 to each element of

**FIGURE 4.1:** Circle graph of **Add(4)**

the subgroup. Similar patterns arise when we use different elements of  $Z_{10}$  instead of 4.



```
CircleGraph(G, LeftMult(Spin))  CircleGraph(G, RightMult(Spin))
```

**FIGURE 4.2:** Circle graphs showing the cosets of  $\{\text{Stay}, \text{Spin}\}$ 

We can try a similar partitioning on non-abelian groups, such as Terry's group. If we consider forming a circle graph that sends each element to that element multiplied by **Spin**, we find we have a choice as to whether we have  $x$  map to  $x \cdot \text{Spin}$  or to  $\text{Spin} \cdot x$ . The circle graph for the first option is shown in the left half of Figure 4.2. This leads to a partition of the group into the sets  $\{\text{Stay}, \text{Spin}\}$ ,  $\{\text{RotRt}, \text{FlipLft}\}$ , and  $\{\text{RotLft}, \text{FlipRt}\}$ . The

latter option, shown on the right side of [Figure 4.2](#), is to multiply on the right instead of the left, giving the partition  $\{\text{Stay}, \text{Spin}\}$ ,  $\{\text{RotRt}, \text{FlipRt}\}$ , and  $\{\text{RotLft}, \text{FlipLft}\}$ . In both cases, one of the sets in the partition is the subgroup

```
G = InitTerry()
H = Group(Spin); H
    {Stay, Spin}
```

but the other sets are different.

**DEFINITION 4.1** Let  $G$  be a group, and let  $H$  be a subgroup of  $G$ . If  $x$  is an element of  $G$ , we define the set

$$xH = \{x \cdot y \mid y \in H\}.$$

The set  $xH$  is called a *left coset* of  $H$ . Likewise,

$$Hx = \{y \cdot x \mid y \in H\}$$

is a *right coset* of  $H$ .

*SageMath* mimics this notation. Thus,

```
H * RotRt
    {RotRt, FlipRt}
```

forms a right coset by multiplying every element in  $H$  by **RotRt**. Likewise

```
RotRt * H
    {RotRt, FlipLft}
```

forms a left coset.

We will denote the set of all *left* cosets of the subgroup  $H$  of  $G$  by  $G/H$ , and will denote the set of all *right* cosets of this subgroup by  $H\backslash G$ . Notice that the notation for right cosets uses a backward slash. In both cases, the subgroup can be considered to be on the “bottom,” but since a right coset  $Hx$  has the subgroup on the left, we use  $H\backslash G$ , which also has  $H$  on the left, to list all such right cosets.

*SageMath* finds all left and right cosets of  $G$  with  $H$  with the commands

```
LftCoset(G, H)
    {{Stay, Spin}, {RotLft, FlipRt}, {RotRt, FlipLft}}
RtCoset(G, H)
    {{Stay, Spin}, {RotLft, FlipRt}, {RotRt, FlipLft}}
```

Each coset is displayed as a list of elements, so we end up with a “list of lists,” giving all of the cosets. These are exactly the partitions we observed

in the circle graphs of **LeftMult(Spin)** and **RightMult(Spin)**. In fact, we begin to see some patterns in the cosets. First of all, all of the cosets are the same size. Also, every element of the group appears once, and only once, in each of the two coset lists. We will prove that these patterns are true in general with two lemmas.

### LEMMA 4.1

*Let  $G$  be a group and  $H$  be a finite subgroup of  $G$ . Then all left and right cosets of  $G$  with respect to  $H$  contain  $|H|$  elements.*

PROOF: It is clear from the definitions that  $Hu$  and  $uH$  each contains at most  $|H|$  elements. In order to prove that the number is exactly  $|H|$  we need to show that two distinct elements of  $H$  produce two different elements in the cosets. Suppose that this were not the case in a right coset. We would have two different elements  $x$  and  $y$  in  $H$  for which

$$x \cdot u = y \cdot u,$$

but multiplying on the right by  $u^{-1}$  gives  $x = y$ , a contradiction. Similar reasoning works for left cosets. If

$$u \cdot x = u \cdot y,$$

multiplying on the left by  $u^{-1}$  shows that  $x = y$ . □

Next we must show that every element of  $G$  is in exactly one left coset and one right coset. This can be worded as follows:

### LEMMA 4.2

*If two left or two right cosets have an element in common, they are in fact the same coset. That is,*

$$Hx \cap Hy \neq \{ \} \quad \text{implies that} \quad Hx = Hy,$$

and

$$xH \cap yH \neq \{ \} \quad \text{implies that} \quad xH = yH.$$

PROOF: We begin with right cosets. Suppose there is an element

$$g \in Hx \cap Hy.$$

Then there are elements  $h$  and  $k$  in  $H$  such that

$$g = h \cdot x = k \cdot y.$$

Therefore,

$$x = h^{-1} \cdot k \cdot y,$$

and so

$$Hx = Hh^{-1} \cdot k \cdot y. \quad (4.1)$$

Since  $H$  is a subgroup,  $h^{-1} \cdot k \in H$ , so that  $Hh^{-1} \cdot k \subseteq H$ . Moreover, if  $u$  is in  $H$ , then

$$u = (u \cdot k^{-1} \cdot h)(h^{-1} \cdot k) \in Hh^{-1} \cdot k.$$

Therefore

$$H \subseteq Hh^{-1} \cdot k,$$

and we have shown that  $H = Hh^{-1} \cdot k$ . Combining this with Equation 4.1 gives us  $Hx = Hy$ .

We can do left cosets in the same way. If there is an element  $g \in xH \cap yH$ , then there are elements  $h$  and  $k$  in  $H$  such that

$$g = x \cdot h = y \cdot k.$$

Therefore,

$$x = y \cdot k \cdot h^{-1},$$

and so

$$xH = y \cdot k \cdot h^{-1}H = yH. \quad \square$$

### **Example 4.1**

Find all of the left and right cosets of the subgroup  $\{1, 11\}$  of the group  $Z_{15}^*$ .  
**SOLUTION:** Since  $Z_{15}^*$  is abelian, the left and right cosets are the same. By Lemmas 4.1 and 4.2, the cosets will be disjoint, and all have 2 elements. One of the cosets will be the subgroup  $\{1, 11\}$ . We pick an element not in the subgroup, say 2, and multiply each element of the subgroup by 2, producing the coset  $\{2, 7\}$ . We pick another element not yet in a coset, and repeat the process. To find the coset containing 4, we multiply the subgroup by 4, to produce the coset  $\{4, 14\}$ . At this point, only 2 elements are unaccounted for, so they must be in their own coset,  $\{8, 13\}$ . So the list of cosets are

$$\{\{1, 11\}, \{2, 7\}, \{4, 14\}, \{8, 13\}\}. \quad \square$$

With these two lemmas, we can show that the size of any subgroup is related to the size of the original group.

### **THEOREM 4.1: Lagrange's Theorem**

*Let  $G$  be a finite group, and  $H$  a subgroup of  $G$ . Then the order of  $H$  divides the order of  $G$ . That is,  $|G| = k \cdot |H|$  for some positive integer  $k$ .*

**PROOF:** We can use either left cosets or right cosets to prove this, so let us use right cosets. Every element of  $x$  in  $G$  is contained in at least one right

coset. For example,  $x$  is contained in  $Hx$ . Let  $k$  be the number of distinct right cosets. Then, if the right cosets are

$$Hx_1, Hx_2, Hx_3, \dots, Hx_k,$$

we can write

$$G = Hx_1 \cup Hx_2 \cup Hx_3 \cup \dots \cup Hx_k.$$

The  $\cup$ 's represent the union of the cosets. But by Lemma 4.2, there are no elements in common among these sets, and so this union defines a partition of  $G$ . By Lemma 4.1, each cosets contains  $|H|$  elements. So  $|G| = k \cdot |H|$ .  $\blacksquare$

Lagrange's theorem (4.1), which seems apparent when looking at the cosets of a subgroup, turns out to have some far-reaching consequences. Let us look at some of the results that can be obtained using Lagrange's theorem.

#### **COROLLARY 4.1**

*Let  $G$  be a finite group, and let  $x$  be an element of  $G$ . Then the order of  $x$  divides  $|G|$ .*

PROOF: The order of  $x$  equals the order of the subgroup  $[x]$  of  $G$ . Therefore, by Lagrange's theorem (4.1), the assertion follows.  $\blacksquare$

#### **COROLLARY 4.2**

*Let  $G$  be a finite group of order  $n$  and let  $x$  be an element of  $G$ . Then*

$$x^n = e.$$

PROOF: Let  $m$  denote the order of  $x$ . By Corollary 4.1,  $n = mk$  for some integer  $k$ . Then we have  $x^n = x^{mk} = (x^m)^k = e^k = e$ .  $\blacksquare$

#### **COROLLARY 4.3**

*A group of prime order is cyclic.*

PROOF: Suppose  $G$  is of order  $p$ , which is prime. Then the only positive divisors of  $p$  are 1 and  $p$ , so by Lagrange's theorem (4.1) any subgroup must be of order 1 or  $p$ . If  $x$  is any element of  $G$  besides the identity, then  $[x]$  contains  $x$  as well as the identity. Thus,  $G = [x]$  so  $G$  is cyclic.  $\blacksquare$

#### **COROLLARY 4.4**

*Let  $n$  be a positive integer, and  $x$  a number coprime to  $n$ . Then*

$$x^{\phi(n)} \equiv 1 \pmod{n},$$

*where  $\phi(n)$  is Euler's totient function.*

PROOF: We simply apply Corollary 4.2 to the group  $Z_n^*$ . This group has  $\phi(n)$  elements, and if  $x$  is coprime to  $n$ , then  $x$  is a generator of  $Z_n$ , so  $x$  is in  $Z_n^*$ .  $\square$

In particular, when  $n = p$  is prime, we have

$$x^{p-1} \equiv 1 \pmod{p}.$$

This result is known as Fermat's little theorem. (See the Historical Diversion on page 103.)

**DEFINITION 4.2** If  $H$  is a subgroup of  $G$ , we define the *index* of  $H$  in  $G$ , denoted  $[G:H]$ , to be the number of right cosets in  $H \setminus G$ . Of course this is the same as the number of left cosets in  $G/H$ .

Notice that when  $G$  is a finite group we have by the argument in Lagrange's theorem (4.1) that  $|G| = |H| \cdot [G:H]$ .

### Problems for §4.1

For Problems 1 through 8: Find all of the cosets of the subgroup  $H$  of the group  $G$ . Since these groups are abelian, the left and right cosets are the same.

- |                                       |                                    |
|---------------------------------------|------------------------------------|
| 1 $G = Z_{10}$ , $H = \{0, 5\}$ .     | 5 $G = Z_{15}^*$ , $H = \{1, 14\}$ |
| 2 $G = Z_{12}$ , $H = \{0, 4, 8\}$ .  | 6 $G = Z_{16}^*$ , $H = \{1, 7\}$  |
| 3 $G = Z_{15}$ , $H = \{0, 5, 10\}$ . | 7 $G = Z_{19}^*$ , $H = \{1, 9\}$  |
| 4 $G = Z_{15}^*$ , $H = \{1, 4\}$     | 8 $G = Z_{24}^*$ , $H = \{1, 5\}$  |

9 List all of the left and right cosets of the subgroup  $\{\texttt{Stay}, \texttt{FlipRt}\}$  of Terry's group. Are the left and right cosets the same?

10 List all of the left and right cosets of the subgroup  $\{e, a \cdot b\}$  of  $S_3$ . Are the left and right cosets the same? See Table 3.3 for the Cayley table of  $S_3$ .

For Problems 11 through 22: Without using *SageMath*, but rather by taking advantage of Corollary 4.4, compute the following modular powers.

- |                           |                          |                          |
|---------------------------|--------------------------|--------------------------|
| 11 $5^{159} \pmod{7}$ .   | 15 $213^{319} \pmod{16}$ | 19 $529^{429} \pmod{29}$ |
| 12 $7^{182} \pmod{13}$ .  | 16 $247^{343} \pmod{20}$ | 20 $617^{581} \pmod{31}$ |
| 13 $13^{245} \pmod{15}$ . | 17 $323^{405} \pmod{21}$ | 21 $739^{625} \pmod{37}$ |
| 14 $175^{203} \pmod{14}$  | 18 $479^{479} \pmod{24}$ | 22 $823^{731} \pmod{41}$ |

23 Prove that the order of  $Z_n^*$  is even whenever  $n > 2$ .  
Hint: Find a subgroup of order 2.

24 Show that if  $H$  is a subgroup of  $G$ , and the left coset  $xH$  is also a subgroup of  $G$ , then  $x$  is in  $H$ .

## Historical Diversion

# Pierre de Fermat (1601–1665)

---

Pierre de Fermat was a French lawyer and amateur mathematician. Although mathematics was only a hobby for him, he made several important contributions to the field. He came up with a method, which he called *adequality*, to find the maxima and minima of functions, and then adapted this method to find the tangent lines to curves. This would later be developed into *differentiable calculus*. He also made notable contributions in analytic geometry, probability and optics.

Fermat also did significant research in number theory. He studied perfect numbers (numbers equal to the sum of their positive divisors excluding the number itself), and amicable numbers, which would later be called Fermat numbers. While researching perfect numbers, he discovered Fermat's little theorem, which state that if  $p$  is a prime number, then  $a^p - a$  is a multiple of  $p$  for all integers  $a$ .

But perhaps his greatest contribution to mathematics was accidental. He had a translation of *Arithmetica*, written by the Greek Diophantus, which in one section explained how to find solutions to the equation  $x^2 + y^2 = z^2$  where  $x$ ,  $y$ , and  $z$  are integers. Fermat wrote in the margin of his book, in Latin,

It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have discovered a truly remarkable proof, but this margin is too small to contain it.

This note, discovered 30 years after Fermat's death by his son, claims that there is no positive integer solution to the equation  $x^n + y^n = z^n$  for  $n > 2$ . Historians figure that his proof of "Fermat's last theorem" was probably flawed, as was the proof of countless mathematicians after him who tried to prove the statement. Yet, because of Fermat's "mistake," several new developments in mathematics occurred in attempt to find a proof. Countless advances in number theory were found in order to prove the theorem for small values of  $n$ . Ernst Kummer discovered rings and ideals in an attempt to correct a proof using unique factorization. Finally, in 1994, Andrew Wiles produced the first successful proof, using the concepts of elliptic curves and modular forms, both of which would have been unknown to Fermat.



**25** Show that if an element  $y$  of a group  $G$  is in the right coset  $Hx$ , where  $H$  is a subgroup of  $G$ , then  $Hy = Hx$ .

**26** Let  $|G| = 33$ . What are the possible orders for the elements of  $G$ ? Show that  $G$  must have an element of order 3.

Hint: Each subgroup of order 11 would contain 10 elements of order 11, along with the identity.

**27** Suppose  $G$  is a group of order  $pq$ , where  $p$  and  $q$  are prime. Show that every non-trivial subgroup is cyclic.

**28** Suppose  $G$  is a group of order  $pq$ , where  $p$  and  $q$  are prime, with  $p \neq q$ . Suppose there is only one subgroup of order  $p$ , and one subgroup of order  $q$ . Prove that  $G$  is cyclic.

**29** Find all subgroups of the group  $Z_{15}^*$ .

Hint: What does Lagrange's theorem say about a non-trivial, non-cyclic subgroup?

**30** Find all subgroups of the group  $Z_{16}^*$ . See the hint for Problem 29.

**31** Find all subgroups of the group  $Z_{20}^*$ . See the hint for Problem 29.

**32** If  $G$  is a group, and  $p$  is prime, show that the number of elements of  $G$  of order  $p$  is a multiple of  $p - 1$ .

### Interactive Problems

**33** Find the left and right cosets of the subgroup  $\{e, c, c^2, c^3\}$  of the octahedral group, given by:

```
InitGroup("e"); AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^4, e)
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
G = Group()
```

Are the left and right cosets the same?

**34** Find the left and right cosets of the subgroup  $\{e, c^2, a \cdot b^2 \cdot c, a \cdot b^2 \cdot c^3\}$  of the octahedral group, given by:

```
InitGroup("e"); AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^4, e)
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
G = Group()
```

Are the left and right cosets the same?

## 4.2 Writing Secret Messages

It was mentioned in the last section that Lagrange's theorem (4.1) has some far-reaching implications. One of these implications is the ability to write a message that no one can read except for the person to whom the message is sent, *even if the whole world knows the code!* This code has applications in internet security and secure data transmissions.

### Motivational Example 4.2

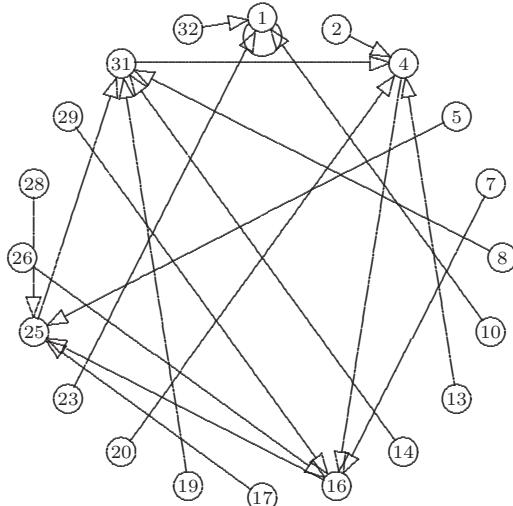
To introduce this code, we begin by considering the group  $Z_{33}^*$ , whose order is  $\phi(33) = 20$ . The elements of  $Z_{33}^*$  are

$$\{1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32\}.$$

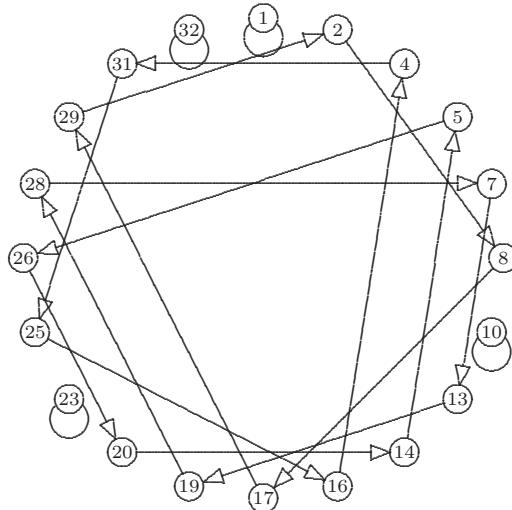
Consider the mapping that sends every element to its square. In essence we are defining a function  $f(x) = x^2$  on this group. We can make a circle graph in *SageMath* that maps each element to its square by the command

```
G = ZStar(33)
CircleGraph(G, Pow(2))
```

which produces Figure 4.3.



**FIGURE 4.3:** Circle graph for squaring in  $Z_{33}^*$



**FIGURE 4.4:** Circle graph for cubing in  $Z_{33}^*$

This graph is rather perplexing. The squares of 2, 13, 20, and 31 are all 4. The elements having “square roots” have four of them, while the majority of the elements do not have square roots.

If we try cubing each element instead, using the command

```
CircleGraph(G, Pow(3))
```

we get [Figure 4.4](#). This graph has a very different behavior: no two elements have the same cube. We see from [Figure 4.4](#) that the cube function is both one-to-one and onto. Thus, every element has a unique cube root.  $\blacksquare$

To understand this example, we notice that the cube root of any element in this group can be found by taking the seventh power of the element! This is because  $\phi(33) = 20$ , so using Corollary 4.4,

$$(x^3)^7 = x^{21} = x^{20} \cdot x = e \cdot x = x.$$

The key difference between the squaring function and the cubing function stems from the fact that 3 is coprime to  $\phi(33) = 20$ , whereas 2 is not.

### PROPOSITION 4.1

Suppose  $G$  is a finite group of order  $m$ , and that  $r$  is some integer which is coprime to  $m$ . Then the function  $f(x) = x^r$  is one-to-one and onto. In other words, we can always find the unique  $r^{\text{th}}$  root of any element in  $G$ .

PROOF: Since  $G$  is of order  $m$ , we have by Corollary 4.2 that  $x^m = e$  for all  $x$  in  $G$ . If  $r$  and  $m$  are coprime, then  $r$  is a generator in the additive group  $Z_m$ . But this means that  $r$  is an element of the group  $Z_m^*$ , and so there is an inverse element  $s = r^{-1}$ . Thus,  $s \cdot r = 1$  in  $Z_m^*$ . Another way we could say this is

$$sr = km + 1$$

for some integer  $k$ .

Now we are ready to take the  $r^{\text{th}}$  root of an element. If  $y$  is an element of  $G$ , then the  $r^{\text{th}}$  root of  $y$  in  $G$  is merely  $y^s$ . To see this, note that

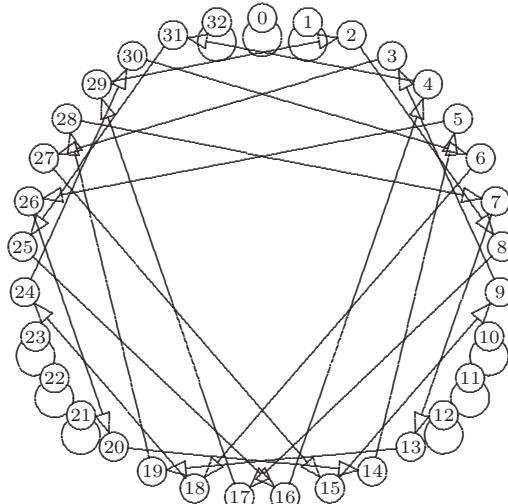
$$(y^s)^r = y^{sr} = y^{(km+1)} = (y^m)^k \cdot y = e^k \cdot y = y.$$

So  $y^s$  is one  $r^{\text{th}}$  root of  $y$ . But  $y^s$  must be a different element for every  $y$  in  $G$ , since the  $r^{\text{th}}$  power of  $y^s$  is different. Since the  $r^{\text{th}}$  root of every element of  $G$  is accounted for, by the pigeonhole principle there cannot be two  $r^{\text{th}}$  roots to any element. Thus,  $y^s$  gives the unique  $r^{\text{th}}$  root of  $y$  in  $G$ .  $\blacksquare$

### Motivational Example 4.3

Let us now consider the cubes of all numbers from 0 to 32. This will no longer be a group, since we have included non-invertible elements. But with the circle graph shown in Figure 4.5, we find that the mapping  $x \rightarrow x^3$  is still one-to-one and onto. Thus, we can still find the cube root of a number modulo 33 by taking the seventh power modulo 33.  $\blacksquare$

The reason is given in the next proposition.



**FIGURE 4.5:** Circle graph for cubing modulo 33

**PROPOSITION 4.2**

Suppose  $n$  is a product of two distinct primes and

$$r \cdot s \equiv 1 \pmod{\phi(n)}.$$

Then for all values of  $x$  less than  $n$ ,

$$(x^r)^s \equiv x \pmod{n}.$$

**PROOF:** The proposition is trivial if  $x = 0$ , so we will assume that  $x > 0$ .

If  $x$  is coprime to  $n$ , then proposition is true by Proposition 4.1. Suppose  $x$  is not coprime to  $n = p \cdot q$ , where  $p$  and  $q$  are the two distinct primes. By the totient function theorem (3.1),  $\phi(n) = (p - 1) \cdot (q - 1)$ . The number  $x$  would be a multiple of either  $p$  or  $q$ , say  $p$ . Then  $x = p \cdot a$  for some integer  $a$ , and so

$$x^{r \cdot s} = (p \cdot a)^{r \cdot s} = p^{r \cdot s} \cdot a^{r \cdot s}$$

will be a multiple of  $p$ . Also,  $x$  is *not* a multiple of  $q$  since  $x$  is less than  $n$ . Since  $r \cdot s \equiv 1 \pmod{(p - 1)(q - 1)}$ ,  $r \cdot s \equiv 1 \pmod{(q - 1)}$ . Thus, by Proposition 4.1 again, we have

$$x^{rs} \equiv x \pmod{q}.$$

Since we also have  $x^{rs} \equiv x \pmod{p}$ , by the Chinese remainder theorem (1.5), we have, since  $p$  and  $q$  are coprime,

$$x^{rs} \equiv x \pmod{pq = n}. \quad \square$$

**Example 4.4**

The function  $x \rightarrow x^3$  is not only one-to-one and onto but also mixes up the numbers 0 through 32 fairly well. This suggests an encryption scheme. We can first convert a message to a sequence of numbers using [Table 4.1](#). For example,

CAN YOU READ THIS

becomes

$$3, 1, 14, 0, 25, 15, 21, 0, 18, 5, 1, 4, 0, 20, 8, 9, 19.$$

The encryption scheme is to replace each number with its cube, modulo 33. This gives us

$$27, 1, 5, 0, 16, 9, 21, 0, 24, 26, 1, 31, 0, 14, 17, 3, 28.$$

To decipher this, one would take the seventh power of each number in the sequence modulo 33, and convert back to letters in the alphabet.  $\square$

The main drawback with this code is that, for longer messages, the letter E which encodes to 26 would appear most frequently in the encoded string.

**TABLE 4.1:** Standard code sending letters to numbers

A	=	1	J	=	10	S	=	19
B	=	2	K	=	11	T	=	20
C	=	3	L	=	12	U	=	21
D	=	4	M	=	13	V	=	22
E	=	5	N	=	14	W	=	23
F	=	6	O	=	15	X	=	24
G	=	7	P	=	16	Y	=	25
H	=	8	Q	=	17	Z	=	26
I	=	9	R	=	18	Space	=	0.

Someone who didn't know the code might deduce that 26 stands for E without knowing anything about algebra. But also anyone who knew how to encrypt the message could use Proposition 4.2 to decipher the message, for they could deduce that 7 is the inverse of 3 modulo 20. What we need is a code in which everyone would know how to encrypt a message, but only the person who originated the code could decipher.

We can solve both of these problems just by picking  $n$  to be the product of two huge prime numbers  $p$  and  $q$ , say 80 digits each. Then  $\phi(n) = (p-1)\cdot(q-1)$ . We then pick  $r$  to be a number of at least four digits that is coprime to  $\phi(n)$ . The encryption scheme is then

$$x \rightarrow y = x^r \pmod{n}.$$

We decode this by finding  $s = r^{-1}$  in the group  $Z_{\phi(n)}^*$ . By Proposition 4.2, the operation

$$y \rightarrow x = y^s \pmod{n}$$

“undoes” the encryption, since

$$(x^r)^s \equiv x \pmod{n}.$$

One big advantage of using huge numbers for the code is that we can encrypt an entire *line* at a time. For example,

CAN YOU READ THIS

can be encrypted by the single number

0301140025152100180501040020080919

by having every two digits represent one letter (still using [Table 4.1](#)). This prevents cracking the code using the frequencies of the letters. But the unusual advantage of this code is that only the originator of the code can decipher a message, even if the encryption scheme and the values of  $n$  and  $r$  were made public.

In order to decode a message, one must know the value of  $s$ , which is given by the inverse of  $r \pmod{\phi(n)}$ . This is easy to do with *SageMath* once  $\phi(n)$  is known, but how difficult it is to find  $\phi(n)!$  One needs to know the prime factorization of  $n$ , which would be about 160 digits long. Even *SageMath* could not factor this in a reasonable amount of time. In fact, adding two digits to  $p$  and  $q$  makes the factorization 10 times harder. So by making the prime numbers large enough, we can be assured that the factorization cannot be done within one's lifetime [6, p. 21]. Thus, without knowing the original primes  $p$  and  $q$  that were multiplied together, it is virtually impossible to determine  $s$ .

This encryption scheme is called the Rivest-Shamir-Adleman encryption [6, p. 374]. *SageMath* has built in routines that allow us to experiment with RSA encryption.

### **Computational Example 4.5**

The function

```
p = NextPrime(123456789012345678901234567890123456789012
34567890123456789012345678901234567890); p
123456789012345678901234567890123456789012345678901234567\
89012345678901234567997
```

finds the next prime number larger than that 80 digit number. Since we want  $n$  to be the product of two large primes, we will find another large prime  $q$ , and multiply these primes together.

```
q = NextPrime(987654321098765432109876543210987654321098
76543210987654321098765432109876543210); q
987654321098765432109876543210987654321098765432109876543\
21098765432109876543391
```

Although the input lines are shown here are broken up to allow it to be printed, in *SageMath* the input would be all on one line. The output uses a backslash to show that the line continues to the next line.

*SageMath* uses a variation of the Agrawal, Kayal, and Saxena primality test to find the next prime number. This test can definitely determine whether a number is prime, in a time that is a polynomial function of the number of digits in  $p$  and  $q$ . Hence, we can quickly know for certain that the numbers  $p$  and  $q$  are prime.

Next, we multiply the two numbers together, and broadcast this number,  $n$ .

```
n = p*q; n
121932631137021795226185032733866788594511507391563633592\
367611644557885992989178890411066640755785539247046441441\
8514328958998221647614501039932917991510457827
```

The number  $n$  can be made public, along with any four digit number  $r$  that is coprime to both  $p - 1$  and  $q - 1$ . For simplicity, we will use a four digit prime number.

```
r = NextPrime(1234); r
1237
```

We can verify that this is coprime to  $(p - 1)(q - 1)$  by computing

```
gcd((p-1)*(q-1), r)
1
```

which returns 1.

To encrypt a message, the command

```
x = MessageToNumber("HERE IS A MESSAGE"); x
805180500091900010013051919010705
```

converts any sentence into a number. Note we put the message in quotation marks. This number can now be encrypted by the command

```
y = PowerMod(x, r, n); y
147247305009975975061020323443960820217332118235485301293\
328137910666009784174590387960261013714614520688073075781\
586039000476825576155377145604282754058969344
```

□

Deciphering a message is very similar, only we will use the secret number  $s$  instead of  $r$ .

### **Computational Example 4.6**

Suppose a friend, knowing the above values of  $n$  and  $r$ , gives the message

```
y = 6955740514702440687061142665742560438277560654407470
32387700788446830783525388331288538827113160595765080505
966693143199918635215093570816224139063616551830794
```

Use *SageMath* to decipher the message.

SOLUTION: To decode the message, we first need to know the value of  $s$ , which is the inverse of  $r$  modulo  $(p - 1)(q - 1)$ . Thus, the command to find  $s$  is given by

```
s = PowerMod(r, -1, (p-1)*(q-1)); s
116609783860223754044120366793989014476400253228956975375\
724239753849619344952453906961891044114511747360397424479\
6004951506912258362719087686981566416986602133
```

Next, compute  $y^s \pmod{n}$  by the command

```
x = PowerMod(y, s, n); x
13555570006355005170003740333006693639300525558596454007 \
05855006958555493
```

Finally, the command

```
NumberToMessage(x)
'Meet me at 7:30 p.m. behind the shed.'
```

puts the message into readable form.

□

You may notice that the encryption in [Table 4.1](#) has been expanded to allow lower case letters and punctuation. There are many other applications to this code besides sending secret messages.

### Computational Example 4.7

Suppose to get an account at the Electronic Bank, you pick two large random prime numbers,  $p$  and  $q$ . The bank then gives you the account number  $n = p \cdot q$ , and a number  $r$ , and makes these public. The bank also gives you the secret number

$$s = r^{-1} \pmod{(p-1)(q-1)}.$$

Although  $s$  is normally used to decode messages, you use the number  $s$  to *sign* messages such as

```
y = MessageToNumber(
"Check 1034: Pay to the order of John Brown $43.50"); y
358555361003130333440001651750070650070585500656854556800 \
655600106558640026865736400833433933530
x = PowerMod(y, s, n); x
582856389557555731159430339514715251572029961076124346556 \
829718227800157027543664564994630786322333669442864481876 \
983813804537827731483093504482242861001933825
```

This number, along with your account number and the number  $r$ , is sent to John Brown. His bank can verify that this number is in fact a check as follows:

```
y = PowerMod(x, r, n)
NumberToMessage(y)
'Check 1034: Pay to the order of John Brown $43.50'
```

This proves that the only person knowing  $s$  sent this message. Hence, the encryption acts as a *signature* to the check. Using this method, one can send an “electronic check” (even through e-mail) that is virtually impossible to forge.

□

## Problems for §4.2

For Problems 1 through 4: Use the code in Example 4.4 to encrypt the following messages.

- |                |              |
|----------------|--------------|
| 1 RSA WORKS    | 3 NO PROBLEM |
| 2 TRUST NO ONE | 4 DONT PANIC |

For Problems 5 through 8: Use the code in Example 4.4 to decipher the following messages.

- 5 14, 17, 3, 28, 0, 3, 28, 26, 1, 20, 16.
- 6 1, 12, 12, 0, 28, 16, 28, 14, 26, 19, 28, 0, 13, 9
- 7 19, 1, 11, 26, 0, 3, 14, 0, 28, 9
- 8 24, 26, 22, 26, 24, 28, 26, 0, 4, 9, 12, 1, 24, 3, 14, 16

- 9 Show that Proposition 4.2 is still true if  $n$  is the product of *three* distinct primes. In fact, many applications of the RSA code use three large primes instead of two.
- 10 Show that Proposition 4.2 is no longer true if we let  $n = p^2$  for some prime  $p$ .

For Problems 11 through 18: Find the inverse of the following functions. Note that some of these require the result of Problem 9.

- |                            |                                |
|----------------------------|--------------------------------|
| 11 $f(x) = x^3 \pmod{51}$  | 15 $f(x) = x^{11} \pmod{217}$  |
| 12 $f(x) = x^7 \pmod{55}$  | 16 $f(x) = x^{13} \pmod{323}$  |
| 13 $f(x) = x^5 \pmod{91}$  | 17 $f(x) = x^7 \pmod{1001}$    |
| 14 $f(x) = x^7 \pmod{143}$ | 18 $f(x) = x^{11} \pmod{2717}$ |

- 19 Use the public key  $n = 2773$  and  $r = 17$  to encrypt “PASCAL” two letters at a time, using [Table 4.1](#). How would you decipher this message?
- 20 [Figure 4.3](#) shows that whenever an element of  $Z_{33}^*$  has a square root, it has 4 of them. Generalize this to any abelian group. If  $R_k(G) = n$  for an abelian group  $G$ , and  $y^k = b$  for some element  $b$ , then there are precisely  $n$  solutions to the equation  $x^k = b$ .

### Interactive Problems

- 21 This exercise is required in order to do the RSA encryption Problem 22 or 23. In order to use the **MessageToNumber** and **NumberToMessage** commands, we can reload the routines needed for RSA, in case the package **absalgtext2.sage** was not loaded.

```
load("RSA.sage")
RSA routines loaded.
```

Now using *SageMath*'s **NextPrime** command, find two large prime numbers  $p$  and  $q$ , at least 80 digits each. This is done by the two commands

```
p = NextPrime( large number goes here ); p
q = NextPrime( another large number goes here ); q
```

We will use the value  $r = 10007$ . Verify that this number is coprime to  $p - 1$  and  $q - 1$  by executing the following:

```
gcd( (p - 1)*(q - 1), 10007)
```

If this yields 10007 instead of 1, go back and find new values for  $p$  and  $q$ . Once the gcd is 1, compute  $n = p \cdot q$ , and save this to a file. To do this, enter

```
n = p*q
print("n = ", n)
```

This line can now be copied and pasted into a text file.

Next, find the secret number  $s$ , which deciphers a message:

```
s = PowerMod(10007, -1, (p - 1)*(q - 1) )
```

You will want to save this number for future reference.

```
print("s = ", s)
```

We will also include a “confirmation number”  $c$ .

```
c = PowerMod(2, s, n )
print("c = ", c)
```

These also can be copied and pasted into a text file. Finally, copy and paste the  $n$  and  $c$  numbers into the body of an e-mail message, sent to the professor. Do not send the number  $s$ . This is your secret number used for signing documents or decrypting messages sent to you. Save this number for future exercises.

- 22** Using Example 4.7 as your guide, and the values of  $n$  and  $s$  from Problem 21, send an “electronic check” to your favorite professor for \$100.00.

```
y = MessageToNumber("Check . . .")
```

Then you must “sign” the check using your secret  $s$  number.

```
x = PowerMod(y, s, n)
print("x = ", x)
```

Then copy and paste the output  $x$  into the body of an e-mail message.

- 23** After doing Problem 21, your instructor will send you a response with a value of  $y$ . Copy and paste this number into an input cell of *SageMath* along with your values of  $n$  and  $s$  from Problem 21, and evaluate them. Using Example 4.6 as your guide, decode the message  $y$  and hand in (on paper) what it says.

**24** B. L. User tried creating his encryption number with the two primes

**24** B. L. User tried creating his encryption number with the two primes

```
p = NextPrime(715870273457197548734156715678567821637415  
61519737155752525673649286739584756092); p  
q = NextPrime( p + 1 ); q
```

When he publicized the product  $n = pq$ , along with the value  $r = 6367$ , he received a message from a friend:

$y = 3092722521993064335403878476414515883199432204869058$   
 $0059761407250735465231068482494915312824566404543856784$   
 $72107616521242043590910817888839981759972041752306977$

What did this message say?

- 25** B. L. User tried again, this time with the two primes

When he publicized the product  $n = pq$ , along with the value  $r = 6367$ , he received the message:

$y = 1558672247570529436516848227697561797460920154529049$   
 $9722240308097127979631683649688737724267018012366968253$   
 $789095615381333414455768854608714790690628382743232001$

What did this message say?

### 4.3 Normal Subgroups

When we defined left cosets and right cosets, we were in essence defining how we could take an element of a group  $G$  and multiply it with a subgroup of  $G$ . But this definition can apply to any subset of  $G$ . We can define a product of any *subset* of a group  $G$  by an element of  $G$  in the same way that we defined a product of a subgroup and an element. That is, if  $X$  is any subset of  $G$ , we can define

$$\begin{aligned} Xu &= \{x \cdot u \mid x \in X\}, \quad \text{and} \\ uX &= \{u \cdot x \mid x \in X\}. \end{aligned}$$

We can also, using the same idea, multiply two subsets of  $G$  together.

**DEFINITION 4.3** *If  $X$  and  $Y$  are two subsets of a group  $G$ , we can define*

$$X \cdot Y = \{x \cdot y \mid x \in X \text{ and } y \in Y\}.$$

By defining the product of subsets in this way, we find that  $\{u\} \cdot X = uX$ . We also discover that

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z.$$

This raises some interesting questions. If  $X$  and  $Y$  are subgroups of  $G$ , will  $X \cdot Y$  be a subgroup? Suppose  $X$  and  $Y$  are cosets of  $G$  with respect to a subgroup  $H$ . Will  $X \cdot Y$  be a coset of  $G$ ?

#### **Exploratory Example 4.8**

We will use the octahedral group of order 24 to experiment. In *SageMath*, this can be reloaded with the commands

```
InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e)
Define(b^3, e)
Define(c^4, e)
Define(b*a, a*b^2)
Define(c*a, a*b*c)
Define(c*b, a*c^2)
G = Group(); G
{e, a, b, a*b, b^2, a*b^2, c, a*c, b*c, a*b*c, b^2*c,
 a*b^2*c, c^2, a*c^2, b*c^2, a*b*c^2, b^2*c^2, a*b^2*c^2,
 c^3, a*c^3, b*c^3, a*b*c^3, b^2*c^3, a*b^2*c^3}
```

Two sample subgroups of order 4 are given by

```
H = Group(c); H
{e, c^2, c, c^3}
K = Group(b*c); K
{e, b*c, a*b*c^2, a*b^2*c^3}
```

We can now explore what happens when we multiply two subgroups together.

```
H*K
{e, a*b, b^2, a*b^2, c, a*c, b*c, a*b^2*c, c^2, a*b*c^2,
b^2*c^2, a*b^2*c^2, c^3, a*c^3, b*c^3, a*b^2*c^3}
```

We can count the number of elements in the set by the command:

```
len(_)
16
```

So  $H \cdot K$  has 16 elements. Apparently, each element of  $H$ , when multiplied by an element in  $K$ , produces a unique element. This cannot be a subgroup by Lagrange's theorem (4.1), since 16 is not a factor of 24.  $\square$

Let us try again using the cosets of a subgroup instead of two subgroups.

### **Exploratory Example 4.9**

The right cosets of  $H$  are given by

```
RtCoset(G, H)
{{e, c, c^2, c^3}, {a, a*b*c, b*c^2, b^2*c^3}, {b, b^2*c,
a*c^2, a*b*c^3}, {a*b, b*c, b^2*c^2, a*c^3}, {b^2, a*c,
a*b*c^2, b*c^3}, {a*b^2, a*b^2*c, a*b^2*c^2, a*b^2*c^3}}
```

Let us try multiplying two right cosets of  $H$ , say the third and the fifth.

```
X = H*b; X
{b, b^2*c, a*c^2, a*b*c^3}
Y = H*b^2; Y
{b^2, a*c, a*b*c^2, b*c^3}
X * Y
{e, a, b, a*b^2, c, a*b*c, b^2*c, a*b^2*c, c^2, a*c^2,
b*c^2, a*b^2*c^2, c^3, a*b*c^3, b^2*c^3, a*b^2*c^3}
```

This also produces something with 16 elements, so this cannot be a subgroup. However, a left coset multiplied by a right coset produces a glimmer of hope:

```
W = b*H; W
{b, b*c^2, b*c, b*c^3}
W * Y
{e, a*b^2*c, a*c^2, b^2*c^3}
```

This, in fact, turns out to be a subgroup! In fact, any left coset times a right coset will produce a set with 4 elements.  $\square$

So what happens if we find a subgroup for which the right cosets and the left cosets are the same? Then the product of a left coset and a right coset would merely be the product of two cosets.

### Motivational Example 4.10

An example of a subgroup for which the left and right cosets are the same is

```
M = Group(a*b*c^2, c^2); M
{e, a*b^2*c, c^2, a*b^2*c^3}
```

which we can verify in *SageMath* by the commands

```
RtCoset(G, M)
{{e, a*b^2*c, c^2, a*b^2*c^3}, {a, b^2*c, a*c^2, b^2*c^3},
 {b, a*b*c, b*c^2, a*b*c^3}, {a*b, b*c, a*b*c^2, b*c^3},
 {b^2, a*c, b^2*c^2, a*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}
LftCoset(G, M)
{{e, a*b^2*c, c^2, a*b^2*c^3}, {a, b^2*c, a*c^2, b^2*c^3},
 {b, a*b*c, b*c^2, a*b*c^3}, {a*b, b*c, a*b*c^2, b*c^3},
 {b^2, a*c, b^2*c^2, a*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}
```

Two of these cosets are

```
H = a*M; H
{a, b^2*c, a*c^2, b^2*c^3}
K = b*M; K
{b, a*b*c, b*c^2, a*b*c^3}
```

and the product

```
H * K
{a*b, b*c, a*b*c^2, b*c^3}
```

turns out to be another coset. In fact, the product of any two cosets of the subgroup  $M$  will yield a coset of  $M$ .  $\square$

First, let us give some terminology for this special type of subgroup.

**DEFINITION 4.4** A subgroup  $H$  of the group  $G$  is said to be *normal* if all left cosets are also right cosets, and conversely, all right cosets are also left cosets. That is,  $H$  is normal if  $G/H = H\backslash G$ .

Next, we need a way to test whether a subset is normal.

**PROPOSITION 4.3**

*A subgroup  $H$  is a normal subgroup of  $G$  if, and only if,  $gHg^{-1} = H$  for all elements  $g$  in  $G$ .*

PROOF: First of all, suppose  $H$  is normal, and let  $g$  be an element of  $G$ . Then  $gH$  and  $Hg$  both contain the element  $g$ . Since the left and right cosets are the same, we have

$$gH = Hg.$$

Multiplying both sides on the right by  $g^{-1}$  gives

$$gHg^{-1} = Hg \cdot g^{-1} = H.$$

Now, suppose that  $gHg^{-1} = H$  for all elements  $g$  in  $G$ . Then

$$Hg = (gHg^{-1}) \cdot g = gHe = gH.$$

Thus, every left coset is also a right coset, and vice versa. □

This gives us a way to determine if a subgroup is normal, but we can improve on this test.

**PROPOSITION 4.4**

*Let  $H$  be a subgroup of  $G$ . Then  $H$  is normal if, and only if,*

$$g \cdot h \cdot g^{-1} \in H$$

*for all elements  $g$  in  $G$ , and  $h \in H$ .*

PROOF: If  $H$  is a normal subgroup of  $G$ , then  $g \cdot h \cdot g^{-1} \in gHg^{-1}$ , which is  $H$  by Proposition 4.3.

Let us suppose that for all  $g$  in  $G$  and  $h$  in  $H$ ,  $g \cdot h \cdot g^{-1} \in H$ . Then

$$gHg^{-1} \subseteq H$$

In particular, if we replace every  $g$  with  $g^{-1}$ , we get

$$g^{-1}H(g^{-1})^{-1} \subseteq H.$$

Multiplying both sides of the equation by  $g$  on the left gives us  $Hg \subseteq gH$ , and multiplying on the right by  $g^{-1}$  gives us  $H \subseteq gHg^{-1}$ . Since we also have that  $gHg^{-1} \subseteq H$ , we can conclude that  $gHg^{-1} = H$ . Then from Proposition 4.3,  $H$  is normal. □

There are many other examples of normal subgroups. For example, if  $G$  is any group, then the subgroups  $\{e\}$  and  $G$  are automatically normal. These

normal subgroups are said to be *trivial*. If  $G$  is commutative, then any subgroup will be a normal subgroup. Here is another example of a subgroup that is always normal.

### **PROPOSITION 4.5**

*If  $H$  is a subgroup of  $G$  with index 2, then  $H$  is a normal subgroup.*

PROOF: Since  $H$  is a subgroup of  $G$  with index 2, there are two left cosets and two right cosets. One of the left cosets is  $eH$ , which is the set of elements in  $H$ . The other left coset must then be the set of elements not in  $H$ . But the same thing is true for the right cosets, so the left and right cosets are the same. Thus,  $H$  is normal.  $\blacksquare$

When we have a normal subgroup, the set of cosets will possess more properties than for standard subgroups. We will explore these in the next section.

### **Problems for §4.3**

- 1 Show that if  $H$  is a subgroup of a group  $G$ , then  $H \cdot H = H$ , where the product of two sets is defined in Definition 4.3.
- 2 Find all of the normal subgroups of  $D_3$ . (This is Terry's group.)
- 3 Let  $H$  be a subgroup of  $G$  such that every left coset  $a \cdot H$  is also a right coset  $H \cdot b$ . Prove that  $H$  is a normal subgroup of  $G$ .
- 4 Prove that the intersection of two normal subgroups of  $G$  is a normal subgroup of  $G$ .
- 5 Let  $N$  be a normal subgroup of  $G$ , and let  $H$  be a subgroup of  $G$  which contains the subgroup  $N$ . Prove that  $N$  is a normal subgroup of  $H$ .
- 6 Show that if  $G$  is an abelian group, and  $X$  and  $Y$  are two subgroups of  $G$ , then  $X \cdot Y$  is a subgroup of  $G$ .
- 7 We saw in Example 4.10 that  $M$  was a normal subgroup of the octahedral group. Find a normal subgroup of  $M$  which is *not* a normal subgroup of the octahedral group.
- 8 Let  $G$  be a group, and let  $Z$  be the set of elements in  $G$  which commute with *all* the elements of  $G$ . That is,

$$Z = \{x \in G \mid g \cdot x = x \cdot g \text{ for all } g \in G\}.$$

Show that  $Z$  is a subgroup of  $G$ .

- 9** Let  $Z$  be the subgroup of Problem 8. Show that  $Z$  is in fact a normal subgroup of  $G$ .
- 10** Suppose a group  $G$  has a normal subgroup  $H$  with only two elements. Show that  $H$  is contained in the subgroup  $Z$  from Problem 8.
- 11** Let  $H$  be a normal *cyclic* subgroup of a finite group  $G$ , and let  $K$  be a subgroup of  $H$ . Show that  $K$  is a normal subgroup of  $G$ . (This would not be true if the word *cyclic* was left out, as indicated by Problem 7.)
- 12** Let  $G$  be the group from Example 2.9 in §2.3, the group of *linear functions* of the form  $f(x) = mx + b$ , with  $m, b \in \mathbb{R}$ ,  $m \neq 0$ . Let  $N$  be the subset of  $G$  for which  $m = 1$ , that is,

$$N = \{\phi(x) = x + b \mid b \in \mathbb{R}\}.$$

Show that  $N$  is a normal subgroup of  $G$ .

- 13** Let  $G$  be the group of *linear functions* as in Problem 12. Let  $T$  be the subset of  $G$  for which  $b = 0$ , that is,

$$T = \{\phi(x) = mx \mid m \in \mathbb{R}, m \neq 0\}.$$

Show that  $T$  is a subgroup of  $G$ , but not a normal subgroup. If  $f(x) = 2x + 3$ , describe both the left and right cosets  $f \cdot T$  and  $T \cdot f$ .

- 14** If  $H$  is a subgroup of  $G$ , and  $K$  is a normal subgroup of  $G$ , show that  $H \cdot K = K \cdot H$ .
- 15** Use Problem 14 to show that  $H \cdot K$  is a subgroup of  $G$ .
- 16** Let  $H$  be a subgroup of  $G$ , and  $K$  a normal subgroup of  $G$ . Show that  $H \cap K$  is a normal subgroup of  $H$ .
- 17** Use Problem 15 to show that if both  $H$  and  $K$  are normal subgroups of  $G$ , then  $H \cdot K$  is a normal subgroup of  $G$ .
- 18** Let  $G$  be a group of order  $2p$ , where  $p$  is prime. Show that if  $H$  is a subgroup that is *not* normal, then  $H$  has precisely two elements.

### Interactive Problems

- 19** Show that there is a group  $Q$  which is generated by two elements  $a$  and  $b$ , for which

$$a^4 = e, \quad b^2 = a^2, \quad b \cdot a = a^3 \cdot b, \quad a^2 \neq e.$$

This can be entered into *SageMath* with the command

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^4, e)
Define(b^2, a^2)
Define(b*a, a^3*b)
Q = Group(a, b); Q
```

Find all subgroups of this group, and show that all subgroups are normal, even though the group is non-abelian. (Write down the list of left cosets and right cosets for each subgroup found.)

- 20** Use *SageMath*, along with a bit of trial and error, to find a subgroup of order 12 of the octahedral group. Show that this subgroup is a normal subgroup. The following reloads the octahedral group:

```
InitGroup("e"); AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^4, e)
Define(b*a, a*b^2); Define(c*a, a*b*c);
Define(c*b, a*c^2)
G = Group()
```

---

## 4.4 Quotient Groups

In the last section we observed a case where  $H$  was a normal subgroup of  $G$ , and the product of two cosets yielded another coset. Let us begin by proving that this will always happen for normal subgroups.

### LEMMA 4.3

If  $N$  is a normal subgroup of  $G$ , then the product of two cosets of  $N$  produces a coset of  $N$ . In fact,

$$aN \cdot bN = (a \cdot b)N.$$

PROOF: We simply observe that

$$aN \cdot bN = a \cdot (Nb) \cdot N = a \cdot (bN) \cdot N = (a \cdot b) \cdot (N \cdot N) = (a \cdot b)N.$$

Note that  $Nb = bN$  because  $N$  is a normal subgroup. □

This proposition is very suggestive. Since we can multiply two cosets together, can the set of all cosets form another group?

### THEOREM 4.2: The Quotient Group Theorem

Let  $N$  be a normal subgroup of  $G$ . Then the set of all cosets is a group, which is denoted by  $G/N$ , called the quotient group of  $G$  with respect to  $N$ .

PROOF: We simply have to check that  $G/N$  satisfies the four requirements in Definition 2.5. The closure property is given by Lemma 4.3. To check associativity,

$$\begin{aligned}aN \cdot (bN \cdot cN) &= aN \cdot (b \cdot c)N = (a \cdot (b \cdot c))N \\&= ((a \cdot b) \cdot c)N = (a \cdot b)N \cdot cN = (aN \cdot bN) \cdot cN.\end{aligned}$$

The identity element is  $eN = N$ , and we can check that

$$\begin{aligned}eN \cdot aN &= (e \cdot a)N = aN, \quad \text{and} \\aN \cdot eN &= (a \cdot e)N = aN.\end{aligned}$$

Finally, the inverse of  $aN$  is  $a^{-1}N$ , since

$$\begin{aligned}aN \cdot a^{-1}N &= (a \cdot a^{-1})N = eN = N, \quad \text{and} \\a^{-1}N \cdot aN &= (a^{-1} \cdot a)N = eN = N.\end{aligned}$$

Thus, the set of all cosets forms a group. □

### **Example 4.11**

One of the easiest groups to consider is the group of integers  $\mathbb{Z}$  under addition. A subgroup of  $\mathbb{Z}$  would consist of all multiples of  $k$ , with  $k \geq 0$ . ( $k = 0$  and  $k = 1$  produce the two trivial subgroups.) We denote this normal subgroup of  $\mathbb{Z}$  by  $k\mathbb{Z}$ . All elements in each coset would be equivalent modulo  $k$ . Thus, there would be  $k$  cosets of  $k\mathbb{Z}$  (except when  $k = 0$ ). Hence,  $\mathbb{Z}/k\mathbb{Z}$  is essentially the same group as  $Z_k$ . That is,  $x$  and  $y$  will be in the same coset if, and only if,

$$x \equiv y \pmod{k}.$$
□

We can extend this notation to any normal subgroup. We say that

$$x \equiv y \pmod{N}$$

to indicate  $x$  and  $y$  belong in the same coset of  $G$  with respect to  $N$ . In fact, if  $x \equiv y \pmod{N}$ , then  $N \cdot x = N \cdot y$ , so  $N \cdot x \cdot y^{-1} = N$ , giving us  $x \cdot y^{-1} \in N$ . Thus, we have

$$x \equiv y \pmod{N} \quad \text{if, and only if, } \quad x \cdot y^{-1} \in N.$$

In §2.2, we defined a equivalence relation as a relation satisfying the three properties

1. (Reflexive) Every element  $x$  is equivalent to itself.
2. (Symmetric) If  $x$  is equivalent to  $y$ , then  $y$  is equivalent to  $x$ .

3. (Transitive) If  $x$  is equivalent to  $y$ , and  $y$  in turn is equivalent to  $z$ , then  $x$  is equivalent to  $z$ .

Because of the fact the two elements are equivalent if they are in the same coset, it is clear that  $x \equiv y \pmod{N}$  is an equivalence relation. The equivalence classes would be the cosets of  $N$  for which the relation is defined.

### **Computational Example 4.12**

In the last section we found a normal subgroup of the octahedral group, namely

```
M = Group(a*b*c^2, c^2); M
{e, a*b^2*c, c^2, a*b^2*c^3}
```

The cosets, or equivalence classes, with respect to this subgroup are given by the command

```
Q = LftCoset(G, M); Q
{{e, a*b^2*c, c^2, a*b^2*c^3}, {a, b^2*c, a*c^2, b^2*c^3},
 {b, a*b*c, b*c^2, a*b*c^3}, {a*b, b*c, a*b*c^2, b*c^3},
 {b^2, a*c, b^2*c^2, a*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}
```

We can use the *SageMath* command **CayleyTable(Q)** to give us the Cayley table of the quotient group  $Q$ , shown in [Figure 4.6](#). Since the names of the elements are so long, *SageMath* uses a color code for the elements, which is shown here as shading. □

Notice that this table is very similar to the table for the group  $S_3$ . This group is already defined in as a subset of the octahedral group, so we can look at its Cayley table.

```
H = [e, b, b^2, a, a*b, a*b^2]; H
{e, b, b^2, a, a*b, a*b^2}
CayleyTable(H)
```

The color patterns are not the same, but this doesn't mean that these two groups are not equivalent. There might be some way to rearrange the elements in the last command so that the color patterns in the two tables match. In fact, the command

```
CayleyTable([e, a*b^2, b, a, b^2, a*b])
```

produces the table in [Table 4.2](#). With this particular arrangement of the elements, we see that the color patterns for  $Q$  and  $H$  match. In [Chapter 5](#), we will define two groups that have the same color pattern as being *isomorphic*.

$\{e, a^*b^2*c, c^2, a^*b^2*c^3\}$						
$\{a, b^2*c, a^*c^2, b^2*c^3\}$						
$\{b, a^*b*c, b*c^2, a^*b*c^3\}$						
$\{a^*b, b*c, a^*b*c^2, b*c^3\}$						
$\{b^2, a^*c, b^2*c^2, a^*c^3\}$						
$\{a^*b^2, c, a^*b^2*c^2, c^3\}$						

**FIGURE 4.6:** Cayley table for the quotient group**TABLE 4.2:** Another Cayley table for  $S_3$ 

.	$e$	$a^*b^2$	$b$	$a$	$b^2$	$a^*b$
$e$	$e$	$a^*b^2$	$b$	$a$	$b^2$	$a^*b$
$a^*b^2$	$a^*b^2$	$e$	$a$	$b$	$a^*b$	$b^2$
$b$	$b$	$a^*b$	$b^2$	$a^*b^2$	$e$	$a$
$a$	$a$	$b^2$	$a^*b$	$e$	$a^*b^2$	$b$
$b^2$	$b^2$	$a$	$e$	$a^*b$	$b$	$a^*b^2$
$a^*b$	$a^*b$	$b$	$a^*b^2$	$b^2$	$a$	$e$

**Problems for §4.4**

For Problems 1 through 9, write the Cayley table for the following quotient groups:

1  $Z_{10}/\{0, 5\}.$

4  $Z_{12}/\{0, 6\}$

7  $Z_{16}^*/\{1, 7\}$

2  $Z_{12}/\{0, 4, 8\}.$

5  $Z_{15}^*/\{1, 4\}$

8  $Z_{13}^*/\{1, 3, 9\}$

3  $Z_{15}/\{0, 5, 10\}.$

6  $Z_{15}^*/\{1, 14\}$

9  $Z_{24}^*/\{1, 5\}$

- 10 Write the Cayley table for the quotient group created by the subgroup **{Stay, RotRt, RotLft}** of Terry's group.

- 11 Write the Cayley table for the quotient group created by the subgroup  $\{e, b, b^2\}$  of  $S_3$ .

- 12** Let  $\mathbb{Q}$  be the additive group of rational numbers. Show that the group of integers  $\mathbb{Z}$  is a normal subgroup of  $\mathbb{Q}$ . Show that  $\mathbb{Q}/\mathbb{Z}$  is an infinite group in which every element has finite order.
- 13** Describe the quotient group  $G/N$  of Problem 12 of §4.3.
- 14** Prove that the quotient group of an abelian group is abelian.
- 15** Prove that the quotient group of a cyclic group is cyclic.
- 16** Let  $G$  be a finite group, and  $H$  a normal subgroup of  $G$ . Prove that the order of the element  $gH$  in the group  $G/H$  divides the order of  $g$  in the group  $G$ .
- 17** Let  $N$  and  $H$  be two normal subgroups of  $G$ , with  $N$  contained inside of  $H$ . Prove that  $H/N$  is a subgroup of  $G/N$ . See Problem 5 of §4.3.
- 18** Let  $N$  and  $H$  be two normal subgroups of  $G$ , with  $N$  contained inside of  $H$ . Show that  $H/N$  is a *normal* subgroup of  $G/N$ . See Problem 17.

### Interactive Problems

- 19** Define in *SageMath* the group  $G = Z_{105}^*$ . How many elements does this group have? Consider the subgroup  $H$  generated by the element 11. A circle graph demonstrating the cosets  $G/H$  can be obtained by the command

**CircleGraph(G, Mult(11))**

By looking at the circle graph, determine the cosets of  $G$  with respect to  $H$ . What is the order of the element  $2 \cdot H$  in the quotient group  $G/H$ ?

- 20** Here is a group of order 20 from Problem 18 of §3.2:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^5, e); Define(b^4, e); Define(b*a, a^2*b)
G = Group()
```

Find a normal subgroup  $H$  of order 5, and form the quotient group  $G/H$ .

# Chapter 5

---

## Mappings between Groups

So far we have not considered the possibility of a *function* defined on a group. This chapter explores the idea of a function, or mapping, which sends elements of one group to another. With such mappings, we will find a way to determine whether two groups are essentially the same. We also will find a connection between group functions and normal subgroups. Finally, we will use function composition to prove three very important theorems in group theory.

---

### 5.1 Isomorphisms

The quotient group  $G/M$  we saw at the end of the last chapter turned out to be very similar to the group  $S_3$ . They are technically distinct, since the names for their elements are totally different. In this section, we will demonstrate the relationship between these two groups, using the concept of a mapping from one group to another.

We begin by finding a correlation between the elements of the two groups so that the corresponding Cayley tables would have identical color patterns.

#### **Motivational Example 5.1**

Here is one such possible correlation between the two groups:

$$\begin{aligned} e &\leftrightarrow \{e, a \cdot b^2 \cdot c, c^2, a \cdot b^2 \cdot c^3\} \\ a \cdot b^2 &\leftrightarrow \{a, b^2 \cdot c, a \cdot c^2, b^2 \cdot c^3\} \\ b &\leftrightarrow \{b, a \cdot b \cdot c, b \cdot c^2, a \cdot b \cdot c^3\} \\ a &\leftrightarrow \{a \cdot b, b \cdot c, a \cdot b \cdot c^2, b \cdot c^3\} \\ b^2 &\leftrightarrow \{b^2, a \cdot c, b^2 \cdot c^2, a \cdot c^3\} \\ a \cdot b &\leftrightarrow \{a \cdot b^2, c, a \cdot b^2 \cdot c^2, c^3\} \end{aligned}$$

Suppose we use this correlation to define a *function*  $f(x)$  sending each element of  $S_3$  to an element of  $G/M$ . Thus,

$$\begin{aligned}
 f(e) &= \{e, a \cdot b^2 \cdot c, c^2, a \cdot b^2 \cdot c^3\} \\
 f(a \cdot b^2) &= \{a, b^2 \cdot c, a \cdot c^2, b^2 \cdot c^3\} \\
 f(b) &= \{b, a \cdot b \cdot c, b \cdot c^2, a \cdot b \cdot c^3\} \\
 f(a) &= \{a \cdot b, b \cdot c, a \cdot b \cdot c^2, b \cdot c^3\} \\
 f(b^2) &= \{b^2, a \cdot c, b^2 \cdot c^2, a \cdot c^3\} \\
 f(a \cdot b) &= \{a \cdot b^2, c, a \cdot b^2 \cdot c^2, c^3\}
 \end{aligned}$$

The fact that the corresponding Cayley tables have the same color patterns can now be expressed simply by

$$f(x \cdot y) = f(x) \cdot f(y).$$

Also, the function  $f(x)$  maps different elements of  $S_3$  to different elements of  $G/M$ . That is,  $f(x)$  is one-to-one, or *injective*. Finally, every element of  $G/M$  appears as  $f(x)$  for some element  $x$ . This is expressed by saying that  $f(x)$  is onto, or *surjective*.

□

**DEFINITION 5.1** Let  $G_1$  and  $G_2$  be two groups, with  $(*)$  being the group operation of  $G_1$ , and  $(\cdot)$  being the group operation of  $G_2$ . An *isomorphism* from  $G_1$  to  $G_2$  is a one-to-one function sending elements of  $G_1$  to elements of  $G_2$  such that

$$f(x * y) = f(x) \cdot f(y) \quad \text{for all } x, y \in G_1.$$

If there exists an isomorphism from  $G_1$  to  $G_2$  that is also onto, then we say that  $G_1$  and  $G_2$  are *isomorphic*, denoted by

$$G_1 \approx G_2.$$

For example,

$$S_3 \approx G/M$$

because of the existence of the function  $f(x)$ , which we saw was both one-to-one and onto.

It should be noted that  $\approx$  is an equivalence relation on groups. (Reflexive property is obvious, symmetric and transitive properties are covered in Problems 1 and 2.) One of the important yet extremely hard problems in group theory is to find all of the non-isomorphic groups of a given order. Although this is still an unsolved problem, we have the following upper bound for the number of groups.

### PROPOSITION 5.1

*There are at most  $n^{(n^2)}$  non-isomorphic groups of order  $n$ .*

PROOF: If two groups have the same Cayley table, they are isomorphic, so a group is completely determined by its Cayley table. Notice that each element of this table must be one of  $n$  elements, and there are  $n^2$  entries in the table. So there are  $n^{(n^2)}$  ways of creating such a table.  $\square$

Of course, not very many of these tables will actually form a group. In fact, in some cases we can show that there is only one non-isomorphic group of order  $n$ .

### **PROPOSITION 5.2**

*For  $n$  a positive integer, every cyclic group of order  $n$  is isomorphic to  $Z_n$ .*

PROOF: Let  $G$  be a group of order  $n$ , and let  $g$  be a generator of  $G$ . For clarity, we will let  $\cdot$  denote the group operation of  $G$ , and  $*$  denote the group operation of  $Z_n$ . Since  $g^n = e$ , we have

$$G = \{e = g^0, g^1, g^2, g^3, \dots, g^{n-1}\}.$$

Define  $f : Z_n \rightarrow G$  by

$$f(x) = g^x \quad (0 \leq x \leq n-1).$$

That is,  $f$  will map the elements of  $Z_n$  to elements of  $G$ . Clearly,  $f$  is one-to-one and onto, and we would like to show that it is an isomorphism. Suppose  $x$  and  $y$  satisfy

$$0 \leq x, y \leq n-1.$$

We let  $z = x * y = (x + y) \bmod n$ . Then we can find an  $m$  such that  $x + y = mn + z$ . Now,  $f(x * y) = f(z) = g^z$  by the definition of  $f$ . Thus,

$$f(x * y) = g^z = g^{(x+y-mn)} = g^x \cdot g^y \cdot (g^n)^{-m} = g^x \cdot g^y = f(x) \cdot f(y).$$

Since  $f$  is an isomorphism of  $Z_n$  onto  $G$ , we have  $Z_n \approx G$ .  $\square$

In particular if  $p$  is prime, Corollary 4.3 indicates all groups of order  $p$  are cyclic. Thus all groups of order  $p$  are isomorphic to  $Z_p$ .

For example, there is only one group each, up to isomorphism, of sizes 2, 3, 5, and 7, namely  $Z_2$ ,  $Z_3$ ,  $Z_5$ , and  $Z_7$ . Our goal for this section is to find all of the possible groups, up to isomorphism, up to order 8. To help us in this endeavor we have the following lemma.

### **LEMMA 5.1**

*Suppose a group  $G$  whose order is greater than 2 has all non-identity elements being of order 2. Then  $G$  has a subgroup isomorphic to  $Z_8^*$ .*

**PROOF:** Since the order of  $G$  is greater than 2, there are two elements  $a$  and  $b$  besides the identity element  $e$ . Since these will have order 2, we have  $a^2 = b^2 = e$ . Consider the product  $a \cdot b$ . It can be neither  $a$  nor  $b$  since this would imply the other was the identity. On the other hand,  $a \cdot b = e$  implies

$$a = a \cdot e = a \cdot (b \cdot b) = (a \cdot b) \cdot b = e \cdot b = b.$$

So  $a \cdot b$  is not the identity either. So there must be a fourth element in  $G$ , which we will call  $c$ , such that  $a \cdot b = c$ . This element will also be of order 2, so we have  $c^2 = e$ .

Finally, note that

$$b \cdot a = e \cdot b \cdot a \cdot e = a \cdot a \cdot b \cdot a \cdot b \cdot b = a \cdot (a \cdot b)^2 \cdot b = a \cdot c^2 \cdot b = a \cdot e \cdot b = a \cdot b = c.$$

With this we can quickly find the remaining products involving  $a$ ,  $b$ , and  $c$ .

$$c \cdot a = b \cdot a \cdot a = b, \quad c \cdot b = a \cdot b \cdot b = a, \quad a \cdot c = a \cdot a \cdot b = b, \quad b \cdot c = b \cdot b \cdot a = a.$$

Hence, the set  $H = \{e, a, b, c\}$  is closed under multiplication, contains the identity, and also contains the inverses of every element in the set. Hence,  $H$  is a subgroup of  $G$ . The Cayley table for  $H$

.	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

shows that this is isomorphic to  $Z_8^*$  using the mapping

$$f(e) = 1,$$

$$f(a) = 3,$$

$$f(b) = 5,$$

$$f(c) = 7.$$

□

We can now find all non-isomorphic groups of order up to 8. For example, if we have a group of order 6, any element of order 6 would imply that the group is isomorphic to  $Z_6$ . We cannot have all non-identity elements to have order 2, or else Lemma 5.1 would give a subset of order 4, violating Lagrange's theorem (4.1). Thus, there must be an element  $a$  of order 3. Then  $H = \{e, a, a^2\}$  is a normal subgroup of order 3 by Proposition 4.5. If  $b$  be any element not in  $H$ , then the two cosets of  $H$  are

$$\{\{e, a, a^2\}, \{b, a \cdot b, a^2 \cdot b\}\}.$$

**TABLE 5.1:** Multiplication table for  $Z_{24}^*$ 

.	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

Because the quotient group is isomorphic to  $Z_2$ , we see that  $b^2$  is in  $H$ . If  $b^2$  is either  $a$  or  $a^2$ , then  $b$  is of order 6, so to get something different  $b^2$  must be  $e$ . Then since  $H$  is normal  $b \cdot a$  is either  $b$ ,  $a \cdot b$ , or  $a^2 \cdot b$ .

The rest of the group can be determined by finding  $b \cdot a$ , which again by the quotient group is not in  $H$ . If  $b \cdot a = b$ , then clearly we have the contradiction  $a = e$ . If  $b \cdot a = a \cdot b$ , then we find that  $a \cdot b$  has order 6. Only the final possibility  $b \cdot a = a^2 \cdot b$  gives a non-cyclic group. Since we know of a non-cyclic group of order 6, namely  $S_3$ , this must be it. Hence, there are two non-isomorphic groups of order 6,  $Z_6$  and  $S_3$ .

A similar exhaustive search can be used to find all groups of order 8. If such a group has all non-identity elements of order 2, then by Lemma 5.1 there is a subgroup  $\{e, a, b, a \cdot b\}$ . By Problem 22 of §2.3, the group is commutative, so if we pick  $c$  to be any other element, then  $c^2 = e$ ,  $c \cdot a = a \cdot c$ , and  $c \cdot b = b \cdot c$ .

```

InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e)
Define(b^2, e)
Define(c^2, e)
Define(b*a, a*b)
Define(c*a, a*c)
Define(c*b, b*c)
G = Group(); G
{e, a, b, a*b, c, a*c, b*c, a*b*c}

```

So there is only one group of order 8 for which all non-identity elements are of order 2. But we can find such a group— $Z_{24}^*$ , whose table is given in Table 5.1.

If  $|G| = 8$  and  $G$  is not isomorphic to either  $Z_8$  or  $Z_{24}^*$ , then there must be an element  $a$  of order 4. Then  $H = \{e, a, a^2, a^3\}$  is a normal subgroup, and we can let  $b$  be any element not in  $H$ . Since  $G/H$  has order 2,  $b^2$  must be in  $H$ , but if either  $b^2 = a$  or  $b^2 = a^3$ , then  $b$  will have order 8. Also,  $b \cdot a \notin H$ ,

but  $b \cdot a \neq b$ , since this would force  $a = e$ . So  $b^2$  is either  $e$  or  $a^2$ , and  $b \cdot a$  is either  $a \cdot b$ ,  $a^2 \cdot b$ , or  $a^3 \cdot b$ . These six possibilities can be tried out in *SageMath*.

If  $b \cdot a = a \cdot b$ , and  $b^2$  is either  $e$  or  $a^2$ , the group become isomorphic to  $Z_{15}^*$ , which we have seen before. Also, both combinations for which  $b \cdot a = a^2 \cdot b$  fail to produce a group. If  $b \cdot a = a^3 \cdot b$  and  $b^2 = e$ , we get the group

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^4, e)
Define(b^2, e)
Define(b*a, a^3*b)
G = Group(); G
{e, a, a^2, a^3, b, a*b, a^2*b, a^3*b}
```

This gives rise to the group  $D_4$ , the symmetry group of the square studied in Problem 1 of §2.1. The Cayley table shown in Table 5.2.

**TABLE 5.2:** Multiplication table for  $D_4$

.	$e$	$a$	$a^2$	$a^3$	$b$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$
$e$	$e$	$a$	$a^2$	$a^3$	$b$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$
$a$	$a$	$a^2$	$a^3$	$e$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$	$b$
$a^2$	$a^2$	$a^3$	$e$	$a$	$a^2 \cdot b$	$a^3 \cdot b$	$b$	$a \cdot b$
$a^3$	$a^3$	$e$	$a$	$a^2$	$a^3 \cdot b$	$b$	$a \cdot b$	$a^2 \cdot b$
$b$	$b$	$a^3 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$e$	$a^3$	$a^2$	$a$
$a \cdot b$	$a \cdot b$	$b$	$a^3 \cdot b$	$a^2 \cdot b$	$a$	$e$	$a^3$	$a^2$
$a^2 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$b$	$a^3 \cdot b$	$a^2$	$a$	$e$	$a^3$
$a^3 \cdot b$	$a^3 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$b$	$a^3$	$a^2$	$a$	$e$

The final possibility is that  $b \cdot a = a^3 \cdot b$ , and  $b^2 = a^2$ . This produces a new group called the quaternion group  $Q$ , described by the following:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^4, e)
Define(b^2, a^2)
Define(b*a, a^3*b)
Q = Group(); Q
{e, a, a^2, a^3, b, a*b, a^2*b, a^3*b}
```

Although the group can be defined in terms of only two generators, it is more natural to use the notation that appears in Table 5.3. Note that  $i$ ,  $j$ , and  $k$  sometimes behave like the vector cross product:

$$i \cdot j = k, \quad j \cdot k = i, \quad k \cdot i = j,$$

and sometimes act like complex numbers:

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1.$$

**TABLE 5.3:** Multiplication table for  $Q$

.	1	$i$	$j$	$k$	-1	$-i$	$-j$	$-k$
1	1	$i$	$j$	$k$	-1	$-i$	$-j$	$-k$
$i$	$i$	-1	$k$	$-j$	$-i$	1	$-k$	$j$
$j$	$j$	$-k$	-1	$i$	$-j$	$k$	1	$-i$
$k$	$k$	$j$	$-i$	-1	$-k$	$-j$	$i$	1
-1	-1	$-i$	$-j$	$-k$	1	$i$	$j$	$k$
$-i$	$-i$	1	$-k$	$j$	$i$	-1	$k$	$-j$
$-j$	$-j$	$k$	1	$-i$	$j$	$-k$	-1	$i$
$-k$	$-k$	$-j$	$i$	1	$k$	$j$	$-i$	-1

In summary, we have the following groups up to order 8:

$n = 1$ : The one element must be the identity, so we have just the trivial group,  $\{e\}$ .

$n = 2$ : Since 2 is prime, the only non-isomorphic group is  $Z_2$ .

$n = 3$ : Since 3 is prime, the only non-isomorphic group is  $Z_3$ .

$n = 4$ : By Lemma 5.1, there are two non-isomorphic groups:  $Z_4$  and  $Z_8^*$ .

$n = 5$ : Since 5 is prime, the only non-isomorphic group is  $Z_5$ .

$n = 6$ : There are two non-isomorphic groups:  $Z_6$  and the non-abelian group  $S_3$ .

$n = 7$ : Since 7 is prime, the only non-isomorphic group is  $Z_7$ .

$n = 8$ : There are three abelian groups,  $Z_8$ ,  $Z_{15}^*$ , and  $Z_{24}^*$  and two non-abelian groups,  $D_4$  and  $Q$ .

Table 5.4 gives of the number of non-isomorphic groups of order  $n$ , when  $n$  is not prime.

The symmetry group of the square,  $D_4$ , can be generalized to produce the symmetry group of the  $n$ -gon, for  $n \geq 3$ , denoted by  $D_n$ . This will be a non-abelian group of order  $2n$ . We can let  $a$  denote the clockwise rotation by

**TABLE 5.4:** Groups of order  $n$ 

$n$	groups								
4	2	26	2	46	2	65	1	85	1
6	2	27	5	48	52	66	4	86	2
8	5	28	4	49	2	68	5	87	1
9	2	30	4	50	5	69	1	88	12
10	2	32	51	51	1	70	4	90	10
12	5	33	1	52	5	72	50	91	1
14	2	34	2	54	15	74	2	92	4
15	1	35	1	55	2	75	3	93	2
16	14	36	14	56	13	76	4	94	2
18	5	38	2	57	2	77	1	95	1
20	5	39	2	58	2	78	6	96	230
21	2	40	14	60	13	80	52	98	5
22	2	42	6	62	2	81	15	99	2
24	15	44	4	63	4	82	2	100	16
25	2	45	2	64	267	84	15	102	4

$360/n$  degrees, so that  $a^n = e$ . We can then let  $b$  denote a reflection about the vertical axis, so that  $b^2 = e$ . Using some geometry, we can see that  $b \cdot a \cdot b$  will be a counter-clockwise rotation by  $360/n$  degrees, so that  $b \cdot a \cdot b = a^{n-1}$ . Hence, we have that  $b \cdot a = a^{-1} \cdot b$ .

The commands

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^n, e)
Define(b^2, e)
Define(b*a, a^-1*b)
Dn = Group(a, b)
```

define the group  $D_n$ . The symbol  $n$  must be replaced with an integer before executing these commands. When  $n = 3$ , we get a non-abelian group of order 6, so  $D_3 \approx S_3$ . We have just introduced  $D_4$ , and when  $n = 5$ , we get a non-abelian group of order 10, given by the following commands.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^5, e)
Define(b^2, e)
Define(b*a, a^-1*b)
D5 = Group(a, b)
CayleyTable(D5)
```

The resulting table is shown in [Table 5.5](#).

**TABLE 5.5:** Multiplication table for  $D_5$ 

.	$e$	$a$	$a^2$	$a^3$	$a^4$	$b$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$	$a^4 \cdot b$
$e$	$e$	$a$	$a^2$	$a^3$	$a^4$	$b$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$	$a^4 \cdot b$
$a$	$a$	$a^2$	$a^3$	$a^4$	$e$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$	$a^4 \cdot b$	$b$
$a^2$	$a^2$	$a^3$	$a^4$	$e$	$a$	$a^2 \cdot b$	$a^3 \cdot b$	$a^4 \cdot b$	$b$	$a \cdot b$
$a^3$	$a^3$	$a^4$	$e$	$a$	$a^2$	$a^3 \cdot b$	$a^4 \cdot b$	$b$	$a \cdot b$	$a^2 \cdot b$
$a^4$	$a^4$	$e$	$a$	$a^2$	$a^3$	$a^4 \cdot b$	$b$	$a \cdot b$	$a^2 \cdot b$	$a^3 \cdot b$
$b$	$b$	$a^4 \cdot b$	$a^3 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$e$	$a^4$	$a^3$	$a^2$	$a$
$a \cdot b$	$a \cdot b$	$b$	$a^4 \cdot b$	$a^3 \cdot b$	$a^2 \cdot b$	$a$	$e$	$a^4$	$a^3$	$a^2$
$a^2 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$b$	$a^4 \cdot b$	$a^3 \cdot b$	$a^2$	$a$	$e$	$a^4$	$a^3$
$a^3 \cdot b$	$a^3 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$b$	$a^4 \cdot b$	$a^3$	$a^2$	$a$	$e$	$a^4$
$a^4 \cdot b$	$a^4 \cdot b$	$a^3 \cdot b$	$a^2 \cdot b$	$a \cdot b$	$b$	$a^4$	$a^3$	$a^2$	$a$	$e$

**Problems for §5.1**

- 1 Prove that if  $f$  is a surjective isomorphism from a group  $G$  to a group  $M$ , then  $f^{-1}$  is a surjective isomorphism from  $M$  to  $G$ .
- 2 If  $G_1$ ,  $G_2$ , and  $G_3$  are three groups, and  $f$  is an isomorphism from  $G_1$  to  $G_2$ , and  $\phi$  is an isomorphism from  $G_2$  to  $G_3$ , prove that  $\phi(f(x))$  is an isomorphism from  $G_1$  to  $G_3$ .
- 3 Find an isomorphism between  $D_3$  (Terry's group) and  $S_3$ .
- 4 Find an isomorphism between the group consisting of the four complex numbers

$$\{1, -1, i, -i\}$$

and the group  $Z_4$ .

For Problems 5 through 13: Find an isomorphism between the two groups, by making Cayley tables of the two groups with the same “color pattern.”

- |                               |                                   |                                   |
|-------------------------------|-----------------------------------|-----------------------------------|
| <b>5</b> $Z_6$ and $Z_7^*$    | <b>8</b> $Z_6$ and $Z_{18}^*$     | <b>11</b> $Z_{12}$ and $Z_{13}^*$ |
| <b>6</b> $Z_6$ and $Z_9^*$    | <b>9</b> $Z_{10}$ and $Z_{11}^*$  | <b>12</b> $Z_{12}$ and $Z_{26}^*$ |
| <b>7</b> $Z_6$ and $Z_{14}^*$ | <b>10</b> $Z_{10}$ and $Z_{22}^*$ | <b>13</b> $Z_8^*$ and $Z_{12}^*$  |

- 14** Let  $G$  be an arbitrary group. Prove or disprove that  $f(x) = x^{-1}$  is an isomorphism from  $G$  to  $G$ .
- 15** Prove that any infinite cyclic group is isomorphic to  $\mathbb{Z}$ .
- 16** Let  $\mathbb{R}$  be the group of real numbers under addition, and let  $G$  be the group of positive real numbers under multiplication. Prove that  $\mathbb{R} \approx G$ , with  $\phi(x) = e^x$ .

- 17** Let  $\phi$  be an isomorphism from a group  $G$  to a group  $M$ . Prove that  $a$  and  $\phi(a)$  have the same order.

### Interactive Problems

- 18** Prove that there are exactly two non-isomorphic groups of order 10,  $Z_{10}$  and  $D_5$ . Have *SageMath* produce the Cayley tables.

Hint: Follow the logic for  $n = 6$ .

- 19** Prove that there are exactly two non-isomorphic groups of order 14,  $Z_{14}$  and  $D_7$ . Have *SageMath* produce the Cayley tables.

Hint: Follow the logic for  $n = 6$ .

For Problems **20** through **22**: Each of the following groups is of order 8. Which of the known five groups ( $Z_8$ ,  $Z_{24}^*$ ,  $Z_{15}^*$ ,  $D_4$ , or  $Q$ ) is each of these isomorphic to? First have *SageMath* display a table of the new group, and then rearrange the elements of one of the five known groups so that the color patterns in the two tables are identical.

**20**  $Z_{16}^*$

**21**  $Z_{20}^*$

**22**  $Z_{30}^*$

## 5.2 Homomorphisms

It is easy to see the application of isomorphisms, since these functions show how two groups are essentially the same. But suppose we have a function between two groups for which  $f(x \cdot y) = f(x) \cdot f(y)$ , but this function may not be one-to-one or onto. Can we still glean some information about the groups from this function?

**DEFINITION 5.2** Let  $G$  and  $M$  be two groups, with  $(*)$  being the group operation of  $G$ , and  $(\cdot)$  being the group operation on  $M$ . A function

$$f : G \rightarrow M$$

mapping elements of  $G$  to elements of  $M$  is called a *homomorphism* if it satisfies

$$f(x * y) = f(x) \cdot f(y) \quad \text{for all } x, y \in G.$$

The group  $G$  is called the *domain* of the homomorphism, and the group  $M$  is called the *target* of the homomorphism. Note that a homomorphism need not be either one-to-one or onto.

Of course, all isomorphisms are also homomorphisms. But we can have many other homomorphisms, as the following examples show.

**Example 5.2**

Let  $G$  be any group, and let  $M$  be a group with identity  $e$ . If we let

$$f(x) = e \quad \text{for all } x \in G$$

then  $f$  will obviously be a homomorphism, since

$$f(x \cdot y) = e = e \cdot e = f(x) \cdot f(y).$$

This is called the *trivial homomorphism*. □

**Example 5.3**

Let  $\mathbb{R}^* = \mathbb{R} - \{0\}$  be the group of nonzero real numbers under multiplication, and let  $f(x) = x^2$ . This forms a homomorphism

$$f : \mathbb{R}^* \rightarrow \mathbb{R}^*,$$

so this gives an example of a homomorphism which maps a group onto itself. Note that this homomorphism is neither one-to-one nor onto since  $f(-2) = f(2) = 4$ , yet there is no real number such that  $f(x) = -1$ . □

**Example 5.4**

We can generalize Example 5.3 as follows: Let  $G$  be any commutative group, and let  $n$  be any integer. We can define  $f(x) = x^n$ . Then  $f(x)$  is a homomorphism from  $G$  to itself, since

$$f(x \cdot y) = (x \cdot y)^n = x^n \cdot y^n = f(x) \cdot f(y). \quad \square$$

We can prove a few properties that must be true of all homomorphisms.

**PROPOSITION 5.3**

Let  $f : G \rightarrow M$  be a homomorphism. Let  $e$  denote the identity of  $G$ . Then  $f(e)$  is the identity element of  $M$ .

PROOF: Since  $e \cdot e = e$  in the group  $G$ , we have

$$f(e) = f(e \cdot e) = f(e) \cdot f(e).$$

Multiplying both sides by  $[f(e)]^{-1}$  gives us that  $f(e)$  is the identity element of  $M$ . □

**PROPOSITION 5.4**

If  $f : G \rightarrow M$  is a homomorphism, then  $f(a^{-1}) = [f(a)]^{-1}$ .

PROOF: We merely need to show that  $f(a) \cdot f(a^{-1})$  is the identity element of  $M$ . If  $e$  represents the identity element of  $G$ , then

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e).$$

By Proposition 5.3 this is the identity element of  $M$ . So

$$f(a^{-1}) = [f(a)]^{-1}. \quad \square$$

### **Example 5.5**

Find a homomorphism from  $Z_{15}^*$  to  $Z_4$  such that  $f(2) = f(7) = 1$ .

SOLUTION: We know from Proposition 5.3 that the identity must map to the identity, so  $f(1) = 0$ . Also,  $f(4) = f(2)^2 = 1^2 = 2$ . (Recall the operation of  $Z_4$  is *addition mod 4*.) Likewise,  $f(8) = f(2)^3 = 3$ ,  $f(13) = f(7)^3 = 3$ ,  $f(14) = f(7) \cdot f(2) = 2$ , and  $f(11) = f(13) \cdot f(2) = 0$ .  $\square$

To define homomorphisms using *SageMath*, we must first define the two groups  $G$  and  $M$  simultaneously, using different sets of letters for the generators.

### **Computational Example 5.6**

Let us create a homomorphism from the octahedral group to the quaternion group.

We first load the octahedral group with the following commands:

```
InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^2, e)
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
Oct = Group(); Oct
{e, a, b, a*b, b^2, a*b^2, c, a*c, b*c, a*b*c, b^2*c,
 a*b^2*c, c^2, a*c^2, b*c^2, a*b*c^2, b^2*c^2, a*b^2*c^2,
 c^3, a*c^3, b*c^3, a*b*c^3, b^2*c^3, a*b^2*c^3}
```

Next let us define the quaternion group  $Q$  from the last section. The easiest way to load this group is with the command

```
Q = InitQuaternions(); Q
{1, i, j, k, -1, -i, -j, -k}
```

Let us define a homomorphism  $F$  from  $Q$  to  $\text{Oct}$ . First we tell *SageMath* that  $F$  will be a homomorphism.

```
F = Homomorph(Q, Oct)
```

We need only define the homomorphism on the *generators* of where the generators are sent, since *SageMath* would then be able to use the properties of the homomorphism to determine where the other elements map to. Thus, to define the mapping

$$\begin{aligned} 1 &\rightarrow e, \\ i &\rightarrow c^2, \\ -1 &\rightarrow e, \\ -i &\rightarrow c^2, \\ j &\rightarrow a \cdot b^2 \cdot c, \\ k &\rightarrow a \cdot b^2 \cdot c^3, \\ -j &\rightarrow a \cdot b^2 \cdot c, \\ -k &\rightarrow a \cdot b^2 \cdot c^3; \end{aligned}$$

we have only to define  $F(i)$  and  $F(j)$ . This is done with the **HomoDef** command.

```
HomoDef(F, i, c^2)
HomoDef(F, j, a*b^2*c)
```

*SageMath* can check whether this function can be expanded to form a homomorphism by the command

```
FinishHomo(F)
'Homomorphism defined'
```

This shows that the function  $F$  is indeed a homomorphism. The command

```
GraphHomo(F)
```

will draw a picture of this homomorphism as shown in [Figure 5.1](#). □

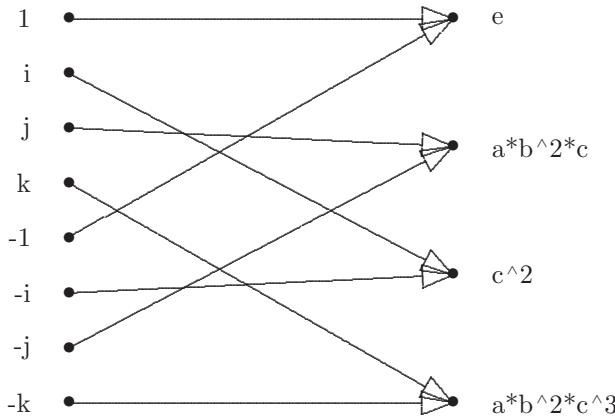
We can apply a homomorphism  $f$  to a *set* of elements by applying the homomorphism to each element in the set, and consider the set of all possible results. For example, consider the set of real numbers  $S = \{-2, -1, 1, 2, 3, 4\}$ . Let  $f(x)$  be the homomorphism in Example 5.3 above,  $f(x) = x^2$ . Then

$$f(S) = \{1, 4, 9, 16\}.$$

The set  $f(S)$  is smaller than the set  $S$ , since the homomorphism mapped two elements to both 1 and 4.

To apply the homomorphism to a set of elements in *SageMath*, we can use the **Image** command using a list for the second argument.

```
Image(F, [i, k, -i, -k])
{c^2, a*b^2*c^3}
Image(F, [1, i, -1, -i])
{e, c^2}
```



**FIGURE 5.1:** Diagram of the homomorphism  $F$

The last example, we see the image of a subgroup of  $Q$  being a subgroup of the octahedral group. It is not hard to prove that this will be the case in general.

**PROPOSITION 5.5**

If  $f : G \rightarrow M$  is a homomorphism and  $H$  is a subgroup of  $G$ , then  $f(H)$  is a subgroup of  $M$ .

**PROOF:** We want to show that  $f(H)$  is a subgroup using Proposition 3.2. If  $u$  and  $v$  are elements in  $f(H)$ , there must be elements  $x$  and  $y$  in  $H$  such that  $f(x) = u$ , and  $f(y) = v$ .

Then  $x \cdot y^{-1}$  is in  $H$ , and so

$$f(x \cdot y^{-1}) = f(x) \cdot f(y^{-1}) = f(x) \cdot [f(y)]^{-1} = u \cdot v^{-1}$$

is in  $f(H)$ . So by Proposition 3.2,  $f(H)$  is a subgroup of  $M$ . □

**DEFINITION 5.3** If

$$f : G \rightarrow M$$

is a homomorphism, then the group  $f(G)$  is called the *range*, or *image* of the homomorphism  $f$ . We denote this set by

$$\text{Im}(f).$$

Since the domain will be a group, by Proposition 5.5 the image will always be a subgroup of the target group.

We can also consider taking the inverse homomorphism  $f^{-1}$  of an element or a set of elements. Because homomorphisms are not always one-to-one,  $f^{-1}(x)$

may not represent a single element. Thus, we will define  $f^{-1}(x)$  to be the *set* of numbers such that  $f(y) = x$ . Likewise, we define

$$f^{-1}(S) = \{y \mid f(y) \in S\}.$$

We can use *SageMath*'s **HomoInv** command to take the inverse homomorphism of an element or set of elements.

**HomoInv(F, c^2)**  
 $\{-i, i\}$

finds  $F^{-1}(c^2)$ , whereas

**HomoInv(F, [a, b, a\*b^2\*c])**  
 $\{-j, j\}$

finds the inverse of a set of elements. Note that not all of the elements in the set have to be in the image of  $F$ . There is one inverse image that is very important.

**DEFINITION 5.4** If  $f$  is a homomorphism from  $G$  to  $M$  and  $e$  is the identity element of  $M$ , then we define the *kernel* of  $f$  to be the set

$$\text{Ker}(f) = f^{-1}(e).$$

That is,  $\text{Ker}(f)$  is the set of elements of  $G$  that map to the identity.

The command

**Kernel(F)**  
 $\{-1, 1\}$

can be used to find the kernel of a homomorphism.

### PROPOSITION 5.6

If  $f$  is a homomorphism from  $G$  to  $M$ , then the kernel of  $f$  is a normal subgroup of the domain  $G$ .

PROOF: First we need to show that the kernel of  $f$  is a subgroup of  $G$ . If  $e$  is the identity element of  $M$ , and if  $a$  and  $b$  are two elements of  $\text{Ker}(f)$ , then

$$f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = e \cdot e^{-1} = e,$$

so  $a \cdot b^{-1}$  is also in the kernel of  $f$ . Thus, by Proposition 3.2,  $\text{Ker}(f)$  is a subgroup.

Now let us show that  $\text{Ker}(f)$  is a normal subgroup of  $G$ . Let  $a$  be an element in  $\text{Ker}(f)$ , and  $g$  be any element in  $G$ . Then by Proposition 4.4, since

$$f(g \cdot a \cdot g^{-1}) = f(g) \cdot f(a) \cdot f(g^{-1}) = f(g) \cdot e \cdot [f(g)]^{-1} = e,$$

$g \cdot a \cdot g^{-1}$  is in  $\text{Ker}(f)$ , and so  $\text{Ker}(f)$  is a normal subgroup. □

Figure 5.1 is very suggestive. The inverse image of any element is a coset of  $\{-1, 1\}$ . The next proposition explains why this is so.

### PROPOSITION 5.7

Let  $f$  be a homomorphism from the group  $G$  to the group  $M$ . Suppose that  $y$  is in the image of  $f$ , and that  $f(x) = y$ . Then

$$f^{-1}(y) = x \cdot \text{Ker}(f).$$

PROOF: First let us consider an element  $z \in x \cdot \text{Ker}(f)$ . Then  $z = x \cdot k$  for some element  $k$  in the kernel of  $f$ . Therefore,

$$f(z) = f(x \cdot k) = f(x) \cdot f(k) = f(x) \cdot e = f(x)$$

since  $k$  is in  $\text{Ker}(f)$ . Here,  $e$  is the identity element of  $M$ . But  $f(x) = y$ , and so  $z \in f^{-1}(y)$ . Thus we have proved that

$$f^{-1}(y) \subseteq x \cdot \text{Ker}(f).$$

To prove the inclusion the other way, note that if  $z \in f^{-1}(y)$ , then  $f(z) = y$ , and so we have

$$f(x^{-1} \cdot z) = f(x)^{-1} \cdot f(z) = y^{-1} \cdot y = e$$

Thus,  $x^{-1} \cdot z$  is in the kernel of  $f$ , and since  $z = x \cdot (x^{-1} \cdot z) \in x \cdot \text{Ker}(f)$ , we have

$$x \cdot \text{Ker}(f) \subseteq f^{-1}(y). □$$

We now have a quick way to determine if a homomorphism is an isomorphism.

### COROLLARY 5.1

Let  $f : G \rightarrow M$  be a homomorphism. Then  $f$  is an injection (one-to-one) if, and only if, the kernel of  $f$  is the identity element of  $G$ .

PROOF: If  $f$  is an injection, clearly the kernel would just be the identity element. Suppose that the kernel is just the identity. Then Proposition 5.7 states that if  $h$  is in the image of  $f$ , then  $f^{-1}(h)$  consists of exactly one element. Therefore,  $f$  is one-to-one. □

In particular, if the image of a homomorphism  $f : G \rightarrow M$  is all of  $M$ , and the kernel is  $\{e\}$ , then  $G \approx M$ .

We can also consider what happens if we take the inverse image of a subgroup.

**COROLLARY 5.2**

Let  $f : G \rightarrow M$  be a homomorphism. Let  $H$  be a subgroup of  $M$ . Then  $f^{-1}(H)$  is a subgroup of  $G$ . Furthermore, if  $H$  is a normal subgroup of  $M$ , then  $f^{-1}(H)$  is a normal subgroup of  $G$ .

**PROOF:** Let  $x$  and  $y$  be in  $f^{-1}(H)$ . Then since  $f(x \cdot y^{-1}) = f(x) \cdot f(y)^{-1}$ , which is in  $H$ , we have that  $x \cdot y^{-1}$  is in  $f^{-1}(H)$ . Thus, by Proposition 3.2,  $f^{-1}(H)$  is a subgroup of  $G$ .

Now suppose that  $H$  is a normal subgroup of  $M$ . Then if  $y$  is in  $f^{-1}(H)$ , and  $g$  is in  $G$ , then  $f(g \cdot y \cdot g^{-1}) = f(g) \cdot f(y) \cdot f(g)^{-1}$ . Since  $f(y)$  is in  $H$ , which is normal in  $M$ , we have that  $f(g) \cdot f(y) \cdot f(g)^{-1}$  is in  $H$ . Thus,  $g \cdot y \cdot g^{-1}$  is in  $f^{-1}(H)$ , and so by Proposition 4.4,  $f^{-1}(H)$  is normal in  $G$ .  $\blacksquare$

We are now in a position to show how homomorphisms can be used to reveal relationships between different groups. There are three such relationships to be revealed, and these are covered in the next section.

### Problems for §5.2

- 1 If  $\phi$  is a homomorphism from a abelian group  $G$  to a group  $M$ , show that  $\text{Im}(\phi)$  is abelian.
- 2 If  $\phi$  is a homomorphism from a cyclic group  $G$  to a group  $M$ , show that  $\text{Im}(\phi)$  is a cyclic group.
- 3 Let  $\mathbb{Z}$  be the group of integers using addition. Show that the function  $\phi(x) = 2x$  is a homomorphism from  $\mathbb{Z}$  to itself. What is the image of this homomorphism? What is the kernel?
- 4 Let  $\mathbb{Z}$  be the group of integers using addition. Show that the function  $\phi(x) = -x$  is a homomorphism from  $\mathbb{Z}$  to itself. Show that this mapping is in fact one-to-one and onto.
- 5 Let  $\mathbb{Z}$  be the group of integers using addition. Show that the function  $\phi(x) = x + 3$  is *not* a homomorphism from  $\mathbb{Z}$  to itself.
- 6 Let  $\mathbb{R}^*$  denote the group of nonzero real numbers, using multiplication as the operation. Let  $\phi(x) = x^6$ . Show that  $\phi$  is a homomorphism from  $\mathbb{R}^*$  to  $\mathbb{R}^*$ . What is the kernel of this homomorphism? What is the image of the homomorphism?
- 7 Let  $\mathbb{R}^*$  denote the group of nonzero real numbers, using multiplication as the operation. Let  $\phi(x) = 2x$ . Show that  $\phi$  is *not* a homomorphism from  $\mathbb{R}^*$  to  $\mathbb{R}^*$ .
- 8 Let  $\mathbb{R}^*$  denote the group of nonzero real numbers, using multiplication as the operation. Recall that  $\mathbb{R}$  is the group of real numbers using addition

- for the operation. Let  $\phi(x) = \ln|x|$ . Show that  $\phi$  is a homomorphism from  $\mathbb{R}^*$  to  $\mathbb{R}$ . What is the kernel of this homomorphism?
- 9** Let  $\mathbb{R}^*$  denote the group of nonzero real numbers, using multiplication as the operation. Recall that  $\mathbb{R}$  is the group of real numbers using addition for the operation. Let  $\phi(x) = e^x$ . Show that  $\phi$  is a homomorphism from  $\mathbb{R}$  to  $\mathbb{R}^*$ . What is the image of this homomorphism?
- 10** Let  $\mathbb{R}[t]$  denote the group of all polynomials in  $t$  with real coefficients under addition, and let  $\phi$  denote the mapping  $\phi(f) = f'$ , which sends each polynomial to its derivative. Show that  $\phi$  is a homomorphism from  $\mathbb{R}[t]$  to  $\mathbb{R}[t]$ . What is the kernel of  $\phi$ ?
- 11** Let  $\mathbb{R}[t]$  denote the group of all polynomials in  $t$  with real coefficients under addition. Prove that the mapping from  $\mathbb{R}[t]$  into  $\mathbb{R}$  given by  $f(t) \rightarrow f(3)$  is a homomorphism. Give a description of the kernel of this homomorphism.
- 12** Find a homomorphism  $\phi$  from  $Z_{15}^*$  to  $Z_{15}^*$  with kernel  $\{1, 11\}$  and with  $\phi(2) = 7$ .
- 13** Find a homomorphism  $\phi$  from  $Z_{30}^*$  to  $Z_{30}^*$  with kernel  $\{1, 11\}$  and with  $\phi(7) = 13$ .
- 14** Find a homomorphism  $\phi$  from  $Z_{32}^*$  to  $Z_{32}^*$  with  $\phi(7) = 1$  and  $\phi(11) = 9$ .
- 15** Find a homomorphism from the quaternion group  $Q$  onto  $Z_8^*$ .  
Hint: The kernel must be a normal subgroup of order 2. See [Table 5.3](#) for a Cayley table of  $Q$ .
- 16** Let  $k$  be a divisor of  $n$ . Show that the mapping  $\phi(x) = x \bmod k$  is a homomorphism from  $Z_n^*$  to  $Z_k^*$ . Find a formula for the number of elements in the kernel.
- 17** Let  $f : G \rightarrow M$  be a homomorphism from a finite group  $G$  onto  $M$ , and  $H$  be a subgroup of  $M$ . Let  $f^{-1}(H)$  be the subgroup from Corollary 5.2. Show that the size of this subgroup is  $|H| \cdot |\text{Ker } f|$ .
- 18** Let  $f : G \rightarrow M$  be a homomorphism from  $G$  onto  $M$ , and let  $H$  be a normal subgroup of  $G$ . Prove that  $f(H)$  is a normal subgroup of  $M$ .

### Interactive Problems

- 19** Define Terry's group in *SageMath* with the command

```
Terry = InitTerry()
```

and then define the group  $S_3$ , using **Stay** as the identity element. (Otherwise, **InitGroup** would clear Terry's group.)

```
AddGroupVar("a", "b")
Define(a^2, Stay)
Define(b^3, Stay)
Define(b*a, a*b^2)
S3 = Group()
```

Now define an isomorphism  $F$  from  $S_3$  to Terry's group. Use *SageMath*'s **FinishHomo** to verify that your function is a homomorphism. Finally, find the kernel of  $F$  to prove that  $F$  is an isomorphism.

- 20** Use *SageMath* to find all of the homomorphisms from  $S_3$  to itself. Label these homomorphisms  $F1, F2, F3$ , etc. How many of these are isomorphisms? The following reloads  $S_3$  into *SageMath*:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^3, e)
Define(b*a, a*b^2)
S3 = Group()
```

### 5.3 The Three Isomorphism Theorems

We have seen in the last section that the kernel  $K$  of a homomorphism is always a normal subgroup of the domain  $G$ . Furthermore, Proposition 5.7 proves what is suggested by Figure 5.1, that the inverse image of any element is essentially a coset of  $K$ . Hence, the inverse image  $f^{-1}(y)$  can be considered as an element of the quotient group  $G/K$ . This leads us to the first of three very useful theorems for finding isomorphisms between groups.

#### **THEOREM 5.1: The First Isomorphism Theorem**

*Let  $f : G \rightarrow M$  be a homomorphism with  $\text{Ker}(f) = K$ , and  $\text{Im}(f) = I$ . Then there is a natural isomorphism*

$$\phi : I \rightarrow G/K$$

*which is onto. Thus,  $I \approx G/K$ .*

PROOF: Note that this theorem states more than just  $I \approx G/K$  but also that there is a *natural* isomorphism between these two groups. This isomorphism is given by

$$\phi(h) = f^{-1}(h).$$

Proposition 5.7 states that whenever  $h$  is in the image of  $f$ ,  $f^{-1}(h)$  is a member of the quotient group  $G/\text{Ker}(f)$ . Thus,  $\phi : I \rightarrow G/K$  is properly defined.

Let us show that the mapping  $\phi$  is one-to-one. Suppose  $\phi(x) = \phi(y)$  for two different elements of  $I$ . Then  $f(\phi(x)) = f(\phi(y))$ . But  $f(\phi(x)) = f(f^{-1}(x))$  is the set containing just the element  $x$ , and also  $f(\phi(y))$  is the set containing just the element  $y$ . Thus,  $x = y$ , and we have shown that  $\phi$  is one-to-one.

Now let us show that  $\phi$  is onto. If  $xK$  is an element of  $G/K$ , then  $f(x) \in I$ . Thus,

$$x \in f^{-1}(f(x)) = \phi(f(x)) \in G/K.$$

So we have that  $x$  is an element of both cosets  $xK$  and  $\phi(f(x))$ . Since two different cosets have no elements in common, we must have  $\phi(f(x)) = xK$ . We therefore have that any coset in  $G/K$  is mapped by  $\phi$  from an element in  $I$ , so  $\phi$  is onto.

Finally, we want to show that  $\phi$  is a homomorphism. That is, we wish to show that

$$f^{-1}(v) \cdot f^{-1}(w) = f^{-1}(v \cdot w).$$

Let  $x \in f^{-1}(v)$  and  $y \in f^{-1}(w)$ . Then  $f(x) = v$  and  $f(y) = w$ , so we have

$$f(x \cdot y) = f(x) \cdot f(y) = v \cdot w.$$

Hence,

$$x \cdot y \in f^{-1}(v \cdot w).$$

Since  $f^{-1}(v) \cdot f^{-1}(w)$  and  $f^{-1}(v \cdot w)$  are two cosets in  $G/K$ , and both contain the element  $x \cdot y$ , they must be the same coset. So we have that

$$\phi(v) \cdot \phi(w) = \phi(v \cdot w).$$

□

This theorem says that whenever we have a homomorphism  $f$  from  $G$  to  $M$  with an image  $I$ , then we get a natural isomorphism  $\phi$  from  $I$  to  $G/\text{Ker}(f)$ .

This suggests that there ought to be a mapping that goes directly from  $G$  to  $G/\text{Ker}(f)$  without involving the homomorphism  $f$ . The next proposition shows how this can be done.

### **PROPOSITION 5.8**

Let  $G$  be a group, and  $N$  be a normal subgroup of  $G$ . Then there is a natural homomorphism

$$i_N : G \rightarrow G/N$$

given by  $i_N(a) = a \cdot N$ . This homomorphism is surjective, and  $\text{Ker}(i_N) = N$ .

$$\begin{array}{ccc}
 G & \xrightarrow{f} & I \\
 i_N \searrow & & \nearrow \phi \\
 & G/\text{Ker}(f) &
 \end{array}$$

**FIGURE 5.2:** Commuting diagram for first isomorphism theorem

**PROOF:** To show that  $i_N$  is a homomorphism, we note that if  $a$  and  $b$  are elements of  $G$ , then

$$i_N(a \cdot b) = a \cdot b \cdot N = a \cdot N \cdot b \cdot N = i_N(a) \cdot i_N(b).$$

Also,  $i_N$  is clearly surjective. To find the kernel of  $i_N$ , we note that the identity element of  $G/N$  is  $eN = N$ , and so  $x$  is in the kernel if, and only if,

$$i_N(x) = N \iff x \cdot N = N \iff x \in N.$$

Therefore, the kernel of  $i_N$  is  $N$ . □

We call the homomorphism  $i_N$  the *canonical homomorphism associated with  $N$* . We can make a diagram of this homomorphism, along with the homomorphisms  $f$  and  $\phi$ , to produce [Figure 5.2](#).

Notice that we now have two ways of getting from  $G$  to  $G/\text{Ker}(f)$ , one route through the canonical homomorphism, and the other route through  $f$  and  $\phi$ . Yet we have drawn this diagram to indicate that  $\phi(f(x)) = i_N(x)$  for all elements in  $G$ . Thus, the two routes from  $G$  to  $G/\text{Ker}(f)$  produce the same function. We express this fact by saying that the *diagram is commutative*. In other words, for a commuting diagram, the functions defined by two paths with the same beginning and ending points produce the same composition function. In this diagram there are arrows going in both directions for the function  $\phi$  to indicate that this is a isomorphism, hence invertible. Hence, by the commuting diagram, we also have the result  $\phi^{-1}(i_N(x)) = f(x)$ . We will later be able to visualize many theorems about homomorphisms by means of commuting diagrams.

We observed in [§4.3](#) that the product of two subgroups  $H$  and  $K$  was not necessarily a subgroup. However, it is possible that if one of the groups is normal, then indeed the product  $H \cdot K$  would be a subgroup. (In fact, this was proven in Problem 15 of [§4.3](#).) Let us try it on the octahedral group.

### Motivational Example 5.7

Explore the product of two subgroups of order 4, one of which is normal, of the octahedral group.

```

InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^2, e)
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
G = Group()
M = Group(a*b^2*c, c^2)
    {e, a*b^2*c, c^2, a*b^2*c^3}
H = Group(c); H
    {e, c^2, c, c^3}
H * M
    {e, a*b^2, c, a*b^2*c, c^2, a*b^2*c^2, c^3, a*b^2*c^3}

```

*SageMath* can verify that these 8 elements form a subgroup. What happens if we try multiplying  $H$  and  $M$  in the other order?

```

M * H
    {e, a*b^2, c, a*b^2*c, c^2, a*b^2*c^2, c^3, a*b^2*c^3}

```

We discovered that not only is  $H \cdot M$  a subgroup, but also  $M \cdot H$  is exactly the same as  $H \cdot M$ .  $\square$

It is not hard to see the connection between these two facts.

### LEMMA 5.2

Suppose  $H$  and  $K$  are two subgroups of  $G$ . Then  $H \cdot K$  is a subgroup if, and only if,

$$H \cdot K = K \cdot H.$$

PROOF: First suppose that  $H \cdot K$  is a subgroup. Let  $h \in H$  and  $k \in K$ . We wish to show that the element  $h \cdot k$  in  $H \cdot K$  is also in  $K \cdot H$ . Since  $H \cdot K$  is a subgroup,  $(h \cdot k)^{-1}$  is in  $H \cdot K$ . Thus,  $(h \cdot k)^{-1} = x \cdot y$  for some  $x \in H$  and  $y \in K$ . But then,  $h \cdot k = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ , and  $y^{-1} \cdot x^{-1}$  is in  $K \cdot H$ . Thus,

$$H \cdot K \subseteq K \cdot H.$$

By a similar argument, the inverse of any element in  $K \cdot H$  must be in  $H \cdot K$ , and so  $K \cdot H \subseteq H \cdot K$ . Therefore, we have  $H \cdot K = K \cdot H$ .

Now, let us suppose that  $H \cdot K = K \cdot H$ . We want to show that  $H \cdot K$  is a subgroup. Let  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$  so both  $h_1 \cdot k_1$  and  $h_2 \cdot k_2$  are elements of  $H \cdot K$ . By Proposition 3.2, it is enough to show that  $(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1}$  is in  $H \cdot K$ . But  $(k_1 \cdot k_2^{-1}) \cdot h_2^{-1}$  is in  $K \cdot H = H \cdot K$ , and so there must be two elements  $h_3 \in H$  and  $k_3 \in K$  such that  $(k_1 \cdot k_2^{-1}) \cdot h_2^{-1} = h_3 \cdot k_3$ . Then we have

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} = h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1} = (h_1 \cdot h_3) \cdot k_3$$

which is in  $H \cdot K$ . Thus,  $H \cdot K$  is a subgroup if, and only if,  $H \cdot K = K \cdot H$ .  $\square$

We are now in a position to show that  $H \cdot K$  is a subgroup if one of the subgroups  $H$  or  $K$  is normal.

### LEMMA 5.3

If  $H$  is a subgroup of  $G$ , and  $N$  is a normal subgroup of  $G$ , then  $H \cdot N$  is a subgroup of  $G$ .

PROOF: If  $h \in H$  and  $n \in N$ , then  $h \cdot n \cdot h^{-1}$  is in  $N$ , since  $N$  is normal. Then

$$h \cdot n = (h \cdot n \cdot h^{-1}) \cdot h$$

is in  $N \cdot H$ . Thus,  $H \cdot N \subseteq N \cdot H$ .

By a similar argument  $N \cdot H \subseteq H \cdot N$ , so  $H \cdot N = N \cdot H$ . Therefore,  $H \cdot N$  is a subgroup by Lemma 5.2.  $\square$

Since we have found a new subgroup of  $G$  which contains the normal subgroup  $M$ , the natural question is whether it is a normal subgroup. We can try to find the left and right cosets of  $H \cdot M$  from the example.

#### **LftCoset (G, H \* M)**

$$\begin{aligned} & \{\{e, a*b^2, c, a*b^2*c, c^2, a*b^2*c^2, c^3, a*b^2*c^3\}, \\ & \{a, b^2, a*c, b^2*c, a*c^2, b^2*c^2, a*c^3, b^2*c^3\}, \\ & \{b, a*b, b*c, a*b*c, b*c^2, a*b*c^2, b*c^3, a*b*c^3\}\} \end{aligned}$$

#### **RtCoset (G, H \* M)**

$$\begin{aligned} & \{\{e, a*b^2, c, a*b^2*c, c^2, a*b^2*c^2, c^3, a*b^2*c^3\}, \\ & \{a, b, a*b*c, b^2*c, a*c^2, b*c^2, a*b*c^3, b^2*c^3\}, \\ & \{a*b, b^2, a*c, b*c, a*b*c^2, b^2*c^2, a*c^3, b*c^3\}\} \end{aligned}$$

We see that these are not the same, so in general,  $H \cdot N$  is not a normal subgroup if only  $N$  is normal. (Note that if both  $H$  and  $N$  were normal, then Problem 17 of §4.3 shows that  $H \cdot N$  is normal.)

But would  $M$  be a normal subgroup of  $H \cdot M$ ?

#### **LftCoset (H \* M, M)**

$$\{\{e, a*b^2*c, c^2, a*b^2*c^3\}, \{a*b^2, c, a*b^2*c^2, c^3\}\}$$

#### **RtCoset (H \* M, M)**

$$\{\{e, a*b^2*c, c^2, a*b^2*c^3\}, \{a*b^2, c, a*b^2*c^2, c^3\}\}$$

We can quickly see in this case it is normal, since  $M$  contains half of the elements of  $H \cdot M$ . But we can prove that this will happen in general, using the fact that  $H \cdot M$  is a subgroup of  $G$ .

### LEMMA 5.4

Let  $N$  be a normal subgroup of  $G$ , and suppose that  $H$  is a subgroup of  $G$  which contains  $N$ . Then  $N$  is a normal subgroup of  $H$ .

PROOF: Since  $N$  is a group and is contained in  $H$ ,  $N$  is a subgroup of  $H$ . For any  $x$  in  $H$ , we have that

$$x \cdot N \cdot x^{-1} = N$$

since  $x$  is also in  $G$ . Therefore, by Proposition 4.4,  $N$  is a normal subgroup of  $H$ .  $\square$

Given two subgroups of a group  $G$ , there is another way of forming a new subgroup. Proposition 3.3 tells us that the intersection of two subgroups will again be a subgroup. Recall that the *SageMath* command

```
R = Intersection(H, M); R
{e, c^2}
```

finds the intersection of two subgroups. If, as in Lemma 5.3, one of the two subgroups is normal, we have the following.

### **LEMMA 5.5**

If  $N$  is a normal subgroup of  $G$ , and  $H$  is a subgroup of  $G$ , then

$$H \cap N$$

is a normal subgroup of  $H$ .

PROOF: Given elements  $h \in H$  and  $x \in H \cap N$ , we note that since  $x$  is in  $N$  which is a normal subgroup of  $G$ ,  $h \cdot x \cdot h^{-1}$  is in  $N$ . Also,  $x$  is in  $H$ , so  $h \cdot x \cdot h^{-1}$  is in  $H$ . Thus,

$$h \cdot x \cdot h^{-1} \in H \cap N,$$

and so by Proposition 4.4, the intersection is a normal subgroup of  $H$ .  $\square$

We can ask whether there is a relationship between two quotient groups  $H/(H \cap N)$  and  $(H \cdot N)/N$ . We can calculate both quotient groups in *SageMath*.

```
LftCoset(H, R)
{{e, c^2}, {c, c^3}}
LftCoset(H * M, M)
{{e, a*b^2*c, c^2, a*b^2*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}
```

Notice that each coset in  $(H \cdot M)/M$  contains one of the cosets from  $H/R$ . In fact, if we threw out all elements in a coset of  $(H \cdot M)/M$  that were not an element of  $H$ , we would get a coset of  $H/R$ . This provides us the mechanism to prove the isomorphism.

### **THEOREM 5.2: The Second Isomorphism Theorem**

Suppose that  $N$  is a normal subgroup of  $G$ , and that  $H$  is a subgroup of  $G$ . Then

$$H/(H \cap N) \approx (H \cdot N)/N.$$

$$\begin{array}{ccc}
 H & \xrightarrow{i} & H \cdot N \\
 \downarrow \phi & & \downarrow f \\
 H/(H \cap N) & \longleftrightarrow & (H \cdot N)/N
 \end{array}$$

**FIGURE 5.3:** Commuting diagram for second isomorphism theorem

**PROOF:** By Lemma 5.3,  $H \cdot N$  is a subgroup, and by Lemma 5.4,  $N$  is a normal subgroup of  $H \cdot N$ . Also, by Lemma 5.5,  $H \cap N$  is a normal subgroup of  $H$ , and so both of the quotient groups are defined.

We will use the two homomorphisms

$$i : H \rightarrow H \cdot N$$

$$f : H \cdot N \rightarrow (H \cdot N)/N$$

where  $i$  is the identity mapping  $i(h) = h$ , and  $f$  is the canonical homomorphism.

We can now consider the combination of the two,

$$f(i(h)) : H \rightarrow (H \cdot N)/N.$$

Let us call the composition function  $\psi(h) = f(i(h))$ . We want to find the kernel of  $\psi$ , for then we can use the first isomorphism theorem (5.1). If we let  $e$  denote the identity element of  $(H \cdot N)/N$ , then

$$\begin{aligned}
 h \in \text{Ker}(\psi) &\iff f(i(h)) = e \\
 &\iff i(h) \in \text{Ker}(f) = N \\
 &\iff h \in N \quad \text{and} \quad h \in H \\
 &\iff h \in H \cap N.
 \end{aligned}$$

So by the first isomorphism theorem (5.1), we have

$$(H \cdot N)/N \approx H/(H \cap N).$$

□

We can describe the second isomorphism theorem (5.2) pictorially through the diagram in [Figure 5.3](#), which is commutative according to the first isomorphism theorem (5.1): Note that this diagram demonstrates that

$$|H|/|H \cap N| = |H \cdot N|/|N|.$$

In fact, we can show that  $|H|/|H \cap N| = |H \cdot N|/|N|$  even when neither of the groups  $H$  nor  $N$  is a normal subgroup.

### **PROPOSITION 5.9**

*Let  $H$  and  $K$  be two subgroups of a finite group  $G$ . Then the number of elements in the product  $H \cdot K$  is given by*

$$|H \cdot K| = \frac{|H| |K|}{|H \cap K|}.$$

**PROOF:** Even though  $H \cdot K$  is not a group, it still makes sense to consider the set of left cosets  $(H \cdot K)/K$ . A typical left coset belonging to  $(H \cdot K)/K$  would be  $h \cdot k \cdot K$ , where  $h$  is an element of  $H$ , and  $k$  is an element of  $K$ . By Lemma 4.1, all cosets contain  $|K|$  elements, and by Lemma 4.2 two cosets would intersect if, and only if, they are equal. Thus the elements of  $H \cdot K$  are distributed into non-overlapping cosets, each having  $|K|$  elements. Thus, the number of cosets in  $(H \cdot K)/K$  is

$$|(H \cdot K)/K| = \frac{|H \cdot K|}{|K|}.$$

Likewise, we have

$$|H/(H \cap K)| = \frac{|H|}{|H \cap K|}.$$

Thus, if we can show that  $|H/(H \cap K)| = |(H \cdot K)/K|$ , we will have proven the proposition. Let us define a mapping (not a homomorphism) that will relate the elements of these two sets. Let

$$\phi : (H \cdot K)/K \rightarrow H/(H \cap K)$$

be defined by

$$\phi(h \cdot K) = h \cdot (H \cap K).$$

To see that this is well defined, note that if  $h_1 \cdot K = h_2 \cdot K$  for two elements  $h_1$  and  $h_2$  in  $H$ , then  $h_2^{-1} \cdot h_1 \cdot K = K$ , so  $h_2^{-1} \cdot h_1$  must be in  $K$ . But  $h_2^{-1} \cdot h_1$  is also in  $H$ , hence in the intersection. Thus,

$$h_2 \cdot (H \cap K) = h_2 \cdot (h_2^{-1} \cdot h_1) \cdot (H \cap K) = h_1 \cdot (H \cap K).$$

So we see that if  $h_1 \cdot K = h_2 \cdot K$ , then  $\phi(h_1 \cdot K) = \phi(h_2 \cdot K)$ , and the function  $\phi$  is well defined.

On the other hand, if  $h_1 \cdot (H \cap K) = h_2 \cdot (H \cap K)$ , then  $h_2^{-1} \cdot h_1$  would have to be in the intersection of  $H$  and  $K$ . So then,  $h_1 \cdot K = h_2 \cdot K$ . Hence the mapping is one-to-one. It is clear that the mapping is also surjective, so  $\phi$  is a bijection, and the proposition is proved.  $\blacksquare$

If we consider a group with two normal subgroups, one of which is a subgroup of the other, we begin to see more patterns. Let us reload the octahedral group, and look at two normal subgroups.

```

InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^2, e)
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
G = Group()

```

### Motivational Example 5.8

The octahedral group has two non-trivial normal subgroups, one being the subgroup of the other. Explore the possible quotient groups.

The two normal subgroups this is referring to are

```

M = Group(a*b^2*c, c^2); M
    {e, a*b^2*c, c^2, a*b^2*c^3}
H = Group(b, c^2); H
    {e, b, b^2, a*c, a*b*c, a*b^2*c, c^2, b*c^2, b^2*c^2,
     a*c^3, a*b*c^3, a*b^2*c^3}

```

The first normal subgroup we have seen before. The latter subgroup  $H$  has 12 elements, so by Proposition 4.5,  $H$  is a normal subgroup.

Since both  $H$  and  $M$  are normal subgroups, we can consider two different quotient groups.

```

Q1 = RtCoset(G, H); Q1
    {{e, b, b^2, a*c, a*b*c, a*b^2*c, c^2, b*c^2, b^2*c^2,
     a*c^3, a*b*c^3, a*b^2*c^3}, {a, a*b, a*b^2, c, b*c,
     b^2*c, a*c^2, a*b*c^2, a*b^2*c^2, c^3, b*c^3, b^2*c^3}}
Q2 = RtCoset(G, M); Q2
    {{e, a*b^2*c, c^2, a*b^2*c^3}, {a, b^2*c, a*c^2, b^2*c^3},
     {b, a*b*c, b*c^2, a*b*c^3}, {a*b, b*c, a*b*c^2, b*c^3},
     {b^2, a*c, b^2*c^2, a*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}

```

At this point there doesn't seem to be much connection between these. But notice that  $M$  is also a subgroup of  $H$ . By Lemma 5.4,  $M$  will be a normal subgroup of  $H$ . This gives us a third quotient group to consider:

```

Q3 = RtCoset(H, M); Q3
    {{e, a*b^2*c, c^2, a*b^2*c^3}, {b, a*b*c, b*c^2, a*b*c^3},
     {b^2, a*c, b^2*c^2, a*c^3}}

```

Note that  $H/M$  will be a subgroup of  $G/M$ . Could this be a normal subgroup? In the case we are looking at,  $\mathbf{Q3} = H/M$  contains half of the elements of  $\mathbf{Q2} = G/M$ , so it is normal, giving us a *fourth* quotient group:

```

Q4 = LftCoset(Q2, Q3); Q4
    {{e, a*b^2*c, c^2, a*b^2*c^3}, {b, a*b*c, b*c^2, a*b*c^3},
     {b^2, a*c, b^2*c^2, a*c^3}}, {{a, b^2*c, a*c^2, b^2*c^3},
     {a*b, b*c, a*b*c^2, b*c^3}, {a*b^2, c, a*b^2*c^2, c^3}}}

```

Before we try to interpret this mess, let us first see why  $H/N$  will be a normal subgroup of  $G/N$  in general.

### **LEMMA 5.6**

*If  $H$  and  $N$  are normal subgroups of  $G$ , and if  $N$  is a subgroup of  $H$ , then  $H/N$  is a normal subgroup of  $G/N$ .*

**PROOF:** From Lemma 5.4,  $N$  is a normal subgroup of  $H$ . A typical element of  $G/N$  is  $gN$ , where  $g$  is an element of  $G$ . A typical element of  $H/N$  is  $hN$ , where  $h$  is an element of  $H$ . Thus,  $H/N$  is contained in  $G/N$ , and so  $H/N$  is a subgroup of  $G/N$ .

To show that  $H/N$  is in fact a normal subgroup of  $G/N$ , we will use Proposition 4.4. That is, we will see if

$$(gN) \cdot (hN) \cdot (gN)^{-1}$$

will always be in  $H/N$ . But this simplifies to  $(g \cdot h \cdot g^{-1}) \cdot N$ , and  $g \cdot h \cdot g^{-1}$  is in  $H$  since  $H$  is a normal subgroup of  $G$ . Therefore,  $(g \cdot h \cdot g^{-1}) \cdot N$  is in  $H/N$ , and hence  $H/N$  is a normal subgroup of  $G/N$ .  $\blacksquare$

The “quotient group of quotient groups” **Q4** =  $(G/N)/(H/N)$  is a list containing two lists, each of which contains several lists of elements. If this is too many nested lists for you to handle, imagine what would happen if we removed the innermost brackets. This would simplify the output to just a list of two lists, each of which contains 12 elements. But by looking carefully, we can see that we would get *exactly Q1*. We can use the canonical homomorphisms as a tool to strip away these inside level brackets.

### **THEOREM 5.3: The Third Isomorphism Theorem**

*Let  $H$  and  $N$  be normal subgroups of  $G$ , and let  $N$  be a subgroup of  $H$ . Then*

$$(G/N)/(H/N) \approx G/H.$$

**PROOF:** We will use the example to guide us in finding a mapping from  $(G/N)/(H/N)$  to a set of elements in  $G$ . We have a canonical mapping from  $G$  to  $G/N$ , and another canonical mapping from  $G/N$  to  $(G/N)/(H/N)$ . Let us call these mappings  $\phi$  and  $f$ , respectively.

For an element  $x$  in  $G$ , the composition homomorphism  $f(\phi(x))$  gives the element of  $(G/N)/(H/N)$  which contains  $x$  somewhere inside of it. Let us call this composition homomorphism  $\psi$ . Since  $f$  and  $\phi$  are both surjective, the composition  $\psi(x) = f(\phi(x))$  is surjective. Thus, the inverse of this homomorphism,  $\psi^{-1}(y)$ , gives a list of elements of  $G$  that are somewhere inside of the element  $y$ . This inverse is the mapping that removes the interior brackets. We only need to check that this is in fact a coset of  $G/H$ . Let us determine the kernel of the composition homomorphism  $\psi(x)$ .

Note that if  $x$  is in  $G$ , and  $e$  is the identity element of  $(G/N)/(H/N)$ , then

$$\begin{aligned} x \in \text{Ker}(\psi) &\iff f(\phi(x)) = e \\ &\iff \phi(x) \in \text{Ker}(f) = H/N \\ &\iff x \in \phi^{-1}(H/N) = H. \end{aligned}$$

Therefore, the kernel of the composition  $\psi$  is  $H$ , and so from the first isomorphism theorem (5.1),

$$(G/N)/(H/N) \approx G/H.$$

□

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G/N \\ i_H \downarrow & & \downarrow f \\ G/H & \longleftrightarrow & (G/N)/(H/N) \end{array}$$

**FIGURE 5.4:** Commuting diagram for third isomorphism theorem

We can describe the third isomorphism theorem visually by the diagram in Figure 5.4. Since  $H$  is the kernel of the composition homomorphism

$$f(\phi) : G \rightarrow (G/N)/(H/N)$$

we have by the first isomorphism theorem that this diagram commutes.

The three isomorphism theorems work not only for groups, but many other objects as well, such as the rings we will study in Chapter 9. Because the same theorems apply to many different types of objects, an abstraction of these theorems can be made which would apply to any object for which there are natural mappings defined, called *morphisms*. This introduces a rich field called *category theory*. Although category theory is another level of abstraction beyond group theory, there are applications in physics and computer languages.

### Problems for §5.3

For Problems 1 through 8: Find, up to isomorphism, the possible homomorphic images of the following groups. That is, for all possible homomorphisms from  $G$  to  $G'$ , what possible images could the homomorphism have?

<b>1</b>	$Z_{10}$	<b>5</b>	$Q$
<b>2</b>	$Z_{12}$	<b>6</b>	$S_3$
<b>3</b>	$Z_{15}^*$	<b>7</b>	$Z_{24}^*$
<b>4</b>	$D_4$	<b>8</b>	The octahedral group (See Example 5.8.)

- 9** Prove that the homomorphic image of a cyclic group is cyclic.
- 10** Find all of the homomorphisms from  $Z_4$  to  $Z_8^*$ .
- 11** Find all of the homomorphisms from  $Z_8^*$  to  $S_3$ .
- 12** Prove that there can be no nontrivial homomorphisms from  $S_3$  to  $Z_3$ .  
Hint: What are the normal subgroups of  $S_3$ ?
- 13** Suppose that there is a homomorphism from a finite group  $G$  onto  $Z_6$ .  
Prove that there are normal subgroups of  $G$  with index 2 and 3.
- 14** Let  $X$ ,  $Y$ , and  $Z$  be three subgroups of a finite group  $G$ , with  $Y$  normal.  
Use Proposition 5.9 to find a formula for the number of elements in  
 $X \cdot Y \cdot Z$ .
- 15** Suppose that  $H$  and  $K$  are distinct subgroups of  $G$  of index 2. Prove that  
 $H \cap K$  is a normal subgroup of  $G$  of index 4 and that  $G/(H \cap K) \approx Z_8^*$ .  
Hint: Use the second isomorphism theorem.
- 16** Demonstrate the second isomorphism theorem using the subgroups  $H = \{1, 2, 4, 8\}$  and  $N = \{1, 4, 7, 13\}$  of  $Z_{15}^*$ .
- 17** Demonstrate the third isomorphism theorem using the subgroups  $\{e, a^2\}$  and  $\{e, a, a^2, a^3\}$  from  $D_4$ .
- 18** Demonstrate the third isomorphism theorem using the subgroups  $\{1, 4\}$  and  $\{1, 2, 4, 8\}$  from  $Z_{15}^*$ .
- 19** Prove or disprove: If  $H$  and  $N$  are two normal subgroups of  $G$ , with  $N$  a subgroup of  $H$ , then

$$(G/N)/(G/H) \approx H/N.$$

### Interactive Problems

- 20** Use *SageMath* to find a non-trivial homomorphism from the octahedral group to  $Q$ .  
(Hint: According to the first isomorphism theorem, what could the image be?)
- 21** Use *SageMath* to find a homomorphism from the octahedral group onto  $S_3$ .  
(Hint: Use the first isomorphism theorem to determine what the kernel must be.)

# Chapter 6

---

## Permutation Groups

Although we have defined a group abstractly, they were not always defined in this way. When Galois introduced the term *group*, he only referred to a subset of permutations that was closed under multiplication. Hence, he only was considering the subgroups of a special type of group, known as *permutation groups*. However, with these permutation groups, he was able to prove that most fifth-degree polynomials cannot be solved in terms of roots. Hence, permutation groups have historically been at the core of abstract algebra.

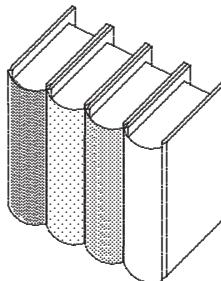
---

### 6.1 Symmetric Groups

This section will introduce the notation for an important class of groups, known as the *permutation groups* or the *symmetric groups*. Although at first they seem like very specialized groups, if fact we will see that every finite group is isomorphic to a subgroup of these symmetric groups. So by studying these groups, by proxy we are studying all finite groups.

We have already seen one example of a symmetric group,  $S_3$ . We can easily generalize this group, and consider the group of all permutations of  $n$  objects. For example, with four books the beginning position would be

**InitBooks (4)**



There are six *SageMath* operations that rearrange these books.

**MoveBooks (First)** swap the first two books.

- MoveBooks (Last)** swap the last two books.  
**MoveBooks (Left)** move the first book to the end,  
 sliding the other books to the left.  
**MoveBooks (Right)** move the last book to the beginning,  
 sliding the other books to the right.  
**MoveBooks (Rev)** reverse the order of the books.  
**MoveBooks (Stay)** leave the books as they are.

For three books, any permutation can be obtained by just one of these six commands. But with four books it is a bit tricky to arrange the books in a particular order. With even more books, it becomes very cumbersome. Let us introduce a notation for a permutation of books that explicitly states where each book ends up.

One natural way to do this is to number the books in consecutive order, and determine the numbers in the final position. For example, if we put the books in their original order, and then shift the books to the left with **MoveBooks (Left)**, we find that if the books started in 1, 2, 3, 4 order, the final position will be 2, 3, 4, 1. We write the ending position below the starting position, as follows.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

We can multiply the permutations using the new notation. For example, to calculate **Left**·**Last**, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

On the other hand, **Last**·**Left** is given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Obviously, **Left**·**Last** does not equal **Last**·**Left**.

We can also interpret each permutation as a *function* whose domain is a subset of the integers. For example, the permutations  $f(x) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$  and  $\phi(x) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$  can be thought of as two functions for which

$$\begin{array}{ll} f(1) = 2 & \phi(1) = 2 \\ f(2) = 3 & \phi(2) = 3 \\ f(3) = 1 & \phi(3) = 4 \\ f(4) = 4 & \phi(4) = 1. \end{array}$$

Note that  $f(x)$  appears directly below  $x$  in the permutation  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ . The product of the permutations is the same as the composition of the two functions. Thus,  $f \cdot \phi$  would be

$$\begin{aligned} f(\phi(1)) &= f(2) = 3 \\ f(\phi(2)) &= f(3) = 1 \\ f(\phi(3)) &= f(4) = 4 \\ f(\phi(4)) &= f(1) = 2. \end{aligned}$$

Thus, the composition function  $f(\phi(x))$ , that is, of doing  $\phi$  first, and then  $f$ , is  $f \cdot \phi = f(\phi(x)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ .

There is something curious here. When we view permutations as ways to rearrange a set of objects, such as books, the permutations are multiplied from left to right, which is the natural order. But when we view permutations as functions, the permutations are multiplied from right to left, which is again the natural order for function composition.

**DEFINITION 6.1** *For the set  $\{1, 2, 3, \dots, n\}$ , we define the group of permutations on the set by  $S_n$ . That is,  $S_n$  is the set of functions which are one-to-one and onto on the set  $\{1, 2, 3, \dots, n\}$ . The group operation is function composition.*

To enter a permutation into *SageMath*, only the bottom line is needed. A permutation in  $S_n$  can be entered as

$$P(x_1, x_2, x_3, \dots, x_n),$$

where  $x_1, x_2, x_3, \dots, x_n$  are distinct integers ranging from 1 to  $n$ . This permutation corresponds to the function

$$\begin{aligned} f(1) &= x_1 \\ f(2) &= x_2 \\ f(3) &= x_3 \\ &\dots \\ f(n) &= x_n. \end{aligned}$$

Thus the product

$$\begin{aligned} \mathbf{P}(5, 4, 1, 2, 3) * \mathbf{P}(4, 3, 5, 1, 2) \\ \mathbf{P}(2, 1, 3, 5, 4) \end{aligned}$$

yields  $P(2, 1, 3, 5, 4)$ . On the other hand, multiplying these permutations in the other order

```
P(4, 3, 5, 1, 2) * P(5, 4, 1, 2, 3)
P(2, 1, 4, 3)
```

yields a different result.

Since the composition function maps 5 to itself, *SageMath* drops the 5, treating this as a permutation on four objects instead. Since all permutations in  $S_4$  can be expressed in terms of some combinations of the **Left** and **Last** book rearrangements, we can find all of the elements of  $S_4$ .

```
S4 = Group(P(2, 3, 4, 1), P(1, 2, 4, 3)); S4
{P(), P(2, 1), P(1, 3, 2), P(3, 1, 2), P(2, 3, 1), P(3, 2, 1),
 P(1, 2, 4, 3), P(2, 1, 4, 3), P(1, 4, 2, 3), P(4, 1, 2, 3),
 P(2, 4, 1, 3), P(4, 2, 1, 3), P(1, 3, 4, 2), P(3, 1, 4, 2),
 P(1, 4, 3, 2), P(4, 1, 3, 2), P(3, 4, 1, 2), P(4, 3, 1, 2),
 P(2, 3, 4, 1), P(3, 2, 4, 1), P(2, 4, 3, 1), P(4, 2, 3, 1),
 P(3, 4, 2, 1), P(4, 3, 2, 1)}
```

```
len(S4)
24
```

Note that the identity element of  $S_4$  is denoted by **P()**, since the corresponding function leaves all objects fixed. We can determine the size of the group  $S_n$  in general, by counting the number of one-to-one and onto functions from the set  $\{1, 2, 3, \dots, n\}$  to itself. We have  $n$  choices for  $f(1)$ , but then there will be only  $n - 1$  choices for  $f(2)$ ,  $n - 2$  choices for  $f(3)$ , and so on. Thus, the size of the group  $S_n$  is given by

$$n \cdot (n - 1) \cdot (n - 2) \cdot (n - 3) \cdots 2 \cdot 1.$$

This product is denoted by  $n!$ , read as “ $n$  factorial.” [Table 6.1](#) gives a short table for  $n!$ .

**TABLE 6.1:**  $n!$  for  $n \leq 10$

1! = 1	6! = 720
2! = 2	7! = 5040
3! = 6	8! = 40320
4! = 24	9! = 362880
5! = 120	10! = 3628800

Both  $S_4$  and the octahedral group have 24 elements, so we could ask if these two groups are isomorphic. The octahedral group can be reloaded by the commands

```
InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^3, e); Define(c^2, e)
```

```
Define(b*a, a*b^2); Define(c*a, a*b*c); Define(c*b, a*c^2)
Oct = Group(a, b, c); Oct
{e, a, b, a*b, b^2, a*b^2, c, a*c, b*c, a*b*c, b^2*c,
 a*b^2*c, c^2, a*c^2, b*c^2, a*b*c^2, b^2*c^2, a*b^2*c^2,
 c^3, a*c^3, b*c^3, a*b*c^3, b^2*c^3, a*b^2*c^3}
```

Let us begin by defining a homomorphism from the subgroup generated by  $a$  and  $b$  to  $S_3$ , since we know that this is an isomorphism.

```
F = Homomorph(Oct, S4)
HomoDef(F, a, P(2,1) )
HomoDef(F, b, P(2,3,1) )
FinishHomo(F)
'Homomorphism consistent, but not defined for the whole
domain.'
```

This shows that so far, the homomorphism is consistent. To finish this homomorphism we only need to define  $F(c)$ . Since  $c$  must map to an element of order 4, there are six possibilities. (See Problem 10.) A little trial and error finds the right combination.

```
HomoDef(F, c, P(2,3,4,1) )
FinishHomo(F)
'Homomorphism defined.'
```

Next we want to see that  $F$  is an isomorphism by showing that the kernel of  $F$  is just the identity.

```
Kernel(F)
{e}
```

Then by the pigeonhole principle, the image of  $F$  must be all of  $S_4$ , so  $G \approx S_4$ .

*SageMath* can use the circle graphs on the set  $\{1, 2, \dots, n\}$  to visualize permutations. For example,

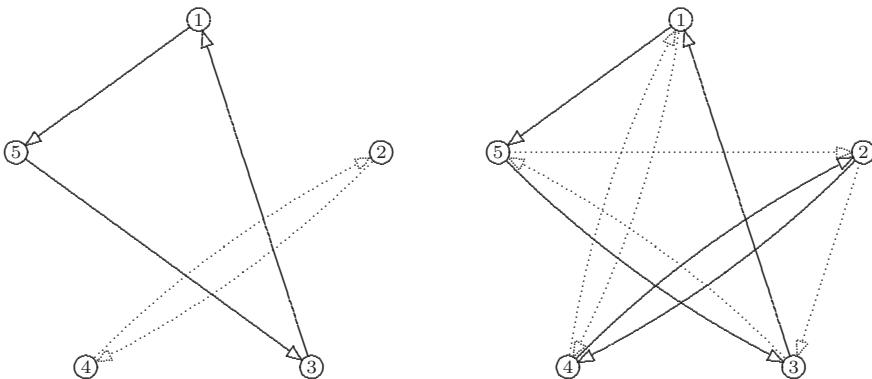
```
CircleGraph([1, 2, 3, 4, 5], P(5, 4, 1, 2, 3))
```

produces the circle graph on the left side of [Figure 6.1](#). The solid arrows form a triangle that connects 1, 5, and 3, while the dotted “double arrow” connects 2 and 4. So this circle graph reveals some additional structure to the permutation that we will study later.

We can graph two or more permutations simultaneously. The command

```
CircleGraph([1,2,3,4,5], P(5,4,1,2,3), P(4,3,5,1,2))
```

produces the circle graph on the right of [Figure 6.1](#). Here, the solid arrows represent the permutation  $P(5, 4, 1, 2, 3)$ , while the dotted arrows represent  $P(4, 3, 5, 1, 2)$ . If one imagines a permutation formed by traveling first through a dotted arrow, and then through a solid arrow, one obtains the permutation



**FIGURE 6.1:** Circle graphs of permutations

$P(2, 1, 3, 5, 4)$ , which is  $P(5, 4, 1, 2, 3) \cdot P(4, 3, 5, 1, 2)$ . Note that the arrows are like functions, in that we apply the arrow of the second permutation first, and then the arrow for the first permutation.

The inverse of a permutation can be found using *SageMath*.

```
P(5, 4, 1, 2, 3)^-1
P(3, 4, 5, 2, 1)
```

The circle graph of the inverse permutation is similar to the circle graph of  $P(5, 4, 1, 2, 3)$  except that all arrows are going in the opposite direction. The product of a permutation and its inverse of course will yield the identity element, denoted by  $P()$  in *SageMath*.

```
P(5, 4, 1, 2, 3) * P(3, 4, 5, 2, 1)
P()
```

*SageMath* can also treat a permutation as a function,

```
P(5, 4, 1, 2, 3)(2)
4
```

showing that  $f(2) = 4$ . In spite of the simplicity of the notations for a permutation, we will find that there is yet another notation that is even more concise. We will study this in the next section.

### Problems for §6.1

For Problems 1 through 8: Compute the following permutation products

**1**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$

**2**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$

**3**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 3 & 4 & 1 \end{pmatrix}.$

**4**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 2 & 5 \end{pmatrix}.$

**5**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 7 & 1 & 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 7 & 2 & 1 & 4 & 5 \end{pmatrix}.$

**6**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 2 & 3 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 7 & 4 & 1 & 5 \end{pmatrix}.$

**7**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 8 & 2 & 4 & 7 & 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 5 & 3 & 8 & 1 & 4 & 6 \end{pmatrix}.$

**8**  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 1 & 8 & 2 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}.$

- 9** Form a Cayley table of  $S_3$  using the permutation notation for the elements. That is, use the elements

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

- 10** Find the six elements of  $S_4$  that are of order 4.

Hint: All four of the numbers must move.

- 11** Find the eight elements of  $S_4$  that are of order 3.

Hint: One number must map to itself.

- 12** Find the nine elements of  $S_4$  that are of order 2.

- 13** Find a nontrivial element of  $S_5$  that commutes with the permutation

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}.$$

- 14** Find a permutation  $x$  in  $S_4$  that solves the equation

$$x \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \cdot x.$$

(There are in fact three different answers.)

- 15** Find a permutation  $x$  in  $S_5$  that solves the equation

$$x \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \cdot x.$$

(There are in fact four different answers.)

- 16** *SageMath* views the permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

as being the same permutation,  $P(2, 1, 4, 3)$ . But are these really the same? If not, why can *SageMath* use the same notation for these two elements?

#### Interactive Problems

For Problems **17** through **20**: Determine how the following permutations can be expressed in terms of the book rearrangements **First**, **Last**, **Left**, **Right**, and **Rev**.

**17**  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

**19**  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

**18**  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$

**20**  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

## 6.2 Cycles

Although we have a notation for the elements of  $S_n$ , it is not the most convenient. We would like a way to express the permutations in a way that is easy to use, and more concise. The key to the new notation is to study the cycle structure of a permutation.

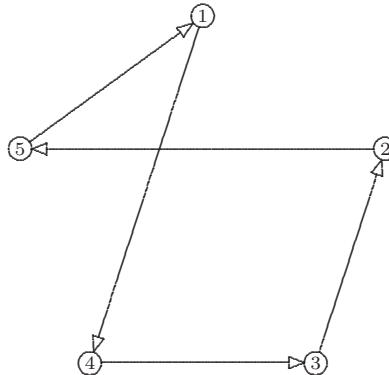
In the circle graph for the permutation  $P(5, 4, 1, 2, 3)$ , we saw that the arrows connecting 1, 5, and 3 were of one color, while a different colored arrow connected 2 and 4. By experimenting, we find that other permutations such as  $P(4, 5, 2, 3, 1)$  have circle graphs with arrows of only one color, as in [Figure 6.2](#).

These arrows indicate that the permutation can be expressed by a single chain

$$1 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 5 \rightarrow 1.$$

Other permutations, such as  $P(2, 4, 1, 6, 5, 3)$ , have every *straight* arrow of the same color, even though there is one point (5) that maps to itself. We can still express this permutation as a single chain

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 6 \rightarrow 3 \rightarrow 1,$$



**FIGURE 6.2:** Circle graph of a cycle

if we stipulate that all numbers that are not mentioned in the chain map to themselves.

**DEFINITION 6.2** Any permutation that can be expressed as a single chain is called a *cycle*. A cycle that moves exactly  $r$  of the numbers is called an  $r$ -*cycle*.

Let us introduce a concise notation for cycles. We can abbreviate a chain such as

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 6 \rightarrow 3 \rightarrow 1,$$

to simply

$$(1\ 2\ 4\ 6\ 3).$$

This is called the *cycle notation* for the permutation. Each number in the cycle is mapped to the next number. The last number in the cycle is mapped to the first number. In general, the  $r$ -cycle

$$(i_1\ i_2\ i_3\ \dots\ i_r)$$

represents the permutation that maps  $i_1$  to  $i_2$ ,  $i_2$  to  $i_3$ , etc., and finally  $i_r$  back to  $i_1$ . Notice that

$$(i_1\ i_2\ i_3\ \dots\ i_r)^{-1} = (i_r\ i_{r-1}\ \dots\ i_3\ i_2\ i_1),$$

so the inverse of an  $r$ -cycle will always be an  $r$ -cycle. The identity element can be written as the 0-cycle () .

A 1-cycle is actually impossible, since if one number is not fixed by a permutation, then the number that it maps to cannot be fixed. Thus, a non-identity permutation must move at least two numbers. We say that an  $r$ -cycle is a *nontrivial cycle* if  $r > 1$ .

Most permutations cannot be written as a single chain. This is evident from looking at the circle graph for the permutation  $P(5, 4, 1, 2, 3)$ . However, the two different types of arrows suggest that this permutation could be expressed as *two cycles*, one that represents the triangle from 1 to 5 to 3, and back to 1, and the other that exchanges 2 and 4. These two permutations are  $P(5, 2, 1, 4, 3)$  and  $P(1, 4, 3, 2, 5)$ . These two cycles multiply together to give  $P(5, 4, 1, 2, 3)$ . In fact, this product can be done in either order. If we write these two permutations in cycle notation,

$$P(5, 2, 1, 4, 3) = (1\ 5\ 3), \quad P(1, 4, 3, 2, 5) = (2\ 4),$$

we notice that there are no numbers in common between these two cycles.

**DEFINITION 6.3** Two cycles

$$(i_1\ i_2\ i_3\ \dots\ i_r) \quad \text{and} \quad (j_1\ j_2\ j_3\ \dots\ j_s)$$

are *disjoint* if  $i_m \neq j_n$  for all  $m$  and  $n$ . That is, there are no integers in common between the two cycles.

**LEMMA 6.1**

Let  $x$  be an element of  $S_n$  which is not the identity. Then  $x$  can be written as a product of nontrivial disjoint cycles. This representation of  $x$  is unique up to the rearrangement of the cycles.

**PROOF:** Let us say that  $x$  fixes the integer  $i$  if  $x(i) = i$ . We will use induction on the number of integers not fixed by  $x$ , denoted by  $m$ . Because  $x$  is not the identity, there is at least one integer not fixed by  $x$ . In fact,  $m$  must be at least 2, for the first integer must have somewhere to go.

If  $m = 2$ , then only two numbers  $i_1$  and  $i_2$  are moved. Since these are the only two integers not fixed,  $x$  must be a 2-cycle  $(i_1\ i_2)$ .

We now will assume by induction that the lemma is true whenever the number of integers not fixed by  $x$  is fewer than  $m$ . Let  $i_1$  be one integer that is not fixed, and let  $i_2 = x(i_1)$ . Then  $x(i_2)$  cannot be  $i_2$  for  $x$  is one-to-one, and if  $x(i_2)$  is not  $i_1$ , we define  $i_3 = x(i_2)$ . Likewise,  $x(i_3)$  cannot be either  $i_2$  or  $i_3$ , since  $x$  is one-to-one. If  $x(i_3)$  is not  $i_1$ , we define  $i_4 = x(i_3)$ .

Eventually this process must stop, for there are only  $m$  elements that are not fixed by  $x$ . Thus, there must be some value  $k$  such that  $x(i_k) = i_1$ . Define the permutation  $y$  to be the  $k$ -cycle  $(i_1\ i_2\ i_3\ \dots\ i_k)$ . Then  $x \cdot y^{-1}$  fixes all of the integers fixed by  $x$ , along with  $i_1, i_2, i_3, \dots, i_k$ . By induction, since there are fewer integers not fixed by  $x \cdot y^{-1}$  than by  $x$ ,  $x \cdot y^{-1}$  can be expressed by a series of nontrivial disjoint cycles  $c_1 \cdot c_2 \cdot c_3 \cdots c_t$ . Moreover, the integers appearing in  $c_1 \cdot c_2 \cdot c_3 \cdots c_t$  are just those that are not fixed by  $x \cdot y^{-1}$ . Thus,  $c_1 \cdot c_2 \cdot c_3 \cdots c_t$  are disjoint from  $y$ . Finally, we have

$$x = y \cdot c_1 \cdot c_2 \cdot c_3 \cdots c_t.$$

Therefore,  $x$  can be written as a product of disjoint nontrivial cycles. By induction, every permutation besides the identity can be written as a product of nontrivial disjoint cycles.

For the uniqueness, suppose that a permutation  $x$  has two ways of being written in terms of nontrivial disjoint cycles:

$$x = c_1 \cdot c_2 \cdot c_3 \cdots c_r = d_1 \cdot d_2 \cdot d_3 \cdots d_s.$$

For any integer  $i_1$  not fixed by  $x$ , one and only one cycle must contain  $i_1$ . Suppose that cycle is  $c_j = (i_1 i_2 i_3 \dots i_q)$ . But by the way we constructed the cycles above, this cycle must also be one of the  $d_k$ 's. Thus, each cycle  $c_j$  is equal to  $d_k$  for some  $k$ . By symmetry, each  $d_k$  is equal to  $c_j$  for some  $j$ . Thus, the two ways of writing  $x$  in terms of nontrivial disjoint cycles are merely rearrangements of the cycles.  $\square$

Lemma 6.1 gives us a succinct way to express permutations. *SageMath* uses the notation

**C(2, 3, 4, 5)**

to denote the cycle  $(2\ 3\ 4\ 5)$ . We can multiply two cycles together,

**C(2, 3, 4, 5) \* C(1, 2, 4)**

$(1, 3, 4)(2, 5)$

forming the answer as a product of two disjoint cycles, expressed using only parentheses. Note that when two cycles are disjoint, they are displayed without the times sign between them. We call this the *cycle decomposition* of the permutation. We can convert from the cycle notation to the permutation and vice versa in *SageMath* with the commands

**CycleToPerm( C(1, 3, 4) \* C(2, 5) )**

$P(3, 5, 4, 1, 2)$

**PermToCycle( P(4, 6, 1, 8, 2, 5, 7, 3) )**

$(1, 4, 8, 3)(2, 6, 5)$

We may even mix the two notations in *SageMath* within an expression, such as:

**C(1, 2, 3) \* P(3, 1, 2, 5, 4) \* C(4, 5)**

$()$

Whenever *SageMath* encounters a mixture like this, it puts the answer in terms of cycles. In this case the result is the identity permutation, so *SageMath* returns the 0-cycle  $()$ .

In *SageMath*, we can create a circle graph of a cycle, or product of cycles, just as we did for permutations. We can even treat a cycle as a function, as we did for permutations. For example,

$\mathbf{C(1, 4, 8, 3)(3)}$ 
 $1$ 

determines where the cycle  $(1\ 4\ 8\ 3)$  sends the number 3. However, to evaluate a product of cycles at a given number, an extra pair of parentheses is needed:

 $(\mathbf{C(1, 4, 8, 3)*C(2, 6, 5))}(2)$ 
 $6$ 

We mentioned that there are no permutations that move just one element, but the permutations which move exactly 2 elements will be important. We will give these 2-cycles a special name.

**DEFINITION 6.4** A *transposition* is a 2-cycle  $(i_1\ i_2)$ , where  $i_1 \neq i_2$ .

Observe that  $i_1$  can be any of the  $n$  numbers, and  $i_2$  can be any of the remaining  $n - 1$  numbers, but this counts each transposition twice, since  $(i_1\ i_2) = (i_2\ i_1)$ . Thus, there are

$$\frac{n(n-1)}{2} = \frac{n^2-n}{2}$$

transpositions of  $S_n$ .

**LEMMA 6.2**

For  $n > 1$ , the set of transpositions in  $S_n$  generates  $S_n$ .

**PROOF:** We need to show that every element of  $S_n$  can be written as a product of transpositions. The identity element can be written as  $(1\ 2)(1\ 2)$ , so we let  $x$  be a permutation that is not the identity. By Lemma 6.1, we can express  $x$  as a product of nontrivial disjoint cycles:

$$x = (i_1\ i_2\ i_3\ \dots\ i_r) \cdot (j_1\ j_2\ \dots\ j_s) \cdot (k_1\ k_2\ \dots\ k_t) \cdots.$$

Now, consider the product of transpositions

$$(i_1\ i_2) \cdot (i_2\ i_3) \cdots (i_{r-1}\ i_r) \cdot (j_1\ j_2) \cdot (j_2\ j_3) \cdots (j_{s-1}\ j_s) \cdot (k_1\ k_2) \cdots (k_{t-1}\ k_t) \cdots.$$

Note that this product is equal to  $x$ . Therefore, we have expressed every element of  $S_n$  as a product of transpositions.  $\square$

Of course, a particular permutation can be expressed as a product of transpositions in more than one way. But an important property of the symmetric groups is that the number of transpositions used to represent a given permutation will always have the same parity, that is, even or odd. To show this, we will first prove the following lemma.

**LEMMA 6.3**

The product of an odd number of transpositions in  $S_n$  cannot equal the identity element.

**PROOF:** Since  $S_2$  only contains one transposition,  $(1\ 2)$ , raising this to an odd power will not be the identity element, so the lemma is true for the case  $n = 2$ . So by induction we can assume that the lemma is true for  $S_{n-1}$ . Suppose that there is an odd number of transpositions producing the identity in  $S_n$ . Then we can find such a product that uses the fewest number of transpositions, say  $k$  transpositions, with  $k$  odd. At least one transposition will involve moving  $n$ , since the lemma is true for  $S_{n-1}$ . Suppose that the  $m^{\text{th}}$  transposition is the last one that moves  $n$ . If  $m = 1$ , then only the first transposition moves  $n$ , so the product will also move  $n$ , so cannot be the identity. We will now use induction on  $m$ . That is, we will assume that no product of  $k$  transpositions can be the identity for a smaller  $m$ . But then the  $(m - 1)^{\text{st}}$  and the  $m^{\text{th}}$  transpositions are one of the four possibilities

$$(n\ x)(n\ x), \quad (n\ x)(n\ y), \quad (x\ y)(n\ x), \quad \text{or} \quad (y\ z)(n\ x)$$

for some  $x$ ,  $y$ , and  $z$ . In the first case, the two transpositions cancel, so we can form a product using a fewer number of transpositions. In the other three cases, we can replace the pair with another pair,

$$(n\ x)(n\ y) = (n\ y)(x\ y); \quad (x\ y)(n\ x) = (n\ y)(x\ y); \quad (y\ z)(n\ x) = (n\ x)(y\ z);$$

for which  $m$  is smaller. Thus, there is no odd product of transpositions in  $S_n$  equaling the identity.  $\square$

We can use this lemma to prove the following theorem.

**THEOREM 6.1: The Signature Theorem**

For the symmetric group  $S_n$ , define the function

$$\sigma : S_n \rightarrow \mathbb{Z}$$

by

$$\sigma(x) = (-1)^{N(x)},$$

where  $N(x)$  is the minimum number of transpositions needed to express  $x$  as a product of transpositions. Then this function, called the signature function, is a homomorphism from  $S_n$  to the set of integers  $\{-1, 1\}$ .

**PROOF:** By Lemma 6.2, every element of  $S_n$  can be written as a product of transpositions, so  $\sigma(x)$  is well defined. Obviously this maps  $S_n$  to  $\{-1, 1\}$ , so we only need to establish that this is a homomorphism. Suppose that  $\sigma(x \cdot y) \neq \sigma(x) \cdot \sigma(y)$ . Then  $N(x \cdot y) - (N(x) + N(y))$  would be an odd number. Since  $N(x^{-1}) = N(x)$ , we would also have  $N(x \cdot y) + N(y^{-1}) + N(x^{-1})$

being an odd number. But then we would have three sets of transpositions, totaling an odd number, which when strung together produce  $x \cdot y \cdot y^{-1} \cdot x^{-1} = ()$ . This contradicts Lemma 6.3, so in fact  $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$  for all  $x$  and  $y$  in  $S_n$ .  $\square$

We can compute the signature function on both permutations and products of cycles, using the **Signature** command.

```
Signature( P(4,3,5,1,2) )
-1
Signature( C(1,4,2,7)*C(6,7,3) )
-1
```

The signature of an  $r$ -cycle will be  $-1$  if  $r$  is even, and  $+1$  if  $r$  is odd.

**DEFINITION 6.5** A permutation is an *alternating permutation* or an *even permutation* if the signature of the permutation is 1. A permutation is an *odd permutation* if it is not even, that is, if the signature is  $-1$ . The set of all alternating permutations of order  $n$  is written  $A_n$ .

### COROLLARY 6.1

The set of all alternating permutations  $A_n$  is a normal subgroup of  $S_n$ . If  $n > 1$ , then  $S_n/A_n$  is isomorphic to  $Z_2$ .

**PROOF:** Clearly,  $A_n$  is a normal subgroup of  $S_n$ , since  $A_n$  is the kernel of the signature homomorphism. Also if  $n > 1$ , then  $S_n$  contains at least one transposition whose signature would be  $-1$ . Thus, the image of the homomorphism is  $\{-1, 1\}$ . This group is isomorphic to  $Z_2$ . Then by the first isomorphism theorem (5.1),  $S_n/A_n$  is isomorphic to  $Z_2$ .  $\square$

### PROPOSITION 6.1

For  $n > 2$ , the alternating group  $A_n$  is generated by the set of 3-cycles.

**PROOF:** Since every 3-cycle is a product of two transpositions, every 3-cycle is in  $A_n$ . Thus, it is sufficient to show that every element in  $A_n$  can be expressed in terms of 3-cycles. We have already seen that any element can be expressed as a product of an even number of transpositions. Suppose we group these in pairs as follows:

$$x = [(i_1 j_1) \cdot (k_1 l_1)] \cdot [(i_2 j_2) \cdot (k_2 l_2)] \cdots \cdots [(i_n j_n) \cdot (k_n l_n)].$$

If we could convert each pair of transpositions into 3-cycles, we would have the permutation  $x$  expressed as a product of 3-cycles. There are three cases to consider:

Case 1:

The integers  $i_m, j_m, k_m, l_m$  are all distinct. In this case,

$$(i_m j_m) \cdot (k_m l_m) = (i_m k_m l_m) \cdot (i_m j_m l_m).$$

Case 2:

Three of the four integers  $i_m, j_m, k_m, l_m$  are distinct. The four combinations that would produce this situation are  $i_m = k_m$ ,  $i_m = l_m$ ,  $j_m = k_m$ , or  $j_m = l_m$ . However, these four possibilities are essentially the same, so we only have to check one of these four combinations:  $i_m = k_m$ . Then we have

$$(i_m j_m) \cdot (i_m l_m) = (i_m l_m j_m).$$

Case 3:

Only two of the four integers  $i_m, j_m, k_m$ , and  $l_m$  are distinct. Then we must either have  $i_m = k_m$  and  $j_m = l_m$ , or  $i_m = l_m$  and  $j_m = k_m$ . In either case, we have

$$(i_m j_m) \cdot (k_m l_m) = () = (1\ 2\ 3)(1\ 3\ 2).$$

In all three cases, we were able to express a pair of transpositions in terms of a product of one or two 3-cycles. Therefore, the permutation  $x$  can be written as a product of 3-cycles. □

Let us use this proposition to find the elements of  $A_4$ . We know that this is generated by 3-cycles, and has  $4!/2 = 12$  elements. Since

**Group( C(1,2,3), C(1,2,4) )**

$$\{(), (1, 3, 2), (1, 2, 3), (1, 2)(3, 4), (2, 4, 3), (1, 4, 3), (2, 3, 4), (1, 4, 2), (1, 3)(2, 4), (1, 3, 4), (1, 2, 4), (1, 4)(2, 3)\}$$

has 12 elements, this must be  $A_4$ . Eight of the twelve elements are 3-cycles. The other four elements form a subgroup that we have seen before.

## Problems for §6.2

For Problems 1 through 4: Find the product of the cycles without using *SageMath*.

<b>1</b> $(1\ 6\ 4) \cdot (2\ 5\ 3\ 4) \cdot (1\ 3\ 6\ 5)$	<b>3</b> $(1\ 7\ 3\ 2\ 8\ 6) \cdot (1\ 5\ 3\ 2\ 6\ 4) \cdot (2\ 7\ 3\ 5\ 8)$
<b>2</b> $(1\ 4\ 7) \cdot (2\ 3\ 5\ 4) \cdot (1\ 4\ 5\ 7\ 6)$	<b>4</b> $(1\ 4\ 3\ 5\ 9\ 7\ 8) \cdot (2\ 8\ 3\ 9\ 5\ 4) \cdot (4\ 7\ 6\ 8)$

**5** Simplify the product of the cycles

$$(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5) \cdots (n-1\ n\ n+1)(n\ n+1\ n+2)$$

for  $n > 1$ .

Hint: Try it with  $n = 2$ ,  $n = 3$ , and  $n = 4$  to see a pattern. Then prove using induction that the pattern persists.

**6** Find the order of the permutations

$$(1\ 2\ 5)(3\ 4) \quad \text{and} \quad (1\ 2\ 5)(3\ 4\ 6\ 7).$$

**7** Prove that the order of a permutation written in disjoint cycles is the least common multiple of the orders of the cycles.

**8** Find an element of  $A_8$  that has order 15.

Hint: See Problem 7.

**9** Find an element of  $A_7$  that has order 6.

Hint: See Problem 7.

**10** What is the smallest  $n$  such that  $A_n$  contains an element of order 12?

Hint: See Problem 7.

**11** Show that if  $H$  is a subgroup of  $S_n$ , then either every member of  $H$  is an even permutation or exactly half of them are even.

Hint: Consider the second isomorphism theorem (5.2).

**12** How many elements of order 5 are there in  $S_6$ ?

**13** Find an element  $g$  in  $S_5$  such that  $g^2 = (1\ 3\ 4\ 2\ 5)$ .

Hint: What order must  $g$  have? What power must we raise  $g^2$  to in order to reconstruct  $g$ ?

**14** A card-shuffling machine will always shuffle cards in the same way relative to the order in which they were given. All of the spades arranged in order from ace to king are put into the machine, and then the shuffled cards are re-entered into the machine again. If the cards after the second shuffle are in the order 10, 9, 4, Q, 6, J, 5, 3, K, 7, 8, 2, A, what order were the cards in after the first shuffle? See the hint for Problem 13.

**15** A subgroup  $H$  of the group  $S_n$  is called *transitive* on  $B = \{1, 2, \dots, n\}$  if for each pair  $i, j$  of elements of  $B$ , there exists an element  $f$  in  $H$  such that  $f(i) = j$ . Show that there exists a cyclic subgroup  $H$  of  $S_n$  that is transitive on  $B$ .

**16** Let  $\phi = (i_1\ i_2\ i_3\ \dots\ i_r)$  denote an  $r$ -cycle in  $S_n$ , and let  $x$  be any permutation in  $S_n$ . Show that  $x \cdot \phi \cdot x^{-1}$  is the  $r$ -cycle  $(x(i_1)\ x(i_2)\ x(i_3)\ \dots\ x(i_r))$ .

**17** Let  $\phi$  and  $f$  denote two disjoint cycles in  $S_n$ , and let  $x$  be any permutation in  $S_n$ . Show that  $x \cdot \phi \cdot x^{-1}$  and  $x \cdot f \cdot x^{-1}$  are disjoint cycles. (See Problem 16.)

- 18** Use *SageMath* to find a pair of 3-cycles whose product is a 3-cycle. Can there be a product of two 4-cycles that yields a 4-cycle?
- 19** The *cycle structure* of a permutation is the number of 2-cycles, 3-cycles, etc. it contains when written as a product of disjoint cycles. For example,  $(1\ 2\ 3)(4\ 5)$  and  $(3\ 4\ 5)(1\ 2)$  have the same cycle structure. Consider the elements

```
a = C(1, 2, 3); a
(1, 2, 3)
b = C(1, 4, 2, 5, 6, 7); b
(1, 4, 2, 5, 6, 7)
```

Predict the cycle structure of  $a^2$ ,  $a^3$ ,  $b^2$ ,  $b^3$ , and  $b^6$ . Check your answers with *SageMath*.

- 20** Calculate  $a \cdot b$  from Problem 19. Predict the cycle structure of  $(a \cdot b)^2$ ,  $(a \cdot b)^3$ , and  $(a \cdot b)^4$ , and verify your predictions with *SageMath*.
- 21** Calculate  $a \cdot b \cdot a^{-1}$  from Problem 19. Notice that it has the same cycle structure as  $b$ . Try this with other random permutations. Does  $a \cdot b \cdot a^{-1}$  always have the same cycle structure as  $b$ ? How do Problems 16 and 17 explain what is happening?
- 

### 6.3 Cayley's Theorem

The circle graphs produced in §6.1 demonstrated the property that every permutation was *one-to-one* and *onto*. In fact, every one-to-one and onto function on a finite set can be seen as a permutation on that set. For example, we saw one-to-one and onto circle graphs in §4.1 while working with cosets. To demonstrate, let us work with the group  $Q$  of order 8:

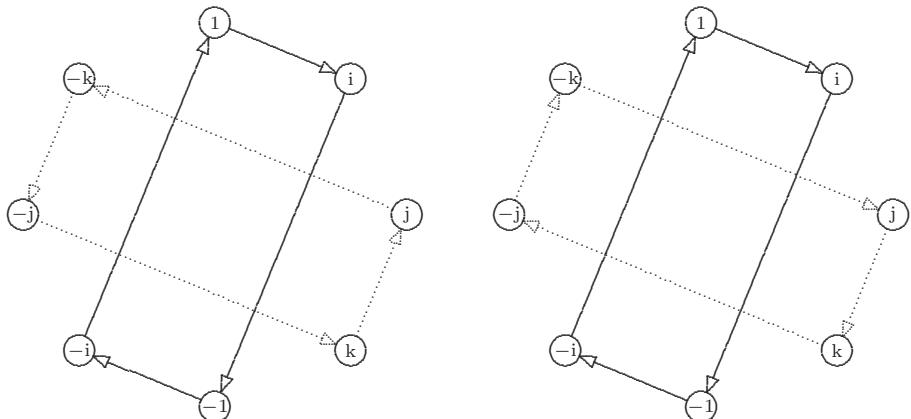
```
Q = InitQuaternions(); Q
{1, i, j, k, -1, -i, -j, -k}
```

To find the left and right cosets of a subgroup generated by  $i$ , we use the commands

```
CircleGraph(Q, LeftMult(i))
CircleGraph(Q, RightMult(i))
```

which produce the two circle graphs in Figure 6.3.

If we number the elements of  $Q$  from 1 to 8, starting with 1 and going clockwise around the circles of Figure 6.3, we find that the left circle graph mimics the permutation  $P(2, 5, 8, 3, 6, 1, 4, 7) = (1\ 2\ 5\ 6)(3\ 8\ 7\ 4)$ , while the second graph is similar to the permutation  $P(2, 5, 4, 7, 6, 1, 8, 3) = (1\ 2\ 5\ 6)(3\ 4\ 7\ 8)$ . If



```
CircleGraph(Q, LeftMult(i))    CircleGraph(Q, RightMult(i))
```

**FIGURE 6.3:** Circle graphs for multiplying by  $i$

we used different elements of  $Q$  in place of the  $i$ , we would have a different set of permutations. Thus, we can define two functions,  $f(x)$  and  $\phi(x)$ , which map elements of  $Q$  to  $S_8$ . Table 6.2 shows both of these two functions.

### Motivational Example 6.1

Let us use *SageMath* to see if either of these is a homomorphism. Normally, in defining a homomorphism, we first determine the domain group and the target group. But in this case the target group is  $S_8$ , which has 40320 elements. Rather than having *SageMath* construct all of the elements of this group, which would take an unreasonable amount of time, we can find the range of the homomorphism by determining which group is generated by  $f(i)$  and  $f(j)$ .

```
T = Group( C(1,2,5,6)*C(3,8,7,4), C(1,3,5,7)*C(2,4,6,8) )
T
{(), (1, 2, 5, 6)(3, 8, 7, 4), (1, 7, 5, 3)(2, 8, 6, 4),
 (1, 8, 5, 4)(2, 3, 6, 7), (1, 5)(2, 6)(3, 7)(4, 8),
 (1, 6, 5, 2)(3, 4, 7, 8), (1, 3, 5, 7)(2, 4, 6, 8),
 (1, 4, 5, 8)(2, 7, 6, 3)}
```

We are now ready for the homomorphism.

```
F = Homomorph(Q, T)
HomoDef(F, i, C(1,2,5,6)*C(3,8,7,4) )
HomoDef(F, j, C(1,3,5,7)*C(2,4,6,8) )
HomoDef(F, k, C(1,4,5,8)*C(2,7,6,3) )
FinishHomo(F)
```

**TABLE 6.2:** Permutations for  $Q$ 

$x$	$f(x)$ LeftMult( $x$ )	$\phi(x)$ RightMult( $x$ )
1	( )	( )
$i$	(1 2 5 6)(3 8 7 4)	(1 2 5 6)(3 4 7 8)
$j$	(1 3 5 7)(2 4 6 8)	(1 3 5 7)(2 8 6 4)
$k$	(1 4 5 8)(2 7 6 3)	(1 4 5 8)(2 3 6 7)
$-1$	(1 5)(2 6)(3 7)(4 8)	(1 5)(2 6)(3 7)(4 8)
$-i$	(1 6 5 2)(3 4 7 8)	(1 6 5 2)(3 8 7 4)
$-j$	(1 7 5 3)(2 8 6 4)	(1 7 5 3)(2 4 6 8)
$-k$	(1 8 5 4)(2 3 6 7)	(1 8 5 4)(2 7 6 3)

$(1, 2, 5, 6)(3, 8, 7, 4) * (1, 3, 5, 7)(2, 4, 6, 8)$  is not  
 $(1, 4, 5, 8)(2, 7, 6, 3)$   
'Homomorphism failed'

So  $f$  must not be a homomorphism. Let us try seeing if  $\phi$  is a homomorphism.

```
T = Group( C(1,2,5,6)*C(3,4,7,8), C(1,3,5,7)*C(2,8,6,4) )
T
{(), (1, 6, 5, 2)(3, 8, 7, 4), (1, 3, 5, 7)(2, 8, 6, 4),
 (1, 8, 5, 4)(2, 7, 6, 3), (1, 5)(2, 6)(3, 7)(4, 8),
 (1, 2, 5, 6)(3, 4, 7, 8), (1, 7, 5, 3)(2, 4, 6, 8),
 (1, 4, 5, 8)(2, 3, 6, 7)}
phi = Homomorph(Q, T)
HomoDef(phi, i, C(1,2,5,6)*C(3,8,7,4) )
HomoDef(phi, j, C(1,3,5,7)*C(2,4,6,8) )
HomoDef(phi, k, C(1,4,5,8)*C(2,7,6,3) )
FinishHomo(phi)
'Homomorphism defined'
```

This time, *SageMath* found that  $\phi$  is a homomorphism, generated by the **RightMult** permutations.  $\square$

We can easily generalize this example to prove the following.

### **THEOREM 6.2: Cayley's Theorem**

*Every finite group of order  $n$  is isomorphic to a subgroup of  $S_n$ .*

PROOF: Let  $G$  be a group of order  $n$ . For each  $g$  in  $G$ , define the mapping

$$p_g : G \rightarrow G$$

by  $p_g(x) = g \cdot x$ . For a given  $g$ , if  $p_g(x) = p_g(y)$ , then  $g \cdot x = g \cdot y$ , so  $x = y$ . Hence,  $p_g$  is a one-to-one mapping. Since  $G$  is a finite group, we can use the pigeonhole principle to show that  $p_g$  is also onto, and hence is a permutation of the elements of  $G$ .

We now can consider the mapping  $\phi$  from  $G$  to the symmetric group  $S_{|G|}$  on the elements of  $G$ , given by

$$\phi(g) = p_g.$$

Now, consider two elements  $\phi(g)$  and  $\phi(h)$ . The product of these is the mapping

$$x \rightarrow (p_g \cdot p_h)(x) = p_g(p_h(x)) = p_g(h \cdot x) = g \cdot (h \cdot x) = (g \cdot h) \cdot x.$$

Since this is the same as  $\phi(g \cdot h)$ ,  $\phi$  is a homomorphism.

The element  $g$  will be in the kernel of the homomorphism  $\phi$  only if  $p_g(x)$  is the identity permutation. This means that  $g \cdot x = x$  for all elements  $x$  in  $G$ . Thus, the kernel consists just of the identity element of  $G$ , and hence  $\phi$  is an isomorphism. Therefore,  $G$  is isomorphic to a subgroup of  $S_{|G|}$ .  $\blacksquare$

Originally, groups were only defined as subgroups of the permutation groups. Cayley's proof showed that this was equivalent to an abstract definition, similar to what we use today. (See the Historical Diversion on page 181.)

### Example 6.2

Find a subgroup of  $S_6$  isomorphic to Terry's dance steps, using [Table 2.2](#).

**SOLUTION:** Since the proof of Cayley's theorem uses multiplication on the right, we will use the *rows* of the Cayley table to produce the permutations. First, we will number Terry's dance steps in the order they appear in the table.

$$\begin{aligned} 1 &\leftrightarrow \textbf{Stay}, & 2 &\leftrightarrow \textbf{FlipRt}, & 3 &\leftrightarrow \textbf{RotRt}, \\ 4 &\leftrightarrow \textbf{FlipLft}, & 5 &\leftrightarrow \textbf{RotLft}, & 6 &\leftrightarrow \textbf{Spin}. \end{aligned}$$

Now, each row in the table converts to a list of numbers, which becomes the lower half of the permutation for that row. For example, the second row in the table,

**FlipRt Stay FlipLft RotRt Spin RotLft**

converts to the numbers 2 1 4 3 6 5, which represents the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}$$

(The row for the identity element will always give the identity permutation.) Doing this for each row, we get the list of permutations

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{pmatrix} \right\}.$$

□

Although this theorem shows that all finite groups can be considered as a subgroup of a symmetric group, the theorem can also apply to infinite groups as well. Of course we then must consider infinite symmetric groups, whose elements would be permutations on an infinite collection of objects. We might have a difficult time expressing some of the permutations! For example, if we had a library of an infinite number of books, we could not begin to express how one could rearrange the books. Some of the permutations could be expressed as one-to-one and onto functions. However, most of the permutations in an infinite symmetric group are not expressible using a finite number of words or symbols. Problems 18 through 22 of [§6.4](#) reveal some of the unusual properties of infinite symmetric groups. Fortunately, we will mainly work with finite symmetric groups.

Although Cayley's theorem (6.2) shows that any finite group  $G$  is a subgroup of  $S_n$ , where  $n$  is the size of the group  $G$ , we often can find a smaller symmetric group that contains an isomorphic copy of  $G$ .

### Motivational Example 6.3

Consider the group  $D_4$ , whose Cayley table is given in [Table 5.2](#).

```
InitGroup("e ")
AddGroupVar("a", "b")
Define(a^4, e)
Define(b^2, e)
Define(b*a, a^3*b)
D4 = ListGroup(); D4
{e, a, a^2, a^3, b, a*b, a^2*b, a^3*b}
```

Let us consider a *non-normal* subgroup of  $D_4$ :

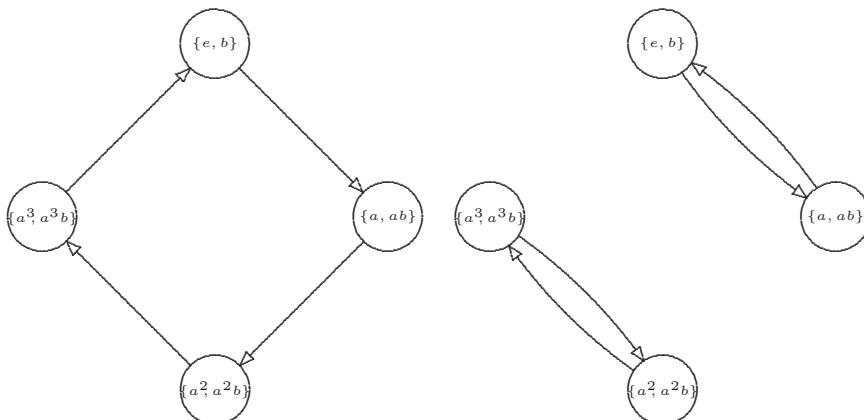
```
H = Group(b)
{e, b}
```

We saw in Cayley's theorem (6.2) that **RightMult** applied to the elements of the group derived a homomorphism. What if we applied **RightMult** to the cosets of the group? Recall that **RightMult(x)** can be thought of as

a function  $p_g(x) = g \cdot x$ , that is, it multiplies the argument of the function to the right of  $g$ . If we apply this function to a left coset of  $H$ , we have  $p_g(xH) = g \cdot xH$ , which yields another left coset. (Right cosets won't work here, since  $p_g(Hx) = g \cdot Hx$ , which is neither a left nor right coset.) The list of left cosets is given by

```
L = LftCoset(D4, H); L
{{e, b}, {a, a*b}, {a^2, a^2*b}, {a^3, a^3*b}}
```

If we multiply each coset to the right of a fixed element of the group, say  $a$  or  $a \cdot b$ , we get the circle graphs in [Figure 6.4](#).



`CircleGraph(L, RightMult(a))`   `CircleGraph(L, RightMult(a*b))`

**FIGURE 6.4:** Circle graphs for multiplying cosets of  $D_4$

We see that each coset is mapped to another coset, so once again we can treat each circle graph as a permutation. By numbering the cosets in the order that they appear in `L`, we see that `RightMult(a)` acts as the permutation  $P(2, 3, 4, 1) = (1\ 2\ 3\ 4)$ , whereas `RightMult(b)` acts as the permutation  $P(1, 4, 3, 2) = (2\ 4)$ . *SageMath* can check that this extends to a homomorphism.

```
S4 = Group( C(1,2), C(1,2,3), C(1,2,3,4) )
F = Homomorph(D4, S4)
HomoDef(F, a, C(1,2,3,4) )
HomoDef(F, b, C(2,4) )
FinishHomo(F)
'Homomorphism defined'
Kernel(F)
{e}
```

Since the kernel is just the identity element, we see that there is a subgroup of  $S_4$  isomorphic to  $D_4$ .  $\blacksquare$

Note that this is a much stronger result than Cayley's theorem (6.2), which only says that  $D_4$  is isomorphic to a subgroup of the larger group  $S_8$ . We can follow this procedure to produce the following result:

**THEOREM 6.3: Generalized Cayley's Theorem**

Let  $G$  be a finite group of order  $n$ , and  $H$  a subgroup of order  $m$ . Then there is a homomorphism from  $G$  to  $S_k$ , with  $k = n/m$ , and whose kernel is a subgroup of  $H$ .

PROOF: Let  $Q$  be the set of left cosets  $G/H$ . For each  $g$  in  $G$ , define the mapping

$$p_g : Q \rightarrow Q$$

by  $p_g(xH) = g \cdot xH$ . Note that this is well defined, since if  $xH = yH$ , then  $g \cdot xH = g \cdot yH$ .

For a given  $g$ , if  $p_g(xH) = p_g(yH)$ , then  $g \cdot xH = g \cdot yH$ , so  $xH = yH$ . Hence,  $p_g$  is a one-to-one mapping. Since  $Q$  is a finite set, by the pigeonhole principle,  $p_g$  must also be onto, and hence is a permutation of the elements of  $Q$ .

We now can consider the mapping  $\phi$  from  $G$  to the symmetric group  $S_{|Q|}$  on the elements of  $Q$ , given by

$$\phi(g) = p_g.$$

Now, consider two elements  $\phi(g)$  and  $\phi(h)$ . The product of these is the mapping

$$xH \rightarrow (p_g \cdot p_h)(xH) = p_g(p_h(xH)) = p_g(h \cdot xH) = g \cdot (h \cdot xH) = (g \cdot h) \cdot xH.$$

Since this is the same as  $\phi(g \cdot h)$ ,  $\phi$  is a homomorphism.

Finally, we must show that the kernel of  $\phi$  is a subgroup of  $H$ . The element  $g$  will be in the kernel of the homomorphism  $\phi$  only if  $p_g(xH)$  is the identity permutation. This means that  $g \cdot xH = xH$  for all left cosets  $xH$  in  $Q$ . In particular, the left coset  $eH = H$  is in  $Q$ , so  $g \cdot H = H$ . This can only happen if  $g$  is in  $H$ . Thus, the kernel is a subgroup of  $H$ . We have found a homomorphism  $\phi$  from the group  $G$  to the group  $S_{|Q|} = S_k$ , whose kernel is a subgroup of  $H$ .  $\blacksquare$

We see one application of this proposition in the case of  $D_4$ . Since  $H$  was a subgroup of order 2 which was not normal, the only normal subgroup of  $G$  that is contained in  $H$  is the trivial subgroup. Thus, the homomorphism is an isomorphism, and we find a copy of  $D_4$  inside of  $S_4$  instead of having to

look in the larger group  $S_8$ . This idea can be applied whenever we can find a subgroup of  $G$  that does not contain any nontrivial normal subgroups of  $G$ .

But there is another important ramification from this proposition. We can prove the existence of a normal subgroup of a group, knowing only the order of the group!

### **COROLLARY 6.2**

*Let  $G$  be a finite group, and  $H$  any subgroup of  $G$ . Then  $H$  contains a subgroup  $N$ , which is a normal subgroup of  $G$ , such that  $|G|$  divides  $(|G|/|H|)! \cdot |N|$ .*

**PROOF:** By the generalized Cayley's theorem (6.3), there exists a homomorphism  $\phi$  from  $G$  to  $S_k$ , where  $k = |G|/|H|$ . Furthermore, the kernel is a subgroup of  $H$ . If we let  $N$  be the kernel, and let  $I$  be the image of the homomorphism, we have by the first isomorphism theorem (5.1) that

$$G/N \approx I.$$

In particular,  $|G|/|N| = |I|$ , and  $|I|$  is a factor of  $|S_k| = k!$ . This means that  $|G|$  is a factor of  $k! \cdot |N|$ . □

Here is an example of how we can prove the existence of a nontrivial normal subgroup, using just the order of the group. Suppose we have a group  $G$  of order 108. Suppose that  $G$  has a subgroup of order 27. (In fact, all groups of order 108 must have a subgroup of order 27.) Using  $|G| = 108$  and  $|H| = 27$ , we find that  $G$  must contain a subgroup  $N$  such that 108 divides  $(108/27)! \cdot |N| = 24 \cdot |N|$ . But this means that  $|N|$  must be a multiple of 9. Since  $N$  is a subgroup of  $H$ , which has order 27, we see that  $N$  is of order 9 or 27. Hence, we have proven that  $G$  contains a normal subgroup of either order 9 or 27. This will go a long way in finding the possible group structures of  $G$ , using only the size of the group  $G$ .

### **Problems for §6.3**

- 1** Find a subgroup of  $S_4$  that is isomorphic to  $Z_8^*$ .

Hint: Look at the proof of Cayley's theorem (6.2).

- 2** Find a subgroup of  $S_5$  that is isomorphic to  $Z_5$ . (Do you really need Cayley's theorem (6.2) for this one?)

- 3** Follow the proof of Cayley's theorem (6.2) to find a subgroup of  $S_8$  isomorphic to  $D_4 = \{e, a, a^2, a^3, b, a \cdot b, a^2 \cdot b, a^3 \cdot b\}$ , using this ordering of the elements.

- 4** Follow the proof of Cayley's theorem (6.2) to find a subgroup of  $S_8$  isomorphic to  $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ , using this ordering of the elements.

## Historical Diversion Arthur Cayley (1821–1895)

Author Cayley was a British mathematician, born in Richmond. He started at Trinity College at the early age of 17. By the time he was 20, he had already published 3 papers in the Cambridge Mathematical Journal. A few years later, Cayley introduced the concept of  $n$ -dimensional geometry. He graduated from Trinity winning the Senior Wrangler (top mathematician). In a competition he won a fellowship to Cambridge University for four years.

After his fellowship was over, at age 25 Cayley chose to be a lawyer. Yet he continued to work on mathematics in his spare time. Of the course of 14 years, Cayley would publish between 200 and 300 papers.

In 1863, a new position was established at Cambridge University, the Sadleirian. Cayley was elected to this position, and remained there the rest of his life. Cayley played a major role to allow women to be admitted to Cambridge.

Although matrices have been around since antiquity, Cayley is considered as the creator of matrix algebra, since he is the first to define the product of matrices. He showed that a square matrix satisfied its own characteristic equation, and made other huge developments in linear algebra.

One of Cayley's major contributions is the first step towards the modern definition of a group. Galois had originally defined a group as a set of permutations which is closed under multiplication. In 1854 Cayley instead defined the group abstractly as a finite set, containing the identity (which he called 1), which was closed under an associative multiplication. He also insisted that the cancellation laws hold, that is,  $a \cdot b = a \cdot c$  or  $b \cdot a = c \cdot a$  implies that  $b = c$ . (From this rule, and the fact that the set is finite, one can prove that inverses exist. See problem 19.) Cayley went on to prove that the two definitions are equivalent, the result currently called Cayley's theorem.

Cayley proceeded to make a multiplication tables for the groups (now called Cayley tables) and showed how the tables revealed many important structures within the group, such as the inverse of the elements.

Unfortunately, Cayley's abstraction of the group definition went virtually unnoticed, and groups continued to mean only permutation groups for 26 more years. The idea of an infinite group did not occur until 1882.

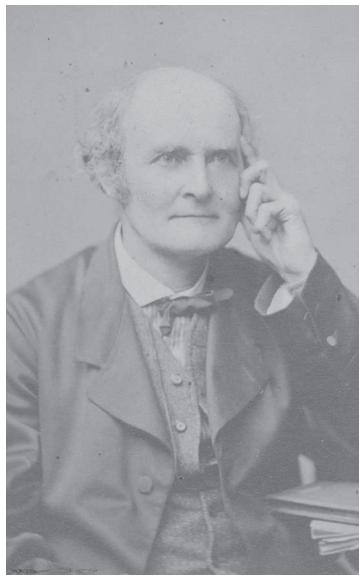


Image source: Wikimedia Commons

- 5** Follow the proof of Cayley's theorem (6.2) to find a subgroup of  $S_8$  isomorphic to  $Z_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$ , using this ordering of the elements.
- 6** According to Cayley's theorem (6.2), the quaternion group  $Q$  is isomorphic to a subgroup of  $S_8$ . Show that  $Q$  is not isomorphic to a subgroup of  $S_7$ . Hint: Assume that a subgroup is isomorphic to  $Q$ . Is the permutation corresponding to  $-1 = i^2$  odd or even? How many disjoint cycles can it contain? What possible permutations can  $i, j, k, -i, -j$ , and  $-k$  be mapped to? From this, produce a contradiction.
- 7** In the text we found a group isomorphic to  $D_4$  actually contained in  $S_4$ , which is a much smaller group than  $S_8$  used by Cayley's theorem (6.2). What is the smallest symmetric group that contains a subgroup isomorphic to  $Z_{24}^*$ ?
- 8** The function  $f(x)$ , which used **LeftMult** instead of **RightMult**, was shown not to be a homomorphism. Show that

$$f(x \cdot y) = f(y) \cdot f(x).$$

A function with this property is called an *anti-homomorphism*.

- 9** Show that if  $G$  is a group of order 35, and  $H$  is a subgroup of order 7, then  $H$  is normal.  
Hint: Use Corollary 6.2.
- 10** Show that if  $G$  is a group of order 36, and  $H$  is a subgroup of order 9, then either  $H$  is normal, or  $H$  contains a subgroup of order 3 which is normal in  $G$ .
- 11** Show that if  $G$  is a group of order 200, and  $H$  is a subgroup of order 25, then either  $H$  is normal, or  $H$  contains a subgroup of order 5 which is normal in  $G$ .
- 12** Show that if  $G$  is a group of order 60, and  $H$  is a subgroup of order 15, then either  $H$  is normal, or  $H$  contains a subgroup of order 5 which is normal in  $G$ .
- 13** Show that if  $G$  is a group of order 189, and  $H$  is a subgroup of order 27, then either  $H$  is normal, or  $H$  contains a subgroup of order 3 or 9 which is normal in  $G$ .
- 14** Use Corollary 6.2 to show that if  $G$  is a group of order  $p \cdot m$ , where  $p$  is prime and  $p > m$ , then any subgroup of order  $p$  is normal.
- 15** Let  $G$  be a group, and  $H$  be a subgroup containing exactly  $1/3$  of the elements of  $G$ . Use Corollary 6.2 to show that either  $H$  is normal, or exactly half the elements of  $H$  form a normal subgroup of  $G$ .

- 16** Suppose  $G$  is a finite group, and let  $p$  be the smallest prime that divides  $|G|$ . Show that a subgroup  $H$  with order  $|G|/p$  must be normal.
- 17** Suppose  $G$  has order  $p^2$ , where  $p$  is prime. Show that all subgroups are normal.
- 18** Show that in Cayley's theorem, the subgroup of  $S_n$  created is transitive in  $S_n$ . See Problem 15 from §6.2 for the definition of transitive.
- 19** Show that Cayley's definition of a finite group agrees with the current definition. (See Historical Diversion on page 181.) That is, show that if the cancellation laws hold for a finite set,  $a \cdot b = a \cdot c$  or  $b \cdot a = c \cdot a$  implies  $a = c$ , then inverses exist.

## Interactive Problems

- 20** Use Cayley's theorem (6.2) to find a subgroup of  $S_{12}$  that is isomorphic to  $Z_{21}^*$ .
- 21** Use Cayley's theorem (6.2) to find a subgroup of  $S_{12}$  that is isomorphic to the following group:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^3, e)
Define(b^4, e)
Define(b*a, a^2*b)
G = Group(); G
{e, a, a^2, b, a*b, a^2*b, b^2, a*b^2, a^2*b^2, b^3, a*b^3,
 a^2*b^3}
```

- 22** Use the generalized Cayley's theorem (6.3) to find a subgroup of  $S_8$  that is isomorphic to the following group:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e)
Define(b^8, e)
Define(b*a, a*b^5)
G = Group(); G
{e, a, b, a*b, b^2, a*b^2, b^3, a*b^3, b^4, a*b^4, b^5,
 a*b^5, b^6, a*b^6, b^7, a*b^7}
```

Hint: Find a subgroup of order 2 that is not normal.

## 6.4 Numbering the Permutations

Although using cycles to denote permutations is in most cases more succinct and more readable, *SageMath* works much faster using the standard permutation notation. Thus, for large time consuming operations, such as checking that a function is a homomorphism, it will actually be faster using the  $P(\dots)$  notation than the  $C(\dots)$  notation. For example, we saw using Cayley's theorem that there was a copy of  $Q$  inside of  $S_8$ . It was generated by the elements

$$\phi(i) = (1\ 2\ 5\ 6)(3\ 4\ 7\ 8) \quad \text{and} \quad \phi(j) = (1\ 3\ 5\ 7)(2\ 8\ 6\ 4).$$

These two elements can be converted to the permutation notation, and use these to generate a subgroup of  $S_8$ . Thus, we could form a group isomorphic to  $Q$  by the command

```
Q = Group({P(2,5,4,7,6,1,8,3), P(3,8,5,2,7,4,1,6)}) ; Q
{P(), P(6, 1, 8, 3, 2, 5, 4, 7), P(3, 8, 5, 2, 7, 4, 1, 6),
 P(8, 7, 2, 1, 4, 3, 6, 5), P(5, 6, 7, 8, 1, 2, 3, 4),
 P(2, 5, 4, 7, 6, 1, 8, 3), P(7, 4, 1, 6, 3, 8, 5, 2),
 P(4, 3, 6, 5, 8, 7, 2, 1)}
```

Alternatively, we could have used the cycle notation.

```
[PermToCycle(x) for x in Q]
[(), (1, 6, 5, 2)(3, 8, 7, 4), (1, 3, 5, 7)(2, 8, 6, 4),
 (1, 8, 5, 4)(2, 7, 6, 3), (1, 5)(2, 6)(3, 7)(4, 8),
 (1, 2, 5, 6)(3, 4, 7, 8), (1, 7, 5, 3)(2, 4, 6, 8),
 (1, 4, 5, 8)(2, 3, 6, 7)]
```

Which method is best? For small groups, using cycles would be a good choice, because the results are easy to read. But for larger groups (say over 100 elements, and yes, we will be working with groups that large in the next chapter) having *SageMath* write out all of the elements in terms of cycles would be time consuming and messy. It would be convenient to have a succinct way to describe each permutation using some type of abbreviation.

This section introduces a way to work with permutations that combines succinctness and speed. *SageMath* has a preset order in which it lists the permutations.

- 1<sup>st</sup> permutation =  $P()$
- 2<sup>nd</sup> permutation =  $P(2, 1)$
- 3<sup>rd</sup> permutation =  $P(1, 3, 2)$
- 4<sup>th</sup> permutation =  $P(3, 1, 2)$

$$\begin{aligned}
 5^{\text{th}} \text{ permutation} &= P(2, 3, 1) \\
 6^{\text{th}} \text{ permutation} &= P(3, 2, 1) \\
 7^{\text{th}} \text{ permutation} &= P(1, 2, 4, 3) \\
 &\dots \quad \dots \\
 24^{\text{th}} \text{ permutation} &= P(4, 3, 2, 1)
 \end{aligned}$$

Notice that the first 2 permutations give the group  $S_2$ , the first 6 give  $S_3$ , and the first 24 elements give  $S_4$ . This pattern can be extended to higher order permutations, so that the first  $n!$  permutations gives the group  $S_n$ .

The order of the permutations are designed so that *SageMath* can quickly find the  $n^{\text{th}}$  permutation on the list. For example, to find out what the 2000th permutation would be on this list, we use the **NthPerm** command.

### **NthPerm(2000)**

```
P(4, 1, 7, 6, 3, 2, 5)
```

We can also quickly determine the position of a given permutation on this list. The command

```
PermToInt( P(4,1,7,6,3,2,5) )
2000
```

converts the permutation back to the number 2000.

Rather than spelling out each permutation, we can now give a single number that describes where the permutation is on the list of permutations. This will be called the *integer representation* of the permutation. Although this representation hides most of the information about the permutation, *SageMath* can quickly recover the needed information to do group operations.

For example, we can multiply the 3rd permutation with the 21st on the list with the command

```
NthPerm(3) * NthPerm(21)
P(3, 4, 2, 1)
```

If we wanted this converted back to a number, we would type

```
PermToInt( NthPerm(3) * NthPerm(21) )
23
```

Hence the 3rd permutation times the 21st permutation gives the 23rd permutation. If we had multiplied in the other order, we would get 19 instead, indicating that the group is non-abelian.

*SageMath* provides an abbreviation to the permutations. By setting the variable **DisplayPermInt** to true, permutations will be displayed as their integer counterpart.

```
DisplayPermInt = true
```

Now, every permutation will be displayed as its integer counterpart.

```
P(4,1,7,6,3,2,5)
```

```
2000
```

This integer representation of the permutations allows us to find other groups within the permutations easily. For example, the quaternion group was generated by the elements

$$(1\ 2\ 5\ 6)(3\ 4\ 7\ 8) \quad \text{and} \quad (1\ 3\ 5\ 7)(2\ 8\ 6\ 4).$$

Converting these to permutations will reveal their integer representation.

```
CycleToPerm( C(1,2,5,6)*C(3,4,7,8) )
```

```
25827
```

```
CycleToPerm( C(1,3,5,7)*C(2,8,6,4) )
```

```
14805
```

So we find that the quaternion group contains the 25827th and 14805th permutations. Now we can form the group using these two permutations as generators.

**TABLE 6.3:** Integer representation of  $Q$

.	1	7526	14805	16992	23617	25827	32484	39728
1	1	7526	14805	16992	23617	25827	32484	39728
7526	7526	23617	16992	32484	25827	1	39728	14805
14805	14805	39728	23617	7526	32484	16992	1	25827
16992	16992	14805	25827	23617	39728	32484	7526	1
23617	23617	25827	32484	39728	1	7526	14805	16992
25827	25827	1	39728	14805	7526	23617	16992	32484
32484	32484	16992	1	25827	14805	39728	23617	7526
39728	39728	32484	7526	1	16992	14805	25827	23617

```
Q = Group(NthPerm(25827), NthPerm(14805)); Q
{1, 7526, 14805, 16992, 23617, 25827, 32484, 39728}
```

This gives the whole group on a single line which encodes the entire structure of the group. Finally, the command **CayleyTable(Q)** produces Table 6.3.

This integer representation of the permutations allows us to form such a table, and has many other advantages over cyclic permutations, especially when we are working with extremely large subgroups of a symmetric group.

There are simple algorithms to convert from the permutation representation to the integer representation and back without a computer. We begin by presenting a method of converting from a permutation to a integer.

**Example 6.4**

Demonstrate without *SageMath* that  $P(4, 1, 7, 6, 3, 2, 5)$  is the 2000th permutation.

**SOLUTION:** For each number in the permutation, we count how many numbers further left are larger than that number. For example, the 4 has no numbers further left, so the count would be 0. The 3, however, has three numbers to the left of it which are larger, namely 4, 7, and 6. Here are the results of these counts.

$$\begin{array}{c} P(4, 1, 7, 6, 3, 2, 5) \\ \quad 0 \ 1 \ 0 \ 1 \ 3 \ 4 \ 2 \end{array}$$

Next, we multiply each of these counts by  $(n - 1)!$ , and add the products together, and finally add 1. Thus,

$$0 \cdot 0! + 1 \cdot 1! + 0 \cdot 2! + 1 \cdot 3! + 3 \cdot 4! + 4 \cdot 5! + 2 \cdot 6! + 1 = 2000. \quad \square$$

A similar algorithm reverses the procedure, and determines the  $n^{\text{th}}$  permutation.

**Example 6.5**

Determine the 4000th permutation without *SageMath*.

**SOLUTION:** We begin by subtracting 1, then using the division algorithm to successively divide by 2, 3, 4, etc., until the quotient is 0.

$$\begin{aligned} 3999 &= 2 \cdot 1999 + 1 \\ 1999 &= 3 \cdot 666 + 1 \\ 666 &= 4 \cdot 166 + 2 \\ 166 &= 5 \cdot 33 + 1 \\ 33 &= 6 \cdot 5 + 3 \\ 5 &= 7 \cdot 0 + 5 \end{aligned}$$

The sequence of remainders produced is called the *Cantor representation* of  $n - 1$ . Since the last division was by  $n = 7$ , the permutation is in  $S_7$ . We will use the remainders to determine the permutation, starting from the last remainder, and working towards the first. We start with a list of numbers from 1 to  $n$ :

$$\{1, 2, 3, 4, 5, 6, 7\}$$

For each remainder  $m$ , we consider the  $(m + 1)^{\text{st}}$  largest number in the list which has not been crossed out. Since the last remainder is 5, we take the 6<sup>th</sup> largest number, which is 2. This eliminates 2 from the list. Here is the result after processing two more remainders.

$$\begin{aligned} 3999 &= 2 \cdot 1999 + 1 \\ 1999 &= 3 \cdot 666 + 1 \\ 666 &= 4 \cdot 166 + 2 \\ 166 &= 5 \cdot 33 + 1 \Rightarrow 6 \\ 33 &= 6 \cdot 5 + 3 \Rightarrow 4 \\ 5 &= 7 \cdot 0 + 5 \Rightarrow 2 \\ &\{1, 2, 3, 4, 5, \emptyset, 7\} \end{aligned}$$

The next remainder is 2, so we take the 3<sup>rd</sup> largest number which is not crossed out, which is 3. Continuing, we get the following.

$$\begin{aligned} 3999 &= 2 \cdot 1999 + 1 \Rightarrow 1 \\ 1999 &= 3 \cdot 666 + 1 \Rightarrow 5 \\ 666 &= 4 \cdot 166 + 2 \Rightarrow 3 \\ 166 &= 5 \cdot 33 + 1 \Rightarrow 6 \\ 33 &= 6 \cdot 5 + 3 \Rightarrow 4 \\ 5 &= 7 \cdot 0 + 5 \Rightarrow 2 \\ &\{1, 2, 3, 4, 5, \emptyset, 7\} \end{aligned}$$

The only number not crossed out is 7, which becomes the first number in the permutation. The rest of the permutation can be read from the new numbers from top to bottom, producing  $P(7, 1, 5, 3, 6, 4, 2)$ . □

The simple algorithms for converting permutations to integers and back make this association more natural. It also explains why *SageMath* is able to convert permutations so quickly.

## Problems for §6.4

For Problems 1 through 8: Convert the following permutations to integers. Note that cycle notations must first be converted to a permutation.

- |          |                          |          |                          |          |                         |
|----------|--------------------------|----------|--------------------------|----------|-------------------------|
| <b>1</b> | $P(5, 1, 3, 6, 4, 2)$    | <b>4</b> | $P(4, 5, 3, 7, 1, 6, 2)$ | <b>7</b> | $(1\ 4\ 3\ 8)(2\ 7\ 6)$ |
| <b>2</b> | $P(3, 6, 2, 1, 5, 4)$    | <b>5</b> | $(1\ 7\ 2)(3\ 6\ 5)$     | <b>8</b> | $(1\ 6\ 8)(2\ 5\ 7\ 4)$ |
| <b>3</b> | $P(2, 6, 1, 3, 5, 7, 4)$ | <b>6</b> | $(1\ 5\ 6\ 2)(4\ 7)$     | <b>9</b> | $(1\ 5)(2\ 6\ 7)(3\ 8)$ |

For Problems 10 through 17: Determine the  $n$ th permutation for the following values of  $n$ ,

- |           |     |           |      |           |      |           |      |
|-----------|-----|-----------|------|-----------|------|-----------|------|
| <b>10</b> | 506 | <b>12</b> | 927  | <b>14</b> | 3816 | <b>16</b> | 6923 |
| <b>11</b> | 629 | <b>13</b> | 2593 | <b>15</b> | 4207 | <b>17</b> | 8510 |

- 18** Let  $S_\infty^0$  be the collection of all one-to-one and onto functions from  $\mathbb{Z}^+$  to  $\mathbb{Z}^+$  that only move a finite number of integers. Prove that  $S_\infty^0$  is a group. This group is called the *finitary symmetric group*. Show that we can write

$$S_\infty^0 = \bigcup_{n=1}^{\infty} S_n.$$

How should we interpret this union?

- 19** Show that the set of elements in  $S_\infty^0$  is countable. See Problem 18 and Definition 1.13.
- 20** Let  $S_\infty$  be the collection of all one-to-one and onto functions from  $\mathbb{Z}^+$  to  $\mathbb{Z}^+$ . Prove that  $S_\infty$  is a group. Find an element of this group that is not in  $S_\infty^0$ . (See Problem 18.)
- 21** Show that  $S_\infty^0$  is a normal subgroup of  $S_\infty$ . (See Problems 18 and 20.)
- 22** Consider the set  $G$  of all one-to-one and onto functions  $f(x)$  from  $\mathbb{Z}^+$  to  $\mathbb{Z}^+$  such that there is some integer  $M$  for which

$$|f(x) - x| < M \quad \forall x \in \mathbb{Z}^+.$$

(The value of  $M$  is different for different elements of the group.)

- (a) Prove that  $G$  is a group containing  $S_\infty^0$ .
- (b) Find an element of  $G$  that is not in  $S_\infty^0$ .
- (c) Find an element of  $S_\infty$  that is not in  $G$ . (See Problems 18 and 20.)

### Interactive Problems

- 23** Find the elements of  $A_4$  converted to the integer representation. Is there a pattern as to which positive integers correspond to the even permutations, and which correspond to odd? Does the pattern continue to  $A_5$ ?
- 24** Use *SageMath* to find all elements of  $S_7$  whose square is  $P(3, 5, 1, 7, 6, 2, 4)$ . Hint: Use a “for” loop to test all of the elements of  $S_7$ :
- ```
for i in range(1, 5041):
    if NthPerm(i)^2 == P(3, 5, 1, 7, 6, 2, 4):
        print(NthPerm(i))
```
- 25** Use *SageMath* to find all elements of  $S_6$  whose cube is  $P(3, 5, 6, 1, 2, 4)$ . (See the hint for Problem 24.)

# Chapter 7

---

## *Building Larger Groups from Smaller Groups*

In this chapter, we will use the smaller groups that we have previously studied as building blocks to form larger groups. We will discover that *all* finite abelian groups can be constructed using just the cyclic groups  $Z_n$ . We will then study a second way of combining two groups which adds a twist to the standard method.

---

### 7.1 The Direct Product

In this section, we will consider the easiest way to combine two groups to form a larger group. In spite of its simplicity, we will find that all finite abelian groups can be constructed from this operation.

One way in which we can create a larger group from two smaller groups is to consider ordered pairs  $(g_1, g_2)$ , in which the first component  $g_1$  is a member of one group, and the second component  $g_2$  is an element of a second group. We then can multiply these ordered pairs component-wise.

**DEFINITION 7.1** Given two groups  $H$  and  $K$ , the *direct product* of  $H$  and  $K$ , denoted  $H \times K$ , is the group of ordered pairs  $(h, k)$  such that  $h \in H$  and  $k \in K$ , with multiplication defined by

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot h_2, k_1 \cdot k_2).$$

The four group properties for the direct product are easy to verify. Certainly  $H \times K$  is closed under multiplication, since the component-wise product of two ordered pairs is again an ordered pair. If  $e_1$  is the identity element for  $H$ , and  $e_2$  the identity element for  $K$ , then  $(e_1, e_2)$  would be the identity element of the direct product. Also, the inverse of an ordered pair  $(h, k)$  is  $(h^{-1}, k^{-1})$ . Finally, the associative law would hold for  $H \times K$ , since it holds for both  $H$  and  $K$ .

**TABLE 7.1:** Cayley table of  $Z_4 \times Z_2$ 

|       | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| (0,0) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) |
| (0,1) | (0,1) | (0,0) | (1,1) | (1,0) | (2,1) | (2,0) | (3,1) | (3,0) |
| (1,0) | (1,0) | (1,1) | (2,0) | (2,1) | (3,0) | (3,1) | (0,0) | (0,1) |
| (1,1) | (1,1) | (1,0) | (2,1) | (2,0) | (3,1) | (3,0) | (0,1) | (0,0) |
| (2,0) | (2,0) | (2,1) | (3,0) | (3,1) | (0,0) | (0,1) | (1,0) | (1,1) |
| (2,1) | (2,1) | (2,0) | (3,1) | (3,0) | (0,1) | (0,0) | (1,1) | (1,0) |
| (3,0) | (3,0) | (3,1) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) |
| (3,1) | (3,1) | (3,0) | (0,1) | (0,0) | (1,1) | (1,0) | (2,1) | (2,0) |

**Example 7.1**

Let  $H = Z_4$  and  $K = Z_2$ . Consider the direct product  $G = Z_4 \times Z_2$ . Since  $Z_4$  consists of the elements  $\{0, 1, 2, 3\}$  and  $Z_2$  consists of  $\{0, 1\}$ , the set of all ordered pairs  $(h, k)$  with  $h \in Z_4$  and  $k \in Z_2$  is

$$\{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}.$$

Thus, we will have a group of order 8. Multiplication is performed component-wise in the two groups.  $\square$

In order to define this group in *SageMath*, we first define the groups  $Z_4$  and  $Z_2$ .

```
z4 = ZGroup(4)
z2 = ZGroup(2)
G = DirectProduct(z4, z2); G
{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)}
```

The Cayley table produced by *SageMath* is given in [Table 7.1](#).

We notice from the table that  $Z_4 \times Z_2$  is commutative, has an element of order 4, yet has no element of order 8. Since we found all groups of order 8 in [Chapter 5](#), we can use process of elimination to determine this group must be isomorphic to  $Z_{15}^*$ .

It is not hard to show that the direct product of two abelian groups will be abelian.

**PROPOSITION 7.1**

*Let  $H$  and  $K$  be two groups. Then  $H \times K$  is commutative if, and only if, both  $H$  and  $K$  are commutative.*

PROOF: First, suppose that  $H$  and  $K$  are both abelian. Then for two elements  $(h_1, k_1)$  and  $(h_2, k_2)$  in  $H \times K$ , we have

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot h_2, k_1 \cdot k_2) = (h_2 \cdot h_1, k_2 \cdot k_1) = (h_2, k_2) \cdot (h_1, k_1).$$

So the two elements in  $H \times K$  commute. Hence,  $H \times K$  is abelian.

Now suppose that  $H \times K$  is commutative. We then have

$$(h_1 \cdot h_2, k_1 \cdot k_2) = (h_1, k_1) \cdot (h_2, k_2) = (h_2, k_2) \cdot (h_1, k_1) = (h_2 \cdot h_1, k_2 \cdot k_1).$$

Comparing components, we see that  $h_1 \cdot h_2 = h_2 \cdot h_1$  and  $k_1 \cdot k_2 = k_2 \cdot k_1$ . Since this is true for all  $h_1$  and  $h_2$  in  $H$ , and all  $k_1$  and  $k_2$  in  $K$ , both  $H$  and  $K$  are abelian.  $\square$

It is easy to find the number of elements in a direct product. If  $H$  has order  $n$ , and  $K$  has order  $m$ , then the number of ordered pairs  $(h, k)$  would be  $n \cdot m$ .

We can generalize the direct product to a set of more than two groups. Let

$$G_1, G_2, G_3, \dots, G_n$$

be a collection of  $n$  groups. Then we define  $G_1 \times G_2 \times G_3 \times \dots \times G_n$  to be the set of ordered  $n$ -tuples  $(g_1, g_2, g_3, \dots, g_n)$  with multiplication defined by

$$(g_1, g_2, \dots, g_n) \cdot (h_1, h_2, \dots, h_n) = (g_1 \cdot h_1, g_2 \cdot h_2, \dots, g_n \cdot h_n).$$

The direct product of more than two groups can also be defined by taking the direct product of direct products. That is, given three groups  $G$ ,  $H$ , and  $K$ , we could define both  $(G \times H) \times K$  and  $G \times (H \times K)$ . But it is trivial to see that the mappings

$$f : (G \times H) \times K \rightarrow G \times H \times K$$

$$\phi : G \times (H \times K) \rightarrow G \times H \times K$$

given by

$$f(((g, h), k)) = (g, h, k) \quad \text{and} \quad \phi((g, (h, k))) = (g, h, k)$$

are both surjective isomorphisms. Thus,

$$(G \times H) \times K \approx G \times H \times K \approx G \times (H \times K).$$

It also should be noted that there is the natural mapping

$$\phi : H \times K \rightarrow K \times H$$

given by  $\phi((h, k)) = (k, h)$ . Thus,  $H \times K \approx K \times H$ .

This shows that the direct product between groups is a commutative operation, as well as associative. This suggests that some groups may be able

to be expressed as a direct product of two or more smaller groups. If this is the case, then the order in which the smaller groups are combined would be irrelevant.

**DEFINITION 7.2** Let  $G$  be a group. We say that  $G$  has a *decomposition* if  $G \approx H \times K$ , where neither  $H$  nor  $K$  is the trivial group.

For example, the group  $Z_{15}^*$  has a decomposition, since we saw in Example 7.1 that this group is isomorphic to  $Z_4 \times Z_2$ . We would like to find a way of testing whether a general group can be decomposed into smaller groups. In the case of  $S_3$ , we could use the fact that all smaller groups are abelian, along with Proposition 7.1 to show that  $S_3$  cannot have a decomposition. But for other groups, the problem is more difficult. The following theorem gives us a way to determine whether a given group has a decomposition.

**THEOREM 7.1: The Direct Product Theorem**

Let  $G$  be a group with identity  $e$ , and let  $H$  and  $K$  be two subgroups of  $G$ . Suppose the following two statements are true:

1.  $H \cap K = \{e\}$ .
2.  $h \cdot k = k \cdot h$  for all  $h \in H$  and  $k \in K$ .

Then  $H \cdot K \approx H \times K$ .

PROOF: First, we show that every element in  $H \cdot K$  can be *uniquely* written in the form  $h \cdot k$ , where  $h \in H$  and  $k \in K$ . Suppose that

$$h_1 \cdot k_1 = h_2 \cdot k_2.$$

Then  $h_2^{-1} \cdot h_1 = k_2 \cdot k_1^{-1}$ . Since this element must be in both  $H$  and  $K$ , and the intersection of  $H$  and  $K$  is the identity element, we have that

$$h_2^{-1} \cdot h_1 = k_2 \cdot k_1^{-1} = e.$$

Thus,  $h_1 = h_2$  and  $k_1 = k_2$ . Therefore, every element of  $H \cdot K$  can be written uniquely as  $h \cdot k$ , where  $h$  is in  $H$ , and  $k$  is in  $K$ .

Next, we need to show that  $H \cdot K$  is a group. Since  $h \cdot k = k \cdot h$  for all  $h \in H$  and  $k \in K$ , we have that  $H \cdot K = K \cdot H$ . Thus, by Lemma 5.2,  $H \cdot K$  is a subgroup of  $G$ .

We can now define a mapping

$$\phi : H \cdot K \rightarrow H \times K$$

by  $\phi(x) = (h, k)$ , where  $h$  and  $k$  are the unique elements such that  $h \in H$ ,  $k \in K$ , and  $x = h \cdot k$ . It is clear that  $\phi$  is one-to-one, since the element  $(h, k)$

can only have come from  $h \cdot k$ . Also,  $\phi$  is onto, for the element  $h \cdot k$  maps to  $(h, k)$ . All that remains to show is that  $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ . Let  $x = h_1 \cdot k_1$ , and  $y = h_2 \cdot k_2$ . Then

$$\begin{aligned}\phi(x \cdot y) &= \phi(h_1 \cdot k_1 \cdot h_2 \cdot k_2) \\ &= \phi(h_1 \cdot h_2 \cdot k_1 \cdot k_2) \\ &= (h_1 \cdot h_2, k_1 \cdot k_2) \\ &= (h_1, k_1) \cdot (h_2, k_2) \\ &= \phi(x) \cdot \phi(y).\end{aligned}$$

Thus,  $\phi$  is an isomorphism, and so  $H \cdot K \approx H \times K$ . □

We can use this theorem to define the direct product of two groups in *SageMath*.

### Computational Example 7.2

Suppose we wish to generate the direct product  $S_3 \times Z_8^*$ . We first must define the two groups in *SageMath* using the same identity element and different letters for the generators. The group  $S_3$  is defined by the commands

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^3, e); Define(b^2, e); Define(b*a, a^2*b)
H = Group(a, b); H
{e, b, a^2*b, a, a^2, a*b}
```

Now let us define  $Z_8^*$ , using  $c$  and  $d$  for the two generators.

```
AddGroupVar("c", "d")
Define(c^2, e); Define(d^2, e); Define(d*c, c*d)
K = Group(c, d); K
{e, c, d, c*d}
```

Of course we did not use the **InitGroup** command before defining the second group, otherwise we would have cleared the first group. Notice that

```
Intersection(H, K)
{e}
```

is just the identity element, so the first condition of the direct product theorem is satisfied.

In order for the second condition of the direct product theorem to be satisfied, every element of  $H$  must commute with every element of  $K$ . This will be true as long as all of the *generators* of  $H$  commute with all of the *generators* of  $K$ . Since there are 2 generators of  $H$  and 2 of  $K$ , we can tell *SageMath* that the generators commute using  $2 \cdot 2 = 4$  definitions:

```
Define(c*a, a*c); Define(c*b, b*c)
Define(d*a, a*d); Define(d*b, b*d)
```

Note that we were consistent in the direction of these definitions. That is, we defined an element of the form  $k \cdot h$  to  $h \cdot k$ , where  $h$  is in  $H$ , and  $k$  is in  $K$ .

According to the direct product theorem  $H \cdot K$  is now the same as  $H \times K$ . Here, then, is the direct product:

```
H * K
{e, b, a^2*b, a, a^2, a*b, c, b*c, d, b*d, a^2*b*c, a*c,
a^2*b*d, a*d, a^2*c, a*b*c, a^2*d, a*b*d, c*d, b*c*d,
a^2*b*c*d, a*c*d, a^2*c*d, a*b*c*d}
```

We would get the same result by finding the smallest group that contains all of the generators.

```
G = Group(a, b, c, d)
len(G)
24
```

This gives us a group of 24 elements. □

Since  $S_4$  also has 24 elements, we could ask if the group in Example 7.2 is isomorphic to  $S_4$ . But recall that  $S_4$  had exactly 9 elements of order 2, whereas the computation

```
RootCount(G, 2)
16
```

reveals that  $G$  has 16 solutions to  $x^2 = e$ , with one being the identity. Thus, there are 15 elements of order 2, so  $S_4$  is not isomorphic to  $S_3 \times Z_8^*$ .

This technique of counting elements of a certain order is an efficient way of showing that two groups are not isomorphic. Recall in §3.3 we denoted the number of solutions to  $x^n = e$  by  $R_n(G)$ . In particular, if  $G$  is cyclic,  $R_n(G) = \gcd(|G|, n)$ . This example shows it would be helpful to know how to calculate  $R_n(G)$  for the direct product  $G = H \times K$ . Then we would have a way to test whether or not two groups expressed as direct products were isomorphic to each other.

### PROPOSITION 7.2

Let  $H$  and  $K$  be finite groups, and let  $n$  be a positive integer. Then

$$R_n(H \times K) = R_n(H) \cdot R_n(K).$$

PROOF: Let  $e_1$  denote the identity element of  $H$ , and  $e_2$  denote the identity element of  $K$ . An element  $x = (h, k)$  in  $H \times K$  solves the equation  $x^n = (e_1, e_2)$  if and only if

$$h^n = e_1 \quad \text{and} \quad k^n = e_2.$$

Since there are  $R_n(H)$  solutions to the former, and  $R_n(K)$  solutions to the latter, there are  $R_n(H) \cdot R_n(K)$  ordered pairs  $(h, k)$  that solve both of these equations. Thus, there are  $R_n(H) \cdot R_n(K)$  elements of  $H \times K$  for which  $x^n = (e_1, e_2)$ .  $\blacksquare$

For example,  $R_2(S_3) = 4$ , since there are 3 elements of order 2 in  $S_4$ , plus the identity. Also, all 4 elements of  $Z_8^*$  satisfy  $x^2 = e$ , so  $R_2(Z_8^*) = 4$ . Thus, there are 16 elements of  $S_3 \times Z_8^*$  that satisfy  $x^2 = e$ , one of which is the identity. Thus, we quickly see that there are 15 elements of order 2.

As powerful as the direct product theorem (7.1) is, it is often difficult to check that  $h \cdot k = k \cdot h$  for all  $h \in H$  and  $k \in K$ . Here is a more convenient way of showing that a group can be expressed as a direct product of two subgroups.

### **COROLLARY 7.1**

*Let  $G$  be a group with identity  $e$ , and let  $H$  and  $K$  be two normal subgroups of  $G$ . Then if  $H \cap K = \{e\}$ , then  $H \cdot K \approx H \times K$ .*

**PROOF:** The first condition of the direct product theorem (7.1) is given, so we only need to show that the second condition holds. That is, we need to show that  $h \cdot k = k \cdot h$  for all  $h$  in  $H$ , and  $k$  in  $K$ . Let  $h \in H$  and  $k \in K$ .

Since  $K$  is a normal subgroup of  $G$ ,  $h \cdot k \cdot h^{-1}$  is in  $K$ . Thus,  $h \cdot k \cdot h^{-1} \cdot k^{-1}$  is also in  $K$ .

But  $H$  is also a normal subgroup of  $G$ , so  $k \cdot h^{-1} \cdot k^{-1}$  is in  $H$ . Hence,  $h \cdot k \cdot h^{-1} \cdot k^{-1}$  is also in  $H$ .

We now use the fact that the only element in both  $H$  and  $K$  is  $e$ . Thus,  $h \cdot k \cdot h^{-1} \cdot k^{-1} = e$ , which implies  $h \cdot k = k \cdot h$ . Therefore, the second condition of the direct product theorem (7.1) holds, and so by this theorem,  $H \cdot K \approx H \times K$ .  $\blacksquare$

This corollary is sometimes more useful than the direct product theorem, even though for abelian groups the two are equivalent, since all subgroups of abelian groups are normal. In the next section we will continue to study the decomposition of abelian groups, and find that all finite abelian groups can be decomposed uniquely into a certain form.

### **Problems for §7.1**

- 1 We have shown by process of elimination that  $Z_4 \times Z_2$  is isomorphic to  $Z_{15}^*$ . Demonstrate the isomorphism by giving Cayley tables for the two groups with the same pattern.
- 2 Demonstrate that  $Z_3 \times Z_2$  is isomorphic to  $Z_6$ .
- 3 Construct a Cayley table for  $Z_2 \times Z_8^*$ .

**4** Construct a Cayley table for  $Z_3 \times Z_8^*$ .

**5** Let  $G = H \times K$ , and define

$$\overline{H} = \{(h, e) \mid h \in H\}$$

and

$$\overline{K} = \{(e, k) \mid k \in K\}.$$

Prove that  $G/\overline{H} \approx K$  and  $G/\overline{K} \approx H$ .

Hint: Use the first isomorphism theorem on an appropriate homomorphism.

For Problems **6** through **13**: Use Proposition 7.2 to find the number of elements of orders 2, 3, and 4 for the following groups.

Hint: First calculate  $R_2(G)$ ,  $R_3(G)$ , and  $R_4(G)$ .

**6**  $Z_2 \times Z_6$

**9**  $S_3 \times Z_3$

**12**  $Z_2 \times Z_3 \times Z_4$

**7**  $Z_3 \times Z_4$

**10**  $S_3 \times Z_4$

**13**  $Z_3 \times S_3 \times Z_4$

**8**  $Z_6 \times Z_8^*$

**11**  $A_4 \times Z_2$

**14**  $Z_4 \times A_4 \times Z_6$

**15** Show that  $Z_2 \times Z_6$  is not isomorphic to  $Z_{12}$ .

**16** Show that  $S_3 \times Z_2$  is not isomorphic to  $A_4$ .

**17** Using only the fact that  $R_2(S_4) = 10$ , prove that  $S_4$  is not the decomposition of two smaller groups. You can use the result of Problem 22 in §3.3.

**18** Using the fact that  $R_3(A_5) = 21$  and  $R_5(A_5) = 25$ , prove that  $A_5$  is not the decomposition of two smaller groups.

### Interactive Problems

**19** Use *SageMath* to define the group  $Z_2 \times Z_6$ , and display the Cayley table. Then have *SageMath* find the Cayley table for  $Z_{21}^*$ , and rearrange the elements to show that these groups are isomorphic.

**20** Use *SageMath* to define the group  $Z_3 \times Z_8^*$ , and display the Cayley table. Then have *SageMath* find the Cayley table for  $Z_{36}^*$ , and rearrange the elements to show that these groups are isomorphic.

## 7.2 The Fundamental Theorem of Finite Abelian Groups

In the last section we promised that we will be able to construct any finite abelian group using as building blocks the groups that we have already learned. In this section, we will use the direct product to show that all finite abelian groups can be expressed in terms of the cyclic groups  $Z_n$ . We will even be able to find all abelian groups of a given order.

### **Example 7.3**

Can we express the group  $Z_6$  as the direct product of two smaller groups?

SOLUTION: By the direct product theorem, we must find two subgroups of  $Z_6$  whose intersection is just the identity element, and whose product is the whole group. It is not hard to see that the subgroups

$$H = \{0, 3\} \quad \text{and} \quad K = \{0, 2, 4\}$$

satisfy these two conditions. Thus,  $Z_6 \approx Z_2 \times Z_3$ . This is easily verified using *SageMath*.

```

Z2 = ZGroup(2); z2
    {0, 1}
Z3 = ZGroup(2); z3
    {0, 1, 2}
G = DirectProduct(z2, z3); G
    {(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)}
RootCount(G, 2)
    2
RootCount(G, 3)
    3

```

Since we only have one element of order 2, and 2 elements of order 3, there must be an element of order 6, so the product  $Z_2 \times Z_3$  must be isomorphic to  $Z_6$ . □

Observe the groups  $H = \{0, 3\}$  and  $K = \{0, 2, 4\}$  in this example. Notice that  $H$  consists of all of the elements such that  $h^2 = 0$ , and  $K$  consists of all the elements such that  $k^3 = 0$ . These two subgroups had only the identity element in common. We can extend this observation to general abelian groups.

### **LEMMA 7.1**

Let  $G$  be an abelian group of order  $mn$ , where  $m$  and  $n$  are coprime. Then

$$H = \{h \in G \mid h^m = e\}$$

and

$$K = \{k \in G \mid k^n = e\}$$

are both subgroups of  $G$ , and  $G \approx H \times K$ .

PROOF: To check that  $H$  and  $K$  are indeed subgroups simply observe that since  $G$  is commutative the functions  $\phi(x) = x^m$  and  $f(x) = x^n$  are both homomorphisms of  $G$ . Then  $H$  and  $K$  are the kernels of the mappings  $\phi$  and  $f$ .

To show that  $H$  and  $K$  have only the identity element in common, we consider an element  $x$  in the intersection. By the Chinese remainder theorem (1.5), there exists a non-negative number  $k < m \cdot n$  such that

$$k \bmod m = 1 \quad \text{and} \quad k \bmod n = 0.$$

Then  $k = 1 + mb$  for some number  $b$ . Thus,

$$x^k = x^{(1+mb)} = x \cdot (x^m)^b = x \cdot e^b = x$$

since  $x$  is in  $H$ . Yet  $k = nc$  for some number  $c$ , so

$$x^k = x^{nc} = (x^n)^c = e^c = e$$

since  $x$  is in  $K$ . Thus,  $x = e$ , and so  $H \cap K = \{e\}$ . Since  $G$  is abelian, the direct product theorem (7.1) proves that

$$H \cdot K \approx H \times K.$$

All that is left to prove is that  $G = H \cdot K$ . Let  $g$  be an element in  $G$ . Since  $m$  and  $n$  are coprime, by Bézout's lemma (1.3) there exists  $a$  and  $b$  such that

$$an + bm = \gcd(m, n) = 1.$$

Then

$$g = g^1 = g^{(an+bm)} = g^{an} \cdot g^{bm}.$$

Now,  $(g^{an})^m = (g^a)^{nm} = e$ , so  $g^{an}$  is in  $H$ . Likewise,  $g^{bm}$  is in  $K$ . Thus, every element of  $G$  is in  $H \cdot K$ , and so

$$G \approx H \times K.$$

□

This lemma tells us that if an abelian group has an order that is a product of two coprime numbers, this group can be written as a direct product of two groups. Unfortunately, the lemma does not tell us that  $H$  and  $K$  are proper subgroups. It is conceivable that either  $H$  or  $K$  from Lemma 7.1 is the whole group, and the other is just the identity element. We would still have  $G = H \times K$ , but this would not give a decomposition of  $G$ .

Here is an example to illustrate the possible problem that could occur. Suppose we know  $G$  is an abelian group of order 24. Since  $24 = 8 \cdot 3$ , we could

let  $m = 8$ , and  $n = 3$  in Lemma 7.1. Then  $H$  would consist of all elements of order 1, 2, 4, or 8, while  $K$  would consist of the elements of order 1 or 3. Then we would have  $G \approx H \times K$ .

But what if  $G$  had no elements of order 3? Then  $K$  would be just the identity element, and  $H$  would have to be all of  $G$ . Lemma 7.1 would hold, but since  $H$  and  $K$  are not proper subgroups, this would not give a decomposition of  $G$ . The next lemma uses induction to show that, in fact,  $G$  must have an element of order 3.

### **LEMMA 7.2**

*If  $G$  is a finite abelian group and  $p$  is a prime that divides the order of  $G$ , then  $G$  has an element of order  $p$ .*

**PROOF:** We will proceed using induction on the order of  $G$ . If  $|G|$  is a prime number, then  $p$  must be  $|G|$ , and  $G$  must be isomorphic to  $\mathbb{Z}_p$ . So there would be an element of order  $p$  in  $G$ .

Suppose that the assumption is true for all groups of order less than  $|G|$ . If  $G$  does not have any proper subgroups, then  $G$  would be a cyclic group of prime order (which we have already covered.) Thus, we may assume that  $G$  has a subgroup  $N$  that is neither  $G$  nor  $\{e\}$ .

Since  $G$  is abelian all subgroups are normal. Thus we could consider the quotient group  $G/N$ . Since  $|G| = |N| \cdot |G/N|$ ,  $p$  must divide either  $|N|$  or  $|G/N|$ . If  $p$  divides  $N$ , then because  $N$  is a smaller group than  $G$ , by induction  $N$  must have an element of order  $p$ , which would be in  $G$ .

If  $p$  does not divide  $|N|$  it must divide  $|G/N|$ . Since  $G/N$  is a smaller group than  $G$ , by induction  $G/N$  must have an element of order  $p$ . This element can be written  $aN$  for some  $a$  in  $G$ .

Since  $aN$  is of order  $p$ ,  $a$  cannot be in  $N$ , yet  $a^p$  must be in  $N$ . If  $q = |N|$ , we would have by Corollary 4.2 that  $(a^p)^q = e$ .

If  $b = a^q$  is not the identity, then  $b^p = e$ , and so  $b$  would be the required element. But if  $b = e$ , then  $(aN)^q = N$ . But  $aN$  was of order  $p$ , and so  $p$  must divide  $q$ . But we assumed that  $p$  did not divide  $q = |N|$ . Hence,  $b$  is not the identity, and so  $G$  has an element of order  $p$ . □

This lemma is known as Cauchy's theorem for abelian groups. (See the Historical Diversion on page 209.) In fact, Cauchy's theorem is true for *all* groups, not just abelian groups. However, the result for abelian groups is sufficient for us to proceed. This lemma guarantees that the subgroups  $H$  and  $K$  generated by Lemma 7.1 must be proper subgroups. In fact, there are times when it is possible to predict the size of the subgroups  $H$  and  $K$ .

### **LEMMA 7.3**

*Let  $G$  be an abelian group of order  $p^n \cdot k$  where  $p$  is prime,  $k$  is not divisible by  $p$ , and  $n > 0$ . Then there are subgroups  $P$  and  $K$  of  $G$  such that  $G \approx P \times K$ , where  $|P| = p^n$ , and  $|K| = k$ .*

PROOF: Since  $p^n$  and  $k$  are coprime, we can use Lemma 7.1 to form the subgroups

$$P = \{x \in G \mid x^{(p^n)} = e\}$$

and

$$K = \{x \in G \mid x^k = e\}.$$

By Lemma 7.1 these two subgroups have only the identity in common, and  $G \approx P \times K$ . If  $p$  divided  $|K|$ , then by Lemma 7.2,  $K$  would contain an element of order  $p$ . But this element would then be in  $P$  as well, which contradicts the fact that only the identity element is in common between  $P$  and  $K$ . So  $p$  does not divide the order of  $K$ .

Also note that the order of every element of  $P$  is a power of  $p$ . Thus, Lemma 7.2 tells us that no other prime other than  $p$  divides  $|P|$ .

Finally, note that  $|G| = p^n \cdot k = |P| \cdot |K|$ . Since  $p$  does not divide  $|K|$ , we have that  $p^n$  must divide  $|P|$ . But no other primes can divide  $|P|$ , and so  $|P| = p^n$ . Hence,  $|K| = k$ .  $\square$

Lemma 7.3 is a tremendous help in finding the decomposition of abelian groups. To illustrate, suppose we have an abelian group  $G$  of order 24. Since  $24 = 2^3 \cdot 3$ , Lemma 7.3 states that  $G$  is isomorphic to a direct product of a group of order 8 and a group of order 3. Thus,  $G$  must be one of the groups

$$Z_8 \times Z_3, \quad Z_{15}^* \times Z_3, \quad \text{or} \quad Z_{24}^* \times Z_3.$$

If we can find all abelian groups of order  $p^n$  for  $p$  a prime number, then we will in a similar manner be able to find all finite abelian groups.

Hence, our next line of attack is abelian groups of order  $p^n$ , where  $p$  is prime. If this is not a cyclic group, we can find a decomposition for this group as well.

#### **LEMMA 7.4**

Suppose  $P$  is an abelian group of order  $p^n$ , where  $p$  is a prime. Let  $x$  be an element in  $P$  that has the maximal order of all of the elements of  $P$ . Then  $P \approx X \times T$ , where  $X$  is the cyclic group generated by  $x$ ,  $T$  is a subgroup of  $P$ , and  $X \cap T = \{e\}$ .

PROOF: We will use induction on  $n$ . If  $n = 1$ , then  $P$  is a cyclic group of order  $p$ , and hence is generated by non-identity element  $x$  in  $P$ . We then have  $X = P$ , so we can let  $T = \{e\}$ , and  $P \approx X \times T$ , with  $X \cap T = \{e\}$ .

Now suppose that the assertion is true for all powers of  $p$  less than  $n$ . Notice that the order of every element of  $P$  is a power of  $p$ . Thus, if we let  $x$  be an element with the largest order, say  $m$ , then the order of all elements in  $P$  must divide  $m$ . Hence,  $g^m = e$  for all elements  $g$  in  $P$ .

We now let  $X$  be the subgroup generated by  $x$ . If  $X = P$ , then we can again let  $T = \{e\}$  and we are done. If  $X$  is not  $P$ , we let  $y$  be an element of  $P$  not in  $X$  which has the *smallest* possible order. Then since the order of  $y^p$  is less than the order of  $y$ ,  $y^p$  must be in  $X$ . This means that  $y^p = x^q$  for some  $0 \leq q < m$ .

Since  $y$  is in  $P$ ,  $y^m = e$ . But

$$y^m = (y^p)^{(m/p)} = (x^q)^{(m/p)} = x^{(mq/p)}.$$

Because  $x$  is of order  $m$ , this can be the identity only if  $mq/p$  is a multiple of  $m$ . Hence,  $q$  is a multiple of  $p$ .

If we let  $k = x^{-(q/p)} \cdot y$ , then  $k$  is not in  $X$  because  $y$  is not, and

$$k^p = \left(x^{-(q/p)}\right)^p \cdot y^p = x^{-q} \cdot y^p = x^{-q} \cdot x^q = e.$$

Therefore, we have found an element  $k$  of order  $p$  that is not in  $X$ . If we let  $K$  be the group generated by the element  $k$ , then  $X \cap K = \{e\}$ .

Consider the quotient group  $P/K$ . What is the order of  $xK$  in  $P/K$ ? We see that

$$(xK)^n = K \iff x^n \in K \iff x^n \in X \cap K \iff x^n = e.$$

Therefore, the order of  $xK$  is the same as the order of  $x$ , which is  $m$ . Also note that no element of  $P/K$  can have an element of higher order since  $g^m = e$  for all elements  $g$  in  $P$ .

Now we use the induction. Since the order of  $P/K$  is less than the order of  $P$ , and  $xK$  is an element of maximal order, we have by induction that

$$P/K \approx Y \times B,$$

where  $Y$  is the subgroup of  $P/K$  generated by  $xK$ , and  $B$  is a subgroup of  $P/K$  such that only the identity element  $K$  is in the intersection of  $Y$  and  $B$ .

Let  $\phi$  be the canonical homomorphism from  $P$  to  $P/K$  given by  $\phi(g) = gK$ . Let  $T = \phi^{-1}(B)$ . Then  $T$  is a subgroup of  $P$ .

If  $g$  is in both  $X$  and  $T$ , then  $\phi(g)$  is in both  $Y$  and  $B$ . Since the intersection of  $Y$  and  $B$  is the identity element, we have  $\phi(g) = g \cdot K = K$ . Thus,  $g$  is in the subgroup  $K$ . But  $X \cap K = \{e\}$ , so we have

$$X \cap T = \{e\}.$$

Thus, by the direct product theorem (7.1), we find that  $X \cdot T \approx X \times T$ .

We finally need to show that  $P = X \cdot T$ . Let  $u$  be an element in  $P$ , and since  $P/K \approx Y \times B$ , we can write  $\phi(u)$  as  $(x^c K) \cdot (kK)$  for some number  $c$ , and some  $kK$  in  $B$ . Then

$$u \in x^c \cdot k \cdot K \subseteq X \cdot T.$$

Thus,  $P = X \cdot T$ , and so  $P \approx X \times T$ . □

To illustrate the application of Lemma 7.4, consider the group  $Z_{24}^*$ . All non-identity elements of  $Z_{24}^*$  are of order 2, so this is the maximal order. Thus, Lemma 7.4 states that  $Z_{24}^*$  can be decomposed into  $Z_2$  and a group of order 4. Since we have seen that  $Z_4 \times Z_2 \approx Z_{15}^*$ , the only other choice is  $Z_2 \times Z_8^*$ .

Now we apply Lemma 7.4 to  $Z_8^*$ . This is of order 4, and all elements besides the identity are of order 2, so  $Z_8^*$  can be decomposed into  $Z_2$  and a group of order 2, which must be  $Z_2$ . Thus,  $Z_8^* \approx Z_2 \times Z_2$ , and so

$$Z_{24}^* \approx Z_2 \times Z_2 \times Z_2.$$

We have found a way to decompose any abelian group, to the point where each factor is a cyclic group whose order is a power of a prime. But now we want to address the issue as to whether a decomposition is *unique*. Can two different decompositions be isomorphic?

The main tool for testing whether two groups are isomorphic is to count elements of a given order. This can be accomplished by computing  $R_n(G)$  for various values of  $n$ . It is natural to compute  $R_n(G)$  for a decomposition of cyclic groups.

### LEMMA 7.5

Let  $p$  be a prime number, and  $G$  be the direct product of cyclic groups

$$Z_{(p^{h_1})} \times Z_{(p^{h_2})} \times \cdots \times Z_{(p^{h_n})} \times Z_{k_1} \times Z_{k_2} \times \cdots \times Z_{k_m},$$

where  $h_1, h_2, \dots, h_n$  are positive integers, and  $k_1, k_2, \dots, k_m$  are coprime to  $p$ . Then if  $q = p^x$ ,

$$R_q(G) = p^{\left(\sum_{i=1}^n \text{Min}(h_i, x)\right)},$$

where  $\text{Min}(h_i, x)$  denotes the minimum of  $h_i$  and  $x$ .

**PROOF:** Since  $G$  is expressed as a direct product we can use Proposition 7.2 and find  $R_q(H)$  for each factor  $H$  in the product, and multiply these numbers together. Since each factor is cyclic, we can use Corollary 3.1. For all of the factors  $Z_{k_1}, Z_{k_2}, \dots, Z_{k_m}$ , since  $\gcd(k_i, q) = \gcd(k_i, p^x) = 1$ ,  $R_q(H)$  would be 1. On the other hand,  $R_q(Z_{(p^{h_i})})$  is

$$\gcd(p^{h_i}, q) = \gcd(p^{h_i}, p^x) = p^{\text{Min}(h_i, x)}.$$

Thus,  $R_q(G)$  is the product of the above for factors 1 through  $n$  of  $G$ , which gives us a grand total of

$$p^{\left(\sum_{i=1}^n \text{Min}(h_i, x)\right)}. □$$

We are now ready to show that *all* finite abelian groups can be represented as the direct product of cyclic groups. However, we would like to show at the

same time that such a representation is unique. To this end we will use the previous lemma to prove the following.

**LEMMA 7.6**

Let  $G$  be the direct product of cyclic groups

$$Z_{q_1} \times Z_{q_2} \times Z_{q_3} \times \cdots \times Z_{q_k}.$$

where each  $q_i$  is a power of a prime. Then for a given prime  $p$  and positive integer  $x$ , the number of  $q_i$  equal to  $p^x$  is given by the formula

$$2 \log_p(R_{p^x}(G)) - \log_p(R_{p^{x-1}}(G)) - \log_p(R_{p^{x+1}}(G)). \quad (7.1)$$

PROOF: Applying Lemma 7.5 simplifies Equation 7.1 to

$$2 \sum_{i=1}^n \text{Min}(h_i, x) - \sum_{i=1}^n \text{Min}(h_i, x-1) - \sum_{i=1}^n \text{Min}(h_i, x+1), \quad (7.2)$$

where  $n$  is the number of the  $q_i$  that are a power of  $p$ . Let us observe the value of the expression

$$2 \text{Min}(h_i, x) - \text{Min}(h_i, x-1) - \text{Min}(h_i, x+1).$$

When  $h_i < x$ , then  $\text{Min}(h_i, x) = \text{Min}(h_i, x-1) = \text{Min}(h_i, x+1) = h_i$ , and so the above evaluates to 0. On the other hand, if  $h_i > x$ , then the above expression simplifies to be

$$2x - (x-1) - (x+1) = 0.$$

However, if  $h_i = x$ , then  $\text{Min}(h_i, x) = x$ ,  $\text{Min}(h_i, x-1) = x-1$ , and  $\text{Min}(h_i, x+1) = x$ . Hence, we have

$$2 \text{Min}(h_i, x) - \text{Min}(h_i, x-1) - \text{Min}(h_i, x+1) = 2x - (x-1) - x = 1.$$

Thus, we see that

$$2 \text{Min}(h_i, x) - \text{Min}(h_i, x-1) - \text{Min}(h_i, x+1) = \begin{cases} 1 & \text{if } h_i = x, \\ 0 & \text{if } h_i \neq x. \end{cases}$$

Thus, if we sum the above expression for  $i$  going from 1 to  $n$ , we will count the number of terms  $h_i$  that are equal to  $x$ . This will give us the number of  $q_i$  that are equal to  $p^x$ . Hence this count will be given by Equation 7.2, and hence Equation 7.1.  $\square$

We can now use Lemmas 7.3 through 7.6 to prove the following.

**THEOREM 7.2: The Fundamental Theorem of Finite Abelian Groups**

A nontrivial finite abelian group is isomorphic to

$$Z_{(p_1^{h_1})} \times Z_{(p_2^{h_2})} \times Z_{(p_3^{h_3})} \times \cdots Z_{(p_n^{h_n})},$$

where  $p_1, p_2, p_3, \dots, p_n$  are prime numbers (not necessarily distinct). Furthermore, this decomposition is unique up to the rearrangement of the factors.

PROOF: We will proceed on induction on the order of the group. If the order of the group is 2, then the theorem is true since the group would be isomorphic to  $Z_2$ . Let  $G$  be a finite abelian group and suppose the theorem is true for all groups of order less than  $G$ . Let  $p$  be a prime that divides the order of  $G$ . By Lemma 7.3,  $G \approx P \times K$ , where  $P$  is the subgroup of  $G$  containing the elements of order  $p^m$  for some  $m$ .

Furthermore, if  $x$  is an element of maximal order in  $P$ , and  $X$  is the group generated by  $x$ , then by Lemma 7.4,  $G \approx X \times T \times K$ . Since  $X$  will be a nontrivial cyclic group, the orders of  $T$  and  $K$  will be less than  $|G|$ . Thus, by induction,  $T$  and  $K$  can be written as a direct product of cyclic groups whose orders are powers of primes. Since  $X$  is also a cyclic group of order  $p^r$  for some  $r$ ,  $G$  can be written as a direct product of cyclic groups whose orders are powers of primes.

We next have to show that this decomposition is *unique*. Using Lemma 7.6, the number of times  $Z_{(p^x)}$  appears in the decomposition is given by

$$2 \log_p(R_{p^x}(G)) - \log_p(R_{p^{x-1}}(G)) - \log_p(R_{p^{x+1}}(G)),$$

which is determined by the group  $G$ . Thus, the decomposition of  $G$  as a direct product of cyclic groups of the form  $Z_{(p^x)}$  is unique.  $\square$

From this theorem, we can easily find all non-isomorphic abelian groups of a given order. For example, to find all non-isomorphic abelian groups of order 16, we note that all such groups are direct products of the cyclic groups of orders 2, 4, 8, or 16. We want to find all possible combinations of 2, 4, 8, and 16 which will multiply to give 16. With a little experimenting, we find that there are five such combinations:

$$2 \cdot 2 \cdot 2 \cdot 2, \quad 2 \cdot 2 \cdot 4, \quad 4 \cdot 4, \quad 2 \cdot 8, \quad \text{and} \quad 16.$$

Thus, there are 5 possible abelian groups of order 16:

$$Z_2 \times Z_2 \times Z_2 \times Z_2, \quad Z_2 \times Z_2 \times Z_4, \quad Z_4 \times Z_4, \quad Z_2 \times Z_8, \quad \text{and} \quad Z_{16}.$$

Since the fundamental theorem (7.2) also states that the representation is unique, these five groups must be non-isomorphic to each other. Notice that there is a correlation between these five groups, and the five ways we can express the number 4 as a sum of positive integers:

$$1 + 1 + 1 + 1 = 4$$

$$1 + 1 + 2 = 4$$

$$2 + 2 = 4$$

$$1 + 3 = 4$$

$$4 = 4$$

This leads us to a way of finding the number of non-isomorphic groups of order  $p^m$  for any  $m$ .

### COROLLARY 7.2

Let  $P(m)$  denote the number of ways in which  $m$  can be expressed as a sum of positive integers, without regard to order. Then if  $p$  is a prime number, there are exactly  $P(m)$  non-isomorphic abelian groups of order  $p^m$ .

PROOF: By the fundamental theorem of abelian groups (7.2), every abelian group of order  $p^m$  must be isomorphic to

$$Z_{(p^{h_1})} \times Z_{(p^{h_2})} \times Z_{(p^{h_3})} \times \cdots \times Z_{(p^{h_n})}.$$

Also,

$$p^{h_1} \cdot p^{h_2} \cdot p^{h_3} \cdots p^{h_n} = p^m.$$

Hence  $h_1 + h_2 + h_3 + \cdots + h_n = m$ . Furthermore, the decomposition of the abelian group is unique up to rearrangement of the factors. Thus, there is a one-to-one correspondence between non-isomorphic abelian groups of order  $p^m$  and ways  $m$  can be written as a sum of positive integers without regard to order.  $\square$

We call  $P(m)$  the number of *partitions* of  $m$ . We can have *SageMath* count the number of partitions for us. For example, to find the number of partitions of the number 4, we can enter

**PartitionsP(4)**

5

to find that there are five groups of order  $2^4$ . We can even have *SageMath* list all of the partitions.

```
[i for i in Partition(4)]
[[4], [3, 1], [2, 2], [2, 1, 1], [1, 1, 1, 1]]
```

Table 7.2 gives the number of partitions  $P(m)$ . The number of partitions increases exponentially with  $m$ ; in fact a *SageMath* plot reveals that it grows approximately like the function  $e^{\sqrt{m}}$ . See Problem 21.

**TABLE 7.2:** Partitions for  $m \leq 15$ 

|            |              |               |
|------------|--------------|---------------|
| $P(1) = 1$ | $P(6) = 11$  | $P(11) = 56$  |
| $P(2) = 2$ | $P(7) = 15$  | $P(12) = 77$  |
| $P(3) = 3$ | $P(8) = 22$  | $P(13) = 101$ |
| $P(4) = 5$ | $P(9) = 30$  | $P(14) = 135$ |
| $P(5) = 7$ | $P(10) = 42$ | $P(15) = 176$ |

We can now find the number of non-isomorphic abelian groups of any order.

### COROLLARY 7.3

Let  $m > 1$  be an integer with prime factorization

$$p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} \cdots p_n^{h_n},$$

where  $p_1, p_2, p_3, \dots, p_n$  are distinct primes. Then the number of non-isomorphic abelian groups of order  $m$  is given by

$$P(h_1) \cdot P(h_2) \cdot P(h_3) \cdots P(h_n).$$

PROOF: We know from the fundamental theorem of abelian groups (7.2) that each such group is isomorphic to a direct product of cyclic groups whose order is a power of a prime. If we collect all factors involving the same primes together, we find that such a group is isomorphic to a direct product of a series of groups of orders  $p_1^{h_1}$ ,  $p_2^{h_2}$ ,  $p_3^{h_3}$ , ..., and  $p_n^{h_n}$ .

We know from Corollary 7.2 that there are exactly  $P(x)$  non-isomorphic abelian groups of order  $p^x$ . Thus, there are  $P(h_i)$  possible groups for the  $i^{\text{th}}$  factor in this decomposition. Therefore, there are

$$P(h_1) \cdot P(h_2) \cdot P(h_3) \cdots P(h_n)$$

possible ways of forming a product of groups with orders

$$p_1^{h_1}, p_2^{h_2}, p_3^{h_3}, \dots, \text{ and } p_n^{h_n}.$$

Since the fundamental theorem of abelian groups (7.2) also states that the decomposition is unique up to the rearrangement of the factors, every group thus formed is isomorphically different. So we have exactly  $P(h_1) \cdot P(h_2) \cdot P(h_3) \cdots P(h_n)$  non-isomorphic abelian groups of order  $m$ .  $\blacksquare$

### Computational Example 7.4

Suppose we wish to find the number of non-isomorphic abelian groups of order 180 billion. Since  $180,000,000,000 = 2^{11} \cdot 3^2 \cdot 5^{10}$ , we have that the number of groups is

**PartitionsP(11) \* PartitionsP(2) \* PartitionsP(10)**

4704

giving us 4704 abelian groups of order 180 billion.  $\blacksquare$

From these two corollaries, we see that all finite abelian groups have been classified. One of the outstanding problems in group theory is to classify all finite groups. This is as yet an unsolved problem although much progress has been made through the use of computers. In the next section we will show another ways of generating larger groups which have become a key to some of the recent work that has been done in group theory.

### Problems for §7.2

- 1** Let  $n$  be any integer greater than 1. Prove that  $Z_n \times Z_n$  is not isomorphic to  $Z_{n^2}$ .
- 2** Let  $G$  be an abelian group with order  $mn$ , where  $m$  and  $n$  are coprime. Prove that  $R_m(G) = m$  and  $R_n(G) = n$ .  
Hint: Use Lemma 7.1 and the strategy of Lemma 7.3.

For Problems **3** through **11**: Find, up to isomorphism, all abelian groups of the following orders:

- |                      |                      |                       |
|----------------------|----------------------|-----------------------|
| <b>3</b> $ G  = 32$  | <b>6</b> $ G  = 300$ | <b>9</b> $ G  = 600$  |
| <b>4</b> $ G  = 200$ | <b>7</b> $ G  = 450$ | <b>10</b> $ G  = 675$ |
| <b>5</b> $ G  = 210$ | <b>8</b> $ G  = 500$ | <b>11</b> $ G  = 900$ |

- 12** What is the smallest positive integer  $n$  for which there are exactly four non-isomorphic abelian groups of order  $n$ ?
- 13** Calculate the number of elements of order 4 in the groups  
 $Z_{16}$ ,     $Z_8 \times Z_2$ ,     $Z_4 \times Z_4$ ,    and     $Z_4 \times Z_2 \times Z_2$ .
- 14** How many elements of order 25 are in  $Z_5 \times Z_{25}$ ? (Do not do this exercise by brute force.)
- 15** An abelian group  $G$  of order 256 has 1 element of order 1, 7 elements of order 2, 24 elements of order 4, 96 elements of order 8, and 128 elements of order 16. Determine up to isomorphism the group  $G$  as a direct product of cyclic groups.  
Hint: First use the information given to find  $R_n(G)$  when  $n$  is a power of 2. Then use Lemma 7.6 to determine how many times  $Z_2$ ,  $Z_4$ ,  $Z_8$ , and  $Z_{16}$  appear in the decomposition.
- 16** An abelian group  $G$  of order 512 has 1 element of order 1, 15 elements of order 2, 112 elements of order 4, 128 elements of order 8, and 256 elements of order 16. Determine up to isomorphism the group  $G$  as a direct product of cyclic groups. See the hint for Problem 15.

## Historical Diversion

# Augustin Cauchy (1789–1857)

Augustin Cauchy was born in Paris, and by the time he was 11, both Laplace and Lagrange had recognized his potential. Lagrange told Laplace, “You see that little young man? He will supplant all of us in so far as we are mathematicians.” On Lagrange’s advice, Cauchy was enrolled in the best secondary school in Paris at the time, the École Centrale du Panthéon. In spite of his many awards in Latin and Humanities, Cauchy chose an engineering career.

At 21, he was given a commission as a civil engineer in Napoleons army. But during this job, Cauchy was doing mathematics on the side, submitting three manuscripts to the Première Classe. In 1812, he became ill from overwork, and returned to Paris to find a mathematical position.

By 1815 Cauchy was recognized as the leading mathematician in France, and was given an appointment at the École Polytechnique. Cauchy, along with Gauss, are considered to be the last two mathematicians to know all known mathematics at their time. Cauchy made contributions to almost every branch of mathematics. He was the first to prove Taylor’s theorem using a remainder term. He was the first to define a complex function of a complex variable. He also worked with permutation groups, proving that if a prime  $p$  divides the order of a group, then some element is of order  $p$ . He introduced a new level of rigor in his proofs, which served as a model for the next generation of mathematicians.

During the French revolution of 1830, when Louis-Philippe succeeded Charles X, Cauchy fled to Fribourg, Switzerland, leaving his family behind. Because he refused to swear an oath of allegiance to the new regime, he lost almost all of his positions in Paris. In 1831, the King of Sardinia offered him a chair of theoretical physics in Turin. In 1833 he left Turin to go to Prague, to become a science tutor of the grandson of Charles X, the thirteen-year old Duke Henri d’Artois. Unfortunately, the Duke acquired a dislike of mathematics, and Cauchy did very little mathematics during these years, although he was promoted to Baron. In 1834, his wife and two daughters joined Cauchy in Prague, and his family was finally reunited.

Cauchy returned to Paris in 1838, but could not secure a position because he still refused to take an oath. In 1848, another revolution broke out, and the oath of allegiance was abolished, allowing Cauchy to have an academic appointment. In 1849, he was reinstated as a professor of mathematical astronomy at the Faculté de Sciences. During these final years, until his death in 1857, Cauchy wrote more than 500 research papers.



- 17** If an abelian group  $G$  of order 40 has exactly three elements of order 2, determine up to isomorphism the group  $G$ .
- 18** Classify the integers  $n$  for which the only abelian groups of order  $n$  are cyclic.
- 19** Recall from Problem 19 from §6.2 that the cycle structure of a permutation is the number of 2-cycles, 3-cycles, etc. it contains when written as a product of disjoint cycles. Show that the number of possible cycle structures in  $S_n$  is  $P(n)$ .

### Interactive Problems

- 20** Use *SageMath*'s **PartitionsP** command to find the number of abelian groups of order 120,000,000.
- 21** Notice that the logarithm of the **PartitionsP** function looks like a sideways parabola.

```
s = list_plot([ln(PartitionsP(i)) for i in range(999)]); s
```

This indicates that the **PartitionsP** function grows like  $e^{c\sqrt{n}}$  for some constant  $c$ . Here is a way we can plot a sideways parabola on top of the above graph.

```
var("x")
P = plot(1.0 * sqrt(x), [x, 1, 999]); P + s
```

Try varying the constant 1.0 until the curves seem to run parallel to each other. Approximately what is this constant?

## 7.3 Automorphisms

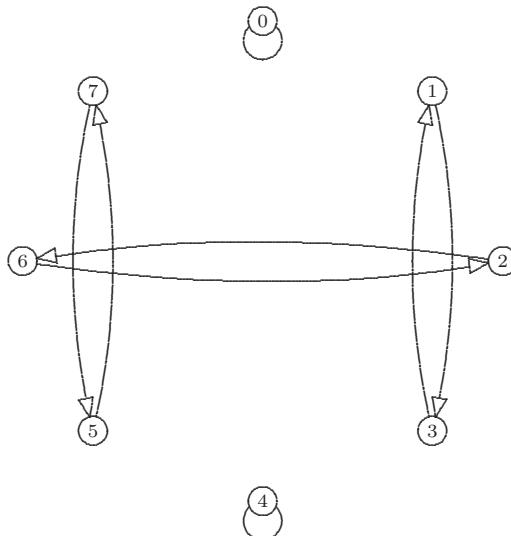
We have already studied several examples of homomorphisms and isomorphisms *between* two groups, but suppose we considered a mapping from a group *to itself*.

### **Motivational Example 7.5**

Find an isomorphism from  $Z_8$  onto itself.

We can consider the following mapping:

```
z8 = ZGroup(8)
CircleGraph(z8, Pow(3))
```



**FIGURE 7.1:**  $x \rightarrow x^3$  in  $Z_8$

which produces Figure 7.1. This mapping could be considered as the permutation  $(1\ 3)(2\ 6)(5\ 7)$  since the element 0 is left fixed. However, to make this into a homomorphism in *SageMath*, we have to define a mapping that sends `z8[1]` to `z8[3]`.

```

F = Homomorph(Z8, Z8)
HomoDef(F, Z8[1], Z8[3])
FinishHomo(F)
'Homomorphism defined'

```

The circle graph of **F** will be the same as Figure 7.1, which shows that in fact the homomorphism is one-to-one and onto.  $\square$

We give such a homomorphism a special name.

**DEFINITION 7.3** An *automorphism* of the group  $G$  is a homomorphism from  $G$  to  $G$  which is one-to-one and onto.

If we study the above automorphism  $f$  on  $Z_8$ , we discover why this works. Recall that the operation of this group is addition modulo 8. Hence the mapping  $x \rightarrow x^3$  in  $Z_8$  will send each number  $x$  to  $(3x) \bmod 8$ . Therefore,

$$f(x \cdot y) = f((x+y) \bmod 8) = (3(x+y)) \bmod 8 = (3x+3y) \bmod 8 = f(x) \cdot f(y).$$

By observing this pattern, we can find another automorphism of  $Z_8$  by sending  $x$  to  $x^5$  instead of  $x^3$ . In fact, it is possible to define the product of two automorphisms as follows: If  $f$  and  $\phi$  are both automorphisms of  $G$ , then  $f \cdot \phi$  is the mapping  $x \rightarrow f(\phi(x))$ . This leads us to the proof of the following.

### **PROPOSITION 7.3**

*Given a group  $G$ , the set of all automorphisms on  $G$  forms a group, denoted  $\text{Aut}(G)$ . In fact,  $\text{Aut}(G)$  is a subgroup of the group of permutations on the elements of  $G$ .*

**PROOF:** The mapping  $i(x) = x$  for all  $x$  in  $G$  is obviously an automorphism on  $G$ , so the set of all automorphisms on  $G$  is non-empty. Also, each automorphism is a permutation on the elements of  $G$ . Suppose  $\phi$  and  $f$  are two automorphisms on  $G$ . Then  $\phi(f(x))$  is a one-to-one and onto mapping from  $G$  to  $G$ .

Furthermore,

$$\phi(f(x \cdot y)) = \phi(f(x) \cdot f(y)) = \phi(f(x)) \cdot \phi(f(y)).$$

So  $\phi(f(x))$  is a homomorphism on  $G$ , so  $\phi \cdot f$  is an automorphism of  $G$ .

Also, since  $f$  is one-to-one and onto,  $f^{-1}$  exists on  $G$ , and

$$f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = x \cdot y.$$

Taking  $f^{-1}$  of both sides of the equation gives us

$$f^{-1}(x) \cdot f^{-1}(y) = f^{-1}(x \cdot y).$$

So  $f^{-1}$  is a homomorphism. Hence both  $f^{-1}$  and  $\phi \cdot f^{-1}$  are automorphisms of  $G$ . Therefore by Proposition 3.2,  $\text{Aut}(G)$  is a subgroup of the group of permutations on the elements of  $G$ . □

### **Example 7.6**

Find the automorphism group for  $Z_8$ .

**SOLUTION:** The element 1 must be mapped by an automorphism to an element of order 8. Thus, 1 is mapped to either 1, 3, 5, or 7. But since 1 is a generator of  $Z_8$ , this would completely define the automorphism. Thus, there at most four elements of  $\text{Aut}(Z_8)$ . But besides the identity mapping, we can easily find three other automorphisms:

$$x \rightarrow x^3, \quad x \rightarrow x^5, \quad \text{and} \quad x \rightarrow x^7.$$

So we have exactly four automorphisms of  $Z_8$ . By converting these mappings to permutations on the non-zero elements of  $Z_8$ , we can express the automorphism group as

$$\{P(), P(3, 6, 1, 4, 7, 2, 5), P(5, 2, 7, 4, 1, 6, 3), P(7, 6, 5, 4, 3, 2, 1)\}.$$

This automorphism group can quickly be seen to be isomorphic to  $Z_8^*$ . □

It is not hard to generalize this result.

#### **PROPOSITION 7.4**

$$\text{Aut}(Z_n) \approx Z_n^*.$$

PROOF: Consider the mapping

$$\psi : Z_n^* \rightarrow \text{Aut}(Z_n)$$

given by  $\psi(j) = f_j$ , where  $f_j(x) = (jx) \bmod n$ . Then given two elements  $j$  and  $k$  in  $Z_n^*$ , we have that

$$f_j(f_k(x)) = (j \cdot (k \cdot x)) \bmod n = ((j \cdot k) \cdot x) \bmod n = f_{j \cdot k}(x).$$

So

$$\psi(j) \cdot \psi(k) = f_j(f_k) = f_{j \cdot k} = \psi(j \cdot k).$$

Hence,  $\psi$  is a homomorphism from  $Z_n^*$  to  $\text{Aut}(Z_n)$ . To see that  $\psi$  is one-to-one, we note that  $f_j(1) = j$ , and so  $f_j = f_k$  only if  $j = k$ .

To see that  $\psi$  is onto, we can use the pigeon-hole principle. If we consider a general automorphism  $f$  of  $Z_n$ , then  $f(1)$  must be a generator of  $Z_n$ , since 1 is a generator. But  $f$  will be completely determined by knowing  $f(1)$ . Thus, the number of automorphisms is at most the number of generators of  $Z_n$ , which is  $\phi(n)$ . Since  $|Z_n^*| = \phi(n)$ , we know the function is one-to-one, so it must also be onto. □

So far, the automorphism group is smaller than the original group, but the goal of this chapter is to form larger groups. Let us consider a non-cyclic group.

#### **Example 7.7**

Find the automorphism group of the group  $Z_8^*$ , which has the following Cayley table.

| . | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

SOLUTION: A good strategy for finding all of the automorphisms is to first determine an upper bound for the number of automorphisms. Suppose  $f$  is an automorphism. Then  $f(1) = 1$ , but all other elements are of order 2. Hence, any of the other elements might map to each other in any way. For example,  $f(3)$  might be 3, 5, or 7. Once we know where 3 is mapped,  $f(5)$  might be either of the other two elements. However, once we know  $f(3)$  and  $f(5)$ , then  $f(7)$  must be  $f(3) \cdot f(5)$ . Thus, there are at most  $3 \cdot 2 = 6$  elements of  $\text{Aut}(Z_8^*)$ . If we find that there are indeed this many automorphisms, then  $\text{Aut}(Z_8^*)$  would be larger than  $Z_8^*$ .

Here is one possible automorphism.

$$\begin{aligned}f(1) &= 1 \\f(3) &= 5 \\f(5) &= 3 \\f(7) &= 7\end{aligned}$$

This can be represented as a transposition  $(3\ 5)$ . Note that here, we are using the cycle notation with *elements* in place of numbers. We can test to see if this is an automorphism by constructing the Cayley table with the new ordering, and see if it has the same “color pattern.” The new table is on the left side.

| . | 1 | 5 | 3 | 7 | . | 1 | 3 | 7 | 5 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 3 | 7 | 1 | 1 | 3 | 7 | 5 |
| 5 | 5 | 1 | 7 | 3 | 3 | 3 | 1 | 5 | 7 |
| 3 | 3 | 7 | 1 | 5 | 7 | 7 | 5 | 1 | 3 |
| 7 | 7 | 3 | 5 | 1 | 5 | 5 | 7 | 3 | 1 |

We can also ask whether there is an automorphism that sends 3 to 3, but exchanges 5 to 7, giving us the transposition  $(5\ 7)$ . The new Cayley table is shown above on the right. Both of these tables preserve the color pattern of the original Cayley table, so both are automorphisms. These two automorphism will generate a copy of  $S_3$ , which gives 6 automorphisms. Since we established that this is the maximum number of automorphisms for  $Z_8^*$ , we have found the entire automorphism group. Hence  $\text{Aut}(Z_8^*) \approx S_3$ . □

For non-commutative groups, there is a quick way to find many of the automorphisms. Let  $G$  be a non-commutative group, and let  $x$  be any element

in  $G$ . The mapping  $f_x : G \rightarrow G$  defined by

$$f_x(y) = x \cdot y \cdot x^{-1}$$

will always be an automorphism, for

$$f_x(y \cdot z) = x \cdot y \cdot z \cdot x^{-1} = (x \cdot y \cdot x^{-1}) \cdot (x \cdot z \cdot x^{-1}) = f_x(y) \cdot f_x(z).$$

So  $f_x(y)$  is a homomorphism. Since the inverse homomorphism can easily be found,

$$y \in f_x^{-1}(v) \iff x \cdot y \cdot x^{-1} = v \iff y = x^{-1} \cdot v \cdot x \iff y = f_{x^{-1}}(v),$$

we have that  $f_x(y)$  is one-to-one and onto, therefore  $f_x(y)$  is an automorphism.

**DEFINITION 7.4** An automorphism  $\phi(y)$  of a group  $G$  is called an *inner automorphism* if there is an element  $x$  in  $G$  such that

$$\phi(y) = x \cdot y \cdot x^{-1} \quad \text{for all } y \in G.$$

The set of inner automorphisms of  $G$  is denoted  $\text{Inn}(G)$ .

### Example 7.8

Find the inner automorphisms of the quaternion group

$$Q = \{1, i, j, k, -1, -i, -j, -k\}.$$

SOLUTION: Let us begin by determining an upper bound for the number of automorphisms. If  $f$  is an automorphism of  $Q$ , then  $f(1) = 1$  but also  $f(-1)$  must be  $-1$ , since this is the only element of order 2. All of the other elements are of order 4, so  $f(i)$  could be any one of the remaining six elements. Once  $f(i)$  is determined, we have that  $f(-i) = f(i)^3$ . Then  $f(j)$  could be one of the remaining four elements. Since  $i$  and  $j$  generate  $Q$ ,  $f$  will be determined by knowing  $f(i)$  and  $f(j)$ . Thus, there is a maximum of  $6 \cdot 4 = 24$  automorphisms.

It is fairly easy to find the inner automorphisms on  $Q$ . If we choose  $x = i$ , we have the mapping

$$\begin{array}{ll} f(1) = i \cdot 1 \cdot (-i) = 1 & f(-1) = i \cdot (-1) \cdot (-i) = -1 \\ f(i) = i \cdot i \cdot (-i) = i & f(-i) = i \cdot (-i) \cdot (-i) = -i \\ f(j) = i \cdot j \cdot (-i) = -j & f(-j) = i \cdot (-j) \cdot (-i) = j \\ f(k) = i \cdot k \cdot (-i) = -k & f(-k) = i \cdot (-k) \cdot (-i) = k \end{array}$$

We can express this automorphism in terms of cycles:  $(j, -j)(k, -k)$ . If we use  $x = j$  or  $x = k$  instead of  $x = i$ , we get the automorphisms  $(i, -i)(k, -k)$  and  $(i, -i)(j, -j)$ . These three automorphisms, along with the identity automorphism, form a group. These are the only 4 inner automorphisms.  $\square$

Although we were able to find the inner automorphisms by hand, we will need *SageMath*'s help to find the rest of the automorphisms.

### Computational Example 7.9

Determine the automorphism group of  $Q$ .

With a bit of trial and error, we can come up with a new automorphism.

```
Q = InitQuaternions(); Q
{1, i, j, k, -1, -i, -j, -k}
X = Homomorph(Q, Q)
HomoDef(X, i, i)
HomoDef(X, j, k)
FinishHomo(X)
'Homomorphism defined'
```

This homomorphism from  $Q$  to itself can be shown to be one-to-one and onto. In fact, it can be represented by the cycle  $(j, k, -j, -k)$ . Also, the commands

```
Y = Homomorph(Q, Q)
HomoDef(Y, i, k)
HomoDef(Y, j, j)
FinishHomo(Y)
'Homomorphism defined'
```

show that there is yet another automorphism on  $Q$ , which can be represented by  $(i, k, -i, -k)$ . These two automorphisms, along with the group of 4 inner automorphisms, generate a total of 24 automorphisms.

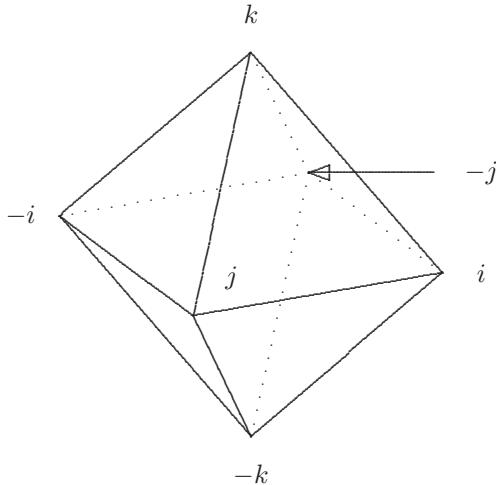
```
A = Group( C(j, -j)*C(k, -k), C(i, -i)*C(k, -k),
C(j, k, -j, -k), C(i, k, -i, -k) ); A
{(), (-i, -j)(-k, k)(j, i), (-i, -j, -k)(k, i, j),
 (-i, -j, k)(-k, i, j), (-i, -j, i, j), (-i, -k)(-j, j)(k, i),
 (-i, -k, -j)(k, j, i), (-i, -k, j)(-j, i, k), (-i, -k, i, k),
 (-i, k)(-j, j)(-k, i), (-i, k, -j)(-k, j, i),
 (-i, k, j)(-j, i, -k), (-i, k, i, -k), (-i, j)(-j, i)(-k, k),
 (-i, j, -k)(-j, k, i), (-i, j, k)(-j, -k, i), (-i, j, i, -j),
 (-i, i)(-j, -k)(k, j), (-i, i)(-j, k)(-k, j), (-i, i)(-j, j),
 (-i, i)(-k, k), (-j, -k, j, k), (-j, k, j, -k),
 (-j, j)(-k, k)}
```

Notice that *SageMath* allows group elements inside of cycles. We can see that the inner automorphisms are embedded in this list. What is this group isomorphic to?

In fact,  $\text{Aut}(Q) \approx S_4$ , as can be seen by [Figure 7.2](#). Each rotation of the octahedron represents an automorphism of  $Q$ . For example, rotating the front face  $120^\circ$  clockwise corresponds to the automorphism

$$(i, j, k)(-i, -j, -k).$$

So the automorphism group is isomorphic to the octahedral group, which we saw was isomorphic to  $S_4$ .  $\square$



**FIGURE 7.2:** Labeling the octahedron to show  $\text{Aut}(Q) \approx S_4$

Although the inner automorphisms did not produce the full automorphism group, this set of inner automorphisms turns out to be a very important subgroup of the automorphism group. Let us discover the first main property of this subgroup.

### PROPOSITION 7.5

Let  $G$  be a group. Then  $\text{Inn}(G)$  is a normal subgroup of  $\text{Aut}(G)$ .

PROOF: First we need to show that  $\text{Inn}(G)$  is a subgroup. Let

$$f_x(y) = x \cdot y \cdot x^{-1}$$

be an inner automorphism. The inverse can be easily found by observing

$$y \in f_x^{-1}(v) \iff x \cdot y \cdot x^{-1} = v \iff y = x^{-1} \cdot v \cdot x \iff y = f_{(x^{-1})}(v),$$

so the inverse of  $f_x$  is also an inner automorphism.

If we consider two inner automorphisms  $f_x$  and  $f_y$ , then

$$(f_x \cdot f_y)(v) = f_x(f_y(v)) = x \cdot (y \cdot v \cdot x^{-1}) \cdot y^{-1} = (x \cdot y) \cdot v \cdot (x \cdot y)^{-1} = f_{(x \cdot y)}(v).$$

Thus the product of two inner automorphisms is also an inner automorphism. So by Proposition 3.2,  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$ .

Finally, we need to show that  $\text{Inn}(G)$  is normal in  $\text{Aut}(G)$ . Let  $\phi$  be any automorphism and let  $f_x = x \cdot y \cdot x^{-1}$  be an inner automorphism. Then

$$(\phi \cdot f_x \cdot \phi^{-1})(v) = \phi(f_x(\phi^{-1}(v))) = \phi(x \cdot (\phi^{-1}(v)) \cdot x^{-1}).$$

Since  $\phi$  is a homomorphism, this will simplify.

$$\begin{aligned} \phi(x \cdot (\phi^{-1}(v)) \cdot x^{-1}) &= \phi(x) \cdot \phi(\phi^{-1}(v)) \cdot \phi(x^{-1}) \\ &= \phi(x) \cdot v \cdot [\phi(x)]^{-1} = f_{\phi(x)}(v). \end{aligned}$$

So  $\phi \cdot f_x \cdot \phi^{-1}$  is an inner automorphism of  $G$ . Therefore, by Proposition 4.4,  $\text{Inn}(G)$  is a normal subgroup of  $\text{Aut}(G)$ .  $\square$

For example, we found four inner automorphisms of  $Q$ . All of them but the identity were of order 2. Thus, we see that  $\text{Inn}(Q) \approx Z_8^*$ .

Because the inner automorphism group is always a normal subgroup, we could consider the quotient group.

**DEFINITION 7.5** We define the *outer automorphism group* to be the quotient group

$$\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G).$$

The outer automorphism group of  $Q$  must contain six elements, and with some experimenting in *SageMath*, one finds that  $\text{Out}(Q)$  is non-abelian. Therefore,  $\text{Out}(Q) \approx S_3$ .

If  $G$  is an abelian group, then the only inner automorphism is the identity automorphism. Thus, for abelian groups,

$$\text{Inn}(G) \approx \{e\} \quad \text{and} \quad \text{Out}(G) \approx \text{Aut}(G).$$

Let us look at one last example, which will create a huge group.

### Computational Example 7.10

Find the automorphism group of  $Z_{24}^*$ .

SOLUTION: Rather than using **zStar(24)**, we will consider this group as  $Z_2 \times Z_2 \times Z_2$  so we can see the relationship with the generators. We can load this group into *SageMath* with the following commands:

```
InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e); Define(b^2, e); Define(c^2, e)
Define(b*a, a*b); Define(c*a, a*c); Define(c*b, b*c)
Y = Group(a, b, c); Y
{e, a, b, a*b, c, a*c, b*c, a*b*c}
```

Once again, we will begin by determining an upper bound for the number of automorphisms. Suppose  $\phi(x)$  is an automorphism of  $Z_{24}^*$ . Naturally  $\phi(e) = e$ , but  $\phi(a)$  could be any of the seven remaining elements of order 2. Also,  $\phi(b)$  could be any one of the remaining six elements. Then we would have  $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ , so four elements will be accounted for. But  $\phi(c)$  could be any of the four elements left over. Since the group is generated by  $\{a, b, c\}$ , there are at most  $7 \cdot 6 \cdot 4 = 168$  possible automorphisms.

One possible automorphism would be to send  $a$  to  $b$ ,  $b$  to  $c$ , and  $c$  back to  $a$ .

```
F = Homomorph(Y, Y)
HomoDef(F, a, b)
HomoDef(F, b, c)
HomoDef(F, c, a)
FinishHomo(F)
'Homomorphism defined'
```

which *SageMath* verifies is an automorphism. Another automorphism, given by

```
G = Homomorph(Y, Y)
HomoDef(G, a, a)
HomoDef(G, b, a*b)
HomoDef(G, c, c)
FinishHomo(G)
'Homomorphism defined'
```

indicates that there may indeed be many automorphisms.

It would be more concise if we could use permutations for a group this large. If we number the non-identity elements in the order they appear in the group list, we have  $a = 1$ ,  $b = 2$ ,  $a \cdot b = 3$ ,  $c = 4$ ,  $a \cdot c = 5$ ,  $b \cdot c = 6$ , and  $a \cdot b \cdot c = 7$ . With this ordering we can convert  $F$  and  $G$  to standard permutations  $(1\ 2\ 4)(3\ 5\ 6)$  and  $(2\ 3)(6\ 7)$ . That is,  $F$  maps element 1 ( $a$ ) to element 2 ( $b$ ), which is mapped to element 4 ( $c$ ), etc. Likewise,  $G$  exchanges the 2nd and 3rd elements, and exchanges the 6th and 7th elements of  $Z_{24}^*$ . Once we have all of the elements as permutations, we can use the integer notation feature to list them.

```
f = CycleToPerm( C(1, 2, 4)*C(3, 6, 5) ); f
P(2, 4, 6, 1, 3, 5)
g = CycleToPerm( C(2, 3)*C(6, 7) ); g
P(1, 3, 2, 4, 5, 7, 6)
DisplayPermInt = true
A = Group(f, g); A
{1, 27, 61, 87, 122, 149, 187, 231, 244, 270, 331, 357, 374,
 404, 437, 467, 496, 548, 558, 593, 640, 670, 684, 714, 723,
 745, 783, 805, 844, 870, 931, 957, 962, 989, 1027, 1071,
```

1096, 1148, 1158, 1193, 1214, 1244, 1277, 1307, 1366, 1384, 1410, 1428, 1445, 1466, 1509, 1549, 1566, 1588, 1653, 1675, 1681, 1707, 1741, 1767, 1822, 1862, 1889, 1902, 1966, 1984, 2010, 2028, 2054, 2084, 2117, 2147, 2166, 2188, 2253, 2275, 2285, 2306, 2349, 2389, 2403, 2425, 2463, 2485, 2566, 2584, 2610, 2628, 2662, 2702, 2729, 2742, 2780, 2798, 2843, 2861, 2897, 2927, 2954, 2984, 3018, 3071, 3076, 3110, 3144, 3185, 3206, 3220, 3288, 3306, 3328, 3346, 3361, 3387, 3421, 3447, 3487, 3517, 3531, 3561, 3618, 3671, 3676, 3710, 3737, 3767, 3794, 3824, 3888, 3906, 3928, 3946, 3984, 4025, 4046, 4060, 4083, 4105, 4143, 4165, 4213, 4231, 4257, 4275, 4362, 4392, 4402, 4432, 4488, 4506, 4528, 4546, 4577, 4607, 4634, 4664, 4703, 4721, 4760, 4778, 4809, 4839, 4849, 4879, 4935, 4953, 4975, 4993}

**len(A)**

168

Since this gives us 168 elements, we know we have all of the automorphisms. Notice that *SageMath* orders the numbers, making it easier to find a particular element. In particular, the elements  $f$  and  $g$  are found to be

**f**

187

**g**

723

So the group  $\text{Aut}(Z_{24}^*)$  is generated by the 187th and 723rd permutations. This group has special properties we will explore in the next chapter.  $\square$

We have now seen several examples where the group of automorphisms is larger than the original group. But this group of automorphisms can also be used as a tool for connecting two groups to form an even larger group, in much the same way that two groups formed the direct product. The next section will explore this methodology.

### Problems for §7.3

For Problems 1 through 6: Determine an upper bound for the size of the automorphism group for the following groups. It helps to first determine how many elements there are of each order.

**1**  $S_3$

**2**  $D_4$

**3**  $Z_{15}^*$

**4**  $Z_6 \times Z_2$

**5**  $Z_3 \times Z_3$

**6**  $Z_2 \times Z_2 \times Z_2 \times Z_2$

**7** Prove that if  $G$  is a finite group of order  $n$ , then  $\text{Aut}(G)$  is isomorphic to a subgroup of  $S_{n-1}$ .

**8** Prove that if  $G$  non-abelian, then there is an inner automorphism that is not trivial.

**9** Prove that if  $G$  abelian, and there is an element of  $G$  with an order greater than 2, then  $\phi(x) = x^{-1}$  is a non-trivial automorphism.

**10** Prove that any finite group of order greater than 2 has at least two automorphisms.

Hint: The only groups not covered by Problems 8 and 9 are isomorphic to  $Z_2 \times Z_2 \times \cdots \times Z_2$ .

**11** Prove that if  $G$  is not abelian, then  $\text{Aut}(G)$  is not cyclic.

**12** Find all of the inner automorphisms of  $S_3$ . Use cycle notation for the automorphisms, as we did for Example 7.8. The Cayley table for  $S_3$  is on page 79.

**13** Find all of the inner automorphisms of  $D_4$ . Use cycle notation for the automorphisms, as we did for Example 7.8. The Cayley table for  $D_4$  is on page 132.

**14** Show that for the group  $D_4$ , there is an automorphism with  $\phi(a) = a$  and  $\phi(b) = a \cdot b$ . Show that the Cayley table with the new ordering of elements created by the automorphism has the same “color pattern” as the table on page 132.

**15** Find the automorphism group of  $S_3$ . See Problem 12.

**16** Find the automorphism group of  $D_4$ . See Problems 13 and 14.

**17** Find  $\text{Aut}(\mathbb{Z})$ .

**18** Find two non-isomorphic groups  $G$  and  $M$  for which  $\text{Aut}(G) \approx \text{Aut}(M)$ .

### Interactive Problems

For Problems **19** through **21**: Find all of the automorphisms of the following groups.

**19**  $Z_{15}^*$

**20**  $Z_{21}^*$

**21**  $D_5$

**22** Find all of the automorphisms of the group  $Z_3 \times Z_3$ . Because of the large number of automorphisms, it is useful to number the non-identity elements of the group as we did for  $\text{Aut}(Z_{24}^*)$  in Example 7.10.

## 7.4 Semi-Direct Products

We have already seen one way to combine two groups  $H$  and  $K$  to form the direct product  $H \times K$ . In this section, we will see another way to combine two groups  $H$  and  $K$ . Once again the larger group will have isomorphic copies of  $H$  and  $K$  as subgroups, but only *one* of the two subgroups will be a normal subgroup.

Suppose that  $H$  and  $K$  are any two groups, and suppose that we have a homomorphism  $\phi : H \rightarrow \text{Aut}(K)$ . Because the function  $\phi$  returns another function, we will write  $\phi_h$  instead of  $\phi(h)$ . The expression  $\phi_h(k)$  represents the automorphism  $\phi_h$  evaluated at the element  $k$ . That is, if  $h_1$  and  $h_2$  are two elements of  $H$ , then  $\phi_{h_1}(k)$  and  $\phi_{h_2}(k)$  will be two automorphisms of  $K$ , and also  $\phi_{h_1 \cdot h_2}(k) = (\phi_{h_1} \cdot \phi_{h_2})(k) = \phi_{h_1}(\phi_{h_2}(k))$ . (Recall that  $\phi_{h_1} \cdot \phi_{h_2}$  means we do  $\phi_{h_2}$  first, then do  $\phi_{h_1}$ .)

There will always be at least one homomorphism from  $H$  to  $\text{Aut}(K)$ , the trivial homomorphism. However, there will often be several nontrivial homomorphisms from  $H$  to  $\text{Aut}(K)$ . For each such homomorphism, we can define a product of  $H$  and  $K$ .

**DEFINITION 7.6** Let  $K$  and  $H$  be two groups, and let  $G$  be the set of all ordered pairs  $(k, h)$ , where  $k$  is in  $K$  and  $h$  is in  $H$ . Let  $\phi$  be a nontrivial homomorphism from  $H$  to  $\text{Aut}(K)$ . Then the *semi-direct product of  $K$  with  $H$  through  $\phi$* , denoted  $K \rtimes_{\phi} H$ , is the set  $G$  with multiplication defined by

$$(k_1, h_1) \cdot (k_2, h_2) = (k_1 \cdot \phi_{h_1}(k_2), h_1 \cdot h_2).$$

### PROPOSITION 7.6

The semi-direct product of  $K$  with  $H$  through  $\phi$  is a group.

**PROOF:** It is clear that the product of two ordered pairs in  $G$  is an ordered pair in  $G$ . If we let  $e_1$  denote the identity element of  $K$ , and  $e_2$  denote the identity element of  $H$ , then

$$\phi_{e_2}(k) = k,$$

since  $\phi$  must map  $e_2$  to the identity automorphism of  $K$ . Thus

$$(k_1, h_1) \cdot (e_1, e_2) = (k_1 \cdot \phi_{h_1}(e_1), h_1 \cdot e_2) = (k_1, h_1),$$

and

$$(e_1, e_2) \cdot (k_2, h_2) = (e_1 \cdot \phi_{e_2}(k_2), e_2 \cdot h_2) = (k_2, h_2).$$

So  $(e_1, e_2)$  acts as the identity element of  $G$ .

Next we note that the element  $(k, h)$  has an inverse  $(\phi_{h^{-1}}(k^{-1}), h^{-1})$ , since

$$\begin{aligned} (\phi_{h^{-1}}(k^{-1}), h^{-1}) \cdot (k, h) &= (\phi_{h^{-1}}(k^{-1}) \cdot \phi_{h^{-1}}(k), h^{-1} \cdot h) \\ &= (\phi_{h^{-1}}(k^{-1} \cdot k), e_2) = (\phi_{h^{-1}}(e_1), e_2) = (e_1, e_2), \end{aligned}$$

and

$$\begin{aligned} (k, h) \cdot (\phi_{h^{-1}}(k^{-1}), h^{-1}) &= (k \cdot \phi_h(\phi_{h^{-1}}(k^{-1})), h \cdot h^{-1}) \\ &= (k \cdot \phi_{e_2}(k^{-1}), e_2) = (k \cdot k^{-1}, e_2) = (e_1, e_2). \end{aligned}$$

The final thing we need to check is that the multiplication on  $G$  is associative. Note that

$$\begin{aligned} [(k_1, h_1) \cdot (k_2, h_2)] \cdot (k_3, h_3) &= (k_1 \cdot \phi_{h_1}(k_2), h_1 \cdot h_2) \cdot (k_3, h_3) \\ &= (k_1 \cdot \phi_{h_1}(k_2) \cdot \phi_{h_1 \cdot h_2}(k_3), (h_1 \cdot h_2) \cdot h_3), \end{aligned}$$

while

$$\begin{aligned} (k_1, h_1) \cdot [(k_2, h_2) \cdot (k_3, h_3)] &= (k_1, h_1) \cdot (k_2 \cdot \phi_{h_2}(k_3), h_2 \cdot h_3) \\ &= (k_1 \cdot \phi_{h_1}(k_2 \cdot \phi_{h_2}(k_3)), h_1 \cdot (h_2 \cdot h_3)) \\ &= (k_1 \cdot \phi_{h_1}(k_2) \cdot \phi_{h_1}(\phi_{h_2}(k_3)), (h_1 \cdot h_2) \cdot h_3) \\ &= (k_1 \cdot \phi_{h_1}(k_2) \cdot \phi_{h_1 \cdot h_2}(k_3), (h_1 \cdot h_2) \cdot h_3). \end{aligned}$$

Hence the multiplication on  $G$  is associative and so  $G$  forms a group. □

### **Example 7.11**

Find a semi-direct product  $Z_3 \rtimes_{\phi} Z_2$ .

SOLUTION: First we find that  $\text{Aut}(Z_3) \approx Z_3^* \approx Z_2$ . Hence, there is only one non-trivial automorphism on  $Z_3$ , which is  $x \rightarrow x^{-1}$ . To get a non-trivial automorphism from  $Z_2$  to  $\text{Aut}(Z_3)$ , we must have 0 map to the identity automorphism, and 1 map to the other automorphism. That is,  $\phi_0(x) = x$  and  $\phi_1(x) = x^{-1}$ . Thus,

$$(2, 1) \cdot (1, 0) = (2 \cdot \phi_1(1), 1 \cdot 0) = (2 \cdot 2, 1 \cdot 0) = (1, 1).$$

The multiplication table is given in [Table 7.3](#). This is a non-abelian group of order 6, so this is isomorphic to  $S_3$ . □

A semi-direct product of two groups acts in many ways like the direct product. One property that is in common is that there are copies of the two original groups within the product. In fact, we have the following:

### **LEMMA 7.7**

Let  $G = K \rtimes_{\phi} H$  be the semi-direct product of  $K$  with  $H$  through the homomorphism  $\phi$ . Suppose that  $e_1$  is the identity element of  $K$ , and  $e_2$  is the identity

**TABLE 7.3:** Cayley table of  $Z_3 \rtimes_{\phi} Z_2$ 

|       | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) |
|-------|-------|-------|-------|-------|-------|-------|
| (0,0) | (0,0) | (0,1) | (1,0) | (1,1) | (2,0) | (2,1) |
| (0,1) | (0,1) | (0,0) | (2,1) | (2,0) | (1,1) | (1,0) |
| (1,0) | (1,0) | (1,1) | (2,0) | (2,1) | (0,0) | (0,1) |
| (1,1) | (1,1) | (1,0) | (0,1) | (0,0) | (2,1) | (2,0) |
| (2,0) | (2,0) | (2,1) | (0,0) | (0,1) | (1,0) | (1,1) |
| (2,1) | (2,1) | (2,0) | (1,1) | (1,0) | (0,1) | (0,0) |

element of  $H$ . Then

$$\overline{H} = \{(e_1, h) \mid h \in H\}$$

is a subgroup of  $G$ , and

$$\overline{K} = \{(k, e_2) \mid k \in K\}$$

is a normal subgroup of  $G$ . Furthermore,  $\overline{H} \approx H$ ,  $\overline{K} \approx K$ , and  $\overline{H} \cap \overline{K}$  is the identity element of  $G$ .

PROOF: We will use Proposition 3.2 and observe that

$$(e_1, h)^{-1} = (\phi_{h^{-1}}(e_1^{-1}), h^{-1}) = (e_1, h^{-1}),$$

so

$$(e_1, h_1) \cdot (e_1, h_2)^{-1} = (e_1, h_1) \cdot (e_1, h_2^{-1}) = (e_1 \cdot \phi_{h_1}(e_1), h_1 \cdot h_2^{-1}) = (e_1, h_1 \cdot h_2^{-1}).$$

Thus, whenever  $a$  and  $b$  are in  $\overline{H}$ ,  $a \cdot b^{-1}$  is in  $\overline{H}$ . So  $\overline{H}$  is a subgroup.

The mapping  $f : G \rightarrow H$  given by

$$f((k, h)) = h$$

is a homomorphism, since

$$f((k_1, h_1) \cdot (k_2, h_2)) = f((k_1 \cdot \phi_{h_1}(k_2), h_1 \cdot h_2)) = h_1 \cdot h_2 = f((k_1, h_1)) \cdot f((k_2, h_2)).$$

The kernel of this homomorphism is  $\overline{K}$ , so  $\overline{K}$  is a normal subgroup of  $G$ . By restricting the function  $f$  to the set  $\overline{H}$ , we find that it is one-to-one and onto. Thus,  $\overline{H} \approx H$ . A similar function  $g : K \rightarrow \overline{K}$ , given by

$$g(k) = (k, e_2)$$

can show that  $\overline{K} \approx K$ . This function is clearly one-to-one and onto, and

$$g(k_1) \cdot g(k_2) = (k_1, e_2) \cdot (k_2, e_2) = (k_1 \cdot \phi_{e_2}(k_2), e_2) = (k_1 \cdot k_2, e_2) = g(k_1 \cdot k_2).$$

Finally, it is clear that the intersections of the two groups give  $\{(e_1, e_2)\}$ .  $\blacksquare$

Since the semi-direct product contains copies of the two smaller groups within itself, the natural question is whether an arbitrary group  $G$  can be expressed as a semi-direct product of two of its subgroups. The conditions for when this happens is set forth in the following theorem.

**THEOREM 7.3: The Semi-Direct Product Theorem**

Suppose that a group  $G$  has two subgroups  $N$  and  $H$  whose intersection is the identity element. Then if  $N$  is a normal subgroup of  $G$  and  $H$  is not a normal subgroup of  $N \cdot H$ , then there exists a nontrivial homomorphism  $\phi$  from  $H$  to  $\text{Aut}(N)$  such that

$$N \cdot H \approx N \rtimes_{\phi} H.$$

PROOF: Note that since  $H$  is a subgroup of  $G$ , and  $N$  is a normal subgroup we have by Lemma 5.3 that  $N \cdot H$  is a subgroup of  $G$ . We next want to define the homomorphism  $\phi$ . For each  $h$  in  $H$ , we define

$$\phi_h(k) = h \cdot k \cdot h^{-1}$$

for all  $k \in N$ . We first need to show that  $\phi_h$  is an automorphism on  $N$  for each  $h$  in  $H$ , and then we need to show that  $\phi$  itself is a nontrivial homomorphism. Note that

$$\phi_h(k_1 \cdot k_2) = h \cdot k_1 \cdot k_2 \cdot h^{-1} = (h \cdot k_1 \cdot h^{-1}) \cdot (h \cdot k_2 \cdot h^{-1}) = \phi_h(k_1) \cdot \phi_h(k_2).$$

So  $\phi_h$  is a homomorphism from  $N$  to  $N$ . Since

$$y \in \phi_h^{-1}(k) \iff h \cdot y \cdot h^{-1} = k \iff y = h^{-1} \cdot k \cdot h$$

we see that  $\phi_h$  is a one-to-one and onto function. Thus,  $\phi_h$  is an automorphism of  $N$ .

Next, we need to see that  $\phi$  itself is a homomorphism from  $H$  to  $\text{Aut}(N)$ . Note that

$$\begin{aligned} (\phi_{h_1} \cdot \phi_{h_2})(k) &= \phi_{h_1}(\phi_{h_2}(k)) \\ &= \phi_{h_1}(h_2 \cdot k \cdot h_2^{-1}) \\ &= h_1 \cdot h_2 \cdot k \cdot h_2^{-1} \cdot h_1^{-1} \\ &= (h_1 \cdot h_2) \cdot k \cdot (h_1 \cdot h_2)^{-1} = \phi_{h_1 \cdot h_2}(k). \end{aligned}$$

So  $\phi_{h_1} \cdot \phi_{h_2} = \phi_{(h_1 \cdot h_2)}$  and we see that  $\phi$  is a homomorphism. In fact, the homomorphism must be nontrivial, because if  $\phi_h(k) = k$  for all  $h$  and  $k$ , then since  $\phi_h(k) = h \cdot k \cdot h^{-1} = k$  we have that  $k \cdot h = h \cdot k$  for all  $h$  in  $H$ , and  $k$  in  $N$ . This would indicate that  $H$  is a *normal* subgroup of  $N \cdot H$ , which contradicts our original assumption. Thus,  $\phi$  is a nontrivial homomorphism.

We can now proceed in a way similar to how we proved the direct product theorem (7.1). As before, we will begin by showing that every element in  $N \cdot H$  can be *uniquely* written in the form  $k \cdot h$ , where  $k \in N$  and  $h \in H$ .

Suppose that we have

$$k_1 \cdot h_1 = k_2 \cdot h_2.$$

Then  $k_2^{-1} \cdot k_1 = h_2 \cdot h_1^{-1}$ . Since this element is in both  $N$  and  $H$ , which has just the identity element in the intersection, we must have

$$k_2^{-1} \cdot k_1 = h_2 \cdot h_1^{-1} = e.$$

Therefore,  $k_1 = k_2$  and  $h_1 = h_2$ . Thus, we have shown that every element of  $N \cdot H$  is written uniquely as  $k \cdot h$ , where  $k$  is in  $N$ , and  $h$  is in  $H$ .

We now want to create a mapping

$$f : N \cdot H \rightarrow N \rtimes_{\phi} H$$

defined by

$$f(x) = (k, h),$$

where  $k$  and  $h$  are the unique elements such that  $k \in N$ ,  $h \in H$ , and  $x = k \cdot h$ . The function  $f$  is one-to-one since the element  $(k, h)$  can only come from  $k \cdot h$ . Also, the element  $k \cdot h$  maps to  $(k, h)$  so  $f$  is onto.

The final step is to show that  $f$  is a homomorphism. Let  $x = k_1 \cdot h_1$ , and  $y = k_2 \cdot h_2$ . Then

$$x \cdot y = k_1 \cdot h_1 \cdot k_2 \cdot h_2 = (k_1 \cdot h_1 \cdot k_2 \cdot h_1^{-1}) \cdot (h_1 \cdot h_2).$$

Since  $N$  is a normal subgroup,  $h_1 \cdot k_2 \cdot h_1^{-1}$  is in  $N$ , and so  $k_1 \cdot h_1 \cdot k_2 \cdot h_1^{-1}$  is in  $N$  while  $h_1 \cdot h_2$  is in  $H$ . Thus,

$$\begin{aligned} f(x \cdot y) &= f((k_1 \cdot h_1 \cdot k_2 \cdot h_1^{-1}) \cdot (h_1 \cdot h_2)) \\ &= (k_1 \cdot h_1 \cdot k_2 \cdot h_1^{-1}, h_1 \cdot h_2) \\ &= (k_1 \cdot \phi_{h_1}(k_2), h_1 \cdot h_2) \\ &= (k_1, h_1) \cdot (k_2, h_2) = f(x) \cdot f(y). \end{aligned}$$

So  $f$  is an isomorphism, and we have  $N \cdot H \approx N \rtimes_{\phi} H$ . □

Note that if both  $N$  and  $H$  are normal subgroups of  $N \cdot H$ , we have by Corollary 7.1 that  $N \cdot H \approx N \times H$ .

We will use the semi-direct product theorem to define this product in *Sage-Math*. After defining the two groups  $N$  and  $H$  using the same identity element, we must find the homomorphism  $\phi$  from  $H$  to  $\text{Aut}(N)$ . As in the case of the direct product, we will want to express every element of the form  $k \cdot h$ , where  $k$  is in  $N$ , and  $h$  is in  $H$ . From the definition, we see that

$$(k, e_2) \cdot (e_1, h) = (k \cdot \phi_{e_2}(e_1), e_2 \cdot h) = (k, h),$$

Thus, we see that  $k \cdot h$  can represent the ordered pair  $(k, h)$ . We need to tell *SageMath* how to handle expressions of the form  $h \cdot k$ .

For each generator  $a$  of  $N$ , and each generator  $b$  of  $H$ , we can calculate how  $\mathbf{b} * \mathbf{a}$  should be defined by evaluating  $(e_1, b) \cdot (a, e_2) = (\phi_b(a), b)$ . Thus we make a definition in *SageMath* of the form

```
Define(b*a, phi_b(a) * b)
```

where we replace the expression  $\phi_b(a)$  with its element of  $N$ . For the group  $Z_3 \rtimes_{\phi} Z_2$  in Example 7.11, we would let  $a$  be the generator of  $Z_3$ , so  $a^3 = e$ , and  $b$  be the generator of  $Z_2$ , so  $b^2 = e$ . Then we would define  $b \cdot a = a^{-1} \cdot b = a^2 \cdot b$ .

### Computational Example 7.12

Use *SageMath* to find a semi-direct product of  $Z_5$  with  $Z_2$ .

SOLUTION: We first must define  $Z_5$  and  $Z_2$  into *SageMath* using the same identity but different generators.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^5, e)
Define(b^2, e)
Z5 = Group(a); z5
{e, a^4, a, a^3, a^2}
Z2 = Group(b); z2
{e, b}
```

After loading the groups  $Z_5$  and  $Z_2$ , we want to find a nontrivial homomorphism  $\phi$  from  $Z_2$  to  $\text{Aut}(Z_5)$ . But  $\text{Aut}(Z_5) \approx Z_5^* \approx Z_4$ . Since the element  $b$  is of order 2,  $\phi_b$  must be of order 2 to keep the homomorphism from being trivial. But it is easy to find the one element of  $\text{Aut}(Z_5)$  of order 2:

$$\phi(k) = k^{-1}.$$

In fact, this will always be an automorphism whenever  $N$  is an abelian group. As long as  $N$  has an element that is not its own inverse, this automorphism will be of order 2. If we let  $\phi_b(k) = k^{-1}$ , then  $\phi_b(a) = a^{-1} = a^4$ . Thus, the definition

```
Define(b*a, a^4*b)
```

completes the definition of the semi-direct product.

```
G = Group(); G
{e, a, a^2, a^3, a^4, b, a*b, a^2*b, a^3*b, a^4*b}
```

The multiplication table is given in Table 7.4, shows that the semi-direct product  $Z_5 \rtimes Z_2$  is a non-abelian group of order 10. Note that when there is

only one possible semi-direct product between two groups, we can leave out the  $\phi$  in the notation.  $\blacksquare$

We can use the command **StructureDescription()** to ask *SageMath* what group this is. This command analyzes the last group defined using the **InitGroup** and **Define** commands.

**StructureDescription()**

D5

**TABLE 7.4:** Multiplication table for  $Z_5 \rtimes Z_2$

| .             | e             | a             | $a^2$         | $a^3$         | $a^4$         | b             | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ | $a^4 \cdot b$ |
|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| e             | e             | a             | $a^2$         | $a^3$         | $a^4$         | b             | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ | $a^4 \cdot b$ |
| a             | a             | $a^2$         | $a^3$         | $a^4$         | e             | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ | $a^4 \cdot b$ | b             |
| $a^2$         | $a^2$         | $a^3$         | $a^4$         | e             | a             | $a^2 \cdot b$ | $a^3 \cdot b$ | $a^4 \cdot b$ | b             | $a \cdot b$   |
| $a^3$         | $a^3$         | $a^4$         | e             | a             | $a^2$         | $a^3 \cdot b$ | $a^4 \cdot b$ | b             | $a \cdot b$   | $a^2 \cdot b$ |
| $a^4$         | $a^4$         | e             | a             | $a^2$         | $a^3$         | $a^4 \cdot b$ | b             | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ |
| b             | b             | $a^4 \cdot b$ | $a^3 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | e             | $a^4$         | $a^3$         | $a^2$         | a             |
| $a \cdot b$   | $a \cdot b$   | b             | $a^4 \cdot b$ | $a^3 \cdot b$ | $a^2 \cdot b$ | a             | e             | $a^4$         | $a^3$         | $a^2$         |
| $a^2 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | b             | $a^4 \cdot b$ | $a^3 \cdot b$ | $a^2$         | a             | e             | $a^4$         | $a^3$         |
| $a^3 \cdot b$ | $a^3 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | b             | $a^4 \cdot b$ | $a^3$         | $a^2$         | a             | e             | $a^4$         |
| $a^4 \cdot b$ | $a^4 \cdot b$ | $a^3 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | b             | $a^4$         | $a^3$         | $a^2$         | a             | e             |

This shows that the group is the dihedral group  $D_{5,}$  which was introduced in § 5.1 as the dihedral group of order 10. Even though we already defined the dihedral groups in § 5.1, we can now define these groups as a semi-direct product.

**DEFINITION 7.7** Let  $n > 2$ , and let  $\phi$  be the homomorphism from  $Z_2 = \{e, b\}$  to  $\text{Aut}(Z_n)$  given by

$$\phi_e(k) = k, \quad \phi_b(k) = k^{-1}.$$

Then the dihedral group  $D_n$  can be expressed as the semi-direct product  $Z_n \rtimes_{\phi} Z_2$ . This group can be defined in *SageMath* by the following commands, replacing  $n$  with an integer before executing the commands.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^n, e)
```

```
Define(b^2, e)
Define(b*a, a^-1*b)
Dn = Group(a, b)
```

It should be noted that the semi-direct product may greatly depend on the choice of the homomorphism  $\phi$ .

### Computational Example 7.13

Consider finding the semi-direct products of  $Z_8$  with  $Z_2$ . Since  $\text{Aut}(Z_8) \approx Z_8^*$  has three elements of order 2, there are three nontrivial homomorphisms from  $Z_2$  to  $\text{Aut}(Z_8)$ . One of these produces the dihedral group  $D_8$  above, but the other two homomorphisms produce different groups. If we let  $\phi_b(a) = a^3$ , we get the following.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^8, e)
Define(b^2, e)
Define(b*a, a^3*b)
G = ListGroup(); G
{e, a, a^2, a^3, a^4, a^5, a^6, a^7, b, a*b, a^2*b, a^3*b,
 a^4*b, a^5*b, a^6*b, a^7*b}
StructureDescription()
QD16
```

*SageMath* calls this group “QD16,” since it is the *quasidihedral group* of order 16, written  $QD_{16}$ . If we let  $\phi_b(a) = a^5$  instead, we get

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^8, e)
Define(b^2, e)
Define(b*a, a^5*b)
M = ListGroup(); M
{e, a, a^2, a^3, a^4, a^5, a^6, a^7, b, a*b, a^2*b, a^3*b,
 a^4*b, a^5*b, a^6*b, a^7*b}
StructureDescription()
Z8 : Z2
```

Even though the list of elements look the same for the two groups, the structure description is different. *SageMath* uses a colon for the semi-direct product symbol  $\rtimes$ , so *SageMath* recognized that the last group was of the form  $Z_8 \rtimes Z_2$ , but otherwise there is no special name for this group. □

Another way of showing that the three groups are different is by having *SageMath* display the multiplication tables, and counting the number of times

the identity element appears along the diagonals. We find that  $R_2(D_8) = 10$ ,  $R_2(QD_{16}) = 6$ , and  $R_2(M) = 4$ , where  $M$  is the last group of the form  $Z_8 \rtimes Z_2$ . Thus, we see that the semi-direct product  $Z_8 \rtimes_{\phi} Z_2$  depends on the choice of the homomorphism  $\phi$ . In fact, even though the three elements of  $\text{Aut}(Z_8)$  of order 2 are essentially equivalent (since the automorphisms of  $Z_8^*$  included all permutations of these three elements), we see that the three elements produced three different semi-direct products.

This example is really more of an exception rather than a rule. Part of what makes this example unusual is that the automorphism group  $Z_8^*$  is abelian, and hence does not have any nontrivial *inner* automorphisms. If two homomorphisms  $\phi$  and  $f$  from  $H$  to  $\text{Aut}(N)$  are related through an inner automorphism of  $\text{Aut}(N)$ , then the corresponding semi-direct products will in fact be isomorphic.

### PROPOSITION 7.7

Let  $\phi$  be a homomorphism from a group  $H$  to the group  $\text{Aut}(N)$ . Suppose that  $f$  is another homomorphism such that

$$f_h(k) = w(\phi_h(w^{-1}(k))),$$

where  $w(k)$  is an automorphism of  $N$ . Then  $N \rtimes_f H \approx N \rtimes_{\phi} H$ .

PROOF: Let us write  $G = N \rtimes_{\phi} H$ , and  $M = N \rtimes_f H$ . These are two different groups, even though they are both written using ordered pairs. Let us define a mapping

$$v : G \rightarrow M$$

defined by

$$v((k, h)) = (w(k), h).$$

Because  $w(k)$  is one-to-one and onto, certainly  $v$  is one-to-one and onto. All we would have to check is that

$$v((k_1, h_1)) \cdot v((k_2, h_2)) = v((k_1, h_1) \cdot (k_2, h_2)).$$

We have that

$$\begin{aligned} v((k_1, h_1)) \cdot v((k_2, h_2)) &= (w(k_1), h_1) \cdot (w(k_2), h_2) \\ &= (w(k_1) \cdot f_{h_1}(w(k_2)), h_1 \cdot h_2) \\ &= (w(k_1) \cdot w(\phi_{h_1}(w^{-1}(w(k_2)))), h_1 \cdot h_2) \\ &= (w(k_1) \cdot w(\phi_{h_1}(k_2)), h_1 \cdot h_2). \end{aligned}$$

On the other hand,

$$\begin{aligned} v((k_1, h_1) \cdot (k_2, h_2)) &= v((k_1 \cdot \phi_{h_1}(k_2), h_1 \cdot h_2)) \\ &= (w(k_1 \cdot \phi_{h_1}(k_2)), h_1 \cdot h_2) \\ &= (w(k_1) \cdot w(\phi_{h_1}(k_2)), h_1 \cdot h_2). \end{aligned}$$

Since these are equal, we have an isomorphism. □

It is also clear that two homomorphisms  $\phi$  and  $f$  are related through an automorphism of  $H$ , the semi-direct products must be isomorphic since we are merely relabeling the elements of  $H$ . As a result there will be many instances in which there will be only one non-isomorphic semi-direct product of  $N$  by  $H$ . In this case, we can denote the semi-direct product as  $N \rtimes H$ , without having to specify the homomorphism  $\phi$ .

We will find that we can describe many groups in terms of semi-direct products that would be hard to describe in any other way. With *SageMath*, the structure of these semi-direct products can easily be studied.

### Problems for §7.4

For Problems 1 through 6: Let  $\phi : Z_8^* \rightarrow \text{Aut}(Z_8^*)$  be defined as follows:  $\phi_1 = \phi_3 = ()$ ,  $\phi_5 = \phi_7 = (3\ 5)$ , where we used the cycle notation for the automorphisms. Compute the following in  $Z_8^* \rtimes_{\phi} Z_8^*$ :

|                                |                        |                                             |
|--------------------------------|------------------------|---------------------------------------------|
| <b>1</b> $(5, 3) \cdot (3, 5)$ | <b>3</b> $(7, 5)^{-1}$ | <b>5</b> $(1, 5) \cdot (3, 7) \cdot (5, 3)$ |
| <b>2</b> $(3, 5) \cdot (5, 3)$ | <b>4</b> $(5, 7)^{-1}$ | <b>6</b> $(5, 3) \cdot (3, 7) \cdot (1, 5)$ |

- 7** Show that there is only one semi-direct product  $Z_8^* \rtimes Z_2$ , and form a Cayley table. Which of the five groups of order 8 is this isomorphic to?

Hint: Use Proposition 7.7.

- 8** Show that there is only one semi-direct product of the form  $Z_8^* \rtimes Z_3$ . Form a Cayley table of this group. You have seen this group before. Do you recognize it?

- 9** Form a Cayley table of the only semi-direct product of the form  $Z_3 \rtimes Z_4$ .

- 10** Show that there is only one semi-direct product of the form  $\mathbb{Z} \rtimes Z_2$ . Describe this group.

- 11** Show that there is only one semi-direct product of the form  $\mathbb{Z} \rtimes \mathbb{Z}$ . Describe this group.

- 12** Let  $G$  be any group, and let  $i$  be the identity mapping from  $\text{Aut}(G)$  to itself. We can define the semi-direct product  $H = G \rtimes_i \text{Aut}(G)$ . The group  $H$  is called the *holomorph* of  $G$ . Show that every automorphism of  $G$  is the restriction of some inner automorphism of the holomorph  $H$ .

- 13** Let  $G$  be a group, and  $n$  a positive integer. We will let  $G^n$  denote the direct product of  $G$  with itself  $n$  times, or the set of  $n$ -tuples in  $G$ . If  $\sigma \in S_n$ , we can define

$$\psi_{\sigma} : G^n \rightarrow G^n \quad \text{by} \quad \psi_{\sigma}(g_1, g_2, \dots, g_n) = (g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \dots, g_{\sigma^{-1}(n)}).$$

Show that  $\psi_{\sigma}$  is an automorphism of  $G^n$ .

- 14** Let  $G^n$  and  $\psi$  be defined as in Problem 13. Show that if  $\sigma$  and  $\tau$  are two elements of  $S_n$ , then  $\psi_\tau(\psi_\sigma(x)) = \psi_{\tau \cdot \sigma}(x)$ .

Hint: Think of an  $n$ -tuple as a function  $f$  from the set  $1 \leq i \leq n$  to  $G$ , with  $f(i)$  being the  $i$ th component of the  $n$ -tuple. Then  $\phi_\sigma(f)$  sends  $f(i)$  to  $f(\sigma^{-1}(i))$ .

- 15** Let  $G$  be a group, and  $H$  a subgroup of  $S_n$ . We define the *wreath product*

$$G \text{ Wr } H$$

as the semi-direct product  $G^n \rtimes_\psi H$ , where  $G^n$  and  $\psi$  are defined as in Problem 13. Show that if  $G$  is a finite group, the wreath product is a finite group of size  $|G|^n \cdot |H|$ .

- 16** Form the multiplication table of  $Z_2 \text{ Wr } S_2$ . See Problem 15.

### Interactive Problems

- 17** Use *SageMath* to find the only semi-direct product  $Z_8^* \rtimes Z_8^*$ . Is this group isomorphic to any of the three groups of order 16 found by considering  $Z_8 \rtimes_\phi Z_2$ ?
- 18** From Problems 16 and 19 from §7.1, Problem 9, and Definition 7.7, we have found six groups of order 12:  $Z_{12}$ ,  $Z_2 \times Z_6$ ,  $A_4$ ,  $D_6$ ,  $S_3 \times Z_2$ , and  $Z_3 \rtimes Z_4$ . Yet Table 5.4 indicates that there are only five non-isomorphic groups of order 12. Which two of these groups are isomorphic? Use *SageMath* to show the isomorphism.
- 19** Use *SageMath* to define the wreath product  $Z_3 \text{ Wr } S_2$ . Then use the command **StructureDescription()** to determine what group this is. See Problem 15.
- 20** Use *SageMath* to define the wreath product  $Z_2 \text{ Wr } A_3$ . Then use the command **StructureDescription()** to determine what group this is. See Problem 15.
- 21** Use *SageMath* to define the wreath product  $Z_2 \text{ Wr } S_3$ . Then use the command **StructureDescription()** to determine what group this is. See Problem 15.

# Chapter 8

---

## The Search for Normal Subgroups

We saw several instances in the last chapter in which the structure of a group hinges on its normal subgroups. Thus, we will want to develop techniques for finding *all* of the normal subgroups of a given group  $G$ . We will discover in the process that some of the normal groups have additional properties. We will naturally concentrate our attention on non-abelian groups, since every subgroup of an abelian group is normal.

---

### 8.1 The Center of a Group

In this section, we will consider a simple way of constructing a normal subgroup from a given group. In fact, the definition was suggested in Problem 8 of §4.3. However, we will find that this particular normal subgroup, called the *center* of the group, has some very curious properties.

#### Motivational Example 8.1

Let us begin by considering the dihedral group  $D_4$ . Table 8.1 gives us the Cayley table of this group.

There are five elements of order 2 in this group, but one of these,  $a^2$ , has

**TABLE 8.1:** Cayley table for  $D_4$

| .             | $e$           | $a$           | $a^2$         | $a^3$         | $b$           | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ |
|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| $e$           | $e$           | $a$           | $a^2$         | $a^3$         | $b$           | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ |
| $a$           | $a$           | $a^2$         | $a^3$         | $e$           | $a \cdot b$   | $a^2 \cdot b$ | $a^3 \cdot b$ | $b$           |
| $a^2$         | $a^2$         | $a^3$         | $e$           | $a$           | $a^2 \cdot b$ | $a^3 \cdot b$ | $b$           | $a \cdot b$   |
| $a^3$         | $a^3$         | $e$           | $a$           | $a^2$         | $a^3 \cdot b$ | $b$           | $a \cdot b$   | $a^2 \cdot b$ |
| $b$           | $b$           | $a^3 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | $e$           | $a^3$         | $a^2$         | $a$           |
| $a \cdot b$   | $a \cdot b$   | $b$           | $a^3 \cdot b$ | $a^2 \cdot b$ | $a$           | $e$           | $a^3$         | $a^2$         |
| $a^2 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | $b$           | $a^3 \cdot b$ | $a^2$         | $a$           | $e$           | $a^3$         |
| $a^3 \cdot b$ | $a^3 \cdot b$ | $a^2 \cdot b$ | $a \cdot b$   | $b$           | $a^3$         | $a^2$         | $a$           | $e$           |

another important property. Notice that the locations of the  $a^2$  in [Table 8.1](#) form a symmetrical pattern reflected along the main diagonal, even though the entire table is not symmetric. This indicates that whenever  $x \cdot y = a^2$ , then  $y \cdot x = a^2$  in  $D_4$ . Hence  $y = x^{-1} \cdot a^2 = a^2 \cdot x^{-1}$  for all elements  $x$ . In order for this to happen,  $a^2$  must commute with *all* of the elements of  $D_4$ .  $\blacksquare$

**DEFINITION 8.1** Given a group  $G$ , the *center* of  $G$  is defined to be the set of elements  $x$  for which  $x \cdot y = y \cdot x$  for all elements  $y \in G$ . The center of a group  $G$  is customarily denoted  $Z(G)$  because of the German word for center, *zentrum*. [1, p. 150]

From this definition, we see that  $a^2 \in Z(D_4)$ . It is also clear that  $e \in Z(G)$  for all groups, since  $e \cdot y = y \cdot e$ . By examining [Table 8.1](#) we find that there are no other elements of  $D_4$  in  $Z(D_4)$ , so  $Z(D_4) = \{e, a^2\}$ . This is obviously a subgroup, but it turns out to be a normal subgroup.

### PROPOSITION 8.1

*Given a group  $G$ , then  $Z(G)$  is a normal subgroup of  $G$ .*

PROOF: First, we need to show that  $Z(G)$  is a subgroup of  $G$ . If  $x$  and  $y$  are in  $Z(G)$ , and  $a$  is any element in  $G$ , then

$$x \cdot y \cdot a = x \cdot a \cdot y = a \cdot x \cdot y.$$

So  $x \cdot y$  commutes with all of the elements of  $G$ . Thus,  $x \cdot y$  is in  $Z(G)$ .

Also, we have

$$x^{-1} \cdot a = (a^{-1} \cdot x)^{-1} = (x \cdot a^{-1})^{-1} = a \cdot x^{-1}.$$

So  $x^{-1}$  must also be in  $Z(G)$ . Thus, by Proposition 3.2,  $Z(G)$  is a subgroup of  $G$ .

Next, we can see that

$$a \cdot x \cdot a^{-1} = x \cdot a \cdot a^{-1} = x.$$

So  $a \cdot x \cdot a^{-1}$  is in  $Z(G)$  whenever  $x$  is in  $Z(G)$  and  $a$  is in  $G$ . Thus, by Proposition 4.4,  $Z(G)$  is a normal subgroup of  $G$ .  $\blacksquare$

We use the command **GroupCenter** to find the center of a group in *Sage-Math*. For example, the command

```
Z = GroupCenter(D4); Z
{e, a^2}
```

verifies our earlier observation that  $Z(D_4) = \{e, a^2\}$ .

Although the center always produces a normal subgroup, this subgroup is not always non-trivial.

**Example 8.2**

Show that the center of the group  $S_3 = \{(), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$  is just the identity element.

**SOLUTION:** Since  $(1\ 2) \cdot (2\ 3) = (1\ 2\ 3) \neq (2\ 3) \cdot (1\ 2) = (1\ 3\ 2)$ , neither  $(1\ 2)$  nor  $(2\ 3)$  are in the center. Also,  $(1\ 3) \cdot (1\ 2\ 3) = (1\ 2) \neq (1\ 2\ 3) \cdot (1\ 3) = (2\ 3)$ , so neither  $(1\ 3)$  nor  $(1\ 2\ 3)$  are in the center. Finally,  $(1\ 3\ 2)$  cannot be in the center, since we have established that  $(1\ 3\ 2)^2 = (1\ 2\ 3)$  is not in the center. Thus, only  $()$  is in the center.  $\square$

Whenever the center is just the identity element, we say the group is *centerless*. In fact, all of the permutation groups  $S_n$  bigger than  $S_3$  are centerless. Since the proof involves an even permutation, we will find the center of  $A_n$  at the same time.

**PROPOSITION 8.2**

*If  $n > 3$ , then the groups  $S_n$  and  $A_n$  are centerless.*

**PROOF:** Suppose that  $\phi$  is an element of  $S_n$  or  $A_n$  which is not the identity. We need to show that  $\phi$  cannot be in the center of either  $S_n$  or  $A_n$ , which amounts to finding an element of  $A_n$  that does not commute with  $\phi$ .

Since  $\phi$  is not the identity, there is some number  $x$  that is not fixed by  $\phi$ , say  $x$  is mapped to  $y$ . Since  $n > 3$ , there is at least one number not in the list  $\{x, y, \phi(y)\}$ . Let  $z$  be one of these remaining numbers. Finally, we let  $f$  be the 3-cycle  $(x\ y\ z)$ .

Since  $f$  is an even permutation  $f$  is in  $A_n$ . Then  $f \cdot \phi$  sends  $x$  to  $z$ , but  $\phi \cdot f$  sends  $x$  to  $\phi(y) \neq z$ . Thus,  $f \cdot \phi \neq \phi \cdot f$ , and  $\phi$  is not in the center of either  $S_n$  or  $A_n$ .  $\square$

The other extreme is if  $Z(G)$  is the entire group  $G$ . This happens if, and only if, the group  $G$  is abelian.

Since  $Z(G)$  is a normal subgroup of  $G$ , what is the quotient group? The answer is rather surprising.

**PROPOSITION 8.3**

*If  $G$  is a group, then  $G/Z(G) \approx \text{Inn}(G)$ .*

**PROOF:** We begin by observing that the mapping

$$\phi : G \rightarrow \text{Inn}(G)$$

given by

$$\phi_x(y) = x \cdot y \cdot x^{-1}$$

is a homomorphism. Note that

$$(\phi_{x_1} \cdot \phi_{x_2})(y) = \phi_{x_1}(\phi_{x_2}(y))$$

$$\begin{aligned}
&= \phi_{x_1}(x_2 \cdot y \cdot x_2^{-1}) \\
&= x_1 \cdot x_2 \cdot y \cdot x_2^{-1} \cdot x_1^{-1} \\
&= (x_1 \cdot x_2) \cdot y \cdot (x_1 \cdot x_2)^{-1} = \phi_{x_1 \cdot x_2}(y).
\end{aligned}$$

So  $\phi_{x_1} \cdot \phi_{x_2} = \phi_{(x_1 \cdot x_2)}$  and we see that  $\phi$  is a homomorphism.

By the definition of the inner automorphisms, this mapping is surjective. However, this mapping is not necessarily injective. Let us determine the kernel of  $\phi$ .

Suppose that  $\phi_x$  is the identity homomorphism. Then  $\phi_x(y) = y$  for all  $y$  in  $G$ . This means that  $x \cdot y \cdot x^{-1} = y$ , or  $x \cdot y = y \cdot x$ , for all  $y$  in  $G$ . Thus,  $x$  is in the center of  $G$ .

Now, suppose  $x$  is in  $Z(G)$ . Then  $\phi_x(y) = x \cdot y \cdot x^{-1} = y \cdot x \cdot x^{-1} = y$ , so  $\phi_x$  is the identity homomorphism. Thus the kernel of  $\phi$  is precisely the center of  $G$ . Therefore, by the first isomorphism theorem (5.1), we have

$$G/Z(G) \approx \text{Inn}(G).$$

□

The center of a group possesses a characteristic that is even stronger than that of a normal subgroup. To illustrate this characteristic, consider the next proposition.

#### **PROPOSITION 8.4**

Let  $N$  be a normal subgroup of a group  $G$ . Then  $Z(N)$  is a normal subgroup not only of  $N$  but also of  $G$ .

**PROOF:** Let  $g$  be an element of  $G$ , and  $z$  an element of  $Z(N)$ . We need to show that  $g \cdot z \cdot g^{-1}$  is in  $Z(N)$ . Since  $N$  is a normal subgroup of  $G$ , we certainly know that  $g \cdot z \cdot g^{-1}$  is in  $N$ , so the way to test that it is in  $Z(N)$  is to show that it commutes with every element of  $N$ .

Let  $n$  be an element of  $N$ . We want to show that  $g \cdot z \cdot g^{-1} \cdot n = n \cdot g \cdot z \cdot g^{-1}$ . Let  $h = g^{-1} \cdot n \cdot g$ . Then  $h$  is in  $N$ , since  $N$  is normal in  $G$ . Also,  $n = g \cdot h \cdot g^{-1}$ , so

$$\begin{aligned}
g \cdot z \cdot g^{-1} \cdot n &= (g \cdot z \cdot g^{-1}) \cdot (g \cdot h \cdot g^{-1}) = g \cdot z \cdot h \cdot g^{-1} = g \cdot h \cdot z \cdot g^{-1} \\
&= (g \cdot h \cdot g^{-1}) \cdot (g \cdot z \cdot g^{-1}) = n \cdot g \cdot z \cdot g^{-1}.
\end{aligned}$$

Hence,  $g \cdot z \cdot g^{-1}$  commutes with every element  $n$  in  $N$ , so  $g \cdot z \cdot g^{-1}$  is in  $Z(N)$ . By Proposition 4.4, we have that  $Z(N)$  is a normal subgroup of  $G$ . □

This proposition demonstrates a rather unusual property of a center of a group. In general, the normal subgroup of a normal subgroup is not necessarily a normal subgroup. Consider  $M = \{(), (12)(34), (13)(24), (14)(23)\}$ , which is a normal subgroup of  $S_4$ , and  $H = \{(), (12)(34)\}$ , which is a normal subgroup of  $M$ .

```

S4 = Group( C(1,2), C(1,2,3), C(1,2,3,4) )
M = Group( C(1,2)*C(3,4), C(1,3)*C(2,4) ); M
{(), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)}
H = Group( C(1,2)*C(3,4) ); H
{(), (1, 2)(3, 4)}

```

We find that  $H$  is *not* a normal subgroup of  $S_4$ .

```

LftCoset(S4, H)
{{(), (1, 2)(3, 4)}, {(1, 2), (3, 4)}, {(2, 3), (1, 3, 4, 2)},
 {(1, 3, 2), (2, 3, 4)}, {(1, 2, 3), (1, 3, 4)},
 {(1, 3), (1, 2, 3, 4)}, {(2, 4, 3), (1, 4, 2)},
 {(1, 4, 3, 2), (2, 4)}, {(1, 2, 4, 3), (1, 4)},
 {(1, 4, 3), (1, 2, 4)}, {(1, 3)(2, 4), (1, 4)(2, 3)},
 {(1, 4, 2, 3), (1, 3, 2, 4)}}

RtCoset(S4, H)
{{(), (1, 2)(3, 4)}, {(1, 2), (3, 4)}, {(2, 3), (1, 2, 4, 3)},
 {(1, 3, 2), (1, 4, 3)}, {(1, 2, 3), (2, 4, 3)},
 {(1, 3), (1, 4, 3, 2)}, {(2, 3, 4), (1, 2, 4)},
 {(1, 3, 4, 2), (1, 4)}, {(2, 4), (1, 2, 3, 4)},
 {(1, 4, 2), (1, 3, 4)}, {(1, 3)(2, 4), (1, 4)(2, 3)},
 {(1, 4, 2, 3), (1, 3, 2, 4)}}

```

Contrast this situation to the center of a group. We found that the center of a group  $Z(N)$  is a normal subgroup of  $G$ , even though  $Z(N)$  contains no information about the larger group  $G$ . Any group that contains  $N$  as a normal subgroup, such as the semi-direct product of  $N$  with another group, will have  $Z(N)$  as a normal subgroup.

## Problems for §8.1

- 1 Find the center of the group  $Q$ .
- 2 Find the center of the group  $D_5$ .
- 3 Must the center of a group be abelian?
- 4 Let  $G$  be a group and  $Z(G)$  the center of  $G$ . Prove that  $G$  is abelian if, and only if,  $G/Z(G)$  is cyclic.  
Hint: Use Proposition 8.3.
- 5 Show that if  $A$  and  $B$  are two groups, then  $Z(A \times B) \approx Z(A) \times Z(B)$ .
- 6 Prove that if a group only has one element of order 2, then that element must be in the center.  
Hint: see Problem 27 from §3.1.

- 7** Prove that if  $H$  is a normal subgroup of  $G$ , and  $|H| = 2$ , then  $H \subseteq Z(G)$ .
- 8** Let  $\phi$  be an automorphism on the group  $G$ , and let  $z \in Z(G)$ . Prove that  $\phi(z) \in Z(G)$ .
- 9** A *characteristic* subgroup of  $G$  is a subgroup  $H$  such that  $\phi(h) \in H$  for all  $h \in H$  and all automorphisms  $\phi$  of  $G$ . Problem 8 shows that  $Z(G)$  is a characteristic subgroup of  $G$ . Prove that all characteristic subgroups are also normal subgroups.
- 10** Let  $H$  be the only subgroup of  $G$  of size  $|H|$ . Prove that  $H$  is a characteristic subgroup of  $G$ . See Problem 9.
- 11** Let  $G$  be an abelian group, and let  $H$  be the subgroup of size  $R_k(G)$  given by

$$\{x \in G \mid x^k = e\}.$$

Prove that  $H$  is a characteristic subgroup of  $G$ . See Problem 9.

- 12** Prove that all subgroups of a cyclic group are characteristic.  
Hint: See Problems 9 and 10.
- 13** Prove that if  $N$  is a characteristic subgroup of  $G$ , and  $H$  is a characteristic subgroup of  $N$ , then  $H$  is a characteristic subgroup of  $G$ . Note this statement is not true if “characteristic” is replaced with “normal.” See Problem 9.
- 14** Prove that if  $N$  is a normal subgroup of  $G$ , and  $H$  is a characteristic subgroup of  $N$ , then  $H$  is a normal subgroup of  $G$ . This generalizes Proposition 8.4, since the center is a characteristic subgroup. See Problem 9.

### Interactive Problems

- 15** Use *SageMath* to find the center of the group  $D_6$ . This can be loaded by the commands:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^6, e); Define(b^2, e); Define(b*a, a^5*b)
D6 = Group(); D6
{e, a, a^2, a^3, a^4, a^5, b, a*b, a^2*b, a^3*b, a^4*b, a^5*b}
```

What familiar group is the quotient group  $D_6/Z(D_6)$  isomorphic to?

- 16** In Problem 22 of §7.3, we computed the group  $G = \text{Aut}(Z_3 \times Z_3)$ . Find the center of this group. What familiar group is  $G/Z(G)$  isomorphic to?
- 17** Find the centers of the groups  $D_3, D_4, D_5, D_6, D_7$ , and  $D_8$ . Do you see any patterns?

## 8.2 The Normalizer and Normal Closure Subgroups

In the last section, we found a subgroup of  $N$  that was not only normal but also was normal in any group  $G$  for which  $N$  was a normal subgroup. In this section, we will essentially turn the question around: Given a subgroup  $H$  of  $G$ , can we find a subgroup  $N$  of  $G$  for which  $H$  lies inside of  $N$  as a normal subgroup?

**DEFINITION 8.2** Let  $S$  be a *subset* of a group  $G$ . We define the *normalizer of  $S$  by  $G$* , denoted  $N_G(S)$ , to be the set

$$N_G(S) = \{g \in G \mid g \cdot S \cdot g^{-1} = S\}.$$

Notice that this definition allows for  $S$  to be merely a *subset* of  $G$ , not necessarily a subgroup. We will later find uses for having a more generalized definition. For now, let us show that the normalizer has some of the properties that we are looking for.

### PROPOSITION 8.5

Let  $S$  be a subset of the group  $G$ . Then  $N_G(S)$  is a subgroup of  $G$ .

PROOF: Suppose  $x$  and  $y$  are in  $N_G(S)$ . Then both  $x \cdot S \cdot x^{-1} = S$ , and  $y \cdot S \cdot y^{-1} = S$ . Thus,  $S = y^{-1} \cdot S \cdot y$ , and so

$$(x \cdot y^{-1}) \cdot S \cdot (x \cdot y^{-1})^{-1} = x \cdot (y^{-1} \cdot S \cdot y) \cdot x^{-1} = x \cdot S \cdot x^{-1} = S.$$

Thus,  $x \cdot y^{-1}$  is in  $N_G(S)$ , and so by Proposition 3.2,  $N_G(S)$  is a subgroup of  $G$ .  $\square$

### Example 8.3

Consider the group  $Q = \{1, i, j, k, -1, -i, -j, -k\}$ . Find the normalizer of the single element  $\{i\}$ .

SOLUTION: We want to find the elements such that  $g \cdot i \cdot g^{-1} = i$ , which clearly contains  $i$ . Since we know from Proposition 8.5 that the normalizer is a subgroup,  $\{1, i, -1, -i\}$  is in the normalizer. But  $j$  is not in the normalizer, so  $N_G(\{i\}) = \{1, i, -1, -i\}$ .  $\square$

If, in addition,  $S$  is a subgroup of  $G$ , then the normalizer lives up to its name.

### PROPOSITION 8.6

Let  $H$  be a subgroup of the group  $G$ . Then  $N_G(H)$  is the largest subgroup of  $G$  that contains  $H$  as a normal subgroup.

PROOF: First, we must check that  $H$  is a normal subgroup of  $N_G(H)$ . But this is obvious, since  $g \cdot H \cdot g^{-1} = H$  for all  $g$  in  $N_G(H)$ .

Next, we must see that  $N_G(H)$  is the largest such group. Suppose that  $Y$  is another subgroup of  $G$  that contained  $H$  as a normal subgroup. Then  $y \cdot H \cdot y^{-1} = H$  for all  $y \in Y$ . Thus,  $Y \subseteq N_G(H)$ .

Since any subgroup of  $G$  that contains  $H$  as a normal subgroup is itself contained in  $N_G(H)$ , we have that  $N_G(H)$  is the largest such group.  $\square$

### **Example 8.4**

Find the normalizer of the subgroup  $[i] = \{1, i, -1, -i\}$  of  $Q$ .

SOLUTION: Since this is a normal subgroup of  $Q$ , the normalizer is all of  $Q$ , since it is the largest group for which  $[i]$  is normal. In general, the normalizer of a *normal* subgroup by  $G$  will produce the whole group  $G$ .  $\square$

The *SageMath* command **Normalizer(G, H)** finds the normalizer  $N_G(H)$  of the set  $H$  in  $G$ . We can verify the last two examples.

```
Q = InitQuaternions(); Q
{1, i, j, k, -1, -i, -j, -k}
H = Normalizer(Q, i); H
{1, i, -1, -i}
Normalizer(Q, H)
{1, i, j, k, -1, -i, -j, -k}
```

Note that if the set is a single element, we do not have to enclose the element in brackets. We can find the normalizer of any subset, even one that is not a subgroup. For example, the normalizer of the subset  $\{i, j\}$  is

```
Normalizer(Q, [i, j])
{1, -1}
```

which contains neither  $i$  nor  $j$ . In general, all we can say is that the normalizer will be a subgroup, which this example illustrates.

There is one other case in which we can say that the normalizer will contain  $H$ . Notice that in the example we did where  $H$  was a single element, the normalizer contained that element. In fact,  $N_G(\{g\})$  will consist of all elements of  $G$  that commute with  $g$ . It should be noted that  $N_G(\{g\})$  is not the same thing as  $N_G([g])$ , the normalizer of the group generated by  $g$ . The former is the set of elements which commute with  $g$ , and the latter is the largest subgroup which contains  $[g]$  as a normal subgroup.

We have seen that the normalizer of a subgroup  $H$  by  $G$  finds the largest subgroup of  $G$  that contains  $H$  as a normal subgroup. What if we asked for the *smallest* subgroup containing  $H$  that is a normal subgroup of  $G$ ? Whether  $H$  is a subgroup or a subset, we can use the following proposition.

**PROPOSITION 8.7**

Let  $S$  be a subset of a group  $G$ . Then the smallest group containing  $S$  that is a normal subgroup of  $G$  is given by

$$N^* = \bigcap_{N \in L} N,$$

where  $L$  denotes the collection of normal subgroups of  $G$  that contain  $S$ .

PROOF: The group  $G$  itself is in the collection  $L$ , so this collection is not empty. Thus, by Proposition 3.3,  $N^*$  is a subgroup of  $G$ .

Also, since each  $N$  in the collection contained the set  $S$ , the intersection will also contain  $S$ . All that needs to be shown is that  $N^*$  is normal.

If  $n$  is an element of  $N^*$ , and  $g$  is an element of  $G$ , then since each  $N$  is a normal subgroup of  $G$ , and  $n$  would be in all of the groups  $N$ ,

$$g \cdot n \cdot g^{-1} \in N \quad \text{for all } N \in L.$$

Thus,  $g \cdot n \cdot g^{-1}$  is in the intersection of all of the  $N$ 's, which is  $N^*$ . Hence, by Proposition 4.4,  $N^*$  is a normal subgroup of  $G$ .  $\square$

We will call this subgroup the *normal closure* of  $S$ . The *SageMath* command **NormalClosure(G, S)** computes this subgroup. With this command, we can systematically find *all* of the normal subgroups of a given group. Note that if  $S$  contains a single element, we can use the element instead of a set.

**Computational Example 8.5**

Find all of the normal subgroups of  $S_3$ , using the generators  $a$  and  $b$ .

SOLUTION: We would like to see if there are any other normal subgroups besides the two trivial groups. Since a proper subgroup must contain one of the elements  $\{a, b, a \cdot b, b^2, a \cdot b^2\}$ , we have five groups to try.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^2, e); Define(b^3, e); Define(b*a, a*b^2)
S3 = Group(); S3
{e, a, b, a*b, b^2, a*b^2}
NormalClosure(S3, a)
{e, a, b, a*b, b^2, a*b^2}
NormalClosure(S3, b)
{e, b, b^2}
NormalClosure(S3, a*b)
{e, a, b, a*b, b^2, a*b^2}
NormalClosure(S3, b^2)
{e, b, b^2}
NormalClosure(S3, a*b^2)
{e, a, b, a*b, b^2, a*b^2}
```

We see that using  $b$  and  $b^2$  produces the normal subgroup of order 3,  $A_3$ . The other elements produced the whole group. In fact, if we considered a normal subgroup generated by *two* elements, it is obvious that this would have to contain a normal subgroup already found. But the smallest found was  $A_3$ , and no larger subgroup could still be proper. Thus, we have used *SageMath* to prove that the only proper normal subgroup of  $S_3$  is  $A_3$ . □

This method of exhaustion works well for small groups, but one can imagine that this method would be time consuming for larger groups. In the next section, we will find a short-cut so that we will not have to try every element of the group, but rather just a handful of elements.

## Problems for §8.2

- 1 For each element  $g$  in  $D_4$ , find the normalizer  $N_{D_4}(\{g\})$ .
- 2 For each element  $g$  in  $D_5$ , find the normalizer  $N_{D_5}(\{g\})$ .
- 3 There are five subgroups of  $D_4$  of order 2:  $\{e, a^2\}$ ,  $\{e, b\}$ ,  $\{e, a \cdot b\}$ ,  $\{e, a^2 \cdot b\}$ , and  $\{e, a^3 \cdot b\}$ . For each subgroup, find  $N_{D_4}(H)$ .
- 4 There are five subgroups of  $D_5$  of order 2:  $\{e, b\}$ ,  $\{e, a \cdot b\}$ ,  $\{e, a^2 \cdot b\}$ ,  $\{e, a^3 \cdot b\}$ , and  $\{e, a^4 \cdot b\}$ . For each subgroup, find  $N_{D_5}(H)$ .
- 5 Must the normalizer of an element  $N_G(\{g\})$  be abelian?
- 6 Let  $G$  be any group. Prove that

$$Z(G) = \bigcap_{g \in G} N_G(\{g\}).$$

- 7 Let  $G$  be a group, and let  $g$  be an element of  $G$ . Prove that

$$N_G(\{g\}) = N_G(\{g^{-1}\}).$$

- 8 Let  $G$  be a group, and let  $g$  be an element of  $G$ , and  $k$  be any integer. Prove that

$$N_G(\{g\}) \subseteq N_G(\{g^k\}).$$

- 9 Let  $G$  be a group. Prove that for any subset  $S$ ,

$$Z(G) \subseteq N_G(S).$$

- 10 Let  $G$  be a group. Prove that  $N_G(\{g\}) = G$  if, and only if,  $g \in Z(G)$ .

For Problems 11 through 16: Find the normal closure of the following sets in  $D_4$ .

11  $\{a\}$   
12  $\{a^2\}$

13  $\{b\}$   
14  $\{a \cdot b\}$

15  $\{a^2, b\}$   
16  $\{b, a \cdot b\}$

For Problems 17 through 20: Find the normal closure of the following sets in  $D_5$ .

17  $\{a\}$

18  $\{a^2\}$

19  $\{b\}$

20  $\{a \cdot b\}$

#### Interactive Problems

- 21 Use *SageMath* to find the normalizer  $N_{D_6}(\{x\})$  for each of the 12 elements of the group  $D_6$  listed in Problem 15 of §8.1. For which elements is the normalizer the same subgroup?
- 22 Use *SageMath*'s **NormalClosure** command to find all of the normal subgroups of the group  $D_6$  given in Problem 15 of §8.1.
- 

### 8.3 Conjugacy Classes and Simple Groups

In the last section, we used the command **NormalClosure(G, S)** to find the smallest group containing the subset  $S$  that was a normal group of  $G$ . Let us look closely at how this *SageMath* command works. We know that if the element  $a$  is in this normal subgroup, then  $g \cdot a \cdot g^{-1}$  must also be in the group for all  $g$  in  $G$ . Many of the elements that must be in the normal subgroup can be found in this way.

**DEFINITION 8.3** Let  $G$  be a group. We say that the element  $u$  is *conjugate* to the element  $v$  if there exists an element  $g$  in  $G$  such that  $u = g \cdot v \cdot g^{-1}$ .

Note that every element is conjugate to itself, for we can let  $g$  be the identity element. Also note that if  $u$  is conjugate to  $v$ , then  $v$  is also conjugate to  $u$ , since

$$v = (g^{-1}) \cdot u \cdot (g^{-1})^{-1}.$$

Finally, if  $u$  is conjugate to  $v$ , and  $v$  in turn is conjugate to  $w$ , we can see that  $u$  is conjugate to  $w$ . This is easy to see, since there is a  $g$  and  $h$  such that  $u = g \cdot v \cdot g^{-1}$  and  $v = h \cdot w \cdot h^{-1}$ . Then

$$u = g \cdot v \cdot g^{-1} = g \cdot (h \cdot w \cdot h^{-1}) \cdot g^{-1} = (g \cdot h) \cdot w \cdot (g \cdot h)^{-1}.$$

Recall that in Definition 2.3, we defined an equivalence relationship as any relationship having three properties:

1. Every element  $u$  is equivalent to itself.
2. If  $u$  is equivalent to  $v$ , then  $v$  is equivalent to  $u$ .
3. If  $u$  is equivalent to  $v$ , and  $v$  in turn is equivalent to  $w$ , then  $u$  is equivalent to  $w$ .

These were called the reflexive, symmetric, and transitive properties. We used the equivalence relationships of cosets in §4.4 to form a partition of the group, which gave us the quotient groups. In the same way, we can use the equivalence relationship of conjugates to form a different partition of the group, called *conjugacy classes*. Unlike cosets, though, the conjugacy classes will not be all the same size. The conjugacy class containing the element  $u$  is given by

$$\{g \cdot u \cdot g^{-1} \mid g \in G\}$$

### Computational Example 8.6

Find all of the conjugacy classes of  $S_4$ .

**SOLUTION:** The *SageMath* command for finding all of the conjugacy classes of a group  $G$  is **ConjugacyClasses(G)**. Let us find the conjugacy classes of  $S_4$ , which are generated by the cycles  $(1\ 2)$  and  $(2\ 3\ 4)$ .

```
S4 = Group( C(1,2), C(2,3,4) ); S4
```

```
{(), (1, 2), (2, 3), (1, 3, 2), (1, 2, 3), (1, 3), (3, 4),
 (1, 2)(3, 4), (2, 4, 3), (1, 4, 3, 2), (1, 2, 4, 3), (1, 4, 3),
 (2, 3, 4), (1, 3, 4, 2), (2, 4), (1, 4, 2), (1, 3)(2, 4),
 (1, 4, 2, 3), (1, 2, 3, 4), (1, 3, 4), (1, 2, 4), (1, 4),
 (1, 3, 2, 4), (1, 4)(2, 3)}
```

```
ConjugacyClasses(S4)
```

```
{ {()}, {(1, 2), (2, 3), (1, 3), (3, 4), (2, 4), (1, 4)},
 {(1, 3, 2), (1, 2, 3), (2, 4, 3), (1, 4, 3), (2, 3, 4),
 (1, 4, 2), (1, 3, 4), (1, 2, 4)}, {(1, 2)(3, 4), (1, 3)(2, 4),
 (1, 4)(2, 3)}, {(1, 4, 3, 2), (1, 2, 4, 3), (1, 3, 4, 2),
 (1, 4, 2, 3), (1, 2, 3, 4), (1, 3, 2, 4)} }
```

The identity element is in a class by itself since  $g \cdot e \cdot g^{-1}$  will always produce  $e$ . But the cycle notation reveals an interesting fact about the other four classes: one contains all of the transpositions, one contains all of the 3-cycles, one contains all of the 4-cycles, and one conjugacy class contains the products of two disjoint transpositions. Problems 16 and 17 of §6.2 may help shed some light on why this happens. □

The conjugacy classes are very useful for finding normal subgroups, since whenever one element of a conjugacy class is in a normal subgroup of  $G$ , the entire conjugacy class must be in the normal subgroup. Thus, in order to find *all* normal subgroups of  $S_4$  we only have to try the unions of different

combinations of the conjugacy classes. Furthermore, the identity element is guaranteed to be in every subgroup.

### **Example 8.7**

Use Example 8.6 to find all of the normal subgroups of  $S_4$ .

SOLUTION: It would be helpful if we label the conjugacy classes.

$$A = \{(12), (13), (14), (23), (24), (34)\}$$

$$B = \{(12)(34), (13)(24), (14)(23)\}$$

$$C = \{(123), (124), (132), (134), (142), (143), (234), (243)\}$$

$$D = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$$

$$E = \{()\}$$

Then a non-trivial normal subgroup would have to be one of the following unions of conjugacy classes.

|                          |             |
|--------------------------|-------------|
| $E \cup A$               | 7 elements  |
| $E \cup B$               | 4 elements  |
| $E \cup C$               | 9 elements  |
| $E \cup D$               | 7 elements  |
| $E \cup A \cup B$        | 10 elements |
| $E \cup A \cup C$        | 15 elements |
| $E \cup A \cup D$        | 13 elements |
| $E \cup B \cup C$        | 12 elements |
| $E \cup B \cup D$        | 10 elements |
| $E \cup C \cup D$        | 15 elements |
| $E \cup A \cup B \cup C$ | 18 elements |
| $E \cup A \cup B \cup D$ | 16 elements |
| $E \cup A \cup C \cup D$ | 21 elements |
| $E \cup B \cup C \cup D$ | 18 elements |

Of course, the last combination  $E \cup A \cup B \cup C \cup D$  would give us the whole group. We actually can test all of these combinations without the help of *SageMath*. This table also includes the number of elements in the subsets, and we can eliminate almost all of these combinations with Lagrange's theorem (4.1). Only the second and eighth combinations has the number of elements divide 24. The combination

$$E \cup B = \{(), (12)(34), (13)(24), (14)(23)\}$$

we have seen before, so we recognize this is the normal subgroup which is isomorphic to  $Z_8^*$ . The other combination,  $E \cup B \cup C$ , contains the even permutations of  $S_4$ , so this is the normal subgroup  $A_4$ . Hence, we can use conjugacy

classes to prove that there are precisely two non-trivial normal subgroups of  $S_4$ .  $\square$

### **Computational Example 8.8**

Use *SageMath* to find all of the normal subgroups of  $A_5$ .

SOLUTION: This group is generated by the cycles  $(1\ 2\ 3)$  and  $(3\ 4\ 5)$ , so the conjugacy classes are as follows:

```
A5 = Group( C(1,2,3), C(3,4,5) )
ConjugacyClasses(A5)
{ {()}, {(1, 3, 2), (1, 2, 3), (2, 4, 3), (1, 4, 3), (2, 3, 4),
 (1, 4, 2), (1, 3, 4), (1, 2, 4), (3, 5, 4), (2, 5, 4),
 (1, 5, 4), (3, 4, 5), (2, 5, 3), (1, 5, 3), (2, 4, 5),
 (2, 3, 5), (1, 5, 2), (1, 4, 5), (1, 3, 5), (1, 2, 5)},
 {(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 2)(4, 5),
 (2, 3)(4, 5), (1, 3)(4, 5), (1, 2)(3, 5), (2, 4)(3, 5),
 (1, 4)(3, 5), (1, 3)(2, 5), (2, 5)(3, 4), (1, 4)(2, 5),
 (1, 5)(2, 3), (1, 5)(3, 4), (1, 5)(2, 4)}, {(1, 5, 4, 3, 2),
 (1, 3, 5, 4, 2), (1, 3, 2, 5, 4), (1, 2, 4, 5, 3),
 (1, 2, 5, 3, 4), (1, 5, 3, 2, 4), (1, 4, 5, 2, 3),
 (1, 4, 3, 5, 2), (1, 5, 2, 4, 3), (1, 2, 3, 4, 5),
 (1, 4, 2, 3, 5), (1, 3, 4, 2, 5)}, {(1, 2, 5, 4, 3),
 (1, 5, 4, 2, 3), (1, 2, 3, 5, 4), (1, 4, 5, 3, 2),
 (1, 5, 3, 4, 2), (1, 4, 2, 5, 3), (1, 3, 4, 5, 2),
 (1, 3, 5, 2, 4), (1, 5, 2, 3, 4), (1, 3, 2, 4, 5),
 (1, 2, 4, 3, 5), (1, 4, 3, 2, 5)} }
```

This group also has only five conjugacy classes, so it should be no more difficult to find the normal subgroups than  $S_4$ . We can pick a representative element from each of the non-trivial conjugacy classes:  $(1\ 2\ 3)$ ,  $(1\ 2)(3\ 4)$ ,  $(1\ 2\ 3\ 4\ 5)$ , and  $(1\ 2\ 3\ 5\ 4)$ . From this point we can proceed as in the  $S_4$  example to show that there are *no* non-trivial normal subgroups of  $A_5$ . (See Problem 7.) However, we can use *SageMath* to speed up the process.

```
len(NormalClosure(A5, C(1,2,3) ))
60
len(NormalClosure(A5, C(1,2)*C(3,4) ))
60
len(NormalClosure(A5, C(1,2,3,4,5) ))
60
len(NormalClosure(A5, C(1,2,3,5,4) ))
60
```

This shows that if any of the 4 representative elements are in a non-trivial normal subgroup of  $A_5$ , the subgroup would have to be all 60 elements of  $A_5$ . Hence, there can be no nontrivial normal subgroups of  $A_5$ .  $\square$

We will see that this is a rather unusual property for a group to have, so we will give this a special name.

**DEFINITION 8.4** A group is said to be *simple* if it contains no normal subgroups besides itself and the identity subgroup.

The groups  $Z_p$ , for  $p$  a prime number, are the first examples we have seen of simple groups. We now have seen an example of a non-cyclic simple group,  $A_5$ . In fact this is the *smallest* non-cyclic simple group!

Let us find other simple groups. The natural place to look is higher order alternating groups. Let us use *SageMath*'s help to find the sizes of the conjugacy classes of  $A_6$ . This group is generated by the cycles  $(1\ 2\ 3)$  and  $(2\ 3\ 4\ 5\ 6)$ .

```
A6 = Group(C(1, 2, 3), C(2, 3, 4, 5, 6))
len(A6)
360
S = ConjugacyClasses(A6)
[ len(x) for x in S ]
[1, 40, 45, 72, 72, 90, 40]
```

Thus, we see that there are 7 conjugacy classes of  $A_6$ , one of size 1 (the identity), two of size 40, two of size 72, one of size 45, and one of size 90.

### Example 8.9

Use the above result to show that  $A_6$  is simple.

SOLUTION: If there were a non-trivial subgroup  $N$ , its size would be a factor of 360, hence  $|N| = 180, 120, 90, 72, 60$ , or 45. Note it cannot be 40 or smaller, since it must contain the identity and at least one other conjugacy class. Clearly,  $|N| \neq 45$  since there is no conjugacy class of size 44. Thus,  $|N|$  is even, so we must include both odd conjugacy classes, 1 and 45, plus at least one other. Hence,  $|N| \geq 86$ . At this point we see that  $|N|$  is a multiple of 5, so both conjugacy classes of size 72 must be included to get the sum to be a multiple of 5. At this point  $|N| \geq 190$ , which is impossible. So  $A_6$  is a simple group.  $\square$

Our goal is to show that  $A_n$  is simple for all  $n > 4$ . We begin by showing that all 3-cycles are in one conjugacy class.

### LEMMA 8.1

If  $n > 4$ , any two 3-cycles are conjugate in  $A_n$ . Furthermore, the conjugate of a 3-cycle is again a 3-cycle.

**PROOF:** We begin by showing that the conjugate of a 3-cycle is again a 3-cycle. Let  $(abc)$  be a 3-cycle, and let  $\phi$  be any permutation in  $A_n$ . Suppose that  $x = \phi(a)$ ,  $y = \phi(b)$ , and  $z = \phi(c)$ . Then we can compute

$$\phi \cdot (abc) \cdot \phi^{-1} = (xyz).$$

Thus the conjugate of a 3-cycle is another 3-cycle.

Next we will show that any 3-cycle is conjugate to the element  $(1\ 2\ 3)$  in  $A_n$ . Let  $(uvw)$  be a 3-cycle. Since  $n > 4$  there must be at least two numbers not mentioned in this 3-cycle, so we will call two of them  $x$  and  $y$ . Consider the permutation

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ u & v & w & x & y & \dots \end{pmatrix}.$$

Here, the dots indicate that when  $n > 5$ , we can complete the permutation in any way so that the numbers on the bottom row will be a permutation of the numbers 1 through  $n$ .

Now  $\phi$  will either be an even permutation or an odd permutation. If  $\phi$  is an odd permutation, we can consider instead the permutation

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ u & v & w & y & x & \dots \end{pmatrix}.$$

So we may assume that  $\phi$  is an even permutation. Thus  $\phi$  is in  $A_n$ , and we can compute

$$\phi \cdot (1\ 2\ 3) \cdot \phi^{-1} = (uvw).$$

Therefore, any 3-cycle is conjugate to  $(1\ 2\ 3)$ , and so any two 3-cycles are conjugate to each other in  $A_n$  whenever  $n > 4$ .  $\square$

With this lemma, we can show that  $A_n$  will be a simple group whenever  $n > 4$ . This was originally proved by Abel using a long case-by-case argument. (See the Historical Diversion on page 253.) Since *SageMath* helped us show that  $A_5$  and  $A_6$  are simple, the argument is greatly simplified.

### **THEOREM 8.1: Abel's Theorem**

*The alternating group  $A_n$  is simple for all  $n > 4$ .*

**PROOF:** Suppose that  $N$  is a proper normal subgroup of  $A_n$ , and let  $\phi$  be an element of  $N$  besides the identity. By Proposition 8.2,  $A_n$  is centerless. Since Proposition 6.1 tells us that  $A_n$  is generated by 3-cycles, there must be at least one 3-cycle that does not commute with  $\phi$ , say  $(abc)$ . Thus,  $\phi \cdot (abc)$  is not equal to  $(abc) \cdot \phi$ , or equivalently,  $(abc) \cdot \phi \cdot (acb) \cdot \phi^{-1}$  is not the identity element.

Since  $N$  is a normal subgroup,  $(abc) \cdot \phi \cdot (acb)$  must be in  $N$ . Therefore,  $(abc) \cdot \phi \cdot (acb) \cdot \phi^{-1}$  must also be in  $N$ . But  $\phi \cdot (acb) \cdot \phi^{-1}$  is the conjugate of a 3-cycle, so by Lemma 8.1 this is also a 3-cycle, say  $(xyz)$ . Thus,  $N$  contains

a product of two 3-cycles,  $(a\ b\ c) \cdot (x\ y\ z)$ , which is not the identity. In essence we can say that there is a non-identity element of  $N$  that moves at most six numbers, labeled  $a$ ,  $b$ ,  $c$ ,  $x$ ,  $y$ , and  $z$ . If there are duplicates in this list, we can add arbitrary numbers so that we have six different numbers.

Here's where we can take advantage of the fact that  $A_6$  is known to be simple. Consider the subgroup  $H$  of  $A_n$  consisting of all even permutations of the six numbers  $a$ ,  $b$ ,  $c$ ,  $x$ ,  $y$ , and  $z$ . We have just showed that there is a nontrivial intersection of  $N$  and  $H$ . Let this intersection be  $M$ . Whenever  $x$  is in  $M$  and  $h$  is in  $H$ , then  $h \cdot x \cdot h^{-1}$  is in both  $H$  and  $N$ . Thus  $h \cdot x \cdot h^{-1}$  is in  $M$ . Hence  $M$  is a nontrivial normal subgroup of  $H$ .

But  $H$  is isomorphic to  $A_6$  which we have proven to be a simple group. Thus  $M$  must be all of  $H$ . In particular  $M$  contains a 3-cycle, and so  $N$  contains a 3-cycle. By Lemma 8.1 all 3-cycles of  $A_n$  are conjugate, so  $N$  contains all 3-cycles of  $A_n$ . Finally, by Proposition 6.1 the 3-cycles generate  $A_n$ , so  $N$  must be all of  $A_n$ . Therefore,  $A_n$  is simple whenever  $n > 4$ .  $\square$

This theorem has an immediate application to the permutation groups  $S_n$ .

### **COROLLARY 8.1**

*If  $n > 4$ , then the only proper normal subgroup of  $S_n$  is  $A_n$ .*

PROOF: Suppose that there were another normal subgroup,  $N$ . Then the intersection of  $N$  with  $A_n$  would be another normal subgroup of  $S_n$ , and so would be a normal subgroup of  $A_n$ . Since  $A_n$  is simple for  $n > 4$ , this intersection must either be the identity or all of  $A_n$ .

Suppose that the intersection is all of  $A_n$ . Then  $N$  contains  $A_n$ , and if  $N$  is not equal to  $A_n$ ,  $N$  would contain more than half of the elements of  $S_n$ . But this would contradict Lagrange's theorem (4.1) unless  $N = S_n$ .

Suppose that the intersection of  $N$  and  $A_n$  is just the identity element. Then since both  $N$  and  $A_n$  are normal subgroups, we have by Corollary 7.1,

$$N \cdot A_n \approx N \times A_n.$$

If  $N$  is not just the identity element, this quickly leads to a contradiction, for  $N$  could have order of at most 2, telling us that  $S_n$  was isomorphic to  $Z_2 \times A_n$ . But this is ridiculous, for we saw in Proposition 8.2 that  $S_n$  was centerless, whereas  $Z_2 \times A_n$  clearly has both  $(0, ( ))$  and  $(1, ( ))$  in its center. Therefore, the only normal subgroups of  $S_n$  for  $n > 4$  are  $S_n$  itself,  $A_n$ , and the identity element.  $\square$

We now have found two sequences of simple groups, namely  $Z_p$  for  $p$  being a prime number, and  $A_n$  for all  $n > 4$ . Are any of the other groups that we have looked at simple groups?

### **Computational Example 8.10**

Find the normal subgroups of the group  $\text{Aut}(Z_{24}^*)$ , the group of order 168

generated by the 187th and 723rd permutation elements.

```
DisplayPermInt = true
A = Group( NthPerm(187), NthPerm(723) ); A
{1, 27, 61, 87, 122, 149, 187, 231, 244, 270, 331, 357, 374,
404, 437, 467, 496, 548, 558, 593, 640, 670, 684, 714, 723,
745, 783, 805, 844, 870, 931, 957, 962, 989, 1027, 1071,
1096, 1148, 1158, 1193, 1214, 1244, 1277, 1307, 1366, 1384,
1410, 1428, 1445, 1466, 1509, 1549, 1566, 1588, 1653, 1675,
1681, 1707, 1741, 1767, 1822, 1862, 1889, 1902, 1966, 1984,
2010, 2028, 2054, 2084, 2117, 2147, 2166, 2188, 2253, 2275,
2285, 2306, 2349, 2389, 2403, 2425, 2463, 2485, 2566, 2584,
2610, 2628, 2662, 2702, 2729, 2742, 2780, 2798, 2843, 2861,
2897, 2927, 2954, 2984, 3018, 3071, 3076, 3110, 3144, 3185,
3206, 3220, 3288, 3306, 3328, 3346, 3361, 3387, 3421, 3447,
3487, 3517, 3531, 3561, 3618, 3671, 3676, 3710, 3737, 3767,
3794, 3824, 3888, 3906, 3928, 3946, 3984, 4025, 4046, 4060,
4083, 4105, 4143, 4165, 4213, 4231, 4257, 4275, 4362, 4392,
4402, 4432, 4488, 4506, 4528, 4546, 4577, 4607, 4634, 4664,
4703, 4721, 4760, 4778, 4809, 4839, 4849, 4879, 4935, 4953,
4975, 4993}
```

SOLUTION: As large as this group is, *SageMath* can still quickly find the conjugacy classes.

#### **ConjugacyClasses (A)**

```
{ {1}, {27, 61, 87, 122, 270, 404, 593, 640, 714, 723, 745,
1566, 1681, 2306, 2425, 3110, 3421, 3767, 4143, 4488, 4528},
{149, 187, 244, 357, 374, 467, 548, 558, 844, 989, 1148,
1307, 1366, 1384, 1410, 1428, 1445, 1588, 1653, 1741, 1767,
1889, 2028, 2147, 2188, 2285, 2389, 2463, 2485, 2566, 2702,
2798, 2984, 3071, 3076, 3220, 3306, 3361, 3387, 3531, 3671,
3737, 3824, 3928, 3984, 4083, 4105, 4213, 4362, 4392, 4402,
4432, 4634, 4703, 4839, 4975}, {231, 331, 437, 496, 670, 684,
783, 805, 870, 962, 1193, 1244, 1466, 1675, 1707, 1822, 2010,
2054, 2166, 2349, 2403, 2584, 2742, 2861, 2927, 3018, 3206,
3346, 3447, 3517, 3710, 3794, 3888, 4025, 4165, 4257, 4506,
4546, 4607, 4760, 4849, 4935}, {931, 1071, 1096, 1277, 1509,
1902, 1984, 2084, 2275, 2610, 2662, 2843, 2954, 3185, 3288,
3487, 3618, 3946, 4046, 4275, 4577, 4778, 4879, 4953},
{957, 1027, 1158, 1214, 1549, 1862, 1966, 2117, 2253, 2628,
2729, 2780, 2897, 3144, 3328, 3561, 3676, 3906, 4060, 4231,
4664, 4721, 4809, 4993} }
```

So we have six conjugacy classes of this group, one of which is just the identity. The other five classes can be represented by first element in each list,

which are the 27th, 149th, 231st, 931st, and 957th permutations. This list alone can be used to show that  $A$  is simple, (see Problem 8), but we can also verify that the normal closure of each of these five elements yields the whole group.

```
len(NormalClosure(A, NthPerm(27) ))
168
len(NormalClosure(A, NthPerm(149) ))
168
len(NormalClosure(A, NthPerm(231) ))
168
len(NormalClosure(A, NthPerm(931) ))
168
len(NormalClosure(A, NthPerm(957) ))
168
```

Thus, any proper normal subgroup cannot contain any of these five elements; we have shown that there are no proper normal subgroups, so  $\text{Aut}(Z_{24}^*)$  is a simple group.  $\square$

This is the second largest non-cyclic simple group. ( $A_5$  is the smallest and  $A_6$  is the third smallest.) See Problems 9 through 15 for more examples of simple groups.

We can have *SageMath* give us a structure description of a permutation group by including the integer representation of a set of generators for the arguments.

```
StructureDescription(187, 723)
PSL(3,2)
```

So one of the official names for the group  $\text{Aut}(Z_{24}^*)$  is  $L_3(2)$ . This group is the beginning of yet another infinite family of simple groups, called the Chevalley groups. We will not go into all of the ways this group can be generalized to produce these other groups, but we will mention an important result that has taken place during the 20th century. It was once thought that *all* finite simple groups were either the cyclic groups of prime order, the alternating groups, or one of the Chevalley or twisted Chevalley groups. (One of these groups turns out to be not quite simple. Yet taking half of the elements forms a new simple group, just as we took half of the elements of  $S_n$  to form the simple groups  $A_n$ .) But there were several other simple groups that were discovered, called *sporadic* groups. In the 1960s and 1970s it was proved that there are exactly 26 sporadic groups, ranging in size from a mere 7,920 elements to the monstrous

808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 elements! These 26 sporadic groups are listed in [13]. Because these have been proven to be the only sporadic groups, all finite simple groups are now known.

**Problems for §8.3**

- 1 Find all of the conjugacy classes of the group  $D_4$ . (See [Table 8.1](#).)
- 2 Find all of the conjugacy classes of the quaternion group  $Q$ . (See [Table 5.3](#) in [Chapter 5](#) for the Cayley table of  $Q$ .)
- 3 Find all of the conjugacy classes of the group  $D_5$ . (See [Table 5.5](#).)
- 4 Show that the conjugacy class for an element  $x$  has only one element if, and only if,  $x$  is in the center of the group.
- 5 Show that if  $G$  is a finite group of odd order, and  $x \in G$  is not the identity, then  $x^{-1}$  is not in the conjugacy class of  $x$ .
- 6 Show that if  $G$  is a finite group, and  $x$  and  $y$  are in the same conjugacy class, then  $|N_G(\{x\})| = |N_G(\{y\})|$ .
- 7 *SageMath* showed that the group  $A_5$  had conjugacy classes of orders 1, 12, 12, 15, and 20. Using this information alone, without using Abel's theorem (8.1), prove that  $A_5$  is simple. Use Example 8.9 as a guide.
- 8 *SageMath* showed that the group  $\text{Aut}(Z_{24}^*)$  had conjugacy classes of orders 1, 21, 24, 24, 42, and 56. Using this information alone, prove that  $\text{Aut}(Z_{24}^*)$  is simple.
- 9 The group  $L_2(8)$  has 504 elements, and has nine conjugacy classes of orders 1, 56, 56, 56, 56, 63, 72, 72, and 72. Prove that  $L_2(8)$  is simple. This is another example of a Chevalley group.
- 10 The group  $L_2(11)$  has 660 elements, and has eight conjugacy classes of orders 1, 55, 60, 60, 110, 110, 132, and 132. Prove this group is simple. This group is related to the group  $\text{Aut}(Z_{11} \times Z_{11})$ .
- 11 The group  $L_2(13)$  has 1092 elements, and has nine conjugacy classes of orders 1, 84, 84, 91, 156, 156, 156, 182, and 182. Prove this group is simple. This group is related to the group  $\text{Aut}(Z_{13} \times Z_{13})$ .
- 12 The group  $L_2(17)$  has 2448 elements, and has eleven conjugacy classes of orders 1, 144, 144, 153, 272, 272, 272, 306, 306, and 306. Prove this group is simple. This group, the seventh smallest non-cyclic simple group, is related to the group  $\text{Aut}(Z_{17} \times Z_{17})$ .
- 13 Looking at the pattern of the last 3 problems, determine the eighth smallest non-cyclic simple group.
- 14 The group  $M_{11}$  has order 7920, and has 10 conjugacy classes of orders 1, 165, 440, 720, 720, 990, 990, 990, 1320, and 1584. Prove that  $M_{11}$  is simple. This is the smallest of the 26 sporadic simple groups.

## Historical Diversion

# Niels Abel (1802–1829)

---

Niels Abel was born in Norway at a time when the country was experiencing extreme poverty and hunger due to the Napoleonic wars. His father, Søren Georg Abel, had degrees in philosophy and theology, and served as a Protestant minister at Gjerstad. Abel was the second of seven children, and was taught by his father until he was 13 years old. The family's poverty was intensified since Abel's father was often drunk, and his mother was accused of lacking morals.

In 1815 Abel was sent to the Cathedral School in Christiania. Abel started out uninspired, but in 1817, a new mathematics teacher Bernt Holmboë joined the school, and took an interest in Abel. Within a year, Abel was reading the works of Euler, Newton, d'Alembert, Lagrange, and Laplace.

But in 1820, Abel's father died, and it was up to Abel to support his mother and family. Holmboë worked to raise money from his colleagues to allow Abel to enter the University of Christiania in 1821. During Abel's final year in school, he worked on the quintic equation, unsolved for 250 years.

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

Abel believed he had solved the equation by radicals, and submitted a paper to the Danish mathematician Ferdinand Degen. Degen asked Abel to provide an example, and as Abel worked out the example, he found an error in his paper. Degen advised Abel to work instead on elliptic integrals, a new field that had promising consequences for both analysis and mechanics.

Abel took Degen's advice, and wrote several papers on functional equations and integrals. On a visit to see Degen, Abel met Christine Kemp, who later became his fiancée. Returning to Christiania, he again worked on the quintic equation, and in 1824 he proved the impossibility of solving the general equation in radicals. He send his proof to Gauss, who dismissed it as a crank, and never read the proof. Abel continued to work on elliptic functions in competition with Carl Jacobi. By this time Abel had become famous among the mathematical centers, and efforts were made to secure him a suitable position.

In 1828, Abel became seriously ill from tuberculosis, and his condition intensified due to Abel's sled trip to visit his fiancée. In spite of a reprieve long enough for the couple to spend Christmas together, he died soon after on April 6, 1829, just 2 days before word arrived that he was appointed as a professor at the University of Berlin.



- 15** The group  $L_3(4)$  has 20160 elements, and has 10 conjugacy classes of orders 1, 315, 1260, 1260, 1260, 2240, 2880, 2880, 4032, and 4032. Prove that this group is simple. Show that even though  $A_8$  is a simple group with the same order, these two groups are not isomorphic.

Hint: How many 3-cycles are in  $A_8$ ? What does Lemma 8.1 say about the 3-cycles?

- 16** Find a representative element for each of the seven conjugacy classes of the group  $A_6$ . The number of elements in each conjugacy class is given in Example 8.9.

Hint: Are  $(1\ 2\ 3\ 4\ 5)$  and  $(1\ 2\ 3\ 5\ 4)$  in the same conjugacy class? Why are  $(1\ 2)(3\ 4\ 5\ 6)$  and  $(1\ 2)(3\ 4\ 6\ 5)$  in the same conjugacy class?

- 17** Using the counting methods used to estimate the 168 elements of  $\text{Aut}(Z_{24}^*)$ , find the maximum number of elements of  $\text{Aut}(Z_2 \times Z_2 \times Z_2 \times Z_2)$ . This group is in fact simple, and contains the number of elements predicted by this estimate. Are there any other simple groups that we have seen of this order?

### Interactive Problems

- 18** The following commands load a group of order 20 into *SageMath*.

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^5, e); Define(b^4, e); Define(b*a, a^2*b)
M = Group()
```

Find the conjugacy classes of this group, and use this to find all of the normal subgroups of  $M$ .

- 19** The following commands load a group of order 24 into *SageMath*.

```
DisplayPermInt = true
G = Group(NthPerm(2374), NthPerm(6212)); G
{1, 2374, 4517, 6212, 6841, 9929, 11637, 13016, 13698, 15367,
 18454, 19853, 21239, 21896, 24132, 25315, 28226, 28986,
 30928, 31590, 33108, 37381, 38807, 39487}
StructureDescription(2374, 6212)
SL(2,3)
```

Find the conjugacy classes of this group, and use this to find all of the normal subgroups of  $G$ .

## 8.4 Subnormal Series and the Jordan-Hölder Theorem

In this section, we will study the concept of *solvable* groups. Every group will be classified either as solvable or insoluble, and in fact most of the groups we have looked at so far turn out to be solvable.

Solvable groups play a key role in studying polynomial equations. Whether or not a given polynomial can be solved in terms of radicals (square roots, cube roots, etc.) depends on whether a certain group corresponding to that polynomial is a solvable group. In fact this application is the origin of the term “solvable group.”

Before we introduce the true definition of a solvable group, we must make some preliminary definitions. We have already encountered situations in which we had a normal subgroup of a normal subgroup, such as in the third isomorphism theorem. But suppose we have a whole series of subgroups of a group  $G$ , each one fitting inside of the previous one like Russian dolls.

**DEFINITION 8.5** A *subnormal series* for a group  $G$  is a sequence  $G_0, G_1, G_2, \dots, G_n$  of subgroups of  $G$  such that

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\},$$

where each  $G_i$  is a normal subgroup of  $G_{i-1}$  for  $i = 1, 2, \dots, n$ .

A subnormal series is called a *normal series* if it satisfies the stronger condition that all of the groups  $G_i$  are normal subgroups of the original group  $G$ . We will be mainly interested in subnormal series, but there are a few of the exercises regarding normal series.

### Motivational Example 8.11

Consider the group  $S_4$ , for which we have seen a normal subgroup of order 4, namely

$$K = \{(), (12)(34), (13)(24), (14)(23)\}.$$

Certainly the identity element is a normal subgroup of  $K$ , so we can write

$$S_4 \supseteq K \supseteq \{()\}$$

which would be a subnormal series of length  $n = 2$ . Is there a way that we can make a longer series out of this one? Because  $A_4$  is also a normal subgroup of  $S_4$ , and  $K$  is a normal subgroup of  $A_4$ , we can slip this group into our series. Also, the group  $K$  contains the subgroup

$$H = \{(), (12)(34)\}$$

which is a normal subgroup of  $K$  since  $K$  is abelian. Therefore, we have a longer subnormal series of length 4:

$$S_4 \supseteq A_4 \supseteq K \supseteq H \supseteq \{()\}.$$

We say that this new subnormal series is a *refinement* of the first subnormal series.  $\square$

**DEFINITION 8.6** We say that a subnormal (or normal) series

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_k = \{e\}$$

is a *refinement* of the subnormal (or normal) series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

if each subgroup  $G_i$  appears as  $H_j$  for some  $j$ .

Is there a way that we can refine our subnormal series to produce an even longer chain? Our definition did not exclude the possibility of two groups in the series being the same, so we could consider

$$S_4 \supseteq A_4 \supseteq A_4 \supseteq K \supseteq H \supseteq H \supseteq H \supseteq \{()\}.$$

Although this is a longer subnormal series, it is usually pointless to repeat the same subgroup in the series.

**DEFINITION 8.7** A *composition series* of a group  $G$  is a subnormal series

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

for which each subgroup is smaller than the proceeding subgroup, and for which there is no refinement that includes additional subgroups.

Using this definition, we see that

$$S_4 \supseteq A_4 \supseteq K \supseteq H \supseteq \{()\}$$

is a composition series for  $S_4$ , since no subgroups are repeated, and there simply is not enough room between two of these subgroups to slip in another subgroup. For example,  $A_4$  is half of  $S_4$ , so any subgroup containing more than  $A_4$  must be all of  $S_4$ . In fact, we can easily test to see whether a subnormal series is a composition series.

### PROPOSITION 8.8

*The subnormal series*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

is a composition series if, and only if, all of the quotient groups  $G_{k-1}/G_k$  are nontrivial simple groups.

**PROOF:** Note that if there are no repeated subgroups in the subnormal series, then each  $G_{k-1}/G_k$  must contain at least two elements. Likewise, if  $G_{k-1}/G_k$  is nontrivial, then  $G_{k-1}$  is not equal to  $G_k$ . So the quotient groups are nontrivial if, and only if, there are no repeated subgroups in the subnormal series.

Suppose that the subnormal series is not a composition series yet does not repeat any subgroups. Then there must be an additional group  $H$  that we can add between  $G_{k-1}$  and  $G_k$ , so that

$$G_{k-1} \supseteq H \supseteq G_k,$$

where  $H$  is a normal subgroup of  $G_{k-1}$  and  $G_k$  is a normal subgroup of  $H$ . Then by Lemma 5.6,  $H/G_k$  will be a normal subgroup of  $G_{k-1}/G_k$ , and since  $H$  is neither  $G_{k-1}$  nor  $G_k$ , we have a proper normal subgroup of  $G_{k-1}/G_k$ .

Now suppose that there is a proper normal subgroup  $N$  of  $G_{k-1}/G_k$ . Can we then lift  $N$  to find a suitable subgroup  $H$  to fit between  $G_{k-1}$  and  $G_k$ ? If we consider the canonical homomorphism  $\phi$  from  $G_{k-1}$  to the quotient group  $G_{k-1}/G_k$  we can take  $H = \phi^{-1}(N)$ . Then since  $N$  is a normal subgroup of  $G_{k-1}/G_k$ , by Corollary 5.2  $H$  will be a normal subgroup of  $G_{k-1}$ . Also,  $G_k$  will be a normal subgroup of  $H$ , for  $H$  is in  $G_{k-1}$ . Because  $N$  has at least two elements,  $H$  will be strictly larger than the kernel of  $\phi$ , yet since  $N$  is not the entire image of  $\phi$ ,  $H$  will be strictly smaller than  $G_k$ . Therefore, the subnormal series is not a composition series.

Thus, a subnormal series is a composition series if, and only if, the quotient groups  $G_{k-1}/G_k$  are nontrivial simple groups.  $\square$

The quotient groups  $G_{k-1}/G_k$  in a composition series for  $G$  are called the *composition factors* of the composition series.

For example, the composition factors for the composition series

$$S_4 \supseteq A_4 \supseteq K \supseteq H \supseteq \{()\}$$

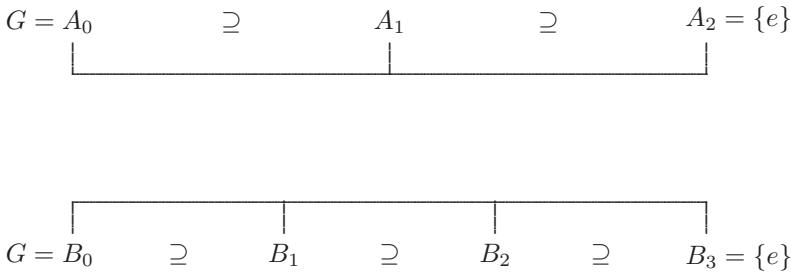
are

$$S_4/A_4 \approx Z_2, \quad A_4/K \approx Z_3, \quad K/H \approx Z_2, \quad \text{and} \quad H/\{()\} \approx Z_2.$$

It is certainly possible for a group to have more than one composition series. For example, we could have picked the subgroup  $B = \{(), (1, 4)(2, 3)\}$  instead of  $H$ , producing the composition series

$$S_4 \supseteq A_4 \supseteq K \supseteq B \supseteq \{()\}.$$

Even though this is a different composition series, the composition factors are isomorphically the same. Our goal for this section is to prove that this happens



**FIGURE 8.1:** Two subnormal series of different lengths

all of the time. However, we have yet to see why two composition series must have the same length. Even if we can prove that the composition series are the same length, the composition factors may not appear in the same order. For example, the group  $Z_{12}$  has the following two subnormal series:

$$Z_{12} \supseteq \{0, 3, 6, 9\} \supseteq \{0\}.$$

$$Z_{12} \supseteq \{0, 2, 4, 6, 8, 10\} \supseteq \{0, 4, 8\} \supseteq \{0\}.$$

No matter how we refine these series, the quotient group isomorphic to  $Z_3$  in the first series will come before any other non-trivial quotient groups, yet any refinement of the second series will have the last non-trivial quotient group isomorphic to  $Z_3$ .

It helps if we use a diagram to demonstrate the strategy that we will be using. Suppose that we have a group  $G$  with two subnormal series, one of length 2, and one of length 3, as pictured in [Figure 8.1](#).

$$G = A_0 \supseteq A_1 \supseteq A_2 = \{e\}, \quad G = B_0 \supseteq B_1 \supseteq B_2 \supseteq B_3 = \{e\}.$$

It is immediately clear that  $A_0 = B_0$  and  $A_2 = B_3$ , but  $A_1$  does not have to be either  $B_1$  or  $B_2$ .

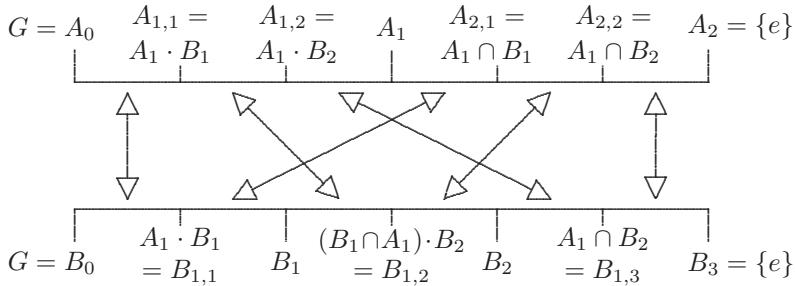
The goal is to refine both of the subnormal series by adding two subgroups within each gap of the  $A$  series, and one subgroup within each gap in the  $B$  series. Here, we will allow the possibility of duplicate subgroups in the refinements. Nonetheless, both series will have length 6, which we can express as follows:

$$G = A_0 \supseteq A_{1,1} \supseteq A_{1,2} \supseteq A_1 \supseteq A_{2,1} \supseteq A_{2,2} \supseteq A_0 = \{e\},$$

$$G = B_0 \supseteq B_{1,1} \supseteq B_1 \supseteq B_{1,2} \supseteq B_2 \supseteq B_{1,3} \supseteq B_0 = \{e\}.$$

[Figure 8.2](#) shows these set inclusions, and also gives a hint on how we are to define these intermediate subgroups.

The next step will be to show that the quotient groups for each interval of the  $A$  series is isomorphic to a quotient group for an interval of the  $B$  series,



**FIGURE 8.2:** Strategy for the refinement theorem

as shown by the arrows in Figure 8.2. Note that this scrambles the order of the quotient groups, so that the  $i^{\text{th}}$  subinterval of the  $j^{\text{th}}$  interval in the  $A$  series corresponds to the  $j^{\text{th}}$  subinterval of the  $i^{\text{th}}$  interval of the  $B$  series.

Although it is clear that

$$\begin{aligned} G \supseteq A_1 \cdot B_1 &\supseteq A_1 \cdot B_2 \supseteq A_1 \supseteq A_1 \cap B_1 \supseteq A_1 \cap B_2 \supseteq \{e\}, & \text{and} \\ G \supseteq A_1 \cdot B_1 &\supseteq B_1 \supseteq (B_1 \cap A_1) \cdot B_2 \supseteq B_2 \supseteq A_1 \cap B_2 \supseteq \{e\}, \end{aligned}$$

it is not at all clear that each is a normal subgroup of the previous group, or even that all of these sets are subgroups of  $G$ . Before we show this, we will need the following lemma.

### LEMMA 8.2

Let  $X$ ,  $Y$ , and  $Z$  be three subgroups of the group  $G$ , with  $Y$  being a subgroup of  $X$ , and  $Y \cdot Z = Z \cdot Y$ . Then

$$X \cap (Y \cdot Z) = Y \cdot (X \cap Z) = (X \cap Z) \cdot Y.$$

PROOF: Note that  $(X \cap Z) \subseteq X$ , and since  $Y \subseteq X$ ,  $Y \cdot (X \cap Z) \subseteq X$ . Also,  $(X \cap Z) \subseteq Z$ , so  $Y \cdot (X \cap Z) \subseteq Y \cdot Z$ . Hence,

$$Y \cdot (X \cap Z) \subseteq X \cap (Y \cdot Z).$$

All we need to do is prove the inclusion in the other direction. Suppose that  $x \in X \cap (Y \cdot Z)$ . Then  $x$  is in  $X$ , and can also be written as  $x = y \cdot z$ , where  $y$  is in  $Y$ , and  $z$  is in  $Z$ . But then  $z = y^{-1} \cdot x$  would be in both  $X$  and  $Z$ . Thus,

$$x = y \cdot (y^{-1} \cdot x) \in Y \cdot (X \cap Z).$$

Therefore, we have inclusions in both directions, so

$$Y \cdot (X \cap Z) = X \cap (Y \cdot Z).$$

So far, we haven't used the fact that  $Y \cdot Z = Z \cdot Y$ . By Lemma 5.2,  $Y \cdot Z$  is a subgroup of  $G$ , and so the intersection of  $X$  with  $Y \cdot Z$  is a subgroup of  $G$ . So by Lemma 5.2 again, we have

$$Y \cdot (X \cap Z) = (X \cap Z) \cdot Y.$$

□

We will need one more lemma that will help us to show the isomorphisms indicated by the arrows in [Figure 8.2](#).

### LEMMA 8.3

*Let  $X$ ,  $Y$ , and  $Z$  be three subgroups of the group  $G$ , with  $Y$  being a normal subgroup of  $X$ , and  $Z$  a normal subgroup of  $G$ . Then  $Y \cdot Z$  is a normal subgroup of  $X \cdot Z$ , and*

$$(X \cdot Z)/(Y \cdot Z) \approx X/(X \cap (Y \cdot Z)).$$

PROOF: Since  $Z$  is a normal subgroup of  $G$ , both  $Y \cdot Z$  and  $X \cdot Z$  are subgroups of  $G$  by Lemma 5.3. If we let  $y \cdot z$  be in  $Y \cdot Z$ , and  $x \cdot w$  be in  $X \cdot Z$ , then

$$\begin{aligned} (x \cdot w) \cdot (y \cdot z) \cdot (x \cdot w)^{-1} &= x \cdot (y \cdot x^{-1} \cdot x \cdot y^{-1}) \cdot w \cdot y \cdot z \cdot w^{-1} \cdot x^{-1} \\ &= (x \cdot y \cdot x^{-1}) \cdot (x \cdot (y^{-1} \cdot w \cdot y) \cdot z \cdot w^{-1} \cdot x^{-1}). \end{aligned}$$

Now,  $x \cdot y \cdot x^{-1}$  is in  $Y$ , since  $Y$  is a normal subgroup of  $X$ . Likewise,  $y^{-1} \cdot w \cdot y$  is in  $Z$ , since  $y$  is in  $G$ . Then  $(y^{-1} \cdot w \cdot y) \cdot z \cdot w^{-1}$  is in  $Z$ , and so  $x \cdot (y^{-1} \cdot w \cdot y) \cdot z \cdot w^{-1} \cdot x^{-1}$  is in  $Z$ , since  $x$  is in  $G$ . Therefore,

$$(x \cdot w) \cdot (y \cdot z) \cdot (x \cdot w)^{-1} \in Y \cdot Z,$$

and so  $Y \cdot Z$  is a normal subgroup of  $X \cdot Z$ .

We now can use the second isomorphism theorem (5.2), using  $K = Y \cdot Z$ . We have that  $X \cdot K = X \cdot Y \cdot Z = X \cdot Z$  since  $Y$  is a subgroup of  $X$ . So

$$(X \cdot Z)/(Y \cdot Z) = (X \cdot K)/K \approx X/(X \cap K) = X/(X \cap (Y \cdot Z)).$$

□

We are now ready to put the pieces together, and show any two subnormal series can be refined in such a way that the quotient groups are isomorphic.

### ***THEOREM 8.2: The Refinement Theorem***

*Suppose that there are two subnormal series for a group  $G$ . That is, there are subgroups  $A_i$  and  $B_j$  such that*

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n = \{e\},$$

and

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_m = \{e\},$$

where each  $A_i$  is a normal subgroup of  $A_{i-1}$ , and each  $B_j$  is a normal subgroup of  $B_{j-1}$ . Then it is possible to refine both series by inserting the subgroups

$$A_{i-1} = A_{i,0} \supseteq A_{i,1} \supseteq A_{i,2} \supseteq \cdots \supseteq A_{i,m} = A_i, \quad i = 1, 2, \dots, n,$$

$$B_{j-1} = B_{j,0} \supseteq B_{j,1} \supseteq B_{j,2} \supseteq \cdots \supseteq B_{j,n} = B_j, \quad j = 1, 2, \dots, m$$

in such a way that

$$A_{i,j-1}/A_{i,j} \approx B_{j,i-1}/B_{j,i}.$$

PROOF: We let

$$A_{i,j} = (A_{i-1} \cap B_j) \cdot A_i \quad \text{and} \quad B_{j,i} = (B_{j-1} \cap A_i) \cdot B_j.$$

To see that these fit the conditions we need, we first want to show that these are groups. Note that both

$$X = (A_{i-1} \cap B_{j-1}) \quad \text{and} \quad Y = (A_{i-1} \cap B_j)$$

are subgroups of  $A_{i-1}$ ,  $Y$  is a subgroup of  $X$ , and  $Z = A_i$  is a normal subgroup of  $A_{i-1}$ .

So by Lemma 5.3, both  $A_{i,j-1} = X \cdot Z$  and  $A_{i,j} = Y \cdot Z$  are subgroups of  $A_{i-1}$ . We can now use Lemma 8.3, using  $G = A_{i-1}$ . Since  $B_j$  is a normal subgroup of  $B_{j-1}$ ,  $Y$  is a normal subgroup of  $X$ , so by Lemma 8.3,  $Y \cdot Z$  is a normal subgroup of  $X \cdot Z$ , and

$$A_{i,j-1}/A_{i,j} = (X \cdot Z)/(Y \cdot Z) \approx X/(X \cap (Y \cdot Z)).$$

Now Lemma 8.2 comes into use. Since  $Y$  is a subgroup of  $X$ ,

$$\begin{aligned} X \cap (Y \cdot Z) &= Y \cdot (X \cap Z) = (A_{i-1} \cap B_j) \cdot (A_{i-1} \cap B_{j-1} \cap A_i) \\ &= (A_{i-1} \cap B_j) \cdot (A_i \cap B_{j-1}) \\ &= (A_i \cap B_{j-1}) \cdot (A_{i-1} \cap B_j). \end{aligned}$$

Thus,

$$A_{i,j-1}/A_{i,j} \approx (A_{i-1} \cap B_{j-1})/[(A_{i-1} \cap B_j) \cdot (A_i \cap B_{j-1})].$$

By switching the roles of the two series we find by the exact same argument that

$$B_{j,i-1}/B_{j,i} \approx (B_{j-1} \cap A_{i-1})/[(B_{j-1} \cap A_i) \cdot (B_j \cap A_{i-1})].$$

Notice that these are exactly the same thing, so

$$A_{i,j-1}/A_{i,j} \approx B_{j,i-1}/B_{j,i}. \quad \square$$

If we now apply the refinement theorem to two composition series we find that the composition factors will be the same.

**THEOREM 8.3: The Jordan-Hölder Theorem**

Let  $G$  be a finite group, and let

$$G = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = \{e\}$$

and

$$G = B_0 \supset B_1 \supset B_2 \supset \cdots \supset B_m = \{e\}$$

be two composition series for  $G$ . Then  $n = m$ , and the composition factors  $A_{i-1}/A_i$  are isomorphic to the composition factors  $B_{j-1}/B_j$  in some order.

**PROOF:** By the refinement theorem (8.2), there is a refinement of both composition series such that the quotient groups of the two subnormal series are isomorphic to each other in some order. In particular, the nontrivial quotient groups of one subnormal series are isomorphic to the nontrivial quotient groups of the other. But these are composition series, so any refinements merely repeat a subgroup a number of times. Thus, by eliminating these repetitions, we eliminate the trivial quotient groups and produce the original two composition series. Thus, the quotient groups  $A_{i-1}/A_i$  are isomorphic to the quotient groups  $B_{j-1}/B_j$  in some order. The fact that  $n = m$  merely comes from the one-to-one correspondence of the nontrivial quotient groups.  $\square$

The Jordan-Hölder theorem (8.3) shows that the composition factors do not depend on the composition series, but rather the finite group  $G$ . This is reminiscent of the unique factorization of integers, where every integer greater than one can be written as a unique product of prime numbers. Since the composition factors are always nontrivial simple groups, in a sense the simple groups play the same role in group theory that prime numbers play in number theory. The correspondence is heightened by the fact that  $Z_p$  is a nontrivial simple group if, and only if,  $p$  is a prime number. However, we have seen that there are other simple groups, such as  $\text{Aut}(Z_{24}^*)$  and  $A_n$  for  $n > 4$ . Since these groups are rather large (at least 60 elements), they will only show up as composition factors for very large groups.

For example, a composition series for  $S_5$  is given by

$$S_5 \supset A_5 \supset \{\()\}, \quad S_5/A_5 \approx Z_2, \quad \text{and} \quad A_5/\{\()\} \approx A_5.$$

Since  $Z_2$  and  $A_5$  are both simple groups, this is a composition series, and so the composition factors of  $S_5$  are  $Z_2$  and  $A_5$ .

A composition series plays a vital role in determining whether a group is solvable or not.

**DEFINITION 8.8** A finite group  $G$  is *solvable* if all of the composition factors of  $G$  are cyclic groups of prime order. A group that is not solvable is called *insoluble*.

We see from this definition that  $S_4$  is solvable, whereas  $S_5$  is insoluble. Why do we want to know whether a group is solvable or not? It turns out that a polynomial equation can be solvable by radicals if, and only if, a corresponding group is solvable. For a fourth degree polynomial, this group will be a subgroup of  $S_4$ , but for a fifth degree polynomial, the group for the polynomial will be a subgroup of  $S_5$ . As a result, every fourth degree polynomial can be solved using square roots and cube roots, but there are many fifth degree polynomials which cannot be solved using radicals.

### Problems for §8.4

**1** Let

$$G = Z_{12} \supseteq A_1 = \{0, 3, 6, 9\} \supseteq \{0\}$$

and

$$G = Z_{12} \supseteq B_1 = \{0, 2, 4, 6, 8, 10\} \supseteq B_2 = \{0, 4, 8\} \supseteq \{0\}$$

be two subnormal series for  $Z_{12}$ . Find all of the subgroups shown in [Figure 8.2](#), and show that the quotient groups indicated by the arrows are indeed isomorphic.

For Problems **2** through **10**: Write out a composition series for the group.

- |                     |                                   |                 |
|---------------------|-----------------------------------|-----------------|
| <b>2</b> $Z_{15}^*$ | <b>5</b> $Z_{12} \times Z_{18}$   | <b>8</b> $D_5$  |
| <b>3</b> $Z_{24}^*$ | <b>6</b> The quaternion group $Q$ | <b>9</b> $D_6$  |
| <b>4</b> $Z_{21}^*$ | <b>7</b> $D_4$                    | <b>10</b> $S_6$ |

- 11** Show that there are exactly three possible composition series for  $A_4$ .
- 12** Find an example of two non-isomorphic groups for which the composition factors are isomorphic.
- 13** Find two groups of the same order with composition series of different lengths.
- 14** Find a non-simple group for which all of the composition factors are non-cyclic.
- 15** Find a simple group for which all of the composition factors are cyclic.
- 16** Find a non-abelian, solvable group for which there is only one composition series.
- 17** Prove that if the refinement theorem (8.2) is applied to two *normal* series, the resulting series will be normal. That is, if  $A_u$  and  $B_v$  are such that

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n = \{e\},$$

and

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_m = \{e\},$$

where each  $A_i$  and  $B_j$  is a normal subgroup of  $G$  (not just the previous group), then the  $A_{i,j}$  and  $B_{j,i}$  given by the refinement theorem will all be normal subgroups of  $G$ .

Hint: Use the result of Problem 17 from §5.3.

- 18** A *chief* series is a normal series for which no refinements produce normal series. Show that the Jordan-Hölder theorem (8.3) applies to chief series as well as to composition series. That is, show that if

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n = \{e\}$$

and

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_m = \{e\}$$

are two chief series, then  $n = m$ , and the quotient groups of the first series are isomorphic to the quotient groups of the second in some order. (Use the result from Problem 17.)

#### Interactive Problems

- 19** Use *SageMath* to find a composition series for the following group of order 20:

```
InitGroup("e")
AddGroupVar("a", "b")
Define(a^5, e); Define(b^4, e); Define(b*a, a^2*b)
M = Group()
```

- 20** Use *SageMath* to find a composition series for the following group:

```
DisplayPermInt = true
G = Group(NthPerm(2374), NthPerm(6212)); G
{1, 2374, 4517, 6212, 6841, 9929, 11637, 13016, 13698, 15367,
18454, 19853, 21239, 21896, 24132, 25315, 28226, 28986,
30928, 31590, 33108, 37381, 38807, 39487}
```

---

## 8.5 Solving the Pyraminx™

We will close this chapter by returning to a problem introduced in §3.3—the Rubik’s Pyraminx™. This example is included because it is a perfect illustration of how the many techniques that we have learned applies to an

actual problem. Although the Rubik's Pyraminx is just a toy, there are important applications to the complex groups produced, such as cryptography. Thus, this example acts as a springboard into applying the principles of group theory to real world applications.

This group was described by four generators,  $r$ ,  $l$ ,  $b$ , and  $f$ , which rotated the right, left, back, or front corners  $120^\circ$  clockwise. The size of the group (933120 elements) makes it infeasible to list the elements in *SageMath*, but we still can use the tools we have learned to analyze this group.

Does the group have a nontrivial center? Notice that the four corner pieces will never change location in the puzzle. The sequence of moves

```
InitPuzzle()
RotatePuzzle(f,r,f,r,r,f,r,f,r,r)
```

rotates one of these corner pieces, returning all other pieces to their original positions. It is clear that this sequence would commute with all other sequences performed on the puzzle. Since the four corners act independently, we would find at least  $3^4 = 81$  elements in the center of the group. Let us call this subgroup  $K$ .

Are there elements in the center besides those in  $K$ ? The sequence

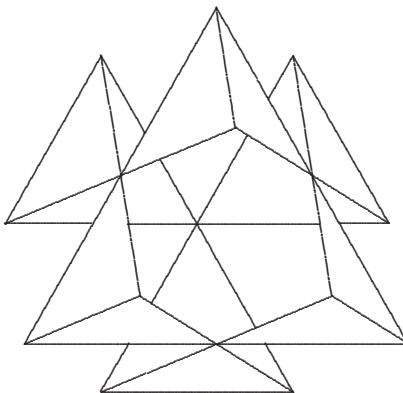
```
InitPuzzle()
RotatePuzzle(l,l,b,f,l,l,b,f,l,l,b,f)
```

returns the four corner pieces to their place, while putting all the edge pieces in the right position, but reversed. If a further sequence of moves was performed from this position rather than the original position, the difference in the end positions would be that all six edges would be reversed. Thus, the above sequence of order 2 will commute with all other elements of the group. It is clear that there can be no more elements in the center, for such an element would have to keep the edge pieces in place. Hence, the center is a normal subgroup isomorphic to the group  $Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_3$ .

Suppose we consider the subgroup  $E$  of actions that return all of the *corners* to their original place. If  $x$  is an element of  $E$ , and  $y$  is a general element, say  $y$  rotates the front corner  $n$  degrees. Then  $y \cdot x \cdot y^{-1}$  rotates the front corner  $n + 0 + (-n) = 0$  degrees, so the front corner would return to its original position. Since the same is true for the other three corners, we see that  $E$  is a normal subgroup.

The intersection of  $E$  and  $K$  would be the only element that leaves both the edges and the corners fixed, the identity element. Since both  $E$  and  $K$  are normal (since  $K$  is in the center), by the direct product theorem,  $E \cdot K$  is isomorphic to  $E \times K$ . Yet any action on the Pyraminx<sup>TM</sup> can be performed by first moving all of the edge pieces, and then moving all of the corners. Thus, the entire group is in  $E \cdot K$ , and so the Pyraminx<sup>TM</sup> group is isomorphic to

$$E \times K \approx E \times Z_3 \times Z_3 \times Z_3 \times Z_3.$$



**FIGURE 8.3:** The Pyraminx<sup>TM</sup> without the corners

To find the structure of the subgroup  $E$ , we analyze the puzzle without the corners, as in [Figure 8.3](#) created by *SageMath*'s **HideCorners** command.

Since there are only 12 triangles remaining, it is clear that each action could be described as a permutation of the 12 triangles. In fact, notice that turning one corner  $120^\circ$  moves 6 triangles—two sets of 3 triangles rotate places. Thus, each turn produces an *even* permutation of the 12 triangles, so  $E$  is a subgroup of  $A_{12}$ .

Let us now try to find a normal subgroup of  $E$ . What if we considered the subgroup of actions that returns the edge pieces to their place, but may reverse some of them? Let us call this subgroup  $H$ . Let  $x$  be an element of  $H$ , and  $y$  an element of  $E$ . The action  $y^{-1} \cdot x \cdot y$  may temporarily move an edge piece out of position, but will return it to its proper place after possibly flipping it. Therefore,  $H$  will be a normal subgroup of  $E$ .

Let us determine the structure of  $H$ . At first one might think that each edge piece can be reversed independently of all of the others, but this is not true. An action that reverses only *one* edge piece would be an *odd* permutation of the triangles. So every element of  $H$  must reverse an even number of edge pieces. The sequence of moves

```
InitPuzzle()
RotatePuzzle(l,f,l,b,l,b,f,b,f)
```

reverses the two front edge pieces, hence it is possible to reverse two edge pieces when they are touching. Using routines like this one, we can reverse any combination of edges as long as the number of edges reversed is even.

How many elements of  $H$  will there be? If we had considered the edge pieces to be reversed independently, there would have been  $2 \times 2 \times 2 \times 2 \times 2 = 64$  elements. Of these 64 possibilities, half of them reverse an even number of edges. By noticing that all elements of  $H$  besides the identity are of order 2, we find that the 32 elements of  $H$  are isomorphic to  $Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$ . The

quotient group  $E/H$  can now be visualized by ignoring whether the six edge pieces are reversed. Certainly this would be a subgroup of the permutations of the six edges. But again we can only consider even permutations, for the edges are moved three at a time. Thus  $E/H$  must be isomorphic to a subgroup of  $A_6$ . It is fairly clear that we can position four of the six edges in any position, so  $E/H \approx A_6$ .

We can use *SageMath* to analyze this group  $E$ . First we consider the subgroup  $H$ , which is the subgroup of flipping an even number of edges. We can represent the edges by disjoint transpositions.

```
H = Group( C(1,2)*C(3,4), C(3,4)*C(5,6), C(5,6)*C(7,8),
    C(7,8)*C(9,10), C(9,10)*C(11,12) )
len(H)
32
```

Next, we consider the subgroup generated of even permutations of the cycles, without flipping them. This subgroup is generated by a three cycle and five cycle of edges.

```
M = Group( C(1,3,5)*C(2,4,6), C(3,5,7,9,11)*
C(4,6,8,10,12) )
len(M)
360
```

We now can combine these subgroups, to form the whole group.

```
G = H * M
len(G)
11520
```

This group is far too large to display, even with integer representation. However, we can determine how many elements there are of a given order, by computing  $R_k(G)$  for various  $k$ .

```
RootCount(G, 2)
392
```

This shows the group has 391 elements of order 2. By changing the value of  $k$ , we can find the number of elements of any given order, summarized in [Table 8.2](#). This table, along with the fact that the Pyraminx group is

$$E \times Z_3 \times Z_3 \times Z_3 \times Z_3,$$

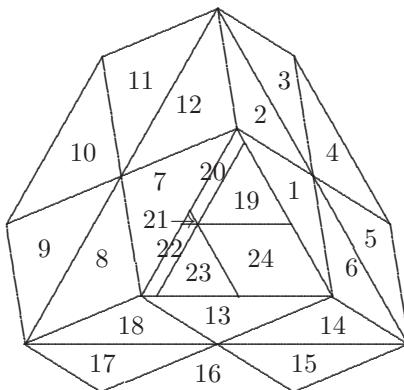
allows us to analyze the Pyraminx group.

Knowing the structure of the group allows us the solve the puzzle! Here is the strategy based on this decomposition of the group.

1. First put all of the edge pieces in place. We can begin with the bottom, then rotate the front and back corners until the back two edges are in the right place (they may be reversed). Finally, rotate the front corner until all six edges are in place.

**TABLE 8.2:** Orders of the group  $E$

|       |                       |
|-------|-----------------------|
| 1     | element of order 1,   |
| 391   | elements of order 2,  |
| 800   | elements of order 3,  |
| 2520  | elements of order 4,  |
| 2304  | elements of order 5,  |
| 1760  | elements of order 6,  |
| 1440  | elements of order 8,  |
| 2304  | elements of order 10, |
| 11520 | elements total.       |



**FIGURE 8.4:** The Pyraminx<sup>TM</sup> with numbered faces

- At this point, an even number of edges will be reversed. We can find routines that will flip two, four, or six of the edges. These may rotate corners in the process.
- Now only the four corner pieces are out of position. We can find routines to rotate these into position.

To find a combination of the four moves  $f$ ,  $b$ ,  $r$ , and  $l$  that will accomplish these goals, we can have *SageMath* help us. First we can number the 24 triangles, as in Figure 8.4. Since we consider the product of several rotations to be done from left to right, we need to convert the rotations to permutations the way that we converted book rearrangements. That is, for each number, we consider what new number will be in that position after the rotation. Thus the permutation  $(4\ 14\ 23)(5\ 15\ 24)(6\ 16\ 19)$  can represent  $r$ ,  $l = (8\ 21\ 16)(9\ 22\ 17)(10\ 23\ 18)$ ,  $f = (1\ 7\ 13)(2\ 8\ 14)(6\ 12\ 18)$ , and finally  $b = (2\ 19\ 10)(3\ 20\ 11)(4\ 21\ 12)$ . We can then enter the Pyraminx<sup>TM</sup> group as a subgroup of  $S_{24}$ .

$$\mathbf{r} = \mathbf{C}(4, 14, 23) * \mathbf{C}(5, 15, 24) * \mathbf{C}(6, 16, 19)$$

```

l = C(8,21,16)*C(9,22,17)*C(10,23,18)
f = C(1,7,13)*C(2,8,14)*C(6,12,18)
b = C(2,19,10)*C(3,20,11)*C(4,21,12)

```

Now that these rotations are entered into *SageMath* as permutations, the natural question is how to express any given permutation in the group generated by these elements in terms of  $f$ ,  $b$ ,  $r$  and  $l$  in the most efficient way. For example, suppose we want to find an efficient way to rotate just the right corner piece clockwise, that is the permutation  $(5\ 15\ 24)$ . *SageMath* can do this with the **ExpressAsWord** command.

```
ExpressAsWord(["r", "l", "f", "b"], C(5,15,24) )
'r*b*r^-2*b^-1*r*b*r*b^-1'
```

This returns a string that describes one of the fastest ways to reach the target permutation from the permutations given. If we evaluate the contents of the string,

```
r*b*r^-2*b^-1*r*b*r*b^-1
(5, 15, 24)
```

we see that indeed this gives us the permutation that we are looking for. Notice that the first argument in **ExpressAsWord** is a list of strings that represent the generating permutations, whose variables have been previously set up. Note that **ExpressAsWord** is not guaranteed to produce the *shortest* solution, merely the first solution it finds. Rearranging the generating permutations may give a different solution.

In flipping edges, we have the advantage that we do not care if corners are rotated in the process. So we can enter versions of  $r$ ,  $l$ ,  $f$ , and  $b$  that ignore the corner pieces.

```

r = C(4,14,23)*C(6,16,19)
l = C(8,21,16)*C(10,23,18)
f = C(2,8,14)*C(6,12,18)
b = C(2,19,10)*C(4,21,12)

```

By ignoring corners, we reduce the number of puzzle positions down to 11520, so it should be easy to find combinations that produce the right flips. For example, to flip the top and front left edges, we need the permutation  $(2\ 12)(8\ 18)$ .

```
ExpressAsWord(["r", "l", "f", "b"], C(2,12)*C(8,18) )
'r*l^-1*b^-1*l*r^-1*f^-1'
r*l^-1*b^-1*l*r^-1*f^-1
(2, 12)(8, 18)
```

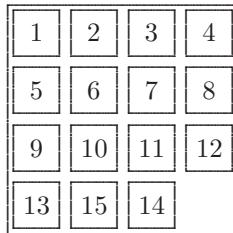
We summarize the necessary moves in [Table 8.3](#). Note that this also includes routines for rotating a corner without changing the rest of the puzzle. By applying these four routines once or twice, we can get all four corners into position, and solve the puzzle!

**TABLE 8.3:** Flipping edges and rotating corners into position

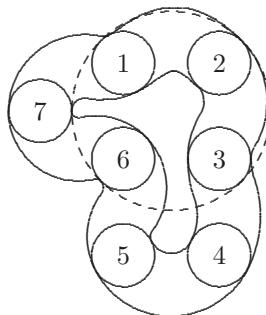
|                                                                                    |                                    |
|------------------------------------------------------------------------------------|------------------------------------|
| $l^{-1} \cdot b \cdot f \cdot l^{-1} \cdot b \cdot f \cdot l^{-1} \cdot b \cdot f$ | flip all six edges                 |
| $f \cdot b \cdot r^{-1} \cdot l \cdot r \cdot b^{-1}$                              | flip two front edges               |
| $b \cdot l \cdot b \cdot r \cdot l \cdot r^{-1} \cdot l^{-1} \cdot b$              | flip top & bottom edges            |
| $f \cdot r \cdot l^{-1} \cdot b \cdot l \cdot r^{-1}$                              | flip top & front left edges        |
| $r \cdot l^{-1} \cdot b \cdot l \cdot r^{-1} \cdot f$                              | flip top & front right edges       |
| $r \cdot b \cdot r \cdot l \cdot b \cdot l^{-1} \cdot b^{-1} \cdot r$              | flip left rear & front right edges |
| $l \cdot r \cdot l \cdot b \cdot r \cdot b^{-1} \cdot r^{-1} \cdot l$              | flip right rear & front left edges |
| $r \cdot b \cdot l^{-1} \cdot f \cdot l \cdot b^{-1}$                              | flip bottom & front right edges    |
| $l \cdot b \cdot f^{-1} \cdot r \cdot f \cdot b^{-1}$                              | flip bottom & front left edges     |
| $b \cdot r \cdot f^{-1} \cdot l \cdot f \cdot r^{-1}$                              | flip top & left rear edges         |
| $b \cdot l \cdot r^{-1} \cdot f \cdot r \cdot l^{-1}$                              | flip top & right rear edges        |
| $b \cdot f \cdot l^{-1} \cdot r \cdot l \cdot f^{-1}$                              | flip rear two edges                |
| $l \cdot f \cdot r^{-1} \cdot b \cdot r \cdot f^{-1}$                              | flip bottom & left rear edges      |
| $r \cdot f \cdot b^{-1} \cdot l \cdot b \cdot f^{-1}$                              | flip bottom & right rear edges     |
| $l \cdot r \cdot b^{-1} \cdot f \cdot b \cdot r^{-1}$                              | flip two left-hand edges           |
| $r \cdot l \cdot f^{-1} \cdot b \cdot f \cdot l^{-1}$                              | flip two right-hand edges          |
| $f \cdot r \cdot f \cdot r^{-1} \cdot f \cdot r \cdot f \cdot r^{-1}$              | rotate front corner 120° clockwise |
| $l \cdot r \cdot l \cdot r^{-1} \cdot l \cdot r \cdot l \cdot r^{-1}$              | rotate left corner 120° clockwise  |
| $r \cdot b \cdot r \cdot b^{-1} \cdot r \cdot b \cdot r \cdot b^{-1}$              | rotate right corner 120° clockwise |
| $b \cdot r \cdot b \cdot r^{-1} \cdot b \cdot r \cdot b \cdot r^{-1}$              | rotate back corner 120° clockwise  |

This same type of analysis can be used to solve other puzzles, such as the Rubik's Cube®. Several problems in the homework relate to this puzzle. Thus, we can see a practical application of the properties of groups that we have studied throughout the course.

But not all applications of groups are fun and games. Group theory has also become the backbone of modern mathematics and many important proofs, such as the impossibility of finding solutions to fifth degree polynomials, hinge entirely on finite groups. The theory of finite groups also has applications in quantum physics and inorganic chemistry and crystallography. Therefore, the material presented in this course has many applications beyond mathematics.

**FIGURE 8.5:** Sam Loyd's 14-15 puzzle for Problem 4**Problems for §8.5**

- 1 Using the orders of the subgroup  $E$  of the Pyraminx<sup>TM</sup> group given in [Table 8.2](#), determine the number of elements of the Pyraminx<sup>TM</sup> group that are of order 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 24, and 30. Verify that the sum of these numbers totals 933,120.
- 2 Consider a  $2 \times 2 \times 2$  Rubik's Cube<sup>®</sup>, consisting of just eight corner pieces. Determine the size of the group of actions on this cube.  
Hint: It is impossible to rotate just one corner, and leave the others in place. Is it possible to move just two of the corners?
- 3 Consider a standard Rubik's Cube<sup>®</sup>. What is the size of the group of actions? What is the center of this group?
- 4 A predecessor to the Rubik's Cube<sup>®</sup> is the puzzle shown in [Figure 8.5](#), introduced in the 1870's. Solvable versions of the puzzle are sold today as party favors. A move consists of sliding one of the fifteen numbered blocks into the lone empty space. The goal is to get all of the numbers into numerical order. Sam Loyd came up with the version shown in [Figure 8.5](#), with the 14 and 15 blocks exchanged. Sam Loyd offered \$1000 for the first person to come up with a solution. Show that in fact, this version of the puzzle is unsolvable.  
Hint: Consider the empty space as a 16, so that the positions are elements of  $S_{16}$ .
- 5 Let  $a = (1\ 2\ 3\ 4\ 5)$  and  $b = (1\ 2\ 4)$  be two elements of  $A_5$ . Find a way to express the element  $(1\ 2)(4\ 5)$  in terms of  $a$  and  $b$ . There is more than one correct answer.  
Hint: Try different combinations of  $a$  and  $b$  to find another 3-cycle.
- 6 Let  $a = (1\ 2\ 3\ 4\ 5)$  and  $b = (1\ 2\ 4)$  be two elements of  $A_5$ . Find a way to express the element  $(1\ 4)(2\ 5)$  in terms of  $a$  and  $b$ . There is more than one correct answer.



**FIGURE 8.6:** Puzzle for Problems 7, 8, and 9

- 7 Consider the puzzle shown in [Figure 8.6](#), in which the seven disks can move within the track, moving  $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7$ , and also the dotted circle can rotate  $180^\circ$ , exchanging  $1 \leftrightarrow 3$  and  $2 \leftrightarrow 6$ . Show that the set of positions that can be obtained from these two moves is a subgroup of  $A_7$ .

#### Interactive Problems

- 8 Consider the puzzle from Problem 7, in which the possible positions are generated from the elements  $a = (1\ 2\ 3\ 4\ 5\ 6\ 7)$  and  $b = (1\ 3)(2\ 6)$ . Find the group generated from these two elements, and show that this is not all of  $A_7$ . How many elements are in this group? Have we seen any other subgroups of  $A_7$  with this number of elements?
- 9 Even though the puzzle from Problem 7 cannot produce all positions in  $A_7$ , the position corresponding to flipping the dotted circle vertically, so that  $1 \leftrightarrow 2$  and  $3 \leftrightarrow 6$  can be obtained. Use **ExpressAsWord** to find a way to express  $(1\ 2)(3\ 6)$  in terms of  $a = (1\ 2\ 3\ 4\ 5\ 6\ 7)$  and  $b = (1\ 3)(2\ 6)$ . This problem is not available in *Mathematica*.
- 10 Suppose we are only allowed to rotate the sides of a  $2 \times 2 \times 2$  Rubik's Cube<sup>®</sup> by  $180^\circ$ . Find the corresponding group of possible positions that can be formed.  
Hint: Since there is no center square, we can fix one corner, so only 21 of the squares can move. There will be 3 axes of rotation, so we have 3 elements of  $S_{21}$ . Find the group generated by these 3 elements.
- 11 First show that  $S_7$  is generated by the elements  $a = (2\ 6\ 3\ 7\ 4)$  and  $b = (1\ 5\ 4\ 2)$ . Then use **ExpressAsWord** to find a way to express  $(1\ 2)$  in terms of  $a$  and  $b$ . This problem is not available in *Mathematica*.
- 12 First show that  $A_7$  is generated by the elements  $a = (1\ 6\ 7)(2\ 5\ 4)$  and  $b = (1\ 3\ 7\ 2)(4\ 6)$ . Then use **ExpressAsWord** to find a way to express  $(1\ 2\ 3)$  in terms of  $a$  and  $b$ . This problem is not available in *Mathematica*.

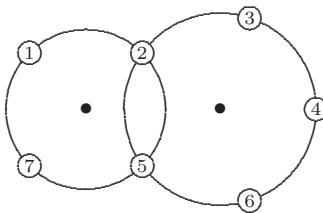


FIGURE 8.7: Puzzle for Problem 13

- 13 Consider the puzzle in Figure 8.7, with 7 disks on 2 wheels. The action  $L$  turns the left wheel  $90^\circ$  clockwise, taking the disks with it. The action  $R$  turns the right wheel  $72^\circ$  clockwise, again taking the disks with it. The goal is to swap disks 5 and 6, so the disks are in consecutive order. Use *SageMath*'s **ExpressAsWord** to solve this puzzle. A few brave souls might try to solve this puzzle without *SageMath*'s help. This problem is not available in *Mathematica*.

# Chapter 9

---

## Introduction to Rings

This section presents the concept of a *ring*, which is a generalization of the addition and multiplication operations of standard numbers. The term *ring* was first coined by David Hilbert in 1892, although he only referred to a particular type of ring. It wasn't until 1920 that Emmy Noether gave an abstract definition of a ring, which would apply to the “hyper-complex” number systems developed earlier by William Hamilton and Hermann Grassmann. (See the Historical Diversion on page 281.) This abstraction can apply to polynomials, infinite series, matrices, and even functions. Hence, ring theory has become a valuable tool for almost every other branch of mathematics.

---

### 9.1 The Definition of a Ring

While studying the previous chapters on groups, we discovered different patterns in the group's structure by which we could predict and prove many useful properties. However, many of the examples of groups we studied possess some additional structure which we have yet to take advantage of. Some of the groups had not just one, but two operations that we could define on the elements.

The simplest example to consider is the group of integers,  $\mathbb{Z}$ . This is a group under the operation of addition, in fact an abelian group with the identity element being 0. However, we can also multiply two integers together, always forming another integer. Is  $\mathbb{Z}$  a group using multiplication instead of addition? No, because most elements do not have an inverse. However, this extra operation gives  $\mathbb{Z}$  a much richer structure than standard groups.

Subgroups of  $\mathbb{Z}$  can also be considered. A typical example would be the set of even integers. Once again, we have both addition and multiplication defined on this set, since both the sum and the product of two even integers yield even integers.

Likewise, the group of rationals  $\mathbb{Q}$  and real numbers  $\mathbb{R}$  have two operations. Although these are both abelian groups under addition, they are *almost* groups under multiplication as well. The multiplicative inverse exists for all

**TABLE 9.1:**  $(\cdot) \bmod 6$ 

| . | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

elements except 0. If we considered the remaining elements  $\mathbb{Q} - \{0\}$  or  $\mathbb{R} - \{0\}$ , we have the multiplicative groups denoted  $\mathbb{Q}^*$  and  $\mathbb{R}^*$ .

Not only do  $\mathbb{Z}$ ,  $\mathbb{Q}$ , and  $\mathbb{R}$  allow for an additional operation to be defined on them but also some groups from [Chapter 2](#). Take for example the groups formed by modular arithmetic, such as  $Z_6 = \{0, 1, 2, 3, 4, 5\}$ . The group operation on  $Z_6$  is addition modulo 6. A natural second operation would be multiplication modulo 6, shown in [Table 9.1](#). Note that this table does not possess the “Latin square” property we have seen in the group tables. However, there is no need for the second operation to have this property.

### Motivational Example 9.1

The following command produces the quaternion group  $Q$  of order 8 which we studied in [Chapter 5](#):

```
Q = InitQuaternions(); Q
{1, i, j, k, -1, -i, -j, -k}
```

We have seen the Cayley table before, in [Table 5.3](#). The quaternion elements are reminiscent of the cross product between two three dimensional vectors. That is,

$$i \cdot j = k \quad j \cdot k = i, \quad \text{and} \quad k \cdot i = j.$$

This suggests that we can also *add* multiples of these elements together like vectors, forming such elements as

```
i - 2*j - k
i - 2*j - k
```

which would represent the vector  $\langle 1, 2, -1 \rangle$ . Two vectors can be added together in the standard way.

```
(i - 2*j - k) + (3*i + j - 2*k)
4*i - j - 3*k
```

producing the vector  $\langle 4, -1, -3 \rangle$ . Unfortunately, as we multiply these “vectors” together using the distributive laws, we find elements of the form

$$(i - 2*j - k) * (3*i + j - 2*k)$$

$$-3 + 5*i - j + 7*k$$

which would represent the *four*-dimensional vector  $\langle -3, 5, -1, 7 \rangle$ . (This extra dimension could represent *time*.) However, we find that the product of any two four-dimensional vectors would give us a product in the form  $a + bi + cj + dk = \langle a, b, c, d \rangle$ . In fact, we are able to find the inverse of a four-dimensional vector.

$$(2 + i + 2*j - k)^{-1}$$

$$1/5 + (-1/10)*i + (-1/5)*j + 1/10*k$$

This suggests we should explore the special properties of these vectors. □

### **PROPOSITION 9.1**

The set of nonzero four-dimensional vectors forms a non-abelian group using the Cayley table for the quaternion group  $Q$ .

PROOF: If

$$x = a + bi + cj + dk$$

is nonzero, then

$$x^{-1} = \frac{a}{a^2 + b^2 + c^2 + d^2} + \frac{-b}{a^2 + b^2 + c^2 + d^2} i$$

$$+ \frac{-c}{a^2 + b^2 + c^2 + d^2} j + \frac{-d}{a^2 + b^2 + c^2 + d^2} k$$

forms a multiplicative inverse, since it is a simple exercise to show that  $x \cdot x^{-1} = x^{-1} \cdot x = 1$ , the multiplicative identity (see Problem 10). Note that since  $x \neq 0$ , the common denominator  $a^2 + b^2 + c^2 + d^2 > 0$ . It is easy to see that multiplication is closed. The only hard part is to show that the associative law holds, which is best done in *SageMath* (see Problem 22). Given that the associative law holds, it is easy to see that the product of two nonzero vectors must be nonzero. If  $x \cdot y = 0$ , and  $x \neq 0$ , then

$$y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

Thus, if both  $x \neq 0$  and  $y \neq 0$ , then  $x \cdot y \neq 0$ . □

We call the group of four-dimensional vectors of the form  $a + bi + cj + dk$  the *quaternions*, denoted by  $\mathbb{H}$  after their discoverer, William Rowan Hamilton (1805-1865).

We have seen many examples of groups that exhibit not one but two operations defined on them. One of these operations is represented with the plus sign, and the other is usually denoted with a dot. Our goal will be to come up with a definition that unites these examples. Let us consider which properties

**TABLE 9.2:** Property checklist for several groups

| Property                                    | $\mathbb{Z}$ | Even Integers | $\mathbb{Q}$ | Reals | $Z_6$ | Quaternions |
|---------------------------------------------|--------------|---------------|--------------|-------|-------|-------------|
| Closed under Addition                       | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| Closed under Multiplication                 | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| $(a + b) + c = a + (b + c)$                 | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| Additive Identity (0)                       | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| Multiplicative Identity (1)                 | ✓            | ✗             | ✓            | ✓     | ✓     | ✓           |
| Additive Inverses Exist                     | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| Multiplicative Inverses Exist Except for 0  | ✗            | ✗             | ✓            | ✓     | ✗     | ✓           |
| $a + b = b + a$                             | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| $a \cdot b = b \cdot a$                     | ✓            | ✓             | ✓            | ✓     | ✓     | ✗           |
| $a \cdot b = 0$ only if $a$ or $b = 0$      | ✓            | ✓             | ✓            | ✓     | ✗     | ✓           |
| $(a + b) \cdot c = a \cdot c + b \cdot c$   | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |
| $a \cdot (b + c) = a \cdot b + a \cdot c$   | ✓            | ✓             | ✓            | ✓     | ✓     | ✓           |

these examples have in common. [Table 9.2](#) organizes our findings, indicating which of the 6 groups that we looked at satisfy various properties.

We want to pay special attention to the properties that hold for *all* of the groups studied so far. In fact, let us define a *ring* as a group possessing all of these properties. In this way, we allow all six of the above examples to be rings.

**DEFINITION 9.1** A *ring* is an abelian group with the operation (+) on which a second associative operation ( $\cdot$ ) is defined such that the two distributive laws

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

and

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

hold for all  $a$ ,  $b$ , and  $c$  in the ring.

For any ring we will use the symbol  $0$  to denote the additive identity of a ring, and the notation  $-x$  for the additive inverse of  $x$ .

Even though we defined a ring such that all six of the groups in [Table 9.2](#) are rings, many of the groups possessed additional properties. We will give names to rings with some of these extra properties.

**DEFINITION 9.2** A ring for which  $x \cdot y = y \cdot x$  for all elements  $x$  and  $y$  is called a *commutative ring*.

**DEFINITION 9.3** A ring for which there is an element  $e$  such that

$$x \cdot e = e \cdot x = x$$

for all elements  $x$  in the ring is called a *unity ring* or *ring with identity*. The element  $e$  is called the *unity* or *multiplicative identity* of the ring, to distinguish it from the additive identity  $0$ .

The next definition will deal with rings for which  $x \cdot y = 0$  implies that either  $x$  or  $y$  must be  $0$ . However, it is reasonable to first prove the following lemma:

### LEMMA 9.1

If  $x$  is any element in a ring, then  $0 \cdot x = x \cdot 0 = 0$ , where  $0$  is the additive identity.

**PROOF:** This proof is just a little tricky because there are no other propositions to rely on. Thus, every step must directly use one of the nine properties of rings. (The temptation is to rely on some property we suspect is true, but haven't yet proven.)

Note that

$$(0 \cdot x + 0 \cdot x) = (0 + 0) \cdot x = 0 \cdot x,$$

so

$$(0 \cdot x + 0 \cdot x) + ((-0 \cdot x)) = 0 \cdot x + ((-0 \cdot x)) = 0.$$

Hence

$$0 \cdot x + (0 \cdot x + (-(0 \cdot x))) = 0,$$

so

$$0 \cdot x + 0 = 0 \cdot x = 0.$$

Similarly,

$$(x \cdot 0 + x \cdot 0) = x \cdot (0 + 0) = x \cdot 0,$$

so

$$(x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) = x \cdot 0 + (-(x \cdot 0)) = 0.$$

Hence

$$x \cdot 0 + (x \cdot 0 + (-(x \cdot 0))) = 0,$$

so

$$x \cdot 0 + 0 = x \cdot 0 = 0. \quad \square$$

This proof shows that we can get the equivalent of subtraction by adding the additive inverse. But although we can add, subtract, and multiply elements in a ring, we cannot, in general, divide elements. In fact, we can find some rings for which the product of two nonzero elements produces 0, such as  $3 \cdot 2 = 0$  in the ring  $Z_6$ .

**DEFINITION 9.4** If  $x$  is a nonzero element of a ring such that either  $x \cdot y = 0$  or  $y \cdot x = 0$  for a nonzero element  $y$ , then  $x$  is called a *zero divisor* of the ring. If a ring has no zero divisors, it is called a *ring without zero divisors*.

We see from this definition that 2 and 3 are zero divisors of the ring  $Z_6$ , since  $3 \cdot 2 = 0$  in this ring. A related definition stems from the product of two elements equaling the unity element.

**DEFINITION 9.5** If, for the element  $x$  in a unity ring, there is an element  $y$  such that

$$x \cdot y = y \cdot x = e,$$

we say that  $x$  has a multiplicative inverse, or is *invertible*.

Just because an element is not a zero divisor does not mean that it is invertible. For example, 2 is not a zero divisor of the ring  $\mathbb{Z}$ , yet 2 is not invertible in this ring.

The smallest possible ring is the *trivial ring*, which is defined by the *Sage-Math* commands

```
G = ZRing(1); G
{0}
AddTable(G)
MultTable(G)
```

|   |   |
|---|---|
| + | 0 |
| 0 | 0 |

|   |   |
|---|---|
| · | 0 |
| 0 | 0 |

This ring is rather unusual because the unity element is 0. Also, 0 is actually invertible in this ring, because  $0^{-1} = 0$ . These two facts are true for no other ring.

**DEFINITION 9.6** A ring for which every nonzero element has a multiplicative inverse is called a *division ring*.

**PROPOSITION 9.2**

A division ring always has a unity and has no zero divisors.

PROOF: We just saw that the trivial ring has a unity and has no zero divisors, so we may assume that the ring has a nonzero element  $y$ . Then  $y$  has a multiplicative inverse  $z$ , so we have  $y \cdot z = e$ , the unity. Thus, every division ring must have a unity.

Now suppose that  $x \cdot y = 0$  in a division ring, with both  $x$  and  $y$  nonzero. Then  $y$  has a multiplicative inverse  $z$ , so that  $y \cdot z = e$ . But then

$$x = x \cdot e = x \cdot (y \cdot z) = (x \cdot y) \cdot z = 0 \cdot z = 0,$$

which contradicts the fact that  $x$  is nonzero. Thus, a division ring has no zero divisors. □

**DEFINITION 9.7** A non-trivial division ring for which  $x \cdot y = y \cdot x$  for all  $x$  and  $y$  is called a *field*. A division ring for which multiplication is not commutative is called a *skew field*.

We can now classify each possible type of ring. For example, the ring  $\mathbb{Z}$  is a commutative unity ring without zero divisors. The ring of even integers, however, has no unity element, so we would call this a commutative ring without zero divisors. Both  $\mathbb{Q}$  and  $\mathbb{R}$  satisfied all 13 properties, so these two rings are fields. The ring  $Z_6$  has zero divisors, so we would call this a commutative unity ring. The quaternions  $\mathbb{H}$  have all the properties of a field except that multiplication is not commutative, so this is an example of a skew field.

### Problems for §9.1

For Problems 1 through 6: Prove the following statements for arbitrary  $x$ ,  $y$ , and  $z$  in a ring  $R$ , using the properties of rings, and Lemma 9.1. You can use the result of a previous problem. Note that  $x - y$  is defined to be  $x + (-y)$ , and  $x^2 = x \cdot x$ .

## Historical Diversion

# Emmy Noether (1882–1935)

Emmy Noether was a Jewish woman from a mathematically talented family. Her father, Max Noether, was a prominent mathematics professor at the University of Erlangen, and played a large part in founding the field of algebraic geometry. Her brother Fritz would also become a mathematics professor at Breslau. However, nothing in her early years would indicate her true mathematical genius.

From 1900 to 1902, she attended the University of Erlangen studying mathematics and languages. But because she was a woman, she could not formally enroll in the courses, but only audit the lectures with the permission of the instructor, which was often denied. She was, however, allowed to take the final university exams which led to a degree, so Emmy Noether was able to pass these exams.

Noether moved to Göttingen to audit classes from the mathematical giants of her day, Felix Klein and David Hilbert. Hilbert specialized in axiomatic approach to number theory. But in 1904 she returned to Erlangen, since they relaxed the rules and allowed women to register for classes. She completed her dissertation in 1907, and continued to teach, without pay, at Erlangen. In 1915, Klein and Hilbert tried to get Noether a faculty position at Göttingen, but their efforts were blocked since she was a woman. Finally, in 1919, she obtained formal admission as an academic lecturer.

Noether's revealed her true genius in 1920, when she published a paper on the theory of ideals, in which she defined the left and right ideals of a ring. Noether incorporated Hibert's axiomatic approach to abstract algebra to be first person to give a modern definition of the ring, although her work focused on commutative rings. The following year she published *Idealtheorie in Ringbereichen* which analyzed the ascending chain conditions among ideals. Today, we refer to a ring as a *Noetherian ring* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

must eventually stop increasing in size, that is, there is some  $I_k$  such that  $I_m = I_k$  for all  $m > k$ .

When Hitler rose to power in 1933, Noether and other Jewish professors at Göttingen were dismissed. Noether fled to the United States, to Bryn Mawr college to be a visiting professor of mathematics. In 1935 she died at age 53 from an infection resulting from an operation to remove a uterine tumor.



- 1**  $(-x) \cdot y = -(x \cdot y)$     **4**  $x \cdot (y - z) = x \cdot y - x \cdot z$   
**2**  $x \cdot (-y) = -(x \cdot y)$     **5**  $(x - y) \cdot z = x \cdot z - y \cdot z$   
**3**  $(-x) \cdot (-y) = x \cdot y$     **6**  $(x + y) \cdot (x - y) = (x^2 - y^2) + (y \cdot x - x \cdot y)$

- 7** If  $a$  and  $b$  are elements of a ring  $R$ , and  $a \cdot b$  is a zero divisor, prove that either  $a$  or  $b$  is a zero divisor.
- 8** For the quaternions,  $\mathbb{H}$ , we define the *conjugate* of an element  $x = a + bi + cj + dk$  to be  $\bar{x} = a - bi - cj - dk$ . Prove that  $\overline{x_1 + x_2} = \overline{x_1} + \overline{x_2}$  for all  $x_1$  and  $x_2$  in  $\mathbb{H}$ .
- 9** Prove or disprove:  $\overline{x_1 \cdot x_2} = \overline{x_1} \cdot \overline{x_2}$  for all  $x_1$  and  $x_2$  in  $\mathbb{H}$ . (See Problem 8.)
- 10** Prove that for  $x$  in  $\mathbb{H}$ ,  $x \cdot \bar{x} = \bar{x} \cdot x = a^2 + b^2 + c^2 + d^2$ . (See Problem 8.)
- 11** For all  $x$  in  $\mathbb{H}$ , we define the *absolute value* of  $x$  to be  $|x| = \sqrt{x \cdot \bar{x}}$ . Prove that  $|x_1 \cdot x_2| = |x_1| |x_2|$ . (See Problem 8.)
- 12** Prove or disprove: For all  $x$  in the quaternions  $\mathbb{H}$ ,  $(x+1) \cdot (x-1) = x^2 - 1$ .
- 13** Prove or disprove: For all  $x$  in the quaternions  $\mathbb{H}$ ,  $(x+i) \cdot (x-i) = x^2 + 1$ .
- 14** Let  $\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}$ .  
 Prove that  $\mathbb{Z}[\sqrt{2}]$  is a ring under the ordinary addition and multiplication of real numbers.
- 15** Consider the set  $\{x + y\sqrt[3]{2} \mid x, y \in \mathbb{Z}\}$ .  
 Is this set a ring under the ordinary addition and multiplication of real numbers?
- 16** Prove that a ring can have at most one multiplicative identity.
- 17** Suppose that  $G$  is an abelian group with additive identity 0. Define a multiplication on  $G$  by  $x \cdot y = 0$  for all  $x$  and  $y$  in  $G$ . Show that  $G$  forms a ring.
- 18** Define new operations of addition and multiplication in  $\mathbb{Z}$  by  $x \oplus y = x + y - 1$  and  $x \otimes y = x + y - xy$ . Verify that  $\mathbb{Z}$  forms a ring with respect to these new operations.
- 19** Let  $R$  be a unity ring without zero divisors. Suppose that  $x \cdot y = e$ . Prove that  $y \cdot x = e$ .
- 20** Fill in the remaining spaces in these addition and multiplication tables so that the resulting set forms a ring.  
 Hint: Use the Latin square property to fill in the addition table. Then use the distributive laws to determine the multiplication table.

| + | 0 | a | b | c |
|---|---|---|---|---|
| 0 |   |   |   |   |
| a |   |   |   |   |
| b |   |   |   | c |
| c |   |   |   |   |

| . | 0 | a | b | c |
|---|---|---|---|---|
| 0 |   |   |   |   |
| a |   |   |   |   |
| b |   |   |   | c |
| c |   |   |   |   |

## Interactive Problems

- 21** We saw that the ring  $Z_6$  had zero divisors. We can enter this ring in *SageMath* with the command

```
R = ZRing(6); R
{0, 1, 2, 3, 4, 5}
```

Try this with  $Z_5$ ,  $Z_7$ ,  $Z_8$ ,  $Z_9$ ,  $Z_{10}$ ,  $Z_{11}$ , and  $Z_{12}$ , and form the multiplication tables of these rings. Which ones have zero divisors? Which ones are fields?

- 22** Use *SageMath* to show that quaternion multiplication is associative. That is, if we define

```
Q = InitQuaternions()
var("a1 a2 a3 b1 b2 b3 c1 c2 c3 d1 d2 d3")
x = a1 + b1*i + c1*j + d1*k
y = a2 + b2*i + c2*j + d2*k
z = a3 + b3*i + c3*j + d3*k
```

then show that  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

## 9.2 Entering Finite Rings into *SageMath*

In the first eight chapters, we entered finite groups into *SageMath* by using the generators of the group. If we consider a finite ring simply as an abelian group under addition, we can find a set of generators  $B$  for this group (ignoring the multiplicative structure). For each element in  $B$  we determine the additive order of the element. That is, for each generator  $x$  we want to find the smallest number  $n$  such that

$$\underbrace{x + x + \cdots + x + x}_{n \text{ times}} = 0.$$

**DEFINITION 9.8** If  $n$  is a positive integer, and  $x$  is any element in a ring, we define  $nx$  inductively by letting  $1x = x$ , and

$$nx = (n - 1)x + x.$$

We also define  $(-n)x$  to be  $-(nx)$  for  $n$  a positive integer. Finally, we define  $0x = 0$ .

Because “multiplication by an integer” is merely a shorthand for repeated addition, we immediately see that

$$(m+n)x = mx + nx \quad \text{and} \quad (mn)x = m(nx)$$

for any element  $x$  and any integers  $n$  and  $m$ . See Problems 13, 14 and 15.

### **LEMMA 9.2**

Let  $x$  and  $y$  be any two elements in a ring, and let  $n$  be an integer. Then

$$(nx) \cdot y = n(x \cdot y) = x \cdot (ny).$$

**PROOF:** We will proceed by induction. The statement is certainly true for  $n = 0$  or  $n = 1$ . Suppose that the statement is true for the previous case  $n - 1$ . But then

$$((n-1)x) \cdot y + x \cdot y = (n-1)(x \cdot y) + x \cdot y = x \cdot ((n-1)y) + x \cdot y.$$

Hence, by the distributive law,

$$((n-1)x + x) \cdot y = ((n-1) + 1)(x \cdot y) = x \cdot ((n-1)y + y),$$

and so

$$(nx) \cdot y = n(x \cdot y) = x \cdot (ny).$$

Hence, the statement is true for all positive integers.

For negative integers, we can merely show that

$$(nx) \cdot y + ((-n)x) \cdot y = (nx + (-n)x) \cdot y = ((n-n)x) \cdot y = 0 \cdot y = 0.$$

$$n(x \cdot y) + (-n)(x \cdot y) = (n-n)(x \cdot y) = 0(x \cdot y) = 0.$$

$$x \cdot (ny) + x \cdot ((-n)y) = x \cdot (ny + (-n)y) = x \cdot ((n-n)y) = x \cdot 0 = 0.$$

Thus,  $((-n)x) \cdot y$ ,  $(-n)(x \cdot y)$ , and  $x \cdot ((-n)y)$  are the additive inverses of  $(nx) \cdot y$ ,  $n(x \cdot y)$ , and  $x \cdot (ny)$ , respectively. But since these latter three are equal for positive  $n$ , we have

$$((-n)x) \cdot y = (-n)(x \cdot y) = x \cdot ((-n)y).$$

Hence the lemma is proven for all integers  $n$ . □

We can now use this notation within *SageMath* to generate a finite ring. To define a ring whose additive group is isomorphic to

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\},$$

we find two elements that generate this group:  $a = 2$  and  $b = 14$ . Since

$$2^4 \equiv 1 \pmod{15} \quad \text{and} \quad 14^2 \equiv 1 \pmod{15},$$

we see that  $a^4 = 1$  and  $b^2 = 1$  in the group  $Z_{15}^*$ . But using ring notation, we write  $4a = 0$  and  $2b = 0$ , since 0 is the additive identity of the ring.

To define a group in *SageMath*, we began by declaring what the identity element will be. But for rings, the additive identity will always be 0, so we don't have any arguments.

### **InitRing()**

Next, we declare that  $a$  and  $b$  will be the generators of the additive group, just as we did with **AddGroupVar** for groups.

### **AddRingVar("a", "b")**

Next, we need to tell *SageMath* what the additive order of these elements will be, using **Define** commands. Since  $a$  is of order 4, and  $b$  is of order 2, we enter:

```
Define(4*a, 0)
Define(2*b, 0)
```

This is sufficient to define the group structure of the ring. The eight elements of the group are denoted as follows:

```
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

We combine two elements of this group with a plus sign rather than the dot that we used for groups. For example, here is the sum of two elements:

```
(3*a+b) + (2*a)
a + b
```

The addition table can be displayed using **AddTable(R)**, producing [Table 9.3](#).

The additive structure of the ring determines an important property of the ring that we will utilize later.

**DEFINITION 9.9** Let  $R$  be a ring. We define the *characteristic* of  $R$  to be the smallest positive integer  $n$  such that  $nx = 0$  for all  $x$  in the ring. If no such positive number exists, we say the ring has *characteristic 0*.

When we define a ring using *SageMath*, the characteristic will simply be the least common multiple of the additive orders of the generators. Thus, for the ring with the additive structure of [Table 9.3](#), the characteristic is  $\text{lcm}(4, 2) = 4$ .

**TABLE 9.3:** Addition table for the ring  $\mathbf{R}$ 

| +        | 0        | $a$      | $2a$     | $3a$     | $b$      | $a + b$  | $2a + b$ | $3a + b$ |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 0        | 0        | $a$      | $2a$     | $3a$     | $b$      | $a + b$  | $2a + b$ | $3a + b$ |
| $a$      | $a$      | $2a$     | $3a$     | 0        | $a + b$  | $2a + b$ | $3a + b$ | $b$      |
| $2a$     | $2a$     | $3a$     | 0        | $a$      | $2a + b$ | $3a + b$ | $b$      | $a + b$  |
| $3a$     | $3a$     | 0        | $a$      | $2a$     | $3a + b$ | $b$      | $a + b$  | $2a + b$ |
| $b$      | $b$      | $a + b$  | $2a + b$ | $3a + b$ | 0        | $a$      | $2a$     | $3a$     |
| $a + b$  | $a + b$  | $2a + b$ | $3a + b$ | $b$      | $a$      | $2a$     | $3a$     | 0        |
| $2a + b$ | $2a + b$ | $3a + b$ | $b$      | $a + b$  | $2a$     | $3a$     | 0        | $a$      |
| $3a + b$ | $3a + b$ | $b$      | $a + b$  | $2a + b$ | $3a$     | 0        | $a$      | $2a$     |

All finite rings will have a positive characteristic, but infinite rings, such as  $\mathbb{Z}$ , can have a characteristic of 0. The characteristic of the ring will play a large role when we start focusing on integral domains and fields.

Notice that there are several differences between defining a group and defining the group structure of a ring. The obvious difference is that we use the plus sign instead of the star for our operation. Also, when we defined a group, we began by telling *SageMath* the identity element. But for a ring, the additive identity is always denoted **0**, and the multiplicative identity may not exist. So the first statement merely has to tell *SageMath* that we are defining a ring. Finally, we do not need an extra **Define** statement to tell *SageMath* that the group is commutative, as we did before for defining  $Z_{15}^*$ .

Although this defines the additive group very quickly, we must be selective in choosing the generators. Suppose we had instead chosen the generators  $a = 2$  and  $b = 7$ . These two elements generate the group  $Z_{15}^*$ , but both are of order 4. So the *SageMath* commands for entering these two generators would be

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0)
Define(4*b, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b, 2 b, a + 2 b,
 2 a + 2 b, 3 a + 2 b, 3 b, a + 3 b, 2 a + 3 b, 3 a + 3 b}
```

This gives 16 elements instead of 8. The problem is that *SageMath* is not using the identity  $2a = 2b$ , which is true since  $2^2 \equiv 7^2 \pmod{15}$ . Trying to add an additional *SageMath* command defining  $2a = 2b$  would produce some potential problems later on. A better solution is simply to make the following restriction on the set of generators.

**DEFINITION 9.10** Let  $G$  be an abelian group. A *basis* is a set of non-

zero elements  $B = \{x_1, x_2, x_3, \dots, x_k\}$  which generates the group such that the only way in which

$$n_1x_1 + n_2x_2 + n_3x_3 + \cdots + n_kx_k = 0$$

for integers  $n_1, n_2, n_3, \dots, n_k$  is if

$$n_1x_1 = n_2x_2 = n_3x_3 = \cdots = n_kx_k = 0.$$

For a finite group, it is clear that if we have a basis, then every combination of the form

$$n_1x_1 + n_2x_2 + n_3x_3 + \cdots + n_kx_k,$$

where each  $n_i$  is non-negative and less than the order of  $x_i$ , forms a distinct element. Also, every element of  $G$  could be put in that form. Thus, the product of the orders of all the elements of  $B$  equals the order of the group.

It should be noted that *any* finite abelian group has a basis, using the fundamental theorem of finite abelian groups (7.2). See Problem 21.

Once we have found a basis for the additive group, and have defined the additive structure into *SageMath*, we are ready to consider the multiplicative definitions. If we have two generators  $\{a, b\}$ , we will need to define  $2^2 = 4$  multiplications:  $a \cdot a$ ,  $a \cdot b$ ,  $b \cdot a$ , and  $b \cdot b$ . These four products could be defined to be any of the elements of the ring. Thus, for ring with the additive structure of  $Z_{15}^*$ , there are up to  $8^4 = 4096$  ways to finish defining the ring! However, very few of these ways of defining the products will satisfy both the distributive laws and the associative law. For example,  $b \cdot b$  cannot be defined to be  $a$ , otherwise we have the contradiction

$$2a = a + a = b \cdot b + b \cdot b = (b + b) \cdot b = (2b) \cdot b = 0 \cdot b = 0.$$

An example of a ring definition that does not produce such a contradiction comes from defining  $a^2 = a$ ,  $b^2 = b$ , and  $a \cdot b = b \cdot a = 0$ . All other products in the ring can be determined from these using the distributive law. For example,

$$(2a + b) \cdot (a + b) = 2a^2 + b \cdot a + 2a \cdot b + b^2 = 2a + 0 + 0 + b = 2a + b.$$

We can enter the four products using four more **Define** commands in *SageMath*. To define the ring described in the above paragraph, we can use

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0)
Define(2*b, 0)
Define(a^2, a)
Define(b^2, b)
Define(a*b, 0)
Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

The addition table was given above in [Table 9.3](#), while the multiplication table is given by

### **MultTable(R)**

producing [Table 9.4](#).

**TABLE 9.4:** Multiplication table for the ring  $\mathbf{R}$

| .        | 0 | $a$  | $2a$ | $3a$ | $b$ | $a + b$  | $2a + b$ | $3a + b$ |
|----------|---|------|------|------|-----|----------|----------|----------|
| 0        | 0 | 0    | 0    | 0    | 0   | 0        | 0        | 0        |
| $a$      | 0 | $a$  | $2a$ | $3a$ | 0   | $a$      | $2a$     | $3a$     |
| $2a$     | 0 | $2a$ | 0    | $2a$ | 0   | $2a$     | 0        | $2a$     |
| $3a$     | 0 | $3a$ | $2a$ | $a$  | 0   | $3a$     | $2a$     | $a$      |
| $b$      | 0 | 0    | 0    | 0    | $b$ | $b$      | $b$      | $b$      |
| $a + b$  | 0 | $a$  | $2a$ | $3a$ | $b$ | $a + b$  | $2a + b$ | $3a + b$ |
| $2a + b$ | 0 | $2a$ | 0    | $2a$ | $b$ | $2a + b$ | $b$      | $2a + b$ |
| $3a + b$ | 0 | $3a$ | $2a$ | $a$  | $b$ | $3a + b$ | $2a + b$ | $a + b$  |

We still have not *proven* that this is a ring, since we have not verified the distributive laws and the associativity law for multiplication. The tedious task of verifying these laws can be handled by the *SageMath* command

### **CheckRing()**

This is a ring.

*SageMath* checks the ring most recently defined, and finds that both the distributive and associative laws hold, so this is a ring. Since  $R$  is obviously commutative from the multiplication table, the next question is whether  $R$  has a unity. *SageMath* can search the ring for a unity element with the command

### **FindUnity(R)**

$a + b$

Even though we did no use the unity to construct the ring, *SageMath* found one.

### **Example 9.2**

Try to define a non-commutative ring using  $Z_{15}^*$  as the additive group.

SOLUTION: If  $a \cdot b = b$ , yet  $b \cdot a = 2a$ , then the ring will not be commutative. Here is one attempt to define such a ring.

### **InitRing()**

```

AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a*b, b); Define(b*a, 2*a)
Define(a^2, 0); Define(b^2, 0)
CheckRing()
    a * ( a * b ) is not ( a * a ) * b
    a * ( b * a ) is not ( a * b ) * a
    Associative law does not hold.

```

This attempt failed, so we must replace the last two **0**'s with other elements of the ring.

It would seem as though there would be 64 possibilities to check, but we can narrow the search by using the associative property. For example,  $(a \cdot b) \cdot a$  must be  $a \cdot (b \cdot a)$ , so  $2a = 2a^2$ . This forces  $a^2$  to be either  $a$  or  $3a$ . Also,  $(b \cdot a) \cdot b$  must be  $b \cdot (a \cdot b)$ , so  $0 = b^2$ .

We now have enough information to try the ring again.

```

InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a*b, b); Define(b*a, 2*a)
Define(a^2, a); Define(b^2, 0)
CheckRing()
    This is a ring.

```

In this case, there is no unity element.

```

R = Ring(); R
    {0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
FindUnity(R)
    No unity element

```

In fact, every nonzero element turns out to be a zero divisor. □

Since we have seen an example of a non-commutative ring without unity, can we find a non-commutative unity ring? The following proposition shows that we will not be able to use  $Z_{15}^*$  for the additive group.

### **PROPOSITION 9.3**

*If a unity ring has an additive structure that can be generated with less than three elements, then the ring is commutative.*

PROOF: Suppose that  $x$  and  $y$  are two elements of the ring that generate the group under addition. That is, every element can be expressed as  $mx + ny$  for integers  $m$  and  $n$ . In particular, the unity

$$e = mx + ny$$

for some integers  $m$  and  $n$ . Since  $e$  commutes with both  $x$  and  $y$ , we have

$$mx \cdot x + ny \cdot x = (mx + ny) \cdot x = e \cdot x = x \cdot e = mx \cdot x + nx \cdot y,$$

so  $ny \cdot x = nx \cdot y$ .

Likewise,

$$mx \cdot y + ny \cdot y = (mx + ny) \cdot y = e \cdot y = y \cdot e = my \cdot x + ny \cdot y,$$

so  $mx \cdot y = my \cdot x$ .

By Bézout's lemma (1.3), there are integers  $u$  and  $v$  such that

$$um + vn = \gcd(m, n).$$

If we let  $c$  denote the greatest common divisor of  $m$  and  $n$ , then

$$c(x \cdot y - y \cdot x) = (um + vn)(x \cdot y - y \cdot x) = u(mx \cdot y - my \cdot x) + v(nx \cdot y - ny \cdot x) = 0.$$

What we need to show is that  $(x \cdot y - y \cdot x) = 0$ . The tempting thing to do is divide by  $c$ , but this operation is not allowed in rings. Instead, we will again utilize the unity. Since  $c = \gcd(m, n)$  there are integers  $a$  and  $b$  such that  $m = ac$  and  $n = bc$ . Then

$$\begin{aligned} x \cdot y - y \cdot x &= e \cdot (x \cdot y - y \cdot x) = (acx + bcy) \cdot (x \cdot y - y \cdot x) \\ &= (ax + by) \cdot (c(x \cdot y - y \cdot x)) = (ax + by) \cdot 0 = 0. \end{aligned}$$

So  $x \cdot y = y \cdot x$ , and the ring is commutative. □

If we were to find a non-commutative unity ring, we need an additive group that requires more than two generators to define. The smallest such group is  $Z_{24}^*$ . We may suppose that the additive group is generated by the unity  $e$ , along with two other elements  $a$  and  $b$ . Suppose that  $a \cdot b = a$ , while  $b \cdot a = b$ . This would make the ring non-commutative. We still need to discern what  $a^2$  and  $b^2$  should be. But  $a^2 = (a \cdot b) \cdot a = a \cdot (b \cdot a) = a \cdot b = a$ , and  $b^2 = (b \cdot a) \cdot b = b \cdot (a \cdot b) = b \cdot a = b$ . So the *SageMath* command for defining this ring would be

```
InitRing()
AddRingVar("e", "a", "b")
Define(2*e, 0); Define(2*a, 0); Define(2*b, 0)
Define(e^2, e); Define(e*a, a); Define(e*b, b)
Define(a*e, a); Define(b*e, b)
Define(a*b, a); Define(b*a, b)
Define(a^2, a); Define(b^2, b)
CheckRing()
```

This is a ring.

```

T8 = Ring(); T8
{0, e, a, e + a, b, e + b, a + b, e + a + b}
FindUnity(T8)
e

```

**TABLE 9.5:** Multiplication for a non-commutative unity ring

| .       | 0 | $e$     | $a$   | $e+a$   | $b$   | $e+b$ | $a+b$ | $e+a+b$ |
|---------|---|---------|-------|---------|-------|-------|-------|---------|
| 0       | 0 | 0       | 0     | 0       | 0     | 0     | 0     | 0       |
| $e$     | 0 | $e$     | $a$   | $e+a$   | $b$   | $e+b$ | $a+b$ | $e+a+b$ |
| $a$     | 0 | $a$     | $a$   | 0       | $a$   | 0     | 0     | $a$     |
| $e+a$   | 0 | $e+a$   | 0     | $e+a$   | $a+b$ | $e+b$ | $a+b$ | $e+b$   |
| $b$     | 0 | $b$     | $b$   | 0       | $b$   | 0     | 0     | $b$     |
| $e+b$   | 0 | $e+b$   | $a+b$ | $e+a$   | 0     | $e+b$ | $a+b$ | $e+a$   |
| $a+b$   | 0 | $a+b$   | $a+b$ | $0 * a$ | $a+b$ | 0     | 0     | $a+b$   |
| $e+a+b$ | 0 | $e+a+b$ | $b$   | $e+a$   | $a$   | $e+b$ | $a+b$ | $e$     |

The multiplication table is given in [Table 9.5](#). Because we will refer back to this ring often we will call this ring  $T_8$ .

It is easy to see that any finite ring can be quickly entered into *SageMath*. In fact many infinite rings such as the quaternions, can also be explored with *SageMath*. This will allow us to experiment with many different rings, and find properties which are common to all rings. In the next section we will look at some of the basic relationships between rings.

## Problems for §9.2

For Problems 1 through 10: Given the few properties of the generators of a ring, complete the list of products  $\{a \cdot b, b \cdot a, a^2, b^2\}$  that would be used to define the ring in *SageMath*.

Hint: Use the associate law to fill in the missing information.

1  $a \cdot b = b, b \cdot a = a$       6  $a \cdot b = a + b, b^2 = a + b$

2  $a \cdot b = a, b \cdot a = 0, b^2 = b$       7  $a \cdot b = a, b^2 = a$

3  $a^2 = b, a \cdot b = a$       8  $a \cdot b = 2b, b \cdot a = a, 3b = 0$

4  $a^2 = a + b, b \cdot a = 0$       9  $a \cdot b = b, b \cdot a = 3a, 4a = 0$

5  $a \cdot b = a, b^2 = a + b$       10  $a^2 = b, b^2 = a, 2a = 2b = 0$

11 If  $a^2 = a + b + c, a \cdot b = c, b \cdot c = a, c \cdot a = a \cdot c = b$ , determine  $b^2, c^2, b \cdot a$ , and  $c \cdot b$ .

12 Prove that a ring with a cyclic additive group must be commutative.

- 13** Prove that for  $m$  a positive integer, and  $x$  and  $y$  elements of a ring, then  $m(x + y) = mx + my$ .
- 14** Prove that for  $m$  and  $n$  positive integers, and  $x$  an element of a ring, then  $(m + n)x = mx + nx$ .
- 15** Prove that for  $m$  and  $n$  positive integers, and  $x$  an element of a ring, then  $(mn)x = m(nx)$ .
- 16** Prove that if  $n$  is an integer, and  $x$  is an element of a ring, then  $n(-x) = -(nx)$ .
- 17** Find the characteristic of the ring  $T_8$  defined by [Table 9.5](#).
- 18** Prove that if  $n > 1$ , the characteristic of  $Z_n$  is  $n$ .
- 19** Let  $R$  be unity ring. If the unity element has a finite order in the additive group, show that this order is the characteristic of the ring.
- 20** Prove that if a ring  $R$  has a finite number of elements, then the characteristic of  $R$  is a positive integer.
- 21** Use the fundamental theorem of abelian groups (7.2) to show that every finite abelian group has a basis.
- 22** Show that  $\{2, 3\}$  is a basis of the group  $Z_6$ . Since  $\{1\}$  is also a basis, this indicates that the number  $k$  in Definition 9.10 is not uniquely determined.

### Interactive Problems

- 23** Use *SageMath* to define a ring of order 2 that has no unity element. Show both the addition table and the multiplication table.
- 24** Use *SageMath* to find a non-commutative ring of order 8, for which the additive group is isomorphic to  $Z_{24}^*$ , formed from the basis  $\{a, b, c\}$ , and for which  $a \cdot b = a$ ,  $b \cdot a = b$ ,  $a \cdot c = c$ , and  $c \cdot a = a$ .  
 Hint: Using the associative law, determine what  $a^2$ ,  $b^2$ , and  $c^2$  must be. Then show that  $c \cdot b$  must commute with  $a$ . Use trial and error to determine  $b \cdot c$ .
- 25** Use *SageMath* to find a non-commutative ring of order 8, for which the additive group is isomorphic to  $Z_{24}^*$ , formed from the basis  $\{a, b, c\}$ , and for which  $a^2 = a + c$ ,  $a \cdot b = b + c$ ,  $b \cdot a = b$ , and  $c \cdot b = c$ .
- 26** Define in *SageMath* a non-commutative ring of order 4.  
 Hint: By Problem 12, the additive group must be isomorphic to  $Z_8^*$ .

### 9.3 Some Properties of Rings

Now that we can enter finite rings into *SageMath*, let us turn our attention to using *SageMath* to help us discover some truths about rings. In particular, we want to study in what circumstances multiplicative inverses exist.

One of the simplest rings to study are the rings  $Z_n$  for  $n > 1$ . We have already learned how to define the additive structure in *SageMath* with a **ZGroup** command, and the multiplication can be defined using a **ZStar** command. We actually can define both of these at once with the command

**z15 = ZRing(15)**

This defines both the addition and multiplication operations at the same time. The elements of  $Z_{15}$  are

**z15**

{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}

We can perform simple operations in  $Z_{15}$  such as

**z15[9] + z15[7]**

1

**z15[9] \* z15[7]**

3

**z15[9] / z15[7]**

12

This last operation shows that we can take multiplicative inverses of some of the elements. Even though multiplicative inverses are not guaranteed to exist for rings, some elements may be invertible.

#### LEMMA 9.3

Let  $x$  be an element in a unity ring. Then if  $x$  has a multiplicative inverse, the inverse is unique. We denote the multiplicative inverse of  $x$  by  $x^{-1}$ .

PROOF: Suppose that  $y$  and  $z$  are two inverses of  $x$ . Then

$$y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z,$$

which is a contradiction. □

#### PROPOSITION 9.4

If  $R$  is a unity ring, then the invertible elements of  $R$  form a group under multiplication. This group is denoted  $R^*$ .

**PROOF:** Since the unity element is invertible,  $R^*$  is non-empty. Also, if  $x$  is invertible, then  $(x^{-1})^{-1} = x$ , so  $x^{-1}$  is also in  $R^*$ . Finally, if  $x$  and  $y$  are both invertible, then since

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot x^{-1} = e,$$

we see that  $x \cdot y$  is invertible. The associative law comes from the associative multiplication of the ring. So the set of invertible elements forms a group.  $\square$

From this, we can find out when  $Z_n$  is in fact a field. The first step is to determine when  $Z_n$  will have zero divisors.

### PROPOSITION 9.5

*For  $n > 1$ , the ring  $Z_n$  has no zero divisors if, and only if,  $n$  is prime.*

**PROOF:** First suppose that  $n$  is not prime. Then we can express  $n = ab$ , where  $a$  and  $b$  are less than  $n$ . Then  $a \cdot b \bmod n = 0$ , so  $a$  and  $b$  are both zero divisors of  $Z_n$ .

Now suppose that  $n$  is prime, and that there are two nonzero elements  $a$  and  $b$  such that  $a \cdot b \bmod n = 0$ . But since  $n$  is prime, we would have to conclude that either  $a$  or  $b$  is a multiple of  $n$ . But this contradicts the fact that both  $a$  and  $b$  are nonzero elements of  $Z_n$ . Thus, if  $n$  is prime, there are no zero divisors in  $Z_n$ .  $\square$

Even if  $n$  is not prime, one of the observations that can be made while studying  $Z_n$  is that the zero divisors were precisely the nonzero elements that did not have an inverse. This is true for many of the rings we have studied.

### LEMMA 9.4

*Let  $a$ ,  $b$ , and  $c$  be elements of a ring. If  $a$  is nonzero and is not a zero divisor, and*

$$a \cdot b = a \cdot c,$$

*then  $b = c$ . Likewise, if*

$$b \cdot a = c \cdot a$$

*for a nonzero and not a zero divisor, then  $b = c$ . This is called the cancellation law for multiplication.*

**PROOF:** The tempting thing to do is to multiply both sides of the equation by  $a^{-1}$ . But the inverse of  $a$  may not exist, so we have to use the properties of rings instead.

If  $a \cdot b = a \cdot c$ , then we have

$$0 = a \cdot b - a \cdot c = a \cdot (b - c).$$

But since  $a$  is not a zero-divisor and is nonzero, we must have that  $b - c = 0$ . Hence  $b = c$ .

Likewise, if  $b \cdot a = c \cdot a$ , then

$$0 = b \cdot a - c \cdot a = (b - c) \cdot a$$

and since  $a$  is nonzero and not a zero divisor,  $b - c = 0$ , and so  $b = c$ . □

We are now ready to show a relationship between zero divisors and invertible elements. Notice that in the ring  $\mathbb{Z}$ , the element 2 is not invertible, but neither is it a zero divisor. This example seems to break the pattern that we have been observing but also notice that  $\mathbb{Z}$  is an *infinite* ring. Perhaps if we consider only *finite* rings we will be able to prove a relationship between zero divisors and invertible elements.

### **PROPOSITION 9.6**

*Let  $R$  be a finite ring. If  $b$  is a nonzero element of  $R$  which is not a zero divisor, then  $R$  has a unity element and  $b$  has a multiplicative inverse in  $R$ . Hence, every nonzero element in  $R$  is either a zero divisor or is invertible.*

**PROOF:** To utilize the fact that  $R$  is finite, let us construct a sequence of powers of  $b$ :

$$\{b^1, b^2, b^3, b^4, \dots\}.$$

Since  $R$  is finite, two elements of this sequence must be equal, say  $b^m = b^n$  for  $m < n$ . Using the law of cancellation, we have  $b^{m-1} = b^{n-1}$ . Continuing this way, we eventually get  $b = b^{n-m+1}$ . (It is tempting to use Lemma 9.4 one more time to get  $e = b^{n-m}$ , but unfortunately we have yet to prove that  $R$  has a unity.)

If we now let  $a = n - m + 1$ , we have that  $a > 1$  and  $b^a = b$ .

Next, let us show that  $b^{a-1}$  is a unity element in  $R$ . For any element  $x$  in  $R$ , we have

$$x \cdot b^a = x \cdot b,$$

and since  $b$  is nonzero and not a zero divisor, we can use the law of cancellation to get

$$x \cdot b^{a-1} = x.$$

Likewise, since  $b^a \cdot x = b \cdot x$ , we have that  $b^{a-1} \cdot x = x$ . Hence, there is a unity element in  $R$ , namely  $b^{a-1}$ .

Finally, we need to construct an inverse for the element  $b$ . If  $a = 2$ , then we have just shown that  $b = e$ , and hence  $b$  is its own inverse. If  $a > 2$ , consider the element  $b^{a-2}$ . We have that

$$b^{a-2} \cdot b = b^{a-1} = e \quad \text{and} \quad b \cdot b^{a-2} = b^{a-1} = e.$$

So  $b^{a-2}$  is the multiplicative inverse of  $b$ . □

**TABLE 9.6:** The non-commutative ring  $T_4$ 

| + | 0 | a | b | c | . | 0 | a | b | c |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | a | b | c | 0 | 0 | 0 | 0 | 0 |
| a | a | 0 | c | b | a | 0 | a | a | 0 |
| b | b | c | 0 | a | b | 0 | b | b | 0 |
| c | c | b | a | 0 | c | 0 | c | c | 0 |

**COROLLARY 9.1**

*Every finite ring without zero divisors is a division ring.*

PROOF: The trivial ring is already considered to be a division ring, so we may assume that the ring is nontrivial. Then there exists a nonzero element that is not a zero divisor, so by Proposition 9.6, the ring has a unity. Also by Proposition 9.6, every nonzero element will have a multiplicative inverse, so the ring is a division ring.  $\square$

We finally can determine which  $Z_n$  are fields.

**COROLLARY 9.2**

*The ring  $Z_n$  is a field if, and only if,  $n$  is prime.*

PROOF: If  $n = 1$ , then the ring  $Z_n = Z_1$  is the trivial ring, which we did not consider to be a field. We may suppose that  $n > 1$ . If  $n$  is prime, then by Proposition 9.5  $Z_n$  has no zero divisors, and so by Corollary 9.1  $Z_n$  is a division ring. Since  $Z_n$  is obviously commutative, this tells us that  $Z_n$  is a field.

Now suppose that  $n > 1$  and  $n$  is not prime. By Proposition 9.5,  $Z_n$  has zero divisors, which cannot exist in a field according to Proposition 9.2. Therefore  $Z_n$  is a field if, and only if,  $n$  is prime.  $\square$

To conclude this chapter, let us find an example of each of the 11 different types of rings that could exist. First we define the rings  $T_4$  in Table 9.6, and we will rewrite the elements of  $T_8$  into a more compact form in Table 9.7. Then every ring will fall into one of the categories given in Table 9.8.

### Problems for §9.3

- Show that the non-commutative ring  $T_4$  given by Table 9.6 has two elements  $r$  such that  $x \cdot r = x$  for all  $x$  in the ring, yet has no element for which  $r \cdot x = x$  for all  $x$  in the ring.
- Let  $x$  be an element of a commutative ring  $R$  which has an inverse  $x^{-1}$ . Let  $y$  be another element of  $R$  such that  $y^2 = 0$ . Prove that  $x + y$  has an inverse in  $R$ .

**TABLE 9.7:** The smallest non-commutative unity ring  $T_8$ 

| + | 0 | e | a | b | c | d | f | g |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | e | a | b | c | d | f | g |
| e | e | 0 | d | f | g | a | b | c |
| a | a | d | 0 | c | b | e | g | f |
| b | b | f | c | 0 | a | g | e | d |
| c | c | g | b | a | 0 | f | d | e |
| d | d | a | e | g | f | 0 | c | b |
| f | f | b | g | e | d | c | 0 | a |
| g | g | c | f | d | e | b | a | 0 |

| . | 0 | e | a | b | c | d | f | g |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| e | 0 | e | a | b | c | d | f | g |
| a | 0 | a | a | a | 0 | 0 | 0 | a |
| b | 0 | b | b | b | 0 | 0 | 0 | b |
| c | 0 | c | c | c | 0 | 0 | 0 | c |
| d | 0 | d | 0 | c | c | d | f | f |
| f | 0 | f | c | 0 | c | d | f | d |
| g | 0 | g | b | a | c | d | f | e |

**TABLE 9.8:** Examples for each possible type of ring

| Type | Name                                                                   | Example(s)                                                                      |
|------|------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| I    | The trivial ring                                                       | Only one such ring, $\{0\}$ .                                                   |
| II   | Fields                                                                 | $\mathbb{R}, \mathbb{Q}, Z_p$ with $p$ prime.                                   |
| III  | Skew fields                                                            | $\mathbb{H}$ = the quaternions.                                                 |
| IV   | Commutative unity rings w/o zero divisors, but are not fields          | $\mathbb{Z}$ , polynomials.<br>These rings are called <i>integral domains</i> . |
| V    | Non-commutative unity rings w/o zero divisors, but are not skew fields | Integer quaternions:<br>$a + bi + cj + dk$ , with $a, b, c, d \in \mathbb{Z}$ . |
| VI   | Commutative rings w/o unity and w/o zero divisors                      | Even integers, multiples of $n$ , $n > 1$ .                                     |
| VII  | Non-commutative rings w/o unity and w/o zero divisors                  | Even quaternions.                                                               |
| VIII | Commutative unity rings w/ zero divisors                               | $Z_n$ whenever $n > 1$ and $n$ is not prime.                                    |
| IX   | Non-commutative unity rings w/ zero divisors                           | $T_8$ in <a href="#">table 9.7</a> .                                            |
| X    | Commutative rings w/o unity and w/ zero divisors                       | The subset $\{0, 2, 4, 6\}$ of $Z_8$ .                                          |
| XI   | Non-commutative rings w/o unity and w/ zero divisors                   | $T_4$ in <a href="#">table 9.6</a> .                                            |

- 3 Let  $x$  be an element of a commutative ring  $R$  which has an inverse  $x^{-1}$ . Let  $y$  be another element of  $R$  such that  $y^3 = 0$ . Prove that  $x + y$  has an inverse in  $R$ .
- 4 Find a specific example of two elements  $x$  and  $y$  in a ring  $R$  such that  $x \cdot y = 0$ , but  $y \cdot x$  is nonzero.

Hint: Which of the 11 types of rings would  $R$  have to be?

- 5** Consider the subset  $\{0, 2, 4, 6, 8\}$  of  $Z_{10}$ . Form addition and multiplication tables of this set. Is this a ring? Which of the 11 types of rings is this?
- 6** Let  $R$  be a ring for which  $x^2 = x$  for all  $x$  in the ring. Prove that  $-x = x$  for all elements  $x$ . Such rings are called *Boolean* rings.
- 7** Let  $R$  be a ring for which  $x^2 = x$  for all  $x$  in the ring. Prove that the ring  $R$  is commutative. (See Problem 6.)
- 8** Let  $R$  be a ring for which  $x^3 = x$  for all  $x$  in the ring. Prove that  $6x = 0$  for all  $x$  in the ring.
- 9** Let  $R$  be a commutative ring of characteristic 2. Prove that  $(x+y)^2 = x^2 + y^2$  for all  $x$  and  $y$  in  $R$ . This property is often referred to as “freshman’s dream.”
- 10** Let  $R$  be a commutative ring of characteristic 2. Prove that  $(x+y)^4 = x^4 + y^4$  for all  $x$  and  $y$  in  $R$ . You can use the result of Problem 9.
- 11** Find an example of a commutative ring of characteristic 4 for which there are elements  $x$  and  $y$  such that  $(x+y)^4 \neq x^4 + y^4$ .
- 12** Find an example of a non-commutative ring of characteristic 4 for which there are elements  $x$  and  $y$  such that  $(x+y)^4 \neq x^4 + y^4$ .
- 13** An element  $a$  in a ring  $R$  is *idempotent* if  $a^2 = a$ . Prove that a nontrivial division ring must contain exactly two idempotent elements.
- 14** Let  $a$  be an idempotent element in a unity ring. Show that  $e - a$  is also an idempotent element. See Problem 13.
- 15** Show that if  $R$  is a commutative ring, and  $x$  and  $y$  are elements of  $R$ , then

$$(x+y)^2 = x^2 + 2xy + y^2$$

and

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

- 16** Let  $R$  be a commutative ring. Define the *binomial coefficient*

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}, \quad (0 \leq k \leq n).$$

Using induction, prove the *binomial theorem* in  $R$ :

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n.$$

- 17** Determine all elements of  $T_8$  in [Table 9.7](#) that have a multiplicative inverse.
- 18** Determine all elements of the ring defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#) that have a multiplicative inverse.
- 19** An *irreducible* element  $p \neq 0$  of a ring  $R$  is a non-invertible element for which the only way for  $p = a \cdot b$  is for either  $a$  or  $b$  to have a multiplicative inverse. Determine the irreducible elements of the ring defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#).
- Hint: Cross out the rows and columns corresponding to the invertible elements. Which elements are no longer in the interior of the table?
- 20** Does  $T_4$  or  $T_8$  in [Tables 9.6](#) and [9.7](#) have any irreducible elements? (See Problem 19.)
- 21** A *prime* element  $p \neq 0$  of a ring  $R$  is a non-invertible element such that, whenever  $a \cdot b$  is a multiple of  $p$ , either  $a$  or  $b$  is a multiple of  $p$ . (A multiple of  $p$  would be any element that can be expressed as either  $x \cdot p$  or  $p \cdot x$ .) Find a prime element of the ring  $T_8$  in [Table 9.7](#).
- Hint: To determine if  $p$  is prime, first find all the multiples of  $p$ . Then cross out the rows and columns of the multiplication table corresponding to those elements. If there are no more multiples of  $p$  remaining, then  $p$  is prime.
- 22** Find a prime element of the ring defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#) that is not irreducible. (See Problems 19 and 21.)

#### Interactive Problems

- 23** Define in *SageMath* the smallest non-commutative ring,  $T_4$  defined by [Table 9.6](#). Use  $a$  and  $c$  as the generators.
- 24** Define in *SageMath* the smallest non-commutative unity ring  $T_8$  defined by [Table 9.7](#).
- Hint: The basis can be chosen to be  $e$ ,  $a$ , and  $b$ .

# Chapter 10

---

## The Structure within Rings

Just as we can have subgroups, normal subgroups, quotient groups, and homomorphisms between groups, we can have similar structures within rings. In fact, ring theory runs almost parallel with the study of groups. In this chapter we will demonstrate the similarities between the two theories. These similarities are startling, since a “normal subring” is defined totally differently than a normal subgroup.

---

### 10.1 Subrings

It is natural to ask whether we can have smaller rings within a larger ring, just as we saw smaller groups inside of a larger group. This suggests the following definition.

**DEFINITION 10.1** Let  $R$  be a ring. A non-empty subset  $S$  is a *subring* if  $S$  is a ring with respect to the addition (+) and multiplication ( $\cdot$ ) of  $R$ .

We have already seen some examples of subrings. For example, the set of even integers is a ring contained in the ring of integers, which is contained in the ring of rational numbers, which in turn is contained in the ring of real numbers. The next proposition gives us a quick way to determine if a subset is indeed a subring.

#### PROPOSITION 10.1

A non-empty subset  $S$  is a subring of a ring  $R$  if, and only if, whenever  $x$  and  $y$  are in  $S$ ,  $x - y$  and  $x \cdot y$  are in  $S$ .

PROOF: Certainly if  $S$  is a subring, then  $x - y$  and  $x \cdot y$  would be in  $S$  whenever  $x$  and  $y$  are in  $S$ . So let us suppose that  $S$  is non-empty and is closed with respect to subtraction and multiplication. If  $x$  is any element in  $S$ , then  $x - x = 0$  is in  $S$ , so  $S$  contains an additive identity. Also,  $0 - x = -x$  would also be in  $S$ , so  $S$  contains additive inverses of all of its elements. Then

whenever  $x$  and  $y$  are in  $S$ ,  $x - (-y) = x + y$  is in  $S$ , so  $S$  is closed with respect to addition. The commutative and associative properties of addition, as well as the associative and two distributive laws for multiplication, come from the original ring  $R$ . Finally,  $S$  is closed with respect to multiplication, so  $S$  is a subring.  $\square$

Notice that from the definition every nontrivial ring  $R$  will contain at least two subrings: the trivial ring  $\{0\}$  will be a subring, as well as the entire ring  $R$ . These two subrings are called the *trivial subrings*.

### Example 10.1

Consider the subset of real numbers of the form

$$S = \{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}.$$

Determine whether or not this is a subring of  $\mathbb{R}$ .

**SOLUTION:** Two typical elements of  $S$  are  $a = x_1 + y_1\sqrt{2}$  and  $b = x_2 + y_2\sqrt{2}$ . Then

$$a - b = (x_1 - x_2) + (y_1 - y_2)\sqrt{2},$$

and

$$a \cdot b = (x_1x_2 + 2y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{2}.$$

Since all expressions in parenthesis are integers, these are in  $S$ . Thus, by Proposition 10.1,  $S$  is a subring of  $\mathbb{R}$ .  $\square$

### Computational Example 10.2

Here is the ring of order 8 we defined by Tables 9.3 and 9.4:

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, b)
Define(a*b, 0); Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

The set

```
S = [0*a, a, 2*a, 3*a]; S
[0, a, 2 a, 3 a]
```

can be seen to be a subring from the addition and multiplication tables in Table 10.1.

One can see that  $S$  is closed with respect to both addition and multiplication. Furthermore, additive inverses exist for all elements, so  $S$  is also closed with respect to subtraction. Thus, by Proposition 10.1, this is a subring.  $\square$

**TABLE 10.1:** Tables for the subring  $S$ 

| $+$  | 0    | $a$  | $2a$ | $3a$ | .    | 0 | $a$  | $2a$ | $3a$ |
|------|------|------|------|------|------|---|------|------|------|
| 0    | 0    | $a$  | $2a$ | $3a$ | 0    | 0 | 0    | 0    | 0    |
| $a$  | $a$  | $2a$ | $3a$ | 0    | $a$  | 0 | $a$  | $2a$ | $3a$ |
| $2a$ | $2a$ | $3a$ | 0    | $a$  | $2a$ | 0 | $2a$ | 0    | $2a$ |
| $3a$ | $3a$ | 0    | $a$  | $2a$ | $3a$ | 0 | $3a$ | $2a$ | $a$  |

One might wonder why we used **0\*a** instead of just **0** as we listed the elements of  $S$ . Although the additive identity of the ring is always *displayed* as 0, if we enter just **0**, *SageMath* will interpret this to mean the *integer* 0, not the zero element of the ring.

```
0 in R
False
```

The work-around is to multiply any of the generators by 0 to get the zero element of the ring.

```
0*a in R
True
```

Ironically, the subring  $S$  has a unity element,

```
FindUnity(S)
a
```

which is different than the unity of  $R$ . In general the existence of a subring's unity is totally independent of the unity of  $R$ .

Recall that the intersection of a number of subgroups was again a subgroup. We could ask whether the same is true for subrings.

### PROPOSITION 10.2

*Given any non-empty collection of subrings of the group  $R$ , denoted by  $L$ , then the intersection of all of the subrings in the collection*

$$H^* = \bigcap_{H \in L} H$$

*is a subring of  $R$ .*

PROOF: First of all, note that  $H^*$  is not the empty set, since 0 is in each  $H$  in the collection. We now can apply Proposition 10.1. Let  $x$  and  $y$  be two elements in  $H^*$ . Then, for every  $H \in L$ , we have  $x, y \in H$ .

Since each  $H$  is a subring of  $R$ , we have  $x - y \in H$  and  $x \cdot y \in H$  for all  $H \in L$ . Therefore,  $x - y$  and  $x \cdot y$  are in  $H^*$ , and so  $H^*$  is a subring of  $R$ .  $\square$

As with subgroups, we now have a general method of producing subrings of a ring  $R$ . Let  $S$  be any subset of  $R$ . We can consider the collection  $L$  of all subrings of  $R$  that contain the set  $S$ . This collection is non-empty since it contains the subring  $R$  itself. So by Proposition 10.2,

$$[S] = H^* = \bigcap_{H \in L} H$$

is a subring of  $R$ . By the way that the collection was defined,  $[S]$  contains  $S$ . Actually,  $[S]$  is the *smallest* subring of  $R$  containing the subset  $S$ . For if  $H$  is a subring of  $R$  which contains  $S$ , then  $H \in L$ , so that  $[S] \subseteq H$ .

**DEFINITION 10.2** We call  $[S]$  the subring of  $R$  *generated* by the set  $S$ .

### Example 10.3

Find the subring of  $T_8$  from Table 9.7 generated by the element  $g$ .

SOLUTION: Clearly, 0 is in the subring, and since  $g + g = 0$ , the set  $\{0, g\}$  is closed under subtraction. But  $g^2 = e$ , so this element is in the subring. This causes  $g + e = c$  to be in the subring as well. The set  $\{0, c, e, g\}$  can be seen to be closed under addition, multiplication, and additive inverses. So  $[g] = \{0, c, e, g\}$ .  $\blacksquare$

Just as in the case for the **Group** command, the command **Ring** finds  $[S]$  for any set  $S$  in *SageMath*. For example, we can find some subrings for the non-commutative group of order 8,

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, b)
Define(a*b, 0); Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

with the commands

```
Ring(0*a)
{0}
Ring(a)
{0, a, 2 a, 3 a}
Ring(2*a)
{0, 2 a}
Ring(2*a, b)
{0, b, 2 a, 2 a + b}
```

In this way, we can find all subrings of the ring  $R$ . Recall that we had to enter  $\mathbf{0}*\mathbf{a}$  instead of  $\mathbf{0}$  for the additive identity of the ring. It turns out that there are six nontrivial subrings for this ring, corresponding to the six nontrivial subgroups of  $Z_{15}^*$ .

We can also find all of the subrings for the infinite ring  $\mathbb{Z}$ .

### **PROPOSITION 10.3**

*A subring of the ring of integers  $\mathbb{Z}$  consists of all multiples of some non-negative number  $n$ . This subring is denoted  $n\mathbb{Z}$ .*

PROOF: First of all, the trivial subring  $\{0\}$  can be considered the set of all multiples of 0. Also, the entire ring  $\mathbb{Z}$  could be considered all of the multiples of 1. Let  $S$  be a nontrivial subring, and let  $x$  be in  $S$ . Then  $-x$  is also in  $S$ , so  $S$  must contain some positive integers. Let  $n$  be the smallest positive integer contained in  $S$ . Certainly all multiples of  $n$  would be in  $S$ , but suppose that some element  $m$  in  $S$  is not a multiple of  $n$ . Then by Bézout's lemma (1.3), there exist two integers  $u$  and  $v$  such that

$$un + vm = \gcd(n, m).$$

Since  $S$  is closed under addition, this implies that  $\gcd(n, m)$  is in  $S$ . But  $m$  is not a multiple of  $n$ , so  $\gcd(n, m) < n$ . But this contradicts the fact that  $n$  is the *smallest* positive integer in  $S$ . Thus,  $S$  consists exactly of all of the multiples of  $n$ , and so  $S = n\mathbb{Z}$ .  $\square$

Although the subrings of  $\mathbb{Z}$  are easily classified, this is not the case with the ring of real numbers. Example 10.1 gives just one of countless subrings of  $\mathbb{R}$ :

$$S = \{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}.$$

It is actually possible to define this subring in *SageMath*. We can let  $e$  represent 1, and  $a$  represent  $\sqrt{2}$ . These two elements are both of infinite additive order. If we do not specify the additive order of an element, *SageMath* will assume that order is infinite. Then  $a^2 = 2e$ , so the ring can be entered by the commands

```
InitRing()
AddRingVar("e", "a")
Define(e^2, e)
Define(e*a, a)
Define(a*e, a)
Define(a^2, 2*e)
Ring()
Ring is infinite.
```

Of course we cannot list the elements, since there are on infinite numbers of elements. But we can still do operations in this ring.

$$(e+2*a) * (4*e-3*a)$$

$$-8 e + 5 a$$

This last statement demonstrates that

$$(1 + 2\sqrt{2}) \cdot (4 - 3\sqrt{2}) = -8 + 5\sqrt{2}.$$

Clearly, the subrings of the real numbers can be much more complicated than the subrings of integers.

### Problems for §10.1

For Problems 1 through 10: Use Proposition 10.1 to determine if the following subsets are subrings of  $\mathbb{R}$ .

- 1  $\{x + y\sqrt{5} \mid x, y \in \mathbb{Z}\}$
- 2  $\{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$
- 3  $\{x \mid x \in \mathbb{R}, x > 0\}$
- 4  $\{x/y \mid x \text{ is an even integer, } y \text{ is an odd integer}\}$
- 5  $\{x/(2^y) \mid x, y \in \mathbb{Z}, y \geq 0\}$
- 6  $\{x + y\sqrt[3]{2} \mid x, y \in \mathbb{Z}\}$
- 7  $\{x + y\sqrt[3]{2} + z\sqrt[3]{4} \mid x, y, z \in \mathbb{Z}\}$
- 8  $\{x + y\sqrt{2} \mid y \in \mathbb{Z}, x \text{ is an even integer}\}$
- 9  $\{x + y\sqrt{2} \mid x, y \in \mathbb{Z}, x + y \text{ is even}\}$
- 10  $\{x + y\sqrt{3} \mid x, y \in \mathbb{Z}, x + y \text{ is even}\}$

- 11 Let  $y$  be an element of a ring  $R$ . Let

$$A = \{x \in R \mid x \cdot y = 0\}.$$

Show that  $A$  is a subring of  $R$ .

- 12 Let  $y$  be an element of a ring  $R$ . Let

$$B = \{x \cdot y \mid x \in R\}.$$

Show that  $B$  is a subring of  $R$ .

- 13 Let  $R$  be a ring, and let

$$Z = \{x \in R \mid x \cdot y = y \cdot x \text{ for all } y \in R\}.$$

Show that  $Z$  is a subring of  $R$ . This subring is called the *center* of  $R$ .

- 14 An element  $x$  of a ring  $R$  is called *nilpotent* if  $x^n = 0$  for some positive number  $n$ . Show that the set of all nilpotent elements in a commutative ring  $R$  forms a subring of  $R$ .

Hint: See Problem 16 of §9.3.

- 15** Show that  $2\mathbb{Z} \cup 3\mathbb{Z}$  is not a subring of  $\mathbb{Z}$ . (The symbol  $\cup$  denotes the *union* of the two sets.)

- 16** Find all of the subrings of the commutative ring of order 8 defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#).

Hint: There are eight subgroups of the additive group  $\mathbb{Z}_{15}^*$ . Find the eight subgroups, and determine which subgroups are in fact subrings.

- 17** Find all of the subrings of  $T_4$  in [Table 9.6](#).

- 18** Find all of the subrings of  $T_8$  in [Table 9.7](#).

Hint: First find all 16 subgroups of the additive group,  $\mathbb{Z}_{24}^*$ .

### Interactive Problems

- 19** Find all of the subrings of the ring of order 8:

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, 0)
Define(a*b, b); Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

- 20** Find all of the subrings of the ring of order 8:

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, 2*a); Define(b^2, 2*a)
Define(a*b, 0); Define(b*a, 2*a)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

## 10.2 Quotient Rings and Ideals

When we studied group theory, one of the most important concepts we discovered was being able to form a quotient group out of the cosets of certain subgroups—namely the normal subgroups. A natural question is whether it is possible to form quotient rings out of the cosets of a subring.

### ***Motivating Example 10.4***

Here is the non-commutative ring of order 8 from the last section.

```

InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, 0)
Define(a*b, b); Define(b*a, 2*a)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}

```

Can we form a quotient ring out of this ring, the way that we constructed a quotient group?

SOLUTION: We found this ring has six nontrivial subrings.

$$\begin{aligned} S_1 &= \{0, a, 2a, 3a\}, & S_2 &= \{0, 2a\}, & S_3 &= \{0, b\}, \\ S_4 &= \{0, a+b, 2a, 3a+b\}, & S_5 &= \{0, 2a+b\}, & S_6 &= \{0, 2a, b, 2a+b\}. \end{aligned}$$

We would expect the additive structure of the quotient ring to be the additive quotient group  $R/S$ . We can use *SageMath* to find the cosets of  $S$  under the operation of addition. Since left and right cosets are the same when working with rings, we will simply use the **Coset** command.

```

S1 = Ring(a); S1
{0, a, 2 a, 3 a}
Q = Coset(R, S1); Q
{{0, a, 2 a, 3 a}, {b, a + b, 2 a + b, 3 a + b}}

```

We can *add* two cosets together using the following definition:

$$X + Y = \{x + y \mid x \in X \text{ and } y \in Y\}.$$

This gives us a natural way to add the elements of the quotient  $Q$ , which is shown in **Table 10.2**, produced by the command **AddTable(Q)**.

**TABLE 10.2:** Addition for the quotient ring  $Q$

| +                          | {0, a, 2a, 3a}             | {b, a + b, 2a + b, 3a + b} |
|----------------------------|----------------------------|----------------------------|
| {0, a, 2a, 3a}             | {0, a, 2a, 3a}             | {b, a + b, 2a + b, 3a + b} |
| {b, a + b, 2a + b, 3a + b} | {b, a + b, 2a + b, 3a + b} | {0, a, 2a, 3a}             |

The natural way to define the product of two sets is the way we defined such a product for groups:

$$X \cdot Y = \{x \cdot y \mid x \in X \text{ and } y \in Y\}.$$

Will such a product of two cosets in  $Q$  yield another coset?

Unfortunately no! The multiplication tables in *SageMath* reveal black squares—which indicate that the product of two cosets is not a coset. The problem lies in the product of the two cosets.

```
Q1 = S1; Q1
{0, a, 2 a, 3 a}
Q2 = b + S1; Q2
{b, a + b, 2 a + b, 3 a + b}
Q1 * Q2
{0, b, a + b, 2 a, 2 a + b, 3 a + b}
```

which produces extra elements. To ensure that  $S$  acts as the zero element in the product of cosets, we need to have  $S$  times any element of  $R$  needs to produce only elements in  $S$ .

Suppose we found a subring  $S$  for which  $S \cdot x$  always was a subset of  $S$ . By the same argument we would also require that  $x \cdot S$  be a subset of  $S$ . Using *SageMath*, we can test the other subrings.

```
S2 = Ring(2*a); S2
{0, 2 a}
S2 * R
{0, 2 a}
R * S2
{0, 2 a}
```

We see that both  $R \cdot S_2$  and  $S_2 \cdot R$  are subsets of  $S_2$ , so this ensures that the additive identity of the quotient group  $\{0, 2a\}$  will behave as the zero element in the product of cosets. The multiplication table for the quotient group is as given by the commands

```
Q = Coset(R, S2); Q
{{0, 2 a}, {a, 3 a}, {b, 2 a + b}, {a + b, 3 a + b}}
MultTable(Q)
```

which produce Table 10.3. □

**TABLE 10.3:** Multiplying cosets of  $S_2$

| .               | {0, 2a} | {a, 3a} | {b, 2a + b} | {a + b, 3a + b} |
|-----------------|---------|---------|-------------|-----------------|
| {0, 2a}         | {0}     | {0, 2a} | {0}         | {0, 2a}         |
| {a, 3a}         | {0, 2a} | {a, 3a} | {b, 2a + b} | {a + b, 3a + b} |
| {b, 2a + b}     | {0}     | {0, 2a} | {0}         | {0, 2a}         |
| {a + b, 3a + b} | {0, 2a} | {a, 3a} | {b, 2a + b} | {a + b, 3a + b} |

This multiplication table is non-commutative, even though all of the subrings of  $R$  are commutative. So this quotient is unlike any of the subrings of  $R$ .

However, not every product yields a coset—sometimes it yields only a *subset* of a coset. One way to rectify this blemish in our multiplication table is to add the identity coset to each entry in the table. That is, instead of defining the product of the cosets  $X$  and  $Y$  to be  $X \cdot Y$ , we define the product of two cosets to be

$$X * Y = X \cdot Y + S.$$

The command

**QuotientRing = true**

creates a multiplication table using this new definition of the product of two cosets. Thus, **MultTable[Q]** produces a similar table as [Table 10.3](#), only every  $\{0\}$  is replaced by  $\{0, 2a\}$ .

The key to getting the quotient ring to work lies in the fact that  $S_2 \cdot R$  and  $R \cdot S_2$  were subsets of  $S_2$ . Let us first define the special type of subring that will allow quotient rings.

**DEFINITION 10.3** A subring  $I$  of a ring  $R$  is called an *ideal* of  $R$  if both  $I \cdot R$  and  $R \cdot I$  are contained in the subring  $I$ . That is,  $a \cdot x$  and  $x \cdot a$  are in  $I$  for all  $a \in I$ , and  $x \in R$ .

We already observed that if a subring is not an ideal, then the quotient ring cannot be defined. Let us now show that a quotient ring can be defined provided that  $I$  is an ideal.

#### PROPOSITION 10.4

Let  $R$  be a ring, and let  $I$  be an ideal of  $R$ . Then the additive quotient group  $R/I$  forms a ring, with the product of two cosets  $X$  and  $Y$  being  $X * Y = X \cdot Y + I$ . This ring is called the quotient ring  $R/I$ .

**PROOF:** The quotient group  $R/I$  is an abelian group, so we need only to check that the multiplication is closed, and that the associativity and two distributive laws hold.

Let  $X$  and  $Y$  be two cosets of  $R/I$ . Let  $x$  be an element in  $X$ , and  $y$  an element in  $Y$ . Then the product of the cosets  $X$  and  $Y$  is

$$X * Y = X \cdot Y + I = (x + I) \cdot (y + I) + I = x \cdot y + I \cdot y + x \cdot I + I \cdot I + I.$$

Because  $I$  is an ideal,  $I \cdot y$ ,  $x \cdot I$ , and  $I \cdot I$  are all subsets of  $I$ . Hence, the sum  $I \cdot y + x \cdot I + I \cdot I + I$  will be a subset of  $I$ . But since the last term of this expression is  $I$ ,  $I \cdot y + x \cdot I + I \cdot I + I$  contains the ideal  $I$ , so this sum equals  $I$ . Thus,

$$(x + I) * (y + I) = X * Y = X \cdot Y + I = x \cdot y + I,$$

which is a coset of  $R/I$ .

Now suppose that  $X$ ,  $Y$ , and  $Z$  are three cosets of  $R/I$  with  $x$ ,  $y$ , and  $z$  being representative elements, respectively. Then

$$\begin{aligned}(X * Y) * Z &= ((x + I) * (y + I)) * (z + I) \\&= (x \cdot y + I) * (z + I) \\&= ((x \cdot y) \cdot z + I) \\&= (x \cdot (y \cdot z) + I) \\&= (x + I) * (y \cdot z + I) \\&= (x + I) * ((y + I) * (z + I)) \\&= X * (Y * Z).\end{aligned}$$

So multiplication is associative. Also,

$$\begin{aligned}X * (Y + Z) &= (x + I) * (y + z + I) \\&= (x \cdot (y + z) + I) \\&= x \cdot y + x \cdot z + I \\&= (x \cdot y + I) + (x \cdot z + I) \\&= X * Y + X * Z,\end{aligned}$$

and

$$\begin{aligned}(X + Y) * Z &= (x + y + I) * (z + I) \\&= ((x + y) \cdot z + I) \\&= x \cdot z + y \cdot z + I \\&= (x \cdot z + I) + (y \cdot z + I) \\&= X * Z + Y * Z.\end{aligned}$$

Thus, the two distributive laws hold, so  $R/I$  is a ring. □

This shows that the ideals play the same role for rings that normal subgroups did for groups, namely that subsets with an additional property allow for quotients to be defined.

### **Example 10.5**

Find the ideals of the ring  $\mathbb{Z}$ , and determine the quotient rings.

SOLUTION: By Proposition 10.3, all subrings are of the form  $S = n\mathbb{Z}$  for some  $n$ . Yet any multiple of  $n$  times an integer yields a multiple of  $n$ , so  $S \cdot \mathbb{Z} = \mathbb{Z} \cdot S = S$ . Therefore, every subring of  $\mathbb{Z}$  is an ideal.

The cosets of the quotient ring  $\mathbb{Z}/(n\mathbb{Z})$  can be expressed in the form

$$a + n\mathbb{Z},$$

where  $a = 0, 1, 2, \dots, n - 1$ . Clearly, the quotient ring behaves exactly like the ring  $Z_n$ . We say that the quotient ring is *isomorphic* to  $Z_n$ .  $\blacksquare$

In contrast, let us consider a ring like the rational numbers  $\mathbb{Q}$ . Even though there are many subrings of  $\mathbb{Q}$ , the only ideals are the trivial subrings. This can be generalized by the following proposition.

**PROPOSITION 10.5**

*Any field or skew field can only have trivial ideals.*

PROOF: Let  $K$  be a field or skew field, and suppose that there is a non-trivial ideal  $I$  of  $K$ . Then there is a nonzero element  $x$  in  $I$ , and hence  $x^{-1}$  exists in  $K$ . Thus

$$e = x \cdot x^{-1} \in I \cdot K \subseteq I.$$

So the unity element  $e$  is contained in  $I$ . But then,

$$K = e \cdot K \subseteq I \cdot K \subseteq I.$$

Hence,  $I = K$ , so the only ideals of  $K$  are the trivial ideals.  $\blacksquare$

We have already observed that the intersection of two subrings is again a subring. The natural question is whether the intersection of two ideals gives an ideal. This will help us to find all of the ideals of a given ring.

**PROPOSITION 10.6**

*If  $L$  is a non-empty collection of ideals of a ring  $R$ , then the intersection of all of these ideals*

$$I^* = \bigcap_{I \in L} I$$

*is an ideal of  $R$ .*

PROOF: Since  $I^*$  is an intersection of subrings of  $R$ , by Proposition 10.2  $I^*$  is a subring of  $R$ . Thus, we only need to check that  $I^* \cdot R$  and  $R \cdot I^*$  are contained in  $I^*$ .

Suppose that  $a$  is an element of  $I^*$ . Then  $a$  is in each  $I \in L$ , and so  $a \cdot R$  and  $R \cdot a$  are subsets of each  $I$  in the collection. Thus,  $a \cdot R$  and  $R \cdot a$  will both be subsets of  $I^*$ . Since this result is true for every  $a$  in  $I^*$ , we have that  $I^* \cdot R$  and  $R \cdot I^*$  are both subsets of  $I^*$ . Therefore,  $I^*$  is an ideal.  $\blacksquare$

We can now define the smallest ideal of  $R$  that contains a subset  $S$ . We proceed as we did for subrings, and consider the collection  $L$  of all ideals of  $R$  containing  $S$ . Then the smallest ideal of  $R$  containing  $S$  would be

$$\langle S \rangle = \bigcap_{I \in L} I.$$

We call  $\langle S \rangle$  the *ideal generated by  $S$* . Notice the distinction between this notation and the notation  $[S]$  of the subring generated by  $S$ . If  $S$  contains only one element, say  $a$ , we will use the notation  $\langle a \rangle$  rather than the cumbersome  $\langle \{a\} \rangle$  to denote the ideal generated by  $a$ .

This proposition allows us to quickly find all ideals of a ring.

### Computational Example 10.6

Find the ideals in the non-commutative ring  $R$  of order 8,

```
InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, 0)
Define(a*b, b); Define(b*a, 2*a)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

SOLUTION: We can find  $\langle S \rangle$  using the *SageMath* command **Ideal(R, S)** for different subsets  $S$ . For example, when  $S = \{a\}$ ,

```
Ideal(R, a)
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

we find that this command produces the whole ring, so  $a$  cannot be contained in any nontrivial ideal. Likewise,  $3a$ ,  $a + b$ , and  $3a + b$  cannot be in a nontrivial ideal. The three remaining nonzero elements,  $2a$ ,  $b$ , and  $2a + b$ , generate different ideals.

```
Ideal(R, 2*a)
{0, 2 a}
Ideal(R, b)
{0, b, 2 a, 2 a + b}
Ideal(R, 2*a+b)
{0, 2 a + b}
```

These three ideals will be denoted by  $\langle 2a \rangle$ ,  $\langle b \rangle$ , and  $\langle 2a + b \rangle$ . It is clear that any ideal containing two out of three of these elements must contain  $b$ , and therefore must be  $\langle b \rangle$ . Hence, there are exactly five ideals in this ring: the two trivial ideals that can be denoted  $\langle 0 \rangle$  and  $\langle a \rangle$ , and the three ideals  $\langle 2a \rangle$ ,  $\langle b \rangle$ , and  $\langle 2a + b \rangle$ . □

Notice that all five ideals can be generated with only one element. We will give a special name for these ideals.

**DEFINITION 10.4** An ideal of  $R$  that is generated by only one element of  $R$  is called a *principal ideal*. If all of the ideals of  $R$  are principal ideals, then the ring is called a *principal ideal ring*.

The ring of integers  $\mathbb{Z}$  is a principal ideal ring, since all ideals (in fact all subrings) are of the form  $n\mathbb{Z}$ , which is generated by the single element  $n$ . Since  $\mathbb{Z}$  is also an integral domain, we will combine the two terms and call  $\mathbb{Z}$  a *principal ideal domain*, or *PID*. Principal ideal domains play an important role in ring theory. In particular, any PID also has a unique factorization property. Unique factorization domains, or UFD's, actually led to the term "ideal" coined by Kummer. (See the Historical Diversion on page 314.)

## Problems for §10.2

- 1** If  $X$  and  $Y$  are ideals of a ring, show that the *sum* of  $X$  and  $Y$ ,

$$X + Y = \{x + y \mid x \in X \text{ and } y \in Y\}$$

is an ideal.

- 2** In the ring of integers, find a positive integer  $n$  such that

$$\langle n \rangle = \langle 12 \rangle + \langle 16 \rangle.$$

(See Problem 1.)

- 3** If  $X$  and  $Y$  are ideals of a ring, show that the *product* of  $X$  and  $Y$ ,

$$X \cdot Y = \{x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n \mid x_i \in X \text{ and } y_i \in Y, n > 0\},$$

is an ideal.

- 4** In the ring of integers, find a positive integer  $n$  such that

$$\langle n \rangle = \langle 12 \rangle \cdot \langle 16 \rangle.$$

(See Problem 3.)

- 5** Let  $X$  and  $Y$  be ideals of a ring. Prove that  $X \cdot Y \subseteq X \cap Y$ . (See Problem 3.)

- 6** Let  $R$  be a ring and let  $p$  be a fixed prime. Define  $I_p$  to be the set of elements for which the additive order of the element is a power of  $p$ . Show that  $I_p$  is an ideal.

- 7** Find all of the ideals of the commutative ring of order 8 defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#). (See Problem 16.)

- 8** Find all of the ideals of  $T_4$  in [Table 9.6](#).

- 9** Find all of the ideals of  $T_8$  in [Table 9.7](#). (See Problem 18 from [§10.1](#).)

## Historical Diversion

# Ernst Kummer (1810–1893)

---

Kummer was a German mathematician, although he was born in what was then Prussia. He started out teaching for 10 years at a *gymnasium*, which is the German equivalent to high school. During these years, he inspired the future mathematician Leopold Kronecker.

Kummer made significant contributions to several areas of mathematics. He worked with Gauss' hypergeometric functions, and used the Maclaurin series of these functions to prove that any three such functions, whose parameters differ by integers, are linearly related. This is known as the *contiguous relations* of the hypergeometric series.

Kummer's greatest accomplishment came in an attempt to prove Fermat's last theorem. (See the Historical Diversion on page 103.) Several years earlier, Gabriel Lamé had a flawed proof of the theorem, based on the assumption that  $\mathbb{Z}[\omega_n]$  had unique factorization. In the cases where  $\mathbb{Z}[\omega_n]$  is a UFD, such as  $n = 3$  and  $n = 4$ , one can prove Fermat's last theorem from

$$z^n = x^n + y^n = (x + y)(x + \omega_n y)(x + \omega_n^2 y) \cdots (x + \omega_n^{n-1} y).$$

However, Kummer had shown three years before Lamé's proof that  $\mathbb{Z}[\omega_n]$  is not a UFD for  $n = 23$ . (It is now known that there are only a finite set of integers for which  $\mathbb{Z}[\omega_n]$  is a UFD.)

Kummer had an idea of replacing elements in a domain with “ideal integers,” which represented a special subring of the domain. This would later lead to the terminology of “ideals” of a ring. Kummer's plan, expressed in modern terminology, was to first prove that every non-trivial ideal can be uniquely expressed as a product of prime ideals, even if the domain was not a UFD. Since some of the ideals were not principal ideals, some of the prime ideals did not correspond to an element in the original domain. By using this “extension” of the domain, Kummer was able to prove Fermat's last theorem for most prime numbers, in particular for all primes less than 100 except 37, 59, and 67.

Because of Kummer's attempt, and partial success, in proving Fermat's last theorem, he paved the way for modern ring theory. Richard Dedekind and Emmy Noether would later use Kummer's ideal numbers to formulate the definition of the “ideal” and “prime ideal” that we use today. (See Historical Diversions on pages 334 and 281.)

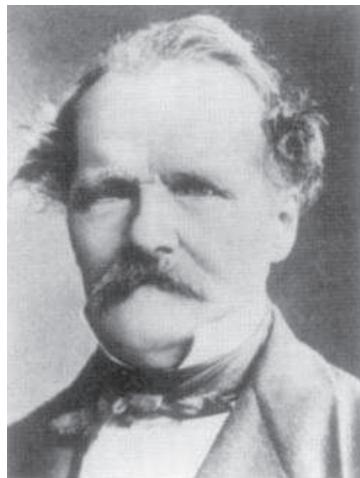


Image source: Wikimedia Commons

- 10** Verify that  $\{0, c\}$  is an ideal of the ring  $T_4$  in [Table 9.6](#). Construct addition and multiplication tables for the quotient ring  $T_4/\{0, c\}$ .
- 11** Verify that  $\{0, 2a\}$  is an ideal of the commutative ring  $R$  of order 8 which is defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#). Construct addition and multiplication tables for the quotient ring  $R/\{0, 2a\}$ .
- 12** Verify that  $\{0, b\}$  is an ideal of the commutative ring  $R$  of order 8 which is defined by [Tables 9.3](#) and [9.4](#) in [Chapter 9](#). Construct addition and multiplication tables for the quotient ring  $R/\{0, b\}$ .
- 13** A *left ideal*  $I$  of a ring  $R$  is a subring for which  $r \cdot x \in I$  when  $r \in R$ , and  $x \in I$ . Find a left ideal of  $T_8$  that is not a standard ideal.
- 14** Verify that  $\{0, c\}$  is an ideal of the ring  $T_8$  in [Table 9.7](#). Construct addition and multiplication tables for the quotient ring  $T_8/\{0, c\}$ .
- 15** Let  $A = \langle 6 \rangle$  be an ideal of the ring  $\mathbb{Z}$ . Construct addition and multiplication tables of the quotient ring  $\mathbb{Z}/(6)$ . What does this ring remind you of?
- 16** Let  $A = \langle 2 \rangle$  and  $B = \langle 6 \rangle$  be two ideals of the ring  $\mathbb{Z}$ . Construct addition and multiplication tables of the quotient ring  $A/B$ .
- 17** If  $R$  is a commutative ring and  $y$  is a fixed element of  $R$ , prove that the set
- $$A = \{x \in R \mid x \cdot y = 0\}$$
- is an ideal in  $R$ . (See Problem 11 in [§10.1](#).)
- 18** If  $R$  is a commutative ring and  $y$  is a fixed element of  $R$ , prove that the set
- $$B = \{x \cdot y \mid x \in R\}$$
- is an ideal of  $R$ .  
Hint: Note that if there is no multiplicative identity,  $y$  may not be in  $B$ .
- 19** An element  $x$  of a ring  $R$  is called *nilpotent* if  $x^n = 0$  for some positive number  $n$ . Show that the set of all nilpotent elements in a commutative ring  $R$  forms an ideal of  $R$ . See Problem 14 of [§10.1](#).
- 20** Let  $R$  be a unity ring, and  $I$  an ideal of  $R$ . Show that  $R/I$  is a unity ring.

## Interactive Problems

- 21** Which of the subrings of the ring of order 8, found in Problem 19 of [§10.1](#) are ideals? The ring is given as follows:

```

InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, 0)
Define(a*b, b); Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}

```

- 22** Which of the subrings of the ring of order 8, found in Problem 20 of §10.1 are ideals? The ring is given as follows:

```

InitRing()
AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, 2*a); Define(b^2, 2*a)
Define(a*b, 0); Define(b*a, 2*a)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}

```

---

### 10.3 Ring Isomorphisms

As we work with different rings, it is natural to ask whether we can consider two rings to be “equivalent” if the elements of one ring can be renamed to form the other ring. We have already seen that the quotient ring  $\mathbb{Z}/(n\mathbb{Z})$  was essentially the same ring as  $Z_n$ . We will proceed the same way we defined isomorphisms with groups.

**DEFINITION 10.5** Let  $A$  and  $B$  be two rings. A *ring isomorphism* from  $A$  to  $B$  is a one-to-one mapping  $f : A \rightarrow B$  such that

$$\begin{aligned} f(x + y) &= f(x) + f(y) && \text{and} \\ f(x \cdot y) &= f(x) \cdot f(y) \end{aligned}$$

for all  $x, y \in A$ . If there exists a ring isomorphism from  $A$  to  $B$  that is surjective, then we say that the rings  $A$  and  $B$  are *isomorphic*, denoted by  $A \approx B$ .

**Example 10.7**

Find an isomorphism from the quotient ring  $\mathbb{Z}/(n\mathbb{Z})$  to  $Z_n$ .

SOLUTION: The natural mapping would be as follows:

$$f(a + n\mathbb{Z}) = a \bmod n,$$

which we can verify is well defined by noting that if  $a + n\mathbb{Z} = b + n\mathbb{Z}$ , then  $a - b$  is a multiple of  $n$ , so  $a \bmod n = b \bmod n$ . Also,  $f$  is an injective and surjective function from  $\mathbb{Z}/(n\mathbb{Z})$  to  $Z_n$ . Furthermore,  $f(a + b) = f(a) + f(b)$ , and  $f(a \cdot b) = f(a) \cdot f(b)$ . So we have that  $\mathbb{Z}/(n\mathbb{Z}) \approx Z_n$ .  $\blacksquare$

### Computational Example 10.8

Two very similar looking rings of order 10 can be defined in *SageMath* as follows:

```
InitRing()
AddRingVar("a")
Define(10*a, 0)
Define(a^2, 2*a)
CheckRing()
    This is a ring.
A = Ring(); A
    {0, a, 2 a, 3 a, 4 a, 5 a, 6 a, 7 a, 8 a, 9 a}
```

A second ring can be defined at the same time if we don't start over with **InitRing()**.

```
AddRingVar("b")
Define(10*b, 0)
Define(b^2, 6*b)
    This is a ring.
B = Ring(b); B
    {0, b, 2 b, 3 b, 4 b, 5 b, 6 b, 7 b, 8 b, 9 b}
```

This actually defines  $B$  to be a subring of a ring with 100 elements, so we have to redefine  $A$  to be a subring as well.

```
A = Ring(a); A
    {0, a, 2 a, 3 a, 4 a, 5 a, 6 a, 7 a, 8 a, 9 a}
```

Show that these rings are isomorphic.

**SOLUTION:** The addition and multiplication tables of  $A$  are shown in [Table 10.4](#). Note that the multiplicative structure is different than  $Z_{10}$ , since there is no multiplicative identity. The addition table for  $B$  is similar, but the multiplication table is shown in [Table 10.5](#).

In spite of the similarities between the two tables, they are not the same "color pattern." If they are isomorphic, it is not immediately clear what the isomorphism should be.

Since  $a$  is an additive generator of  $A$ , we know that it should map to one of the additive generators of  $B$ ,  $\{b, 3b, 7b, 9b\}$ . In *SageMath*, the command **RingHomo** defines a ring homomorphism, similar to the way that **Homomorph** defined a group homomorphism. So let us see if we can create an isomorphism.

**TABLE 10.4:** Addition and multiplication in the ring  $A$ 

| $+$  | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ |
|------|------|------|------|------|------|------|------|------|------|------|
| 0    | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ |
| $a$  | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    |
| $2a$ | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  |
| $3a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ |
| $4a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ |
| $5a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ | $4a$ |
| $6a$ | $6a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ |
| $7a$ | $7a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ |
| $8a$ | $8a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ |
| $9a$ | $9a$ | 0    | $a$  | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ |

| $\cdot$ | 0 | $a$ | $2a$ | $3a$ | $4a$ | $5a$ | $6a$ | $7a$ | $8a$ | $9a$ |
|---------|---|-----|------|------|------|------|------|------|------|------|
| 0       | 0 | 0   | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    |
| $a$     | 0 | 2a  | 4a   | 6a   | 8a   | 0    | 2a   | 4a   | 6a   | 8a   |
| $2a$    | 0 | 4a  | 8a   | 2a   | 6a   | 0    | 4a   | 8a   | 2a   | 6a   |
| $3a$    | 0 | 6a  | 2a   | 8a   | 4a   | 0    | 6a   | 2a   | 8a   | 4a   |
| $4a$    | 0 | 8a  | 6a   | 4a   | 2a   | 0    | 8a   | 6a   | 4a   | 2a   |
| $5a$    | 0 | 0   | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    |
| $6a$    | 0 | 2a  | 4a   | 6a   | 8a   | 0    | 2a   | 4a   | 6a   | 8a   |
| $7a$    | 0 | 4a  | 8a   | 2a   | 6a   | 0    | 4a   | 8a   | 2a   | 6a   |
| $8a$    | 0 | 6a  | 2a   | 8a   | 4a   | 0    | 6a   | 2a   | 8a   | 4a   |
| $9a$    | 0 | 8a  | 6a   | 4a   | 2a   | 0    | 8a   | 6a   | 4a   | 2a   |

**TABLE 10.5:** The ring  $B$ 

| $\cdot$ | 0 | $b$  | $2b$ | $3b$ | $4b$ | $5b$ | $6b$ | $7b$ | $8b$ | $9b$ |
|---------|---|------|------|------|------|------|------|------|------|------|
| 0       | 0 | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    |
| $b$     | 0 | $6b$ | $2b$ | $8b$ | $4b$ | 0    | $6b$ | $2b$ | $8b$ | $4b$ |
| $2b$    | 0 | $2b$ | $4b$ | $6b$ | $8b$ | 0    | $2b$ | $4b$ | $6b$ | $8b$ |
| $3b$    | 0 | $8b$ | $6b$ | $4b$ | $2b$ | 0    | $8b$ | $6b$ | $4b$ | $2b$ |
| $4b$    | 0 | $4b$ | $8b$ | $2b$ | $6b$ | 0    | $4b$ | $8b$ | $2b$ | $6b$ |
| $5b$    | 0 | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    | 0    |
| $6b$    | 0 | $6b$ | $2b$ | $8b$ | $4b$ | 0    | $6b$ | $2b$ | $8b$ | $4b$ |
| $7b$    | 0 | $2b$ | $4b$ | $6b$ | $8b$ | 0    | $2b$ | $4b$ | $6b$ | $8b$ |
| $8b$    | 0 | $8b$ | $6b$ | $4b$ | $2b$ | 0    | $8b$ | $6b$ | $4b$ | $2b$ |
| $9b$    | 0 | $4b$ | $8b$ | $2b$ | $6b$ | 0    | $4b$ | $8b$ | $2b$ | $6b$ |

```

F = RingHomo (A, B)
HomoDef (F, a, b)
FinishHomo (F)
    b + b is not 6 b
    'Homomorphism failed'
F = RingHomo (A, B)
HomoDef (F, a, 3*b)
FinishHomo (F)
    3 b + 3 b is not 4 b
    'Homomorphism failed'
F = RingHomo (A, B)
HomoDef (F, a, 7*b)
FinishHomo (F)
    'Homomorphism defined'
  
```

**TABLE 10.6:** Multiplication in  $2Z_{20}$ 

| .  | 0 | 2  | 4  | 6  | 8  | 10 | 12 | 14 | 16 | 18 |
|----|---|----|----|----|----|----|----|----|----|----|
| 0  | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 2  | 0 | 4  | 8  | 12 | 16 | 0  | 4  | 8  | 12 | 16 |
| 4  | 0 | 8  | 16 | 4  | 12 | 0  | 8  | 16 | 4  | 12 |
| 6  | 0 | 12 | 4  | 16 | 8  | 0  | 12 | 4  | 16 | 8  |
| 8  | 0 | 16 | 12 | 8  | 4  | 0  | 16 | 12 | 8  | 4  |
| 10 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 12 | 0 | 4  | 8  | 12 | 16 | 0  | 4  | 8  | 12 | 16 |
| 14 | 0 | 8  | 16 | 4  | 12 | 0  | 8  | 16 | 4  | 12 |
| 16 | 0 | 12 | 4  | 16 | 8  | 0  | 12 | 4  | 16 | 8  |
| 18 | 0 | 16 | 12 | 8  | 4  | 0  | 16 | 12 | 8  | 4  |

**Kernel(F)**

$$\{0\}$$

Because the last mapping has a kernel of the additive identity, we know from group homomorphisms that this mapping must be one-to-one. So we have found an isomorphism from  $A$  to  $B$ , but it was far from obvious.  $\blacksquare$

We would like a way to generalize this example so we can determine if two similar rings are isomorphic.

One way to help find an isomorphism between  $A$  and  $B$  is to show that both of these are isomorphic to a subring of the  $Z_n$  for some  $n$ . For example, consider  $2Z_{20}$ , the even elements of  $Z_{20}$ .

```

Z20 = ZRing(20); Z20
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,
 18, 19}
R = Ring(Z20[2]); R
{0, 2, 4, 6, 8, 10, 12, 14, 16, 18}
MultTable(R)

```

which produces [Table 10.6](#). One can see that the color patterns for  $A$  and  $R$  are the same, so that  $A \approx 2Z_{20}$ .

We can now generalize this example as follows.

### PROPOSITION 10.7

Let  $R$  be a finite ring whose additive structure is a cyclic group of order  $n$ . Let  $x$  be a generator of the additive group. Then  $x^2 = kx$  for some positive integer  $k \leq n$ , and

$$A \approx kZ_{kn}.$$

PROOF: If  $x^2 = 0$ , we can let  $k = n$ , so that  $k$  will be positive and  $kx = 0 = x^2$ . If  $x^2$  is not zero, then since  $x$  generates the additive group, there is a  $k$  such that  $x^2 = kx$  with  $0 < k < n$ .

Now the natural mapping is one that sends  $f(a \cdot x) = k \cdot a \pmod{kn}$ . This is obviously one-to-one and onto, since the value of  $a$  ranges from 0 to  $n - 1$ . To check that this is an isomorphism, note that

$$\begin{aligned} f(a \cdot x + b \cdot x) &= f((a + b) \cdot x) = k \cdot (a + b) \pmod{kn} \\ &= (k \cdot a \pmod{kn} + k \cdot b \pmod{kn}) \pmod{kn} \\ &= f(a \cdot x) + f(b \cdot x). \end{aligned}$$

Also,

$$\begin{aligned} f((a \cdot x) \cdot (b \cdot x)) &= f(a \cdot b \cdot x^2) \\ &= f(a \cdot b \cdot k \cdot x) \\ &= k \cdot a \cdot b \cdot k \pmod{kn} \\ &= ((k \cdot a \pmod{kn}) \cdot (k \cdot b \pmod{kn})) \pmod{kn} \\ &= f(a \cdot x) \cdot f(b \cdot x). \end{aligned}$$

Therefore,  $f$  is an isomorphism, and  $R \approx k\mathbb{Z}_{kn}$ . □

This proposition shows not only that  $A \approx 2\mathbb{Z}_{20}$  but also that  $B \approx 6\mathbb{A}_{60}$ , since  $b^2 = 6b$  in this ring.

**DEFINITION 10.6** A *cyclic ring* is a ring whose additive group is cyclic.

Note that this definition of cyclic rings also includes the infinite rings  $\mathbb{Z}$  and its subrings  $k\mathbb{Z}$ .

In order to prove that in fact  $A \approx B$ , we will need a few lemmas about number theory. Once these are proven, we will be able to determine *all* non-isomorphic rings of order 10.

### LEMMA 10.1

Let  $d$  be a positive divisor of  $n$ , and let  $f$  be the largest divisor of  $d$  that is coprime to  $(n/d)$ . Then if  $q$  is coprime to both  $f$  and  $(n/d)$ , then  $q$  is coprime to  $n$ .

PROOF: Suppose that  $\gcd(q, n)$  is not 1. Then there is a prime number  $p$  that divides neither  $f$  nor  $(n/d)$ , yet divides  $n$ . Thus,  $p$  must divide  $d$ .

Now  $f \cdot p$  will be coprime to  $(n/d)$  since both  $f$  and  $p$  are. Also, since  $f$  is not a multiple of  $p$  while  $d$  is,  $f \cdot p$  will be a divisor of  $d$ . But we defined  $f$  to be the *largest* factor of  $d$  coprime to  $(n/d)$ . This contradiction shows that  $\gcd(q, n) = 1$ . □

**LEMMA 10.2**

Given two positive numbers  $x$  and  $y$ , there exist  $u$  and  $v$  in  $\mathbb{Z}$  such that

$$ux + vy = \gcd(x, y),$$

where  $u$  is coprime to  $y$ .

PROOF: Bézout's lemma (1.3) would give us values for  $u$  and  $v$ , but there would be no way to guarantee that  $u$  would be coprime to  $y$ .

Let  $k = \gcd(x, y)$ . Then  $(x/k)$  and  $(y/k)$  are coprime, so  $(x/k)$  has an multiplicative inverse in  $Z_{(y/k)}$ , say  $n$ . That is,

$$\frac{x}{k} \cdot n \equiv 1 \left( \text{mod } \frac{y}{k} \right).$$

Let  $f$  be the largest divisor of  $k$  that is coprime to  $(y/k)$ . By the Chinese remainder theorem (1.5), there is a number  $u$  such that

$$u \equiv n \left( \text{mod } \frac{y}{k} \right)$$

and

$$u \equiv 1 \left( \text{mod } f \right).$$

Since  $n$  is coprime to  $(y/k)$ ,  $u$  is coprime to  $(y/k)$ . Also,  $u$  is coprime to  $f$ , so by Lemma 10.1  $u$  is coprime to  $y$ . Also,

$$u \cdot \frac{x}{k} \equiv 1 \left( \text{mod } \frac{y}{k} \right)$$

so there is a  $v$  such that  $u \cdot \frac{x}{k} + v \cdot \frac{y}{k} = 1$ . Multiplying both sides by  $k$  gives us

$$u \cdot x + v \cdot y = k = \gcd(x, y).$$

□

**THEOREM 10.1: The Cyclic Ring Theorem**

If  $x$  and  $n$  are positive integers, then

$$xZ_{x \cdot n} \approx kZ_{k \cdot n},$$

where  $k = \gcd(x, n)$ .

PROOF: Since  $k = \gcd(x, n)$  by Lemma 10.2 we can find integers  $u$  and  $v$  such that  $u \cdot x + v \cdot n = k$ , where  $u$  is coprime to  $n$ . We now define a mapping  $f$  from  $kZ_{kn}$  to  $xZ_{xn}$  as follows:

$$f(k \cdot w \text{ mod } (kn)) = uxw \text{ mod } (xn).$$

Note that this is well-defined, since if  $k \cdot w$  is equivalent to  $k \cdot p$  (mod  $kn$ ), then

$$\begin{aligned} w \equiv p \pmod{n} &\implies xw \equiv xp \pmod{xn} \\ &\implies uxw \equiv uxp \pmod{xn}. \end{aligned}$$

Next we need to show that  $f$  is a homomorphism from  $kZ_{kn}$  to  $xZ_{xn}$ . If  $a \equiv k \cdot w \pmod{kn}$  and  $b \equiv k \cdot z \pmod{kn}$ , then

$$\begin{aligned} f(a+b) &= f((k \cdot w + k \cdot z) \pmod{kn}) = u \cdot (x \cdot w + x \cdot z) \pmod{xn} \\ &= (u \cdot x \cdot w + u \cdot x \cdot z) \pmod{xn} = f(a) + f(b). \end{aligned}$$

$$\begin{aligned} f(a \cdot b) &= f((k \cdot w \cdot k \cdot z) \pmod{kn}) = (u \cdot x \cdot w \cdot k \cdot z) \pmod{xn} \\ &= (u \cdot x \cdot w \cdot (u \cdot x + v \cdot n) \cdot z) \pmod{xn} \\ &= (u \cdot x \cdot w \cdot u \cdot x \cdot z + u \cdot x \cdot w \cdot v \cdot n \cdot z) \pmod{xn} \\ &= ((u \cdot x \cdot w) \cdot (u \cdot x \cdot z)) \pmod{xn} = f(a) \cdot f(b). \end{aligned}$$

So  $f$  is indeed a homomorphism from  $kZ_{kn}$  to  $xZ_{xn}$ .

Since  $u$  is coprime to  $n$ ,  $u$  has an inverse,  $u^{-1} \pmod{n}$ . Then we see that  $f$  is onto, since any element  $x \cdot a \pmod{xn}$  in  $xZ_{xn}$  can be obtained by taking

$$f(k \cdot a \cdot u^{-1} \pmod{kn}) = (u \cdot x \cdot a \cdot u^{-1}) \pmod{xn} = x \cdot a \pmod{xn}.$$

Finally, both  $xZ_{xn}$  and  $kZ_{kn}$  contain  $n$  elements, so by the pigeonhole principle  $f$  must be a one-to-one function. Thus,  $f$  is an isomorphism, and  $xZ_{xn} \approx kZ_{kn}$ .  $\square$

Because  $2 = \gcd(6, 10)$ , we see that  $A \approx 2Z_{20}$  is isomorphic to  $B \approx 6Z_{60}$ .

In fact, since the only rings of order 10 are cyclic rings, there are four possible non-isomorphic rings of order 10:

$$Z_{10}, \quad 2Z_{20}, \quad 5Z_{50}, \quad \text{and} \quad 10Z_{100}.$$

It is easy to see that these rings are all distinct by looking at the multiplication tables.

### COROLLARY 10.1

*The number of non-isomorphic cyclic rings of order  $n$  is precisely the number of divisors of  $n$  (including 1 and  $n$ ).*

**PROOF:** By Proposition 10.7 every cyclic ring of order  $n$  is isomorphic to  $kZ_{kn}$  for some value of  $k$ . By the cyclic ring theorem, we see that this is isomorphic to  $dZ_{dn}$ , where  $d = \gcd(k, n)$ . Hence  $d$  is a divisor of  $n$ . We need to show that two different rings of this form are non-isomorphic. Consider the rings  $A = dZ_{dn}$  and  $B = fZ_{fn}$ , where  $d$  and  $f$  are different divisors of  $n$ . Perhaps the easiest way to show that these are different is to count the number of elements in  $A$  and  $B$  that can appear in the multiplication tables. The elements that can appear in the table for  $A$  are

$$d^2, 2d^2, 3d^2, \dots, nd = 0$$

while the elements appearing in the multiplication table of  $B$  are

$$f^2, 2f^2, 3f^2, \dots, nf = 0.$$

Thus, there are  $n/d$  such elements of  $A$ , and  $n/f$  elements of  $B$ . Since  $d$  and  $f$  are different, we see that the rings  $A$  and  $B$  are not isomorphic. Therefore, there is a one-to-one correspondence between the factors of  $n$  and the cyclic rings of order  $n$ .  $\square$

Although this corollary seems to be a big help in finding *all* finite rings, there are, in fact, many non-cyclic rings. For example, there are 8 non-cyclic rings of order 4, which when combined with the 3 cyclic rings from Corollary 10.1 gives a total of 11 rings of order 4. There are 52 rings of order 8 (4 cyclic, 20 with additive group  $Z_{15}^*$ , and 28 with an additive group  $Z_{24}^*$ ).

**Table 10.7** shows the number of rings of a given order. There are at least 18,590 rings of order 32, but it has not been proven that these are all of them.

**TABLE 10.7:** Rings of order  $n$

| $n$ | rings | $n$ | rings | $n$ | rings | $n$ | rings |
|-----|-------|-----|-------|-----|-------|-----|-------|
| 1   | 1     | 9   | 11    | 17  | 2     | 25  | 11    |
| 2   | 2     | 10  | 4     | 18  | 22    | 26  | 4     |
| 3   | 2     | 11  | 2     | 19  | 2     | 27  | 59    |
| 4   | 11    | 12  | 22    | 20  | 22    | 28  | 22    |
| 5   | 2     | 13  | 2     | 21  | 4     | 29  | 2     |
| 6   | 4     | 14  | 4     | 22  | 4     | 30  | 8     |
| 7   | 2     | 15  | 4     | 23  | 2     | 31  | 2     |
| 8   | 52    | 16  | 390   | 24  | 104   | 32  | ???   |

In *SageMath*, we can load any of the rings of order 15 or less. The command **NumberSmallRings** will produce the number of rings of a given order, up to order 15.

**NumberSmallRings (8)**

52

Now we can load any of these 52 rings.

```
R = SmallRing(8, 51); R
{0, a, b, a+b, c, a+c, b+c, a+b+c}
MultTable(R)
```

The multiplication table for this ring is shown in [Table 10.8](#).

**TABLE 10.8:** Ring number 51 of order 8

| .       | 0 | $a$     | $b$   | $a+b$   | $c$   | $a+c$ | $b+c$ | $a+b+c$ |
|---------|---|---------|-------|---------|-------|-------|-------|---------|
| 0       | 0 | 0       | 0     | 0       | 0     | 0     | 0     | 0       |
| $a$     | 0 | $a$     | $b$   | $a+b$   | $c$   | $a+c$ | $b+c$ | $a+b+c$ |
| $b$     | 0 | $b$     | $b+c$ | $c$     | $b$   | 0     | $c$   | $b+c$   |
| $a+b$   | 0 | $a+b$   | $c$   | $a+b+c$ | $b+c$ | $a+c$ | $b$   | $a$     |
| $c$     | 0 | $c$     | $b$   | $b+c$   | $c$   | 0     | $b+c$ | $b$     |
| $a+c$   | 0 | $a+c$   | 0     | $a+c$   | 0     | $a+c$ | 0     | $a+c$   |
| $b+c$   | 0 | $b+c$   | $c$   | $b$     | $b+c$ | 0     | $b$   | $c$     |
| $a+b+c$ | 0 | $a+b+c$ | $b+c$ | $a$     | $b$   | $a+c$ | $c$   | $a+b$   |

### Problems for §10.3

- 1 Suppose  $\phi$  is an isomorphism between  $R$  and  $S$ . Show that if  $S$  is commutative, then so is  $R$ .
- 2 Suppose  $\phi$  is a surjective isomorphism between  $R$  and  $S$ . Show that if  $S$  has a unity element, then so does  $R$ .
- 3 Suppose  $\phi$  is an isomorphism between  $R$  and  $S$ . Show that if  $R$  has a zero divisor, then so does  $S$ .
- 4 Suppose  $\phi$  is an isomorphism between  $R$  and  $S$ . Show that if  $R$  has a non-zero idempotent element, then so does  $S$ . See Problem 13 of §9.3.
- 5 Find a subring of the ring  $T_8$  in Table 9.7 that is isomorphic to the ring  $T_4$  in Table 9.6.
- 6 Let  $R$  be a non-commutative ring. Define the operation  $x*y = y \cdot x$ . Show that the set  $R$  forms a ring using the operations  $*$  and  $+$  instead of  $\cdot$  and  $+$ . This new ring is called the *opposite ring* of  $R$  and is denoted  $R^{\text{op}}$ .
- 7 Show that the ring  $T_4$  in Table 9.6 is not isomorphic to its opposite. (See Problem 6.)
- 8 Show that the quotient ring  $R/S_2$  in Table 10.3 is isomorphic to  $T_4^{\text{op}}$ . (See Problem 6.)
- 9 Show that the ring  $T_8$  in Table 9.7 is isomorphic to its opposite. (See Problem 6.)  
Hint: First construct the multiplication table for  $T_8^{\text{op}}$ , then determine how to rearrange the elements of  $T_8$  so that the patterns match.
- 10 Prove that a non-commutative ring of order 4 or less must be isomorphic to either  $T_4$  from Table 9.6 or  $T_4^{\text{op}}$ . (See Problem 6.)  
Hint: Use Problem 12 from §9.2.

- 11** Is the ring  $2\mathbb{Z}$  isomorphic to the ring  $3\mathbb{Z}$ ? Why or why not?
- 12** Let  $A = \langle 2 \rangle$  and  $B = \langle 8 \rangle$  be two ideals of the ring  $\mathbb{Z}$ . Show that the group  $A/B$  is isomorphic to  $Z_4$ , but the ring  $A/B$  is not isomorphic to the ring  $Z_4$ .
- 13** Is the ring  $\mathbb{R}$  isomorphic to the ring of complex numbers  $\mathbb{C}$ ?

For Problems **14** through **17**, find all non-isomorphic rings of the following order.

**14** 6

**15** 21

**16** 30

**17** 210

- 18** Let  $R$  be a ring with unity  $e$ , and let  $S$  be the subring  $[e]$  generated from the unity element. Show that  $S$  is isomorphic to either  $\mathbb{Z}$  or  $Z_n$  for some  $n$ .

### Interactive Problems

- 19** Load the rings  $Z_{12}$  and  $Z_6$  into *SageMath* simultaneously with the commands:

```
Z12 = ZRing(12)
Z6 = ZRing(6)
```

Show that  $I = \{0, 6\}$  is an ideal of  $Z_{12}$ , and display addition and multiplication tables of the quotient ring  $Z_{12}/I$ , showing that  $Z_{12}/I$  is isomorphic to  $Z_6$ .

- 20** Use *SageMath* to find the eight non-isomorphic non-cyclic rings of order 4.

Hint: The additive group must be isomorphic to  $Z_8^*$ , so the ring is defined by:

```
InitRing(); AddRingVar(" a", " b")
Define(2*a, 0); Define(2*b, 0)
Define(a^2, ???); Define(b^2, ???)
Define(a*b, ???); Define(b*a, ???)
CheckRing()
```

Fill in each ??? with a member of  $\{0, a, b, a + b\}$  to see whether a ring is formed. Is there a faster way than trying all  $4^4 = 256$  combinations?

- 21** Use *SageMath* to display the multiplication tables of all rings of order 6.

## 10.4 Homomorphisms and Kernels

Since we defined a ring isomorphism in a similar fashion as group isomorphisms, we naturally will define ring homomorphisms by mimicking group homomorphisms.

**DEFINITION 10.7** If  $A$  and  $B$  are two rings, then a mapping  $f : A \rightarrow B$  such that

$$f(x + y) = f(x) + f(y),$$

and

$$f(x \cdot y) = f(x) \cdot f(y),$$

for all  $x$  and  $y$  in  $A$  is called a *ring homomorphism*.

Notice that a ring homomorphism preserves both of the ring operations. In particular, a ring homomorphism will also be a group homomorphism from the additive group of  $A$  to the additive group of  $B$ . Thus, we can immediately apply the results of group homomorphisms to see two properties of ring homomorphisms.

If  $f$  is a ring homomorphism from  $A$  to  $B$ , then

$$f(0) = 0$$

and

$$f(-x) = -f(x) \quad \text{for all } x \in A.$$

Any isomorphism is certainly a homomorphism. But let us see how to define a homomorphism between two non-isomorphic rings.

### Example 10.9

Let  $n$  be a positive integer. Find a homomorphism between  $\mathbb{Z}$  and  $Z_n$ .

SOLUTION: The natural mapping is

$$f(x) = x \bmod n.$$

Proposition 1.2 can be restated as  $f(x + y) = f(x) + f(y)$ , and  $f(x \cdot y) = f(x) \cdot f(y)$ . Thus, this is a homomorphism. □

### Computational Example 10.10

Use *SageMath* to find a homomorphism from  $Z_3$  to  $Z_6$ .

SOLUTION: First we define  $Z_3$  and  $Z_6$  simultaneously.

```
Z3 = ZRing(3); Z3
{0, 1, 2}
Z6 = ZRing(6); Z6
{0, 1, 2, 3, 4, 5}
```

The homomorphism is determined completely by the value of  $f(1)$ . A natural choice would be to let  $f(1) = 2 \bmod 6$ . To define a ring homomorphism, we use the command **RingHomo** instead of **Homomorph**.

```
F = RingHomo(Z3, Z6)
HomoDef(F, 1, 2)
```

Even though 1 and 2 are technically elements of  $\mathbb{Z}$ , not  $Z_3$  or  $Z_6$ , *SageMath* makes the natural translations, knowing the arguments are expected to be in the rings  $Z_3$  and  $Z_6$ . We can now use the command **FinishHomo** to check if  $F$  is a ring homomorphism.

```
FinishHomo(F)
2 * 2 is not 2
'Homomorphism failed'
```

*SageMath* shows that this would not produce a homomorphism. One way to correct this problem would be to send  $f(a)$  to the zero element of  $Z_6$ .

```
F = RingHomo(Z3, Z6)
HomoDef(F, 1, 0)
FinishHomo(F)
'Homomorphism defined'
```

Although this works, this is a rather trivial example, since it sends *all* elements to 0. After some experimenting, we can find a more interesting example.

```
F = RingHomo(Z3, Z6)
HomoDef(F, 1, 4)
FinishHomo(F)
'Homomorphism defined'
```

Thus,  $f(1) = 4$ , so  $f(2) = 2$ , and of course  $f(0) = 0$ . □

There will always be at least one homomorphism between two rings, that sends all elements to zero.

**DEFINITION 10.8** If  $A$  and  $B$  are any two rings, then the mapping  $f : A \rightarrow B$

$$f(x) = 0 \quad \text{for all } x \in A$$

is called the *zero homomorphism from  $A$  to  $B$* .

As with groups, we define  $f(S)$ , where  $S$  is a set of elements in the domain of  $f$ , to be the set of all values  $f(x)$ , where  $x$  is in  $S$ . We can also define the inverse image of an element  $y$  to be  $f^{-1}(y)$ , the set of elements such that  $f(x) = y$ . In fact, we can define the inverse image of a set of elements in the same way:  $f^{-1}(T)$  is the set of elements such that  $f(x)$  is in  $T$ . We can find images and inverse images of ring homomorphisms the same way we did for group homomorphisms. Here is a new homomorphism going from  $Z_6$  to  $Z_3$ .

```

G = RingHomo (Z6, Z3)
HomoDef (G, 1, 1)
FinishHomo (G)
    'Homomorphism defined'
G(4)
    1
Image (G, Z6)
    {0, 1, 2}
HomoInv (G, 2)
    {2, 5}
HomoInv (G, [0, 1])
    {0, 1, 3, 4}

```

We can ask whether the image or inverse image of a subring will again be a subring. This is actually very easy to prove, as seen in the next proposition.

### PROPOSITION 10.8

Suppose  $f$  is a homomorphism from the ring  $A$  to the ring  $B$ . Then if  $S$  is a subring of  $A$ , then  $f(S)$  is a subring of  $B$ . Likewise, if  $T$  is a subring of  $B$ , then  $f^{-1}(T)$  will be a subring of  $A$ .

**PROOF:** Suppose  $S$  is a subring of  $A$ . We will use Proposition 10.1 to show that  $f(S)$  is a subring of  $B$ . The element  $f(0) = 0$  is in  $f(S)$ , so  $f(S)$  is non-empty. If  $u$  and  $v$  are two elements of  $f(S)$ , then there exist elements  $x$  and  $y$  in  $S$  such that

$$f(x) = u$$

and

$$f(y) = v.$$

But  $x \cdot y$  and  $x - y$  are also in  $S$ , and so

$$f(x \cdot y) = f(x) \cdot f(y) = u \cdot v$$

and

$$f(x - y) = f(x) - f(y) = u - v$$

must be in  $f(S)$ . Thus, by Proposition 10.1,  $f(S)$  is a subring of  $B$ .

Now suppose that  $T$  is a subring of  $B$ . Since  $0$  is contained in  $f^{-1}(T)$ , we have that  $f^{-1}(T)$  is non-empty. If  $x$  and  $y$  are two elements of  $f^{-1}(T)$ , then  $f(x)$  and  $f(y)$  will be two elements of  $T$ . Thus,

$$f(x \cdot y) = f(x) \cdot f(y)$$

and

$$f(x - y) = f(x) - f(y)$$

would be elements of  $T$ . Hence,  $x \cdot y$  and  $x - y$  are in  $f^{-1}(T)$ . Thus, by Proposition 10.1,  $f^{-1}(T)$  is a subring of  $A$ .  $\square$

We can define the kernel and the image of a homomorphism in the same way that we did for group homomorphisms.

**DEFINITION 10.9** Given a homomorphism  $f$  from the ring  $A$  to the ring  $B$ , the *kernel* of  $f$  is  $f^{-1}(0)$ , denoted  $\text{Ker}(f)$ . The *image* of  $f$  is  $f(A)$ , denoted  $\text{Im}(f)$ .

In *SageMath*, we can use the **HomoInv** command to find the kernel of a homomorphism, or we can use the command

**Kernel(G)**  
 $\{0, 3\}$

as we did for group homomorphisms.

When we have a homomorphism from  $A$  to  $B$ , we have by Proposition 10.8 that the image will be a subring of  $B$ . Likewise, the kernel of a homomorphism will be a subring of  $A$ . However, we can say even more about the kernel.

### PROPOSITION 10.9

If  $f$  is a homomorphism from the ring  $A$  to the ring  $B$ , then the kernel of  $f$  is an ideal of  $A$ . Furthermore,  $f$  is injective if, and only if,  $\text{Ker}(f) = \{0\}$ .

PROOF: Suppose that  $x$  is in the kernel of  $f$ , and  $y$  is any other element of  $A$ . Then

$$f(x \cdot y) = f(x) \cdot f(y) = 0 \cdot f(y) = 0,$$

and

$$f(y \cdot x) = f(y) \cdot f(x) = f(y) \cdot 0 = 0.$$

Hence,  $x \cdot y$  and  $y \cdot x$  are in the kernel of  $f$ , so the kernel is an ideal of  $A$ .

If  $f$  is injective, then  $f^{-1}(0)$  can only contain one element, which must be  $0$ . On the other hand, if  $f^{-1}(0) = \{0\}$ , then

$$\begin{aligned} f(x) = f(y) &\implies f(x) - f(y) = 0 \\ &\implies f(x - y) = 0 \end{aligned}$$

$$\begin{aligned} &\implies x - y = 0 \\ &\implies x = y. \end{aligned}$$

Therefore,  $f$  is injective if, and only if,  $\text{Ker}(f) = \{0\}$ . □

### Motivational Example 10.11

Find a non-zero homomorphism from the non-commutative ring  $R$  of order 8 used throughout §10.2, to some other ring.

SOLUTION: The kernel would have to be an ideal of  $R$ . But  $R$  has only three nontrivial ideals:

```
InitRing(); AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, 0)
Define(a*b, b); Define(b*a, 2*a)
R = Ring(); R
    {0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
I1 = Ideal(R, 2*a); I1
    {0, 2 a}
I2 = Ideal(R, 2*a + b); I2
    {0, 2 a + b}
I3 = Ideal(R, b); I3
    {0, b, 2 a, 2 a + b}
```

To produce an interesting homomorphism, we would use one of these ideals as the kernel. To which ring should we map  $R$ ?

The natural answer would be the quotient ring. Since there is a natural group homomorphism from  $R$  to  $R/I$ , we can ask whether this group homomorphism extends to become a ring homomorphism.

Let us define  $Q = R/I_1$ .

```
Q = Coset(R, I1); Q
    {{0, 2 a}, {a, 3 a}, {b, 2 a + b}, {a + b, 3 a + b}}
```

We wish to define a homomorphism  $i(x)$  which maps an element in  $R$  to the coset of  $Q$  containing that element. We only need to define  $i(a)$  and  $i(b)$  to complete the definition.

```
i = RingHomo(R, Q)
HomoDef(i, a, a + I1)
HomoDef(i, b, b + I1)
FinishHomo(i)
'Homomorphism defined'
```

The kernel of this homomorphism,

**Kernel(i)**  
 $\{0, 2 \text{ a}\}$

which is of course  $I_1$ . □

In general, we can form a homomorphism from a ring  $R$  to a quotient ring  $R/I$  using the same technique. We will state this as a lemma:

**LEMMA 10.3**

If  $I$  is an ideal of the ring  $R$ , then the natural mapping  $i : R \rightarrow R/I$  defined by  $i(x) = x + I$  is a surjective ring homomorphism from  $R$  to  $R/I$  with the kernel being  $I$ .

**PROOF:** It is clear that the rule  $i(x) = x + I$  defines a surjective mapping  $i$  from  $R$  to  $R/I$ , and that  $\text{Ker}(i) = I$ . We need only to check that  $i(x)$  is a homomorphism.

Since

$$\begin{aligned} i(x+y) &= (x+y) + I \\ &= (x+I) + (y+I) \\ &= i(x) + i(y) \end{aligned}$$

and

$$\begin{aligned} i(x \cdot y) &= x \cdot y + I \\ &= (x+I) \cdot (y+I) \\ &= i(x) \cdot i(y), \end{aligned}$$

we see that  $i(x)$  is indeed a surjective homomorphism. □

In the homomorphisms produced by Lemma 10.3, the image of the homomorphism is isomorphic to  $R/\text{Ker}(f)$ . The first isomorphism theorem studied in the volume on groups shows that the additive group on  $\text{Im}(f)$  would be group isomorphic to the additive structure of  $R/\text{Ker}(f)$ . It is easy to show that the ring  $\text{Im}(f)$  is isomorphic to the ring  $R/\text{Ker}(f)$  as well, giving us an isomorphism theorem for rings.

**THEOREM 10.2: The First Ring Isomorphism Theorem**

Let  $f$  be a ring homomorphism from a ring  $R$  to a ring  $S$ , whose image is  $H$ . If the kernel of  $f$  is  $I$ , then there is a natural surjective isomorphism  $\phi : R/I \rightarrow H$  which causes the diagram in Figure 10.1 to commute. (Here,  $i(x)$  is the homomorphism defined in Lemma 10.3.) Thus,  $H \approx R/I$ .

$$\begin{array}{ccc}
 R & \xrightarrow{i} & R/I \\
 f \searrow & & \swarrow \phi \\
 & H &
 \end{array}$$

**FIGURE 10.1:** Commuting diagram for Theorem 10.2

**PROOF:** Figure 10.1 actually helps us determine how  $\phi$  must be defined. For each coset  $(x + I)$  in  $R/I$ , we need to have

$$\phi(x + I) = f(x)$$

in order for the diagram to commute. To prove that this rule defines a mapping, we need to show that this is well defined. That is, if  $x + I = y + I$  it needs to be true that  $f(x) = f(y)$ , or else there would be a contradiction in the definition of  $\phi$ . But

$$\begin{aligned}
 x + I = y + I &\iff x - y \in I \\
 &\iff f(x - y) = 0 \\
 &\iff f(x) = f(y) \\
 &\iff \phi(x + I) = \phi(y + I).
 \end{aligned}$$

So we see that the definition of  $\phi$  will not produce any such contradictions.

To show that  $\phi$  is a homomorphism, we have that

$$\begin{aligned}
 \phi((x + I) + (y + I)) &= \phi(x + y + I) \\
 &= f(x + y) \\
 &= f(x) + f(y) \\
 &= \phi(x + I) + \phi(y + I),
 \end{aligned}$$

and

$$\begin{aligned}
 \phi((x + I) \cdot (y + I)) &= \phi(x \cdot y + I) \\
 &= f(x \cdot y) \\
 &= f(x) \cdot f(y) \\
 &= \phi(x + I) \cdot \phi(y + I).
 \end{aligned}$$

So  $\phi$  is a homomorphism from  $R/I$  to  $H$ . It is apparent that this homomorphism is onto, and

$$\phi(x + I) = 0 \iff f(x) = 0$$

$$\begin{aligned} &\iff x \in I \\ &\iff x + I = I. \end{aligned}$$

So the kernel of  $\phi$  is  $\{I\}$ , the zero element of  $R/I$ . Thus,  $\phi$  is an isomorphism from  $R/I$  onto  $H$ , so  $R/I \approx H$ . Since the mapping  $\phi$  was defined so that the diagram in [Figure 10.1](#) commutes, the theorem is proved.  $\square$

It should be noted that there are second and third ring isomorphism theorems. These are considered in Problems 18 and 19.

### Problems for §10.4

- 1** Find all ring homomorphisms from  $Z_6$  to  $Z_6$ .
- 2** Find all ring homomorphisms from  $Z_{10}$  to  $Z_{10}$ .
- 3** Show that if  $\phi(x) = 2x$ , then  $\phi$  is *not* a ring homomorphism from  $\mathbb{R}$  to  $\mathbb{R}$ .
- 4** Is the mapping  $\phi$  from  $Z_5$  to  $Z_{30}$  given by  $\phi(x) = 6x$  a ring homomorphism?
- 5** Is the mapping  $\phi$  from  $Z_5$  to  $Z_{20}$  given by  $\phi(x) = 4x$  a ring homomorphism?
- 6** Is the mapping  $\phi$  from  $Z_{30}$  to  $Z_5$  given by  $\phi(x) = x \bmod 5$  a ring homomorphism?
- 7** Is the mapping  $\phi$  from  $Z_{20}$  to  $Z_5$  given by  $\phi(x) = x \bmod 5$  a ring homomorphism?
- 8** Is the mapping  $\phi$  from  $Z_{20}$  to  $Z_{10}$  given by  $\phi(x) = 6x \bmod 10$  a ring homomorphism?
- 9** Is the mapping  $\phi$  from  $Z_2$  to  $Z_4$  given by  $\phi(x) = x$  a ring homomorphism?
- 10** Determine all ring homomorphisms from the rationals  $\mathbb{Q}$  to  $\mathbb{Q}$ .  
Hint: What are the possible kernels? If  $\phi(1) = 1$ , show that  $\phi(x) = x$ .
- 11** Let  $\mathbb{C}$  denote the set of numbers of the form  $a + bi$ , where  $i = \sqrt{-1}$  and  $a$  and  $b$  are real. ( $\mathbb{C}$  is in fact a subring of the quaternions  $\mathbb{H}$ .) Let  $\phi(a + bi) = a - bi$ . Show that  $\phi$  is a ring homomorphism from the ring  $\mathbb{C}$  to itself.  
Hint: Let  $x = a + bi$ , and  $y = c + di$ .
- 12** Show that if  $\phi$  is a homomorphism from a ring  $R$  to a ring  $S$ , then an idempotent element of  $R$  must be sent to an idempotent element of  $S$ . See Problem 13 of [§9.3](#).

## Historical Diversion

# Richard Dedekind (1831–1916)

---

Dedekind was born Julius Wilhelm Richard Dedekind in Braunschweig, Germany, but he never used his first two names as an adult. He attended Collegium Carolinum in 1848, and then moved to the University of Göttingen in 1850. He attended lectures under Carl Gauss, but he was teaching mainly elementary level mathematics at the time. Dedekind is considered to be Gauss' last student. Dedekind received his doctorate in 1852.

Since the University of Berlin was considered the leading center for mathematics, Dedekind went to Berlin for two years.

There he met a contemporary Bernhard Riemann, and together in 1854 they were awarded the habilitation, which is the highest academic award a scholar could achieve. Dedekind returned to Göttingen to teach as a Privatdozent, and was the first at Göttingen to lecture on Galois theory. Dedekind understood the importance of group theory for algebra and arithmetic.

In 1858, he began to teach at the Polytechnic in Zürich. While teaching calculus for the first time, he came up with the idea we now call the Dedekind cut. He associated every real number  $a$  with a set of rational numbers less than  $a$ . Limits can then be expressed in terms of set theory. With this idea Dedekind could show that there were no gaps, or discontinuities, on the number line. This put the real number system on a firm foundation.

Dedekind also worked with infinite sets, defining two sets as “similar” if there is a one-to-one and onto mapping between the two sets. This led to the first precise definition of an infinite set. In 1872, He met Georg Cantor while on holiday in Interlaken. Dedekind became a close ally of Cantor during his philosophical battles with Kronecker. (See Historical Diversion on page 39.)

In 1879, Dedekind generalized Kummer's *ideal numbers* to formulate a definition of an ideal. (See Historical Diversion on page 314.) His definition was a subset of a set of numbers, all of which were *algebraic integers*, that is, they satisfied a polynomial equation with integer coefficients, and a leading coefficient of 1. Dedekind's definition of an ideal would later be generalized by Emmy Noether. (See Historical Diversion on page 281.)

Dedekind is also known for the Dedekind domain, which is an integral domain for which every non-trivial ideal factors into a product of prime ideals. If such a factorization is possible, it is unique up to the orders of the factors. Kummer showed that  $\mathbb{Z}[\omega_n]$  has this property for all  $n$ , but Dedekind generalized this for all domains of algebraic integers.



- 13** Show that if  $\phi$  is a homomorphism from a ring  $R$  to a ring  $S$ , then a nilpotent element of  $R$  must be sent to a nilpotent element of  $S$ . See Problem 14 of §10.1.
- 14** Show that if  $\phi$  is a homomorphism from a ring  $R$  to a ring  $S$ , and  $R$  is a principle ideal ring, then  $\text{Im}(\phi)$  is also a principle ideal ring.
- 15** A non-trivial ideal  $I$  of a ring  $R$  is said to be a *prime ideal* of  $R$  if whenever  $x \cdot y$  is in  $I$ , with  $x, y \in R$ , then either  $x$  or  $y$  is in  $I$ . Show that the prime ideals of the ring  $\mathbb{Z}$  are the ideals  $\langle p \rangle$  with  $p$  prime. Prime ideals are important in Dedekind domains. (See the Historical Diversion on page 334.)
- 16** Let  $R$  be any commutative unity ring, and let  $I = \langle p \rangle$  be a principle ideal of  $R$ . Show that  $I$  is a prime ideal if, and only if,  $p$  is a prime element of  $R$ , as defined in Problem 21 of §9.3. See Problem 15.
- 17** Let  $R$  be any commutative unity ring, and  $I$  a non-trivial ideal of  $R$ . Show that  $I$  is a prime ideal of  $R$  if, and only if, the quotient ring  $R/I$  has no zero divisors. See Problem 15.
- 18** Prove the second ring isomorphism theorem: If  $K$  and  $I$  are two ideals of a ring  $R$ , then
- $$K/(K \cap I) \approx (K + I)/I.$$
- (See Problem 1 of §10.2 for the definition of  $K + I$ .)
- 19** Prove the third ring isomorphism theorem: If  $K$  and  $I$  are two ideals of a ring  $R$ , where  $K \subseteq I$ , then  $K$  is an ideal of  $I$ ,  $I/K$  is an ideal of  $R/K$ , and
- $$(R/K)/(I/K) \approx R/I.$$
- 20** Find all the non-trivial homomorphisms from  $T_8$  to  $T_4$ .  
Hint: Consider Problems 9 and 20 from §10.2.

#### Interactive Problems

- 21** The ring of Example 10.11 also has an ideal  $I_2 = \{0, 2a + b\}$ . Define a homomorphism from the ring  $R$  to  $R/I_2$ .
- 22** The ring of Example 10.11 also has an ideal  $I_3 = \{0, b, 2a, 2a+b\}$ . Define a homomorphism from the ring  $R$  to  $R/I_3$ .
- 23** Use *SageMath* to find a non-trivial homomorphism from the ring of Example 10.11 to itself, which is not an automorphism.

# Chapter 11

---

## Integral Domains and Fields

Although we have already defined integral domains and fields, this chapter focuses on particular cases of integral domains and fields. For example, one can construct a larger integral domain from a field or integral domain by considering polynomials over the original ring. Likewise, one can expand any integral domain into a field by forcing division to be possible. These provide us with useful examples for experimentation in hopes of finding properties of general integral domains and fields. We will also study what may be the most important field of all, the field of complex numbers.

---

### 11.1 Polynomial Rings

The study of polynomials is the oldest topic of algebra. The Babylonians were able to solve the quadratic equation around 1600 B.C., and the cubic equations were being solved in Arabia in 825 A.D., even before modern algebraic notation. (Polynomials were written out with words.) In 1535, Tartaglia demonstrated how to solve the general cubic equation, and shortly thereafter Ferrari found the solution to the general fourth-degree equation. This led to a great surge of interest in the *theory of equations*, as mathematicians raced to find a general formula for the quintic, or fifth-degree equation. Finally, Abel and Galois independently proved in the 1820's that it was in fact impossible to find such a formula for the quintic equation, utilizing group theory.

The reader is obviously familiar with polynomials for which the coefficients are real numbers. However, we can construct polynomials from any ring, and the set of all such polynomials will be a new ring, called a *polynomial ring*. But only the polynomial rings formed either from fields or integral domains will have the properties that we are used to.

**DEFINITION 11.1** Let  $K$  be a commutative ring. We define the set of polynomials in  $x$  over  $K$ , denoted  $K[x]$ , to be the set of all expressions of the form

$$k_0 + k_1x + k_2x^2 + k_3x^3 + \dots$$

where the coefficients  $k_n$  are elements of  $K$ , and only a *finite* number of the coefficients are nonzero. If  $k_d$  is the last nonzero coefficient, then  $d$  is called the *degree* of the polynomial.

Notice that if  $d = 0$ , we essentially obtain the nonzero elements of  $K$ . These polynomials are referred to as *constant polynomials*. The degree for the zero polynomial

$$0 + 0x + 0x^2 + 0x^3 + 0x^4 + \dots$$

is not defined.

By convention, the terms with zero coefficients are omitted when writing polynomials. Thus, the second degree polynomial in  $\mathbb{Z}[x]$

$$1 + 0x + 3x^2 + 0x^3 + \dots$$

would be written  $1 + 3x^2$ . The one exception to this convention is the zero polynomial, which is written as 0.

We can define the sum and product of two polynomials in the familiar way. If

$$\begin{aligned} A &= a_0 + a_1x + a_2x^2 + a_3x^3 + \dots && \text{and} \\ B &= b_0 + b_1x + b_2x^2 + b_3x^3 + \dots \end{aligned}$$

then

$$A + B = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + (a_3 + b_3)x^3 + \dots$$

and

$$A \cdot B = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (a_i \cdot b_j) x^{i+j}.$$

Although this looks like a double infinite sum, only a finite number of the terms will be nonzero. In fact, this product could be written as

$$\begin{aligned} A \cdot B &= a_0 \cdot b_0 \\ &\quad + (a_0 \cdot b_1 + a_1 \cdot b_0)x \\ &\quad + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 \\ &\quad + (a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0)x^3 + \dots \end{aligned}$$

so each coefficient is determined by a finite sum.

### LEMMA 11.1

*Let  $A$  and  $B$  be two nonzero polynomials in  $x$  over  $K$  of degree  $m$  and  $n$  respectively, where  $K$  has no zero divisors. Then  $A \cdot B$  is a polynomial of degree  $m + n$ , and  $A + B$  is a polynomial of degree no greater than the larger of  $m$  or  $n$ .*

PROOF: Let  $A$  be a polynomial of degree  $m$ ,

$$A = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots a_mx^m$$

and  $B$  be a polynomial of degree  $n$ ,

$$B = b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots b_nx^n.$$

Here,  $a_m$  and  $b_n$  are nonzero elements of  $K$ . The product is determined by

$$A \cdot B = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (a_i \cdot b_j) x^{i+j}.$$

Note that  $a_i$  and  $b_j$  are zero for  $i > m$  and  $j > n$ . If  $i + j > m + n$ , either  $i > m$  or  $j > n$ , and in either case  $a_i \cdot b_j = 0$ . Thus, there are no nonzero terms in  $A \cdot B$  with coefficients larger than  $m + n$ . However, if  $i + j = m + n$ , the only nonzero term would be the one coming from  $i = m$  and  $j = n$ , giving

$$a_m \cdot b_n x^{m+n}.$$

Since there are no zero divisors in  $K$ ,  $a_m \cdot b_n$  is nonzero, so  $A \cdot B$  is a polynomial of degree  $m + n$ .

Next we turn our attention to  $A + B$ . We may assume without loss of generality that  $m$  is no more than  $n$ . Then the sum of  $A$  and  $B$  can be expressed as

$$(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots (a_m + b_m)x^m + b_{m+1}x^{m+1} + \cdots b_nx^n.$$

If  $m < n$ , this clearly is a polynomial with degree  $n$ . Even if  $m = n$ , this still gives a polynomial whose degree cannot be more than  $n$ .  $\square$

We still have to show that  $K[x]$  will be a ring. But if  $K$  is an integral domain or field, we will be able to say more about  $K[x]$ .

### LEMMA 11.2

*Let  $R$  be a commutative ring. Then the set of polynomials in  $x$  over  $R$  forms a commutative ring.*

PROOF: We have seen that  $R[x]$  is closed under addition and multiplication. By the commutativity of  $R$ , addition and multiplication are obviously commutative. It is also clear that the zero polynomial acts as the additive identity in  $R[x]$ . Also, the additive inverse of

$$A = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$$

is given by

$$-A = (-a_0) + (-a_1)x + (-a_2)x^2 + (-a_3)x^3 + \cdots,$$

since the sum of these two polynomials is

$$A + (-A) = 0 + 0x + 0x^2 + 0x^3 + \cdots = 0.$$

To check associativity of addition and multiplication, we need three polynomials

$$\begin{aligned} A &= a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots, \\ B &= b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots, \quad \text{and} \\ C &= c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots. \end{aligned}$$

Then

$$\begin{aligned} (A + B) + C &= (a_0 + b_0) + c_0 + ((a_1 + b_1) + c_1)x + ((a_2 + b_2) + c_2)x^2 + \cdots \\ &= a_0 + (b_0 + c_0) + (a_1 + (b_1 + c_1))x + (a_2 + (b_2 + c_2))x^2 + \cdots \\ &= A + (B + C). \end{aligned}$$

Also,

$$\begin{aligned} A \cdot (B \cdot C) &= A \cdot \left( \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} b_j \cdot c_k x^{j+k} \right) \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} a_i \cdot (b_j \cdot c_k) x^{i+j+k} \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} (a_i \cdot b_j) \cdot c_k x^{i+j+k} = (A \cdot B) \cdot C. \end{aligned}$$

The two distributive laws are also easy to verify using the summation notation.

$$\begin{aligned} A \cdot (B + C) &= A \cdot \left( \sum_{j=0}^{\infty} (b_j + c_j) x^j \right) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i \cdot (b_j + c_j) x^{i+j} \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (a_i \cdot b_j + a_i \cdot c_j) x^{i+j} \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i \cdot b_j x^{i+j} + \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i \cdot c_j x^{i+j} = A \cdot B + A \cdot C. \end{aligned}$$

We can use the fact that multiplication is commutative to show that  $(A + B) \cdot C = A \cdot C + B \cdot C$ . Thus,  $R[x]$  is a commutative ring.  $\blacksquare$

Let us consider the commutative ring of order 8 from Tables 9.3 and 9.4 in Chapter 9.

```
InitRing(); AddRingVar("a", "b")
Define(4*a, 0); Define(2*b, 0)
Define(a^2, a); Define(b^2, b)
Define(a*b, 0); Define(b*a, 0)
R = Ring(); R
{0, a, 2 a, 3 a, b, a + b, 2 a + b, 3 a + b}
```

We form a polynomial ring over  $R$  by defining a new symbol  $x$ , which is an indeterminant over the ring  $R$ .

**AddPolyVar("x")**

A typical polynomial would be

```
Y = a*x + b; Y
a*x + b
```

If we consider raising this polynomial to a power,

```
Y^4
a*x^4 + b
```

we find that this polynomial ring has a rather bizarre properties. In fact, sometimes the square of a first degree polynomial is not a second degree polynomial. Consider

```
(2*a*x + a + b)^2
a + b
```

which yields the identity element in  $R$ . Thus,  $2ax + a + b$  is its own multiplicative inverse. To further complicate matters, polynomials may be “factored” in more than one way. The two products

```
(2*a*x + b) * (a*x + b)
2 a*x^2 + b
(2*a*x + b) * (a*x + 2*a + b)
2 a*x^2 + b
```

yield the same quadratic polynomial. Because of the bizarre properties of polynomials over general rings, we mainly will focus our attention to polynomial rings  $K[x]$ , where  $K$  is an integral domain or field.

### **PROPOSITION 11.1**

*Let  $K$  be an integral domain or a field. Then the set of polynomials in  $x$  over  $K$  forms an integral domain.*

PROOF: We have by Lemma 11.2 that  $K[x]$  is a commutative ring. The polynomial with  $b_0 = e$ , and  $b_j = 0$  for all positive  $j$ ,

$$I = e + 0x + 0x^2 + 0x^3 + \dots,$$

acts as the multiplicative identity, since

$$I \cdot A = A \cdot I = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i \cdot b_j x^{i+j} = \sum_{i=0}^{\infty} a_i \cdot e x^i = A.$$

Next, let us show that  $K[x]$  has no zero divisors. Suppose that  $A \cdot B = 0$ , with both  $A$  and  $B$  being nonzero polynomials. Say that  $A$  has degree  $m$  and  $B$  has degree  $n$ . Then by Lemma 11.1  $A \cdot B$  has degree  $m+n$ , which is impossible if either  $m$  or  $n$  were positive. But if  $A$  and  $B$  are constant polynomials, then  $a_0 \cdot b_0 = 0$ , which would indicate that either  $a_0$  or  $b_0$  is 0, since  $K$  has no zero divisors. Thus, either  $A$  or  $B$  would have to be 0, so we have that  $K[x]$  has no zero divisors.

Finally, let us show that  $K[x]$  is not a field, by showing that the polynomial  $(e+x)$  is not invertible. Suppose that there was a polynomial  $A$  such that  $A \cdot (e+x) = 1$ . Then  $A \neq 0$ , so suppose  $A$  has degree  $m$ . Then by Lemma 11.1, we have  $m+1 = 0$ , telling us  $m = -1$ , which is impossible. Thus,  $(e+x)$  has no inverse in  $K[x]$ , and therefore  $K[x]$  is an integral domain.  $\square$

Recall that in §9.2 we defined the characteristic of a ring to be the smallest positive integer  $n$  such that  $nx = 0$  for all elements  $x$  of  $R$ . If no such positive integer exists, we said the ring has characteristic 0. For integral domains or fields, the characteristic plays an extremely important role, as the next proposition illustrates.

### PROPOSITION 11.2

*Let  $R$  be a nontrivial ring without zero-divisors. If the characteristic is 0, then for  $n$  an integer and  $x$  a nonzero element of  $R$ ,  $nx = 0$  only if  $n = 0$ . If the characteristic is positive, then it is a prime number  $p$ , and for nonzero  $x$ ,  $nx = 0$  if, and only if,  $n$  is a multiple of  $p$ .*

PROOF: Suppose that  $nx = 0$  for some nonzero  $x \in R$ . Then for another nonzero element  $y$  of  $R$ ,

$$0 = (nx) \cdot y = n(x \cdot y) = x \cdot (ny).$$

But  $x$  is nonzero, and the ring has no zero divisors, so we have  $ny = 0$ . This argument works in both ways, so

$$nx = 0 \iff ny = 0 \quad \text{if } x \neq 0 \text{ and } y \neq 0. \tag{11.1}$$

If  $n$  was not zero, then  $|n|$  would be a positive number such that  $nx = 0$  for all  $x$  in the ring, forcing the characteristic to be positive. Hence, if the ring has characteristic 0, then  $nx = 0$  implies that either  $x = 0$  or  $n = 0$ .

Now suppose that the ring has positive characteristic, and let  $x$  be any nonzero element of  $R$ . Let  $p$  be the smallest positive integer for which  $p \cdot x = 0$ . If  $p$  is not prime, then  $p = ab$  with  $0 < a < p$  and  $0 < b < p$ . But then

$$(ax) \cdot (bx) = (ab)(x^2) = (px) \cdot x = 0 \cdot x = 0.$$

Since the ring has no zero divisors, either  $ax = 0$  or  $bx = 0$ . But this contradicts the fact that  $p$  was the *smallest* number such that  $px = 0$ . Thus,  $p$  is prime. By Equation 11.1 we have that  $py = 0$  for *every* element in  $R$ , and since this cannot be true for any smaller integer, we have that the characteristic of the ring is the prime number  $p$ .

It is easy to see that if  $n$  is a multiple of  $p$ , then  $n = cp$  for some integer  $c$ . Thus, for any element  $x$  in  $R$ ,

$$nx = (cp)x = c(px) = c0 = 0.$$

Suppose that  $nx = 0$  for some  $n$  that is not a multiple of  $p$ . Then  $\gcd(n, p)$  must be 1, and so by Bézout's lemma (1.3), there are integers  $u$  and  $v$  such that  $un + vp = 1$ . But then

$$x = 1 \cdot x = (un + vp)x = u(nx) + v(px) = u \cdot 0 + v \cdot 0 = 0.$$

So for nonzero  $x$ ,  $nx = 0$  if, and only if,  $n$  is a multiple of  $p$ . □

Characteristics are important because they provide a new way of defining integral domains and fields in *SageMath*. We begin by telling *SageMath* the characteristic  $p$  of the ring we want to define with the command **InitDomain(p)**. Because of Proposition 11.2, we see that  $p$  must either be 0 or a prime number. This command does three things. First, it tells *SageMath* that the ring to be defined is commutative. *SageMath* also defines the identity element to be 1. Finally, *SageMath* assumes that the ring to be defined has no zero-divisors, and may latter report an error if zero divisors are found.

For example, let us find a new ring with characteristic 3. We begin with the command

**InitDomain(3)**

This actually defines the field  $Z_3$ , as we can see with the command

```
Z3 = Field(); z3
{0, 1, 2}
```

We can create polynomials over this new domain by the **AddFieldVar** command.

**AddFieldVar("i")**

Now we can do computations in the polynomial ring  $Z_3[i]$ .

```
2*i + 5*i
      i
(2*i + 1)^2
      i^2 + i + 1
```

Let us try imitating the complex numbers, and tell *SageMath* that  $i^2 = -1$ .

```
Define(i^2, -1)
K = Field(); K
{0, 1, 2, i, i + 1, i + 2, 2*i, 2*i + 1, 2*i + 2}
AddTable(K)
MultTable(K)
```

This produces Tables 11.1 and 11.2.

**TABLE 11.1:** Addition of “complex numbers modulo 3”

| +      | 0      | 1      | 2      | $i$    | $2i$   | $1+i$  | $2+i$  | $1+2i$ | $2+2i$ |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0      | 0      | 1      | 2      | $i$    | $2i$   | $1+i$  | $2+i$  | $1+2i$ | $2+2i$ |
| 1      | 1      | 2      | 0      | $1+i$  | $1+2i$ | $2+i$  | $i$    | $2+2i$ | $2i$   |
| 2      | 2      | 0      | 1      | $2+i$  | $2+2i$ | $i$    | $1+i$  | $2i$   | $1+2i$ |
| $i$    | $i$    | $1+i$  | $2+i$  | $2i$   | 0      | $1+2i$ | $2+2i$ | 1      | 2      |
| $2i$   | $2i$   | $1+2i$ | $2+2i$ | 0      | $i$    | 1      | 2      | $1+i$  | $2+i$  |
| $1+i$  | $1+i$  | $2+i$  | $i$    | $1+2i$ | 1      | $2+2i$ | $2i$   | 2      | 0      |
| $2+i$  | $2+i$  | $i$    | $1+i$  | $2+2i$ | 2      | $2i$   | $1+2i$ | 0      | 1      |
| $1+2i$ | $1+2i$ | $2+2i$ | $2i$   | 1      | $1+i$  | 2      | 0      | $2+i$  | $i$    |
| $2+2i$ | $2+2i$ | $2i$   | $1+2i$ | 2      | $2+i$  | 0      | 1      | $i$    | $1+i$  |

We can see that this ring has nine elements and has no zero divisors. By Corollary 9.1,  $K$  is a field. We could call  $K$  the field of “complex numbers modulo 3.”

*SageMath* offers a shortcut for working with polynomials over an integral domain. We can add an additional parameter for the **InitDomain** command that will tell *SageMath* the name of the polynomial variable, usually “ $x$ ”. For example, the command

```
InitDomain(3, "x")
```

defines the integral domain  $Z_3[x]$  in one step. We can now do operations in  $Z_3[x]$ .

```
(x + 2)^2
x^2 + x + 1
factor(x^2 + 1)
```

**TABLE 11.2:** Multiplication for “complex numbers modulo 3”

| .      | 0 | 1      | 2      | $i$    | $2i$   | $1+i$  | $2+i$  | $1+2i$ | $2+2i$ |
|--------|---|--------|--------|--------|--------|--------|--------|--------|--------|
| 0      | 0 | 0      | 0      | 0      | 0      | 0      | 0      | 0      | 0      |
| 1      | 0 | 1      | 2      | $i$    | $2i$   | $1+i$  | $2+i$  | $1+2i$ | $2+2i$ |
| 2      | 0 | 2      | 1      | $2i$   | $i$    | $2+2i$ | $1+2i$ | $2+i$  | $1+i$  |
| $i$    | 0 | $i$    | $2i$   | 2      | 1      | $2+i$  | $2+2i$ | $1+i$  | $1+2i$ |
| $2i$   | 0 | $2i$   | $i$    | 1      | 2      | $1+2i$ | $1+i$  | $2+2i$ | $2+i$  |
| $1+i$  | 0 | $1+i$  | $2+2i$ | $2+i$  | $1+2i$ | $2i$   | 1      | 2      | $i$    |
| $2+i$  | 0 | $2+i$  | $1+2i$ | $2+2i$ | $1+i$  | 1      | $i$    | $2i$   | 2      |
| $1+2i$ | 0 | $1+2i$ | $2+i$  | $1+i$  | $2+2i$ | 2      | $2i$   | $i$    | 1      |
| $2+2i$ | 0 | $2+2i$ | $1+i$  | $1+2i$ | $2+i$  | $i$    | 2      | 1      | $2i$   |

$$(x + 1) * (x + 2)$$

```
factor(x^2 + 1)
x^2 + 1
```

If we continue to expand the field to the “complex numbers modulo 3,”

```
AddFieldVar("i")
Define(i^2, -1)
```

the variable  $x$  automatically promotes to a variable of the larger field. Thus, we can form polynomials like

```
y = (1 + i)*x + 2; y
(i + 1)*x + 2
z = (2 + i)*x^2 + 2*i*x + 1 + 2*i; z
(i + 2)*x^2 + 2*i*x + 2*i + 1
y^2
2*i*x^2 + (i + 1)*x + 1
y*z
x^3 + (i + 2)*x^2 + (i + 2)*x + i + 2
```

*SageMath* can factor polynomials defined over any finite field. It turns out that such factorizations are unique. If *SageMath* tries to factor  $x^2 + 1$  in the standard way, (using the ring  $\mathbb{Z}$ ),

```
var("X")
factor(X^2 + 1)
X^2 + 1
```

it finds the polynomial is irreducible. But if we factor the polynomial over the field of “complex numbers modulo 3,”

```
factor(x^2 + 1)
(x + i) * (x + 2*i)
```

we find that it does factor. Hence, whether a polynomial factors or not depends largely on which integral domain or field we are using.

The polynomial rings defined over integral domains give us some good examples of integral domains. In the next chapter we will find other ways of forming integral domains, some of which have some unusual properties. But even these are based on polynomial rings. So polynomials are the basic building blocks that are used for forming new integral domains and fields.

### Problems for §11.1

For Problems 1 through 6: Expand the following polynomials using the ring defined by [Tables 9.3](#) and [9.4](#).

- |                           |                                            |
|---------------------------|--------------------------------------------|
| 1 $(2ax + b)^2$           | 4 $(2ax^2 + ax + b)(bx + a)$               |
| 2 $(bx + a)(bx - a)$      | 5 $(ax^2 + (a + b)x + 2a)(2ax + b)$        |
| 3 $(2ax + a + b)(ax + b)$ | 6 $(bx^2 + (2a + b)x + a)(bx^2 + 2ax - a)$ |

For Problems 7 through 12: Expand the following polynomials using the “complex numbers modulo 3” given by [Tables 11.1](#) and [11.2](#).

- |                                  |                                            |
|----------------------------------|--------------------------------------------|
| 7 $(x + 1 + i)^2$                | 10 $(x^2 + ix + 2)(ix + 2)$                |
| 8 $(x + 2 + i)(x + 1 + 2i)$      | 11 $(x^2 + (1 + i)x + 2)(2x + i)$          |
| 9 $((1 + 2i)x + i)(ix + 1 + 2i)$ | 12 $(ix^2 + (2 + i)x + 2)(2x^2 + 2ix + 1)$ |

- 13 Let  $D$  be an integral domain with positive characteristic. Prove that all nonzero elements of  $D$  have the same additive order.
- 14 Show an example for which Problem 13 is not true for arbitrary rings.
- 15 Let  $\{0, e, a, b\}$  be a field of order 4, with  $e$  as the unity. Construct addition and multiplication tables for the field.
- 16 For the field  $K$  of “complex numbers modulo 3,” let  $\phi(x)$  denote the complex conjugate **mod** 3, that is,  $\phi(a + bi) = a + 2bi$  **mod** 3 for  $a, b \in Z_3$ . Show that  $\phi(x)$  is a ring isomorphism from  $K$  to itself.
- 17 For the field  $K$  of “complex numbers modulo 3,” use [Table 11.2](#) to show that every element cubed is the complex conjugate of Problem 16. That is,  $\phi(x) = x^3$ .
- 18 Show that in fact for every commutative ring of characteristic 3, the function  $\phi(x) = x^3$  will be a ring homomorphism from the ring to itself.
- 19 Show that if the ring of Problem 18 is an integral domain of characteristic 3, then the homomorphism  $\phi(x) = x^3$  is in fact one-to-one.
- 20 List all polynomials in  $Z_3[x]$  that have degree 2.

- 21** Of the second degree polynomials in  $Z_3[x]$  listed in Problem 20, which ones cannot be factored?

Hint: A quadratic polynomial in  $Z_3[x]$  cannot be factored if neither 0, 1, nor 2 are roots.

- 22** We saw that the polynomial  $x^2 + 1$  factored over the “complex numbers modulo 3” as  $(x+i)(x+2i)$ , even though this polynomial is irreducible in  $Z_3[x]$ . Find any *other* second degree irreducible polynomial in  $Z_3[x]$  from Problem 21, and show that it also factors over the “complex numbers modulo 3.”

- 23** List all polynomials in  $Z_2[x]$  that have degree 3.

- 24** Of the third degree polynomials in  $Z_2[x]$  listed in Problem 23, which ones cannot be factored?

Hint: A cubic polynomial in  $Z_2[x]$  cannot be factored if neither 0 nor 1 are roots.

### Interactive Problems

- 25** In the field of “complex numbers modulo 3”:

```
InitDomain(3, "x")
AddFieldVar("i")
Define(i^2, -1)
K = Field(); K
{0, 1, 2, i, i + 1, i + 2, 2*i, 2*i + 1, 2*i + 2}
```

Factor the polynomials  $x^3 + 1$ ,  $x^3 + 2$ ,  $x^3 + i$ ,  $x^3 + 2i$ . What do you notice about the factorizations? Knowing how *real* polynomials factor, explain what is happening.

- 26** Explain why the ring “complex numbers modulo 5”:

```
InitDomain(5)
AddFieldVar("i")
Define(i^2, -1)
```

does not form a field. Can you determine a pattern as to which integers “complex numbers modulo  $n$ ” form a field?

## 11.2 The Field of Quotients

In the last section, we found a way to form integral domains by imitating the familiar polynomials from high school algebra. In this section, we will

show how we can form a field from an integral domain, imitating grade school fractions.

We view a standard fraction as one integer divided by another. We want to extend this idea, and form fractions out of any integral domain. However, even with standard fractions there is a complication, since we consider

$$\frac{2}{4} = \frac{3}{6},$$

even though both the numerators and denominators are different. What we mean to say is that these two fractions are *equivalent*, where we define

$$\frac{x}{y} \equiv \frac{u}{v} \quad \text{if, and only if,} \quad x \cdot v = y \cdot u.$$

This forms an equivalence relation on the set of fractions  $x/y$ . We have already seen equivalence relations while working with cosets of a group. What we call a rational number is really a set of fractions of the form  $x/y$  that are all equivalent.

**DEFINITION 11.2** Let  $K$  be an integral domain, and let  $P$  denote the set of all ordered pairs  $(x, y)$  of elements of  $K$ , with  $y$  nonzero:

$$P = \{(x, y) \mid x, y \in K \text{ and } y \neq 0\}.$$

We define a relation on  $P$  by

$$(x, y) \equiv (u, v) \quad \text{if} \quad x \cdot v = y \cdot u.$$

### LEMMA 11.3

The above relation is an equivalence relation on  $P$ .

**PROOF:** We need to show that the relation is reflexive, symmetric, and transitive. Let  $(x, y)$ ,  $(u, v)$ , and  $(s, t)$  be arbitrary elements of  $P$ .

Reflexive:

$$(x, y) \equiv (x, y)$$

is equivalent to saying  $x \cdot y = x \cdot y$  which is, of course, true. So this relation is reflexive.

Symmetric:

$$(x, y) = (u, v) \implies x \cdot v = y \cdot u \implies u \cdot y = v \cdot x \implies (u, v) \equiv (x, y),$$

so this relation is also symmetric.

Transitive:

If  $(x, y) \equiv (u, v)$  and  $(u, v) \equiv (s, t)$ , then

$$(x, y) \equiv (u, v) \implies x \cdot v = y \cdot u \implies x \cdot v \cdot t = y \cdot u \cdot t,$$

$$(u, v) \equiv (s, t) \implies u \cdot t = v \cdot s \implies u \cdot t \cdot y = v \cdot s \cdot y.$$

These two statements imply that  $x \cdot v \cdot t = v \cdot s \cdot y$ . Notice that in the last step we had to use the commutativity of multiplication. Using commutativity again, we have  $x \cdot t \cdot v = y \cdot s \cdot v$ , and since  $K$  has no zero divisors and  $v$  is nonzero, we can use Lemma 9.4 to say that  $x \cdot t = y \cdot s$ . Then

$$x \cdot t = y \cdot s \implies (x, y) \equiv (s, t),$$

so we have the transitive law holding. Therefore, this relation is an equivalence relation.  $\square$

**DEFINITION 11.3** Let  $K$  be an integral domain, let  $P$  denote the set

$$P = \{(x, y) \mid x, y \in K \text{ and } y \neq 0\},$$

and let the equivalence relation on  $P$  be

$$(x, y) \equiv (u, v) \quad \text{if} \quad x \cdot v = y \cdot u.$$

For each  $(x, y)$  in  $P$ , let  $(\frac{x}{y})$  denote the equivalence class of  $P$  that contains  $(x, y)$ . Let  $Q$  denote the set of all equivalence classes  $(\frac{a}{b})$ . The set  $Q$  is called the *set of quotients* for  $K$ .

This definition allows us to replace an equivalence of two expressions with an equality. We now have that

$$\left(\frac{x}{y}\right) = \left(\frac{u}{v}\right) \quad \text{if, and only if, } x \cdot v = u \cdot y.$$

The next step is to define addition and multiplication on our set of quotients  $Q$ . Once again, we will use the rational numbers to guide us in the definition.

#### LEMMA 11.4

Let  $K$  be an integral domain, and let  $Q$  be the set of quotients for  $K$ . The addition and multiplication of two equivalence classes in  $Q$ , defined by

$$\left(\frac{x}{y}\right) + \left(\frac{u}{v}\right) = \left(\frac{x \cdot v + u \cdot y}{y \cdot v}\right)$$

and

$$\left(\frac{x}{y}\right) \cdot \left(\frac{u}{v}\right) = \left(\frac{x \cdot u}{y \cdot v}\right),$$

are both well-defined operations on  $Q$ . That is, the sum and product do not depend on the choice of the representative elements  $(x, y)$  and  $(u, v)$  of the equivalence classes.

PROOF: The first observation we need to make is that the formulas for the

sum and product both form valid elements of  $Q$ , since  $y \cdot v$  is nonzero as long as  $y$  and  $v$  are both nonzero.

Next let us work to show that addition does not depend on the choice of representative elements  $(x, y)$  and  $(u, v)$ . That is, if  $(\frac{x}{y}) = (\frac{a}{b})$ , and  $(\frac{u}{v}) = (\frac{c}{d})$ , we need to show that

$$\left(\frac{x}{y}\right) + \left(\frac{u}{v}\right) = \left(\frac{a}{b}\right) + \left(\frac{c}{d}\right).$$

That is, we have to prove that

$$\left(\frac{x \cdot v + u \cdot y}{y \cdot v}\right) = \left(\frac{a \cdot d + c \cdot b}{b \cdot d}\right).$$

Since  $(\frac{x}{y}) = (\frac{a}{b})$  and  $(\frac{u}{v}) = (\frac{c}{d})$ , we have  $x \cdot b = a \cdot y$  and  $u \cdot d = c \cdot v$ . Multiplying the first equation by  $v \cdot d$  and the second by  $y \cdot b$ , we get

$$x \cdot b \cdot v \cdot d = a \cdot y \cdot v \cdot d$$

and

$$u \cdot d \cdot y \cdot b = c \cdot v \cdot y \cdot b.$$

Adding this two equations together and factoring, we get

$$(x \cdot v + u \cdot y) \cdot b \cdot d = (a \cdot d + c \cdot b) \cdot y \cdot v.$$

This gives us

$$\left(\frac{x \cdot v + u \cdot y}{y \cdot v}\right) = \left(\frac{a \cdot d + c \cdot b}{b \cdot d}\right),$$

which is what we wanted.

We also need to show that multiplication is well defined, that is

$$\left(\frac{x}{y}\right) \cdot \left(\frac{u}{v}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right).$$

But since  $x \cdot b = a \cdot y$  and  $u \cdot d = c \cdot v$ , we can multiply these two equations together to get

$$x \cdot b \cdot u \cdot d = a \cdot y \cdot c \cdot v,$$

or

$$(x \cdot u) \cdot (b \cdot d) = (a \cdot c) \cdot (y \cdot v).$$

Therefore,

$$\left(\frac{x \cdot u}{y \cdot v}\right) = \left(\frac{a \cdot c}{b \cdot d}\right),$$

so multiplication also is well defined. □

### ***THEOREM 11.1: The Field of Quotients Theorem***

*Let  $K$  be an integral domain, and let  $Q$  be the set of quotients for  $K$ . Then  $Q$  forms a field using the above definitions of addition and multiplication. The field  $Q$  is called the field of quotients for  $K$ .*

PROOF: We have already noted that addition and multiplication are closed in  $Q$ .

We next want to look at the properties of addition. From the definition,

$$\left(\frac{x}{y}\right) + \left(\frac{u}{v}\right) = \left(\frac{x \cdot v + u \cdot y}{y \cdot v}\right) = \left(\frac{u}{v}\right) + \left(\frac{x}{y}\right),$$

we see that addition is commutative. Let  $z$  be any nonzero element of  $K$ . Then  $\left(\frac{0}{z}\right)$  acts as the additive identity:

$$\left(\frac{u}{v}\right) + \left(\frac{0}{z}\right) = \left(\frac{0}{z}\right) + \left(\frac{u}{v}\right) = \left(\frac{0 \cdot v + u \cdot z}{z \cdot v}\right) = \left(\frac{u \cdot z}{v \cdot z}\right) = \left(\frac{u}{v}\right).$$

Likewise,  $\left(\frac{-u}{v}\right)$  is the additive inverse of  $\left(\frac{u}{v}\right)$ :

$$\left(\frac{u}{v}\right) + \left(\frac{-u}{v}\right) = \left(\frac{-u}{v}\right) + \left(\frac{u}{v}\right) = \left(\frac{-u \cdot v + u \cdot v}{v \cdot v}\right) = \left(\frac{0}{v \cdot v}\right) = \left(\frac{0}{z}\right).$$

The associativity of addition is straightforward:

$$\begin{aligned} \left(\left(\frac{x}{y}\right) + \left(\frac{u}{v}\right)\right) + \left(\frac{a}{b}\right) &= \left(\frac{x \cdot v + u \cdot y}{y \cdot v}\right) + \left(\frac{a}{b}\right) \\ &= \left(\frac{x \cdot v \cdot b + u \cdot y \cdot b + a \cdot y \cdot v}{y \cdot v \cdot b}\right), \end{aligned}$$

while

$$\begin{aligned} \left(\frac{x}{y}\right) + \left(\left(\frac{u}{v}\right) + \left(\frac{a}{b}\right)\right) &= \left(\frac{x}{y}\right) + \left(\frac{u \cdot b + a \cdot v}{v \cdot b}\right) \\ &= \left(\frac{x \cdot v \cdot b + u \cdot y \cdot b + a \cdot y \cdot v}{y \cdot v \cdot b}\right). \end{aligned}$$

So  $Q$  forms a group with respect to addition.

Next we look at the properties of multiplication. Multiplication is obviously commutative, since

$$\left(\frac{x}{y}\right) \cdot \left(\frac{u}{v}\right) = \left(\frac{x \cdot u}{y \cdot v}\right) = \left(\frac{u \cdot x}{v \cdot y}\right) = \left(\frac{u}{v}\right) \cdot \left(\frac{x}{y}\right).$$

We also have associativity for multiplication:

$$\begin{aligned} \left(\left(\frac{x}{y}\right) \cdot \left(\frac{u}{v}\right)\right) \cdot \left(\frac{a}{b}\right) &= \left(\frac{x \cdot u}{y \cdot v}\right) \cdot \left(\frac{a}{b}\right) \\ &= \left(\frac{x \cdot u \cdot a}{y \cdot v \cdot b}\right) = \left(\frac{x}{y}\right) \cdot \left(\frac{u \cdot a}{v \cdot b}\right) = \left(\frac{x}{y}\right) \cdot \left(\left(\frac{u}{v}\right) \cdot \left(\frac{a}{b}\right)\right). \end{aligned}$$

The element  $\left(\frac{z}{z}\right)$  acts as the multiplicative identity for any  $z \neq 0$ .

$$\left(\frac{z}{z}\right) \cdot \left(\frac{x}{y}\right) = \left(\frac{x}{y}\right) \cdot \left(\frac{z}{z}\right) = \left(\frac{x \cdot z}{y \cdot z}\right) = \left(\frac{x}{y}\right).$$

If  $x = 0$ , then  $(\frac{x}{y}) = (\frac{0}{z})$ . Otherwise, the multiplicative inverse of  $(\frac{x}{y})$  is  $(\frac{y}{x})$ , since

$$\left(\frac{x}{y}\right) \cdot \left(\frac{y}{x}\right) = \left(\frac{x \cdot y}{y \cdot x}\right) = \left(\frac{z}{z}\right).$$

Thus, every nonzero element of  $Q$  has a multiplicative inverse. Finally, we have the two distribution laws. Because of the commutativity of multiplication, we only need to check one. Since

$$\left(\left(\frac{u}{v}\right) + \left(\frac{a}{b}\right)\right) \cdot \left(\frac{x}{y}\right) = \left(\frac{u \cdot b + a \cdot v}{v \cdot b}\right) \cdot \left(\frac{x}{y}\right) = \left(\frac{u \cdot b \cdot x + a \cdot v \cdot x}{v \cdot b \cdot y}\right),$$

while

$$\begin{aligned} \left(\frac{u}{v}\right) \cdot \left(\frac{x}{y}\right) + \left(\frac{a}{b}\right) \cdot \left(\frac{x}{y}\right) &= \left(\frac{u \cdot x}{v \cdot y}\right) + \left(\frac{a \cdot x}{b \cdot y}\right) \\ &= \left(\frac{u \cdot x \cdot b \cdot y + a \cdot x \cdot v \cdot y}{v \cdot y \cdot b \cdot y}\right) \\ &= \left(\frac{u \cdot x \cdot b + a \cdot x \cdot v}{v \cdot y \cdot b}\right), \end{aligned}$$

we have the distributive laws holding, and therefore  $Q$  is a field. □

In the construction of the field  $Q$ , we never used the identity element of  $K$ . Hence, if we started with a commutative ring without zero divisors instead of an integral domain, the construction would still produce a field. We can mention this as a corollary.

### COROLLARY 11.1

*Let  $K$  be any commutative ring without zero divisors. Then the set of quotients  $Q$  defined above forms a field.*

Although the field of quotients was designed from the way we formed rational numbers from the set of integers, we can apply the field of quotients to any other integral domain. What happens if we form a field of quotients for the polynomial ring  $K[x]$ ?

Let us first consider the most familiar polynomial ring  $\mathbb{Z}[x]$ —the polynomials with integer coefficients. An element in the field of quotients would be of the form  $p(x)/q(x)$ , where  $p(x)$  and  $q(x)$  are polynomials with integer coefficients. But we consider two such fractions  $p(x)/q(x)$  and  $r(x)/s(x)$  to be equivalent if  $p(x) \cdot s(x) = r(x) \cdot q(x)$ . For example, the two fractions

```
var("x")
A = (3*x^2 + 5*x - 2) / (2*x^2 + 7*x + 6); A
(3*x^2 + 5*x - 2)/(2*x^2 + 7*x + 6)
B = (3*x^2 - 4*x + 1) / (2*x^2 + x - 3); B
(3*x^2 - 4*x + 1)/(2*x^2 + x - 3)
```

can be seen to be equivalent, since

```
expand((3*x^2 + 5*x - 2) * (2*x^2 + x - 3))
6*x^4 + 13*x^3 - 8*x^2 - 17*x + 6
expand((3*x^2 - 4*x + 1) * (2*x^2 + 7*x + 6))
6*x^4 + 13*x^3 - 8*x^2 - 17*x + 6
```

yield the same result. Other ways of showing that  $A$  and  $B$  are equivalent is by computing either of these two commands:

```
Together(A - B)
0
Together(A/B)
1
```

We call the field of quotients for the polynomials  $\mathbb{Z}[x]$  the *field of rational functions in  $x$* , denoted  $\mathbb{Z}(x)$ .

It should be mentioned that a rational function, in this context, is not a function! The rational functions  $A$  and  $B$  are merely *elements* of  $\mathbb{Z}(x)$ , which may in turn be arguments for some homomorphism. To say that “ $A$  is undefined when  $x = -2$ ” or “ $B$  is undefined at  $x = 1$ ” is meaningless, since  $x$  is not a variable for which numbers can be plugged in. Rather,  $x$  is merely a symbol that is used as a place holder. This is why we can say that  $A$  and  $B$  are truly equal, even though their “graphs” would disagree at two points.

We can form rational functions from any integral domain  $K$ . This produces the field  $K(x)$ , the *rational functions in  $x$  over  $K$* .

### Computational Example 11.1

Simplify the rational function

$$\frac{(1+i)x^2 + (2+2i)x + 2}{x^2 + ix + 1}$$

defined over the field of order 9 that was defined by [Tables 11.1](#) and [11.2](#).

SOLUTION: First we set up the field.

```
InitDomain(3, "x")
AddFieldVar("i")
Define(i^2, -1)
```

*SageMath* will automatically simplify the rational function for us.

```
A = ((1 + i)*x^2 + (2 + 2*i)*x + 2) / (x^2 + i*x + 1); A
((i + 1)*x + i + 2)/(x + 2*i + 1)
```

However, if we consider the simpler looking rational function

```
B = (2*x - i) / (x - i*x + i); B
(2*x + 2*i)/((2*i + 1)*x + i)
```

we find that they are equal.

**A – B**

0

□

As you can see from this example, the definition of the quotient field does not depend on whether elements in the integral domain can be factored uniquely. It turns out that the polynomial ring  $K[x]$  used in the above example really does have a type of unique factorization, but we will not go into this. Instead, we will focus on some of the more familiar fields: the rational numbers, the real numbers, and the complex numbers. These fields will be the basis for defining many other fields, so it is natural to learn the properties of these fields.

### Problems for §11.2

**1** If  $Q$  is the field of quotients of an integral domain, show that  $(\frac{-a}{b})$  is the additive inverse of  $(\frac{a}{b})$  in  $Q$ .

**2** If  $Q$  is the field of quotients of an integral domain, show that the left distributive property holds for  $Q$ :

$$\left(\frac{u}{v}\right) \cdot \left(\left(\frac{x}{y}\right) + \left(\frac{z}{w}\right)\right) = \left(\frac{u}{v}\right) \cdot \left(\frac{x}{y}\right) + \left(\frac{u}{v}\right) \cdot \left(\frac{z}{w}\right).$$

**3** If  $Q$  is the field of quotients of an integral domain, show that the multiplication in  $Q$  is associative.

**4** Investigate what happens if we compute the field of quotients of a ring that is already a field. Let  $K = Z_3$ , and let  $P$  be the set of ordered pairs

$$P = \{(x, y) \mid x, y \in Z_3 \text{ and } y \neq 0\}.$$

Write a list of all ordered pairs in  $P$ , and determine which pairs are equivalent under the relation

$$(x, y) \equiv (u, v) \quad \text{if} \quad x \cdot v \equiv y \cdot u \pmod{3}.$$

If  $Q$  is the set of equivalence classes, construct addition and multiplication tables for  $Q$  and show that  $Q$  is isomorphic to  $Z_3$ .

**5** Repeat Problem 4, using  $Z_5$  instead of  $Z_3$ .

**6** Prove that if  $K$  is a field, then the field of quotients of  $K$  is isomorphic to  $K$ .

**7** Show that if we apply Corollary 11.1 to the ring of even integers, we obtain a field isomorphic to  $\mathbb{Q}$ .

- 8** What is the quotient field for the ring given by

$$\{x + y\sqrt{2} \mid x, y \in \mathbb{Z}\}?$$

- 9** Show by cross multiplying that the two rational functions  $A$  and  $B$  from Example 11.1 are indeed equal.

For Problems **10** through **17**: Perform the following operations in  $Z_2(x)$ , the rational functions over  $Z_2$ .

|                                                           |                                                                     |
|-----------------------------------------------------------|---------------------------------------------------------------------|
| <b>10</b> $\frac{x^2 + x + 1}{x + 1} + \frac{x + 1}{x}$   | <b>14</b> $\frac{x^2 + x + 1}{x + 1} \cdot \frac{x}{x + 1}$         |
| <b>11</b> $\frac{x + 1}{x^2 + x + 1} + \frac{1}{x^2 + x}$ | <b>15</b> $\frac{x^2 + 1}{x^2 + x + 1} \cdot \frac{x^2}{x + 1}$     |
| <b>12</b> $\frac{x^2 + 1}{x} + \frac{x^2 + x + 1}{x + 1}$ | <b>16</b> $\frac{x^2 + x + 1}{x^2 + x} \cdot \frac{x^2 + 1}{x}$     |
| <b>13</b> $\frac{x^2 + x}{x^2 + x + 1} + \frac{x}{x + 1}$ | <b>17</b> $\frac{x^2}{x^2 + x + 1} \cdot \frac{x + 1}{x^2 + x + 1}$ |

#### Interactive Problems

- 18** Have *SageMath* simplify the rational function over  $Z_2(x)$ :

$$\frac{x^4 + x^3 + x + 1}{x^3 + x^2 + x + 1}.$$

- 19** Try squaring different elements of  $Z_2(x)$ . What do you observe? Any explanations?

- 20** Have *SageMath* compute the following operation in the rational function field of Example 11.1.

$$\frac{(1+i)x+2}{x^2+2ix+2+i} + \frac{2x+1+i}{x^2+(2+i)x+2}.$$

- 21** It was mentioned that the definition of the quotient field does not depend on whether elements in the integral domain have unique factorization. An example of such a domain is  $\mathbb{Z}[\sqrt{-5}]$ , which we can enter in *SageMath* as follows:

```
InitDomain(0, "x")
AddFieldVar("a")
Define(a^2, -5)
```

Show that the two fractions

$$\frac{3x + 3a}{(1+a)x} \quad \text{and} \quad \frac{(1-a)x + 5 + a}{2x}$$

are in fact equal, even though neither can simplify.

### 11.3 Complex Numbers

We have already seen some examples of complex numbers in the form  $a+bi$ , where  $i$  represents the “square root of negative one.” *SageMath* uses a capital **I** to enter and display the imaginary number. This allows us to perform standard arithmetic on complex numbers.

```
(2 + 3*I) + (4 - I)
2*I + 6
(2 + 3*I)*(4 - I)
10*I + 11
(2 + 3*I)/(4 - I)
14/17*I + 5/17
```

You may have noticed that *SageMath* puts the complex part of the number first. In this presentation, is not at all clear where the “**I**” came from. This gives the complex numbers a rather mysterious quality that is compounded by their common misnomer, “imaginary numbers.”

We would like to show how complex numbers are a natural extension of the real numbers. Instead of considering quantities of the form  $a+bi$ , we will consider ordered pairs  $(a,b)$ . We will declare the following properties for ordered pairs of real numbers:

1.  $(a,b) = (c,d)$  if, and only if,  $a = c$  and  $b = d$ .
2.  $(a,b) + (c,d) = (a+c, b+d)$ .
3.  $(a,b) \cdot (c,d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$ .

We define  $\mathbb{C}$  to be the set of all ordered pairs of real numbers.

#### **PROPOSITION 11.3**

*The set  $\mathbb{C}$  forms a field, called the field of complex numbers. This field contains a subfield isomorphic to the real numbers.*

**PROOF:** Because the real numbers are closed with respect to both addition and multiplication, it is clear that both  $(a+c, b+d)$  and  $(a \cdot c - b \cdot d, a \cdot d + b \cdot c)$  would be defined for all real numbers  $a$ ,  $b$ ,  $c$ , and  $d$ . Thus,  $\mathbb{C}$  is closed with respect to both addition and multiplication. Furthermore, since

$$(c,d) + (a,b) = (c+a, d+b) = (a+c, b+d) = (a,b) + (c,d)$$

and

$$(c,d) \cdot (a,b) = (c \cdot a - d \cdot b, c \cdot b + d \cdot a) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c) = (a,b) \cdot (c,d),$$

we see that both addition and multiplication are commutative. The element  $(0, 0)$  acts as the zero element, since

$$(0, 0) + (a, b) = (a, b).$$

The addition inverse of  $(a, b)$  is  $(-a, -b)$ , since

$$(a, b) + (-a, -b) = (0, 0).$$

Note that the order on the last two sums is irrelevant, since addition has already been shown to be commutative.

To show that addition is associative, we note that

$$\begin{aligned} (a, b) + [(c, d) + (e, f)] &= (a, b) + (c + e, d + f) = (a + c + e, b + d + f) \\ &= (a + c, b + d) + (e, f) = [(a, b) + (c, d)] + (e, f). \end{aligned}$$

To show that multiplication is associative is a little more complicated. We have

$$\begin{aligned} (a, b) \cdot [(c, d) \cdot (e, f)] &= (a, b) \cdot (c \cdot e - d \cdot f, c \cdot f + d \cdot e) = \\ &(a \cdot c \cdot e - a \cdot d \cdot f - b \cdot c \cdot f - b \cdot d \cdot e, a \cdot c \cdot f + a \cdot d \cdot e + b \cdot c \cdot e - b \cdot d \cdot f), \end{aligned}$$

and

$$\begin{aligned} [(a, b) \cdot (c, d)] \cdot (e, f) &= (a \cdot c - b \cdot d, a \cdot d + b \cdot c) \cdot (e, f) = \\ &(a \cdot c \cdot e - b \cdot d \cdot e - a \cdot d \cdot f - b \cdot c \cdot f, a \cdot c \cdot f - b \cdot d \cdot f + a \cdot d \cdot e + b \cdot c \cdot e). \end{aligned}$$

By comparing these two, we see that they are equal, so multiplication is associative.

We need to test the distributive laws next. The left distributive law we can get by expanding:

$$\begin{aligned} (a, b) \cdot [(c, d) + (e, f)] &= (a, b) \cdot (c + e, d + f) \\ &= (a \cdot c + a \cdot e - b \cdot d - b \cdot f, a \cdot d + a \cdot f + b \cdot c + b \cdot e) \\ &= (a \cdot c - b \cdot d, a \cdot d + b \cdot c) + (a \cdot e - b \cdot f, a \cdot f + b \cdot e) \\ &= (a, b) \cdot (c, d) + (a, b) \cdot (e, f). \end{aligned}$$

Thus, the left distributive law is satisfied. However, the right distributive law follows from the left distributive law, and using the commutative multiplication:

$$\begin{aligned} [(a, b) + (c, d)] \cdot (e, f) &= (e, f) \cdot [(a, b) + (c, d)] \\ &= (e, f) \cdot (a, b) + (e, f) \cdot (c, d) \\ &= (a, b) \cdot (e, f) + (c, d) \cdot (e, f). \end{aligned}$$

We have now shown that the set  $\mathbb{C}$  forms a commutative ring. To show that this ring has a multiplicative identity, we consider the element  $(1, 0)$ . Since the ring is commutative, we only need to check

$$(1, 0) \cdot (a, b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b).$$

Finally, we need to show that every nonzero element has an inverse. If  $(a, b)$  is nonzero, then  $a^2 + b^2$  will be a positive number. Hence

$$\left( \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

is an element of  $\mathbb{C}$ . The product

$$(a, b) \cdot \left( \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = \left( \frac{a^2 + b^2}{a^2 + b^2}, \frac{-a \cdot b + a \cdot b}{a^2 + b^2} \right) = (1, 0)$$

verifies that

$$(a, b)^{-1} = \left( \frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

since multiplication is commutative. Therefore, the set  $\mathbb{C}$  forms a field.

The second part of this proposition is to show that  $\mathbb{C}$  contains a copy of the real numbers as a subfield. Consider the mapping  $f$ , which maps real numbers to  $\mathbb{C}$ , given by

$$f(x) = (x, 0).$$

To check that  $f$  is a homomorphism, we check that

$$f(x) + f(y) = (x, 0) + (y, 0) = (x + y, 0) = f(x + y)$$

and

$$f(x) \cdot f(y) = (x, 0) \cdot (y, 0) = (x \cdot y + 0, 0 + 0) = (x \cdot y, 0) = f(x \cdot y).$$

Thus,  $f$  is a homomorphism from the reals to  $\mathbb{C}$ . It is clear that  $f$  is one-to-one, since  $(x, 0) = (y, 0)$  if, and only if,  $x = y$ . Thus the image of  $f$ :

$$\{(x, 0) \mid x \in \mathbb{R}\}$$

is isomorphic to the real numbers. Hence, we have found a subring of  $\mathbb{C}$  isomorphic to  $\mathbb{R}$ . □

The purpose of constructing the complex numbers was to produce a field for which we can take the square root of negative one. We can now show that we have succeeded in doing this.

### **LEMMA 11.5**

*There are exactly two solutions to the equation  $x^2 = (-1, 0)$  in the field  $\mathbb{C}$ , given by  $(0, \pm 1)$ .*

PROOF: If  $(a, b)$  solves the equation  $x^2 = (-1, 0)$ , we have that

$$(a, b)^2 = (a^2 - b^2, 2ab) = (-1, 0).$$

Thus,  $a$  and  $b$  must satisfy the two equations

$$a^2 - b^2 = -1$$

and

$$2ab = 0.$$

The second equation implies that either  $a$  or  $b$  must be 0. But if  $b = 0$ , then the first equation becomes  $a^2 = -1$ , which has no real solutions. Thus,  $a = 0$ , and  $-b^2 = -1$ . There are two real solutions for  $b$ ,  $\pm 1$ . Thus,  $(0, 1)$  and  $(0, -1)$  both solve the equations for  $a$  and  $b$ , and so

$$(0, 1)^2 = (0, -1)^2 = (-1, 0). \quad \square$$

By defining the complex numbers as ordered pairs, we have taken some of the mystery out of the complex numbers. Lemma 11.5 shows that the square root of negative one comes as a natural consequence of the way we defined the product.

We can now convert ordered pairs to the customary notation by defining  $i = (0, 1)$ , and identifying the identity element  $(1, 0)$  with 1. Then any complex number  $(a, b)$  can be written

$$(a, b) = (a, 0) + (0, b) = a \cdot (1, 0) + b \cdot (0, 1) = a + bi.$$

We can rewrite the rules for addition and multiplication in  $\mathbb{C}$  as follows:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

$$(a + bi) \cdot (c + di) = (a \cdot c - b \cdot d) + (b \cdot c + a \cdot d)i.$$

In working with groups, we found that the group automorphisms revealed many of the important properties of the group. This will also be true for rings. Let us extend the group automorphisms to apply to rings.

**DEFINITION 11.4** A *ring automorphism* is a one-to-one and onto ring homomorphism that maps a ring to itself.

### LEMMA 11.6

The set of all ring automorphisms of a given ring forms a group.

PROOF: We first note that if  $f(x)$  is an automorphism of a ring  $R$ , then  $f^{-1}(x)$  is well defined, since  $f(x)$  is both one-to-one and onto. We see that

$$f(f^{-1}(x) + f^{-1}(y)) = f(f^{-1}(x)) + f(f^{-1}(y)) = x + y,$$

so  $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$ . Also,

$$f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = x \cdot y,$$

so  $f^{-1}(x \cdot y) = f^{-1}(x) \cdot f^{-1}(y)$ . Thus,  $f^{-1}$  is a ring homomorphism. Since  $f$  was both one-to-one and onto,  $f^{-1}$  is both one-to-one and onto. Therefore,  $f^{-1}$  is a ring automorphism.

If  $f$  and  $\phi$  are two ring automorphisms, then

$$f(\phi(x + y)) = f(\phi(x) + \phi(y)) = f(\phi(x)) + f(\phi(y))$$

and

$$f(\phi(x \cdot y)) = f(\phi(x) \cdot \phi(y)) = f(\phi(x)) \cdot f(\phi(y)).$$

The combination  $f(\phi(x))$  is also one-to-one and onto, so this product, which we can denote  $f \cdot \phi$ , is a ring automorphism. Since the set of all ring automorphisms is closed with respect to multiplication and inverses, and the set of all ring automorphisms is a subgroup of the set of all *group* automorphisms with respect to addition, we see that this set is a group.  $\square$

The natural question that arises is determining the group of ring automorphisms of  $\mathbb{C}$ . This is in fact a difficult question to answer, but if we only consider the automorphisms that send each real number to itself, the question becomes easy to answer.

#### **PROPOSITION 11.4**

*Besides the identity automorphism, there is another ring automorphism on  $\mathbb{C}$ , given by*

$$\phi(a + bi) = a - bi.$$

*In fact, these are the only automorphisms for which  $\phi(x) = x$  for all real numbers  $x$ .*

PROOF: We check that

$$\begin{aligned} \phi(a + bi) + \phi(c + di) &= (a - bi) + (c - di) = a + c - (b + d)i \\ &= \phi(a + c + (b + d)i) = \phi((a + bi) + (c + di)). \end{aligned}$$

$$\begin{aligned} \phi(a + bi) \cdot \phi(c + di) &= (a - bi) \cdot (c - di) = (a \cdot c - b \cdot d) - (a \cdot d + b \cdot c)i \\ &= \phi((a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)i) = \phi((a + bi) \cdot (c + di)). \end{aligned}$$

Thus,  $\phi$  is a homomorphism. Since  $a - bi = 0$  if, and only if,  $a$  and  $b$  are both 0, the kernel of  $\phi$  is just  $\{0\}$ , and so  $\phi$  is one-to-one. Also,  $\phi$  is onto, since  $\phi(a - bi) = a + bi$ . Therefore,  $\phi$  is an automorphism.

To show that there are exactly two such automorphisms, suppose that  $f(x)$  is an automorphism of  $\mathbb{C}$  for which  $f(x) = x$  for all real numbers  $x$ . Then

$f(i)^2 = f(i^2) = f(-1) = -1$ , so by Lemma 11.5  $f(i) = \pm i$ . If  $f(i) = i$ , then  $f(x) = x$  for all  $x \in \mathbb{C}$ , and if  $f(i) = -i$ , then  $f(x) = \phi(x)$  for all  $x$ .  $\blacksquare$

The ring automorphism found in Proposition 11.4 is called the *conjugate*. The conjugate of  $z$  is generally denoted by  $\bar{z}$ . That is, if  $z = a + bi$ , then  $\bar{z} = \phi(z) = a - bi$ . The conjugate automorphism is defined in *SageMath* as

```
conjugate(3 + 4*I)
-4*I + 3
```

It is an easy computation to see that

$$z \cdot \bar{z} = (a + bi) \cdot (a - bi) = a^2 + b^2.$$

Thus,  $z \cdot \bar{z}$  is always a non-negative real number.

**DEFINITION 11.5** We say the *absolute value* of a complex number  $z = a + bi$  is

$$|z| = \sqrt{z \cdot \bar{z}}.$$

The geometric interpretation of  $|z|$  is the distance from  $(a, b)$  to the origin. In *SageMath*, the function **abs (z)** gives the absolute value for both real and complex numbers.

```
abs(3 + 4*I)
5
```

The familiar property for the absolute value of real numbers holds for all complex numbers as well.

### PROPOSITION 11.5

For any two elements  $x$  and  $y$  in  $\mathbb{C}$ ,

$$|x \cdot y| = |x| \cdot |y|.$$

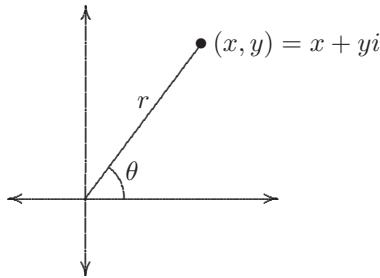
PROOF: We have

$$|x \cdot y| = \sqrt{x \cdot y \cdot \bar{x} \cdot \bar{y}} = \sqrt{x \cdot y \cdot \bar{x} \cdot \bar{y}} = \sqrt{x \cdot \bar{x} \cdot y \cdot \bar{y}} = \sqrt{x \cdot \bar{x}} \cdot \sqrt{y \cdot \bar{y}} = |x| \cdot |y|.$$

Thus,  $|x \cdot y| = |x| \cdot |y|$ .  $\blacksquare$

Since there is a geometric interpretation of the absolute value, this proposition suggests that there is also a geometric interpretation to the product of two complex numbers.

From polar coordinates it is known that any point in the plane can be located by knowing its distance  $r$  from the origin, and its angle  $\theta$  from the positive  $x$ -axis.



**FIGURE 11.1:** Polar coordinates for a complex number

Since  $r$  is the absolute value of  $(x+yi)$ , perhaps the angle  $\theta$  is also significant to the complex number. By using trigonometry in Figure 11.1, we have that

$$x + yi = r(\cos \theta + i \sin \theta).$$

This form is called the *polar form* of the complex number  $x + yi$ . The angle  $\theta$  is called the *argument* of  $x + yi$ . We can find the approximate argument of a complex number (in radians) with the *SageMath* command

```
N(arg(3 + 4*I))
0.927295218001612
```

*SageMath* always finds an angle  $\theta$  between  $-\pi$  and  $\pi$ , but we can also consider the angles

$$\dots, \theta - 6\pi, \theta - 4\pi, \theta - 2\pi, \theta, \theta + 2\pi, \theta + 4\pi, \theta + 6\pi, \dots.$$

All of these angles have the same sine and cosine, and hence are interchangeable in the polar coordinate system. We call these angles *co-terminal*. The set of angles co-terminal to  $\theta$  can be written

$$\{\theta + 2\pi n \mid n \in \mathbb{Z}\}.$$

For example, the polar form of  $-\sqrt{3} - i$  is given by

$$2 \left( \cos \left( \frac{-5\pi}{6} \right) + i \sin \left( \frac{-5\pi}{6} \right) \right),$$

as seen from the commands

```
simplify(abs(-sqrt(3) - I))
2
simplify(arg(-sqrt(3) - I))
-5/6*pi
```

However, we could have used any co-terminal angle instead of the one *Sage-Math* gave us. Thus,

$$2 \left( \cos \left( \frac{7\pi}{6} \right) + i \sin \left( \frac{7\pi}{6} \right) \right), \quad 2 \left( \cos \left( \frac{19\pi}{6} \right) + i \sin \left( \frac{19\pi}{6} \right) \right), \quad \dots$$

are also polar forms of  $-\sqrt{3} - i$ . The usefulness of the polar form of a complex number is hinted at by the next lemma, which makes use of the trigonometric identities

$$\begin{aligned} \cos(A + B) &= \cos(A)\cos(B) - \sin(A)\sin(B), & \text{and} \\ \sin(A + B) &= \sin(A)\cos(B) + \cos(A)\sin(B). \end{aligned}$$

### **LEMMA 11.7**

If  $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$  and  $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$ , then

$$z_1 \cdot z_2 = r_1 \cdot r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)).$$

So the argument of the product is the sum of the arguments.

PROOF: We note that

$$\begin{aligned} z_1 \cdot z_2 &= r_1(\cos \theta_1 + i \sin \theta_1) \cdot r_2(\cos \theta_2 + i \sin \theta_2) = \\ r_1 \cdot r_2 &((\cos \theta_1 \cdot \cos \theta_2 - \sin \theta_1 \cdot \sin \theta_2) + i \cdot (\cos \theta_1 \cdot \sin \theta_2 + \sin \theta_1 \cdot \cos \theta_2)). \end{aligned}$$

Using the trigonometric identities, this simplifies to

$$z_1 \cdot z_2 = r_1 \cdot r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)). \quad \square$$

We can now use induction to prove the following important theorem:

### **THEOREM 11.2: De Moivre's Theorem**

If  $n$  is an integer, and  $z = r(\cos \theta + i \sin \theta)$  is a nonzero complex number in polar form, then

$$z^n = r^n (\cos(n\theta) + i \sin(n\theta)).$$

PROOF: Let us first prove the theorem for positive values of  $n$ . For  $n = 1$ , the statement is obvious. Let us assume that the statement is true for the previous case. That is,

$$z^{n-1} = r^{n-1} (\cos((n-1)\theta) + i \sin((n-1)\theta)).$$

We want to prove that the theorem holds for  $n$  as well. Using Lemma 11.7, we have

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

Thus, the theorem is true for  $n$ , and hence by induction it is true whenever  $n$  is positive.

If  $z$  is nonzero, then letting  $n = 0$  gives

$$r^0(\cos(0\theta) + i \sin(0\theta)) = 1(1 + i \cdot 0) = 1 = z^0.$$

So the theorem holds for  $n = 0$ . If  $z$  is nonzero, then  $r > 0$ , and so

$$\begin{aligned} (r^{-n}(\cos(-n\theta) + i \sin(-n\theta))) \cdot (r^n(\cos(n\theta) + i \sin(n\theta))) &= \\ r^{-n+n}(\cos(-n\theta + n\theta) + i \sin(-n\theta + n\theta)) &= r^0(\cos 0 + i \sin 0) = 1. \end{aligned}$$

Now, if  $n < 0$ , then the theorem holds for  $-n$ , and so

$$z^{-n}(r^n(\cos(n\theta) + i \sin(n\theta))) = 1,$$

hence

$$r^n(\cos(n\theta) + i \sin(n\theta)) = z^n$$

even when  $n < 0$ . □

De Moivre's theorem (11.2) allows us to quickly raise a complex number to an integer power.

### **Example 11.2**

Compute  $(-\sqrt{3} - i)^5$ .

SOLUTION: Since  $r = \sqrt{(-\sqrt{3})^2 + (-1)^2} = 2$ , and  $\theta = \tan^{-1}((-1)/(-\sqrt{3})) - \pi = -5\pi/6$ , then  $(-\sqrt{3} - i)^5$  is

$$2^5 \left( \cos \left( \frac{-25\pi}{6} \right) + i \sin \left( \frac{-25\pi}{6} \right) \right) = 32 \left( \frac{\sqrt{3}}{2} - \frac{i}{2} \right) = 16\sqrt{3} - 16i. \quad \square$$

We can also use De Moivre's theorem (11.2) to find the  $n^{\text{th}}$  root of 1. We first define

$$\omega_n = \cos \left( \frac{2\pi}{n} \right) + i \sin \left( \frac{2\pi}{n} \right).$$

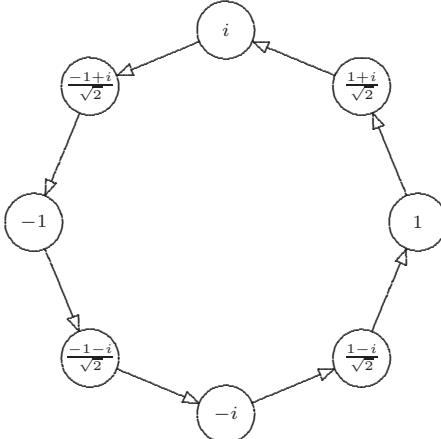
For example,  $\omega_1 = 1$ ,  $\omega_2 = -1$ ,  $\omega_3 = (-1 + i\sqrt{3})/2$ , and  $\omega_4 = i$ , etc. Then

$$(\omega_n)^n = \cos(2\pi) + i \sin(2\pi) = 1,$$

so  $\omega_n$  is indeed one  $n^{\text{th}}$  root of unity. In fact, all  $n^{\text{th}}$  roots of 1 are given by the numbers  $\omega_n, \omega_n^2, \omega_n^3, \dots$  up to  $(\omega_n)^n = 1$ .

### **Computational Example 11.3**

The eighth root of unity,  $\omega_8$ , can be entered into *SageMath* using the commands

**FIGURE 11.2:** The eight roots of unity

```
w8 = (1/2 + I/2)*sqrt(2); w8
(1/2*I + 1/2)*sqrt(2)
```

This allows us to consider the group generated by  $\omega_8$ :

```
G = Group(w8); G
{ (1/2*I + 1/2)*sqrt(2), I, (1/2*I - 1/2)*sqrt(2), -1,
  -(1/2*I + 1/2)*sqrt(2), -I, -(1/2*I - 1/2)*sqrt(2), 1}
```

This gives the eight roots of unity, and shows that these elements form a group. In fact, the  $n^{\text{th}}$  roots of unity will form a cyclic group isomorphic to  $\mathbb{Z}_n$ . □

By rearranging the elements of  $G$ , we can create a circle graph as in [Figure 11.2](#) with the elements in the proper positions in the complex plane.

```
G = [I, (1/2+I/2)*sqrt(2), 1, (1/2-I/2)*sqrt(2), -I,
      (-1/2-I/2)*sqrt(2), -1, (-1/2+I/2)*sqrt(2)]
CircleGraph(G, Mult(w8))
```

We are mainly interested in those elements of this subgroup that are generators.

**DEFINITION 11.6** A complex number  $z$  is called a *primitive  $n^{\text{th}}$  root of unity* if the powers of  $z$  produce all  $n$  solutions to the equation  $x^n = 1$ .

It is clear that  $\omega_n$  is a primitive  $n^{\text{th}}$  root of unity, but also  $(\omega_n)^k$  is a primitive  $n^{\text{th}}$  root of unity if  $k$  and  $n$  are coprime.

We have seen that we can use De Moivre's theorem (11.2) to raise a complex number to an integer power, or even a rational power. Is it possible to use

this formula to raise a complex number to any real number, or even raise a number to a *complex* power?

In most fields, raising an element to the power of an *element* is absurd. Even in the real number system we will discover that we must utilize the exponential function  $e^x$  to compute quantities such as  $2^{\sqrt{2}}$ . We use that fact that  $2 = e^{\ln 2}$ , and so

$$2^{\sqrt{2}} = (e^{\ln 2})^{\sqrt{2}} = e^{(\ln 2)\sqrt{2}}.$$

The key algebraic property of the exponential function is that

$$e^{x+y} = e^x \cdot e^y \quad \text{for all } x, y \in \mathbb{R}.$$

This indicates that the exponential function is a *group* homomorphism mapping the additive group of real numbers to the multiplicative group of real numbers. This homomorphism enables us to consider raising an element of the real numbers to the power of an *element*.

Can we extend the exponential function into a group homomorphism from the additive structure of  $\mathbb{C}$  (denoted  $\mathbb{C}^+$ ), to the multiplicative structure  $\mathbb{C}^*$ ? If such a group homomorphism exists, then

$$e^{a+bi} = e^a \cdot e^{bi} = e^a \cdot (e^i)^b.$$

*SageMath* indicates that the value of  $e^i$  is  $(\cos 1 + i \sin 1)$ . Problems 1 through 3 show three ways of proving this, all involving calculus. There is in fact no way to prove that  $e^i = \cos 1 + i \sin 1$  without calculus. But given that this is true, we then have by De Moivre's theorem (11.2) that

$$e^{a+bi} = e^a \cdot (e^i)^b = e^a \cdot (\cos b + i \sin b)$$

whenever  $b$  is an integer. We will define this as the exponential function for all complex numbers. Notice that radian measure must be used in this formula.

### PROPOSITION 11.6

For  $z = a + bi$ , the function

$$f(z) = e^a \cdot (\cos b + i \sin b)$$

defines a group homomorphism from  $\mathbb{C}^+$  to  $\mathbb{C}^*$ , which is an extension of the standard exponential function. This function is called the complex exponential function and is also denoted  $e^z$ .

PROOF: If  $z_1 = a_1 + b_1i$ , and  $z_2 = a_2 + b_2i$ , we observe that

$$f(z_1 + z_2) = e^{a_1+a_2}(\cos(b_1 + b_2) + i \sin(b_1 + b_2)).$$

By Lemma 11.7, this equals

$$e^{a_1}(\cos(b_1) + i \sin(b_1)) \cdot e^{a_2}(\cos(b_2) + i \sin(b_2)) = f(z_1) \cdot f(z_2).$$

Thus,  $f$  is a group homomorphism from  $\mathbb{C}^+$  to  $\mathbb{C}^*$ . □

This allows us another way of expressing  $\omega_n$ . Notice that

$$e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) = \omega_n.$$

So we now have a more succinct way of defining the  $n^{\text{th}}$  root of 1.

The real exponential function is one-to-one, but is not onto since there is no number for which  $e^x = -1$ . However, the complex exponential function *is* onto, since for every nonzero complex number in polar form,  $z = r(\cos\theta + i \sin\theta)$ , there is a complex number whose exponential is  $z$ , namely  $\ln(r) + i\theta$ . The drawback of the complex exponential function is that it is *not* one-to-one! The kernel of this homomorphism is the set

$$N = f^{-1}(1) = \{2k\pi i \mid k \in \mathbb{Z}\}.$$

**DEFINITION 11.7** For any nonzero complex number  $z$ , we define the *complex logarithm* of  $z$ , denoted  $\log(z)$ , to be the set of elements  $x$  such that  $e^x = z$ .

Notice that we use the function  $\ln(x)$  to denote the *real* logarithm, while we use  $\log(z)$  to denote the complex logarithm. We have already observed that when  $z$  is written in polar form,  $z = r(\cos\theta + i \sin\theta)$ , that one value of  $x$  that satisfies the equation is  $x = \ln(r) + i\theta$ . We also know that  $f^{-1}(z)$  will be a coset of the kernel of  $f$ . Thus, we have  $\log(z) = \ln(r) + i\theta + N$ .

For example,  $\log(-1)$  is the set

$$\{\pi i + 2k\pi i \mid k \in \mathbb{Z}\} = \{\dots, -5\pi i, -3\pi i, -\pi i, \pi i, 3\pi i, 5\pi i, \dots\}.$$

The *SageMath* **log** function works for complex numbers, but only gives one element of the set. Thus, we must add the kernel  $N$  to this result to obtain the set given by  $\log(z)$ .

To help visualize the complex logarithm, we can graph the complex part of  $\log(x + iy)$ , but since this gives multiple values for each input value, we get a surface that resembles a parking garage or a spiral staircase. See [Figure 11.3](#).

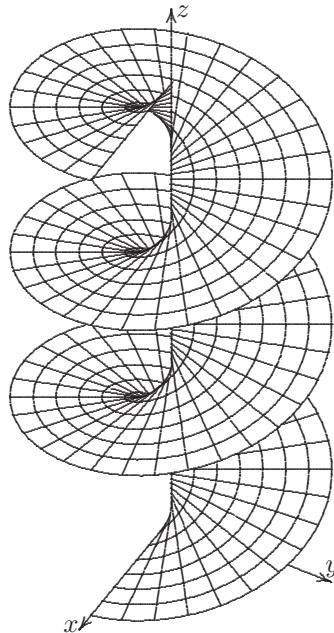
We can now define a complex number raised to a complex power, by saying

$$x^z = (e^{\log(x)})^z = e^{z \cdot \log(x)}.$$

Notice that this gives a *set* of numbers, not just a single number. Although there will at times be an infinite number of elements in the set  $x^z$ , this will not always be the case.

### PROPOSITION 11.7

For each integer  $n > 0$ , and any nonzero complex number  $z$ , then there are exactly  $n$  values for  $z^{(1/n)}$ . Thus, there are exactly  $n$  solutions for  $x$  to the equation  $x^n = z$ .



**FIGURE 11.3:** Imaginary portion of the complex logarithm function

PROOF: Let  $z$  have the polar form

$$z = r(\cos \theta + i \sin \theta).$$

Then  $\log(z)$  is the set

$$\{\ln(r) + \theta i + 2k\pi i \mid k \in \mathbb{Z}\}.$$

Thus,  $\log(z)/n$  is given by the set

$$\left\{ \frac{\ln(r)}{n} + \frac{(\theta + 2k\pi)i}{n} \mid k \in \mathbb{Z} \right\}.$$

Thus, the exponential function of the elements of this set is given by

$$\begin{aligned} & \left\{ e^{(\ln(r)/n} \cdot \left( \cos \left( \frac{(\theta + 2k\pi)}{n} \right) + i \sin \left( \frac{(\theta + 2k\pi)}{n} \right) \right) \mid k \in \mathbb{Z} \right\} \\ &= \left\{ r^{(1/n)} \cdot \left( \cos \left( \frac{(\theta + 2k\pi)}{n} \right) + i \sin \left( \frac{(\theta + 2k\pi)}{n} \right) \right) \mid k \in \mathbb{Z} \right\}. \end{aligned}$$

Notice that for two different values of  $k$  that differ by  $n$ , the arguments of the cosine and sine will differ by  $2\pi$ . Hence, we only have to consider the values of  $k$  from 0 to  $(n - 1)$ . This gives us the set

$$\left\{ r^{(1/n)} \cdot \left( \cos \left( \frac{(\theta + 2k\pi)}{n} \right) + i \sin \left( \frac{(\theta + 2k\pi)}{n} \right) \right) \mid k = 0, 1, 2, \dots, n - 1 \right\}.$$

However, these  $n$  solutions will have arguments that differ by less than  $2\pi$  so these  $n$  solutions are distinct.

Finally, we must show that  $x$  is an element of  $z^{(1/n)}$  if, and only if,  $x$  solves the equation  $x^n = z$ . But for any element in the above expression, we have that

$$\begin{aligned}x^n &= r^{n(1/n)} \cdot \left( \cos\left(\frac{n(\theta + 2k\pi)}{n}\right) + i \sin\left(\frac{n(\theta + 2k\pi)}{n}\right)\right) \\&= r(\cos \theta + i \sin \theta) = z.\end{aligned}$$

Likewise, if  $x^n = z$ , we can raise both sides to the  $(1/n)^{\text{th}}$  power to get that the two sets  $(x^n)^{(1/n)}$  and  $z^{(1/n)}$  are equal. Since the element  $x$  is certainly in the first set, it must also be in the set  $z^{(1/n)}$  that we have just computed.  $\blacksquare$

This last proposition is very useful for finding square roots and cube roots of complex numbers. This turns out to have some important applications in finding the roots of real polynomials! In fact, complex numbers and the functions we have defined in this section have many applications in the real world. The complex exponential function was fundamental to the invention of the short wave radio. The complex logarithm can be used in solving real valued differential equations. So even though these numbers are labeled “imaginary,” they are by no means just a figment of someone’s imagination.

### Problems for §11.3

- 1** Assume that the Taylor series for the exponential function

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \cdots$$

is valid for complex numbers as well as for real numbers. Prove that  $e^i = (\cos 1 + i \sin 1)$ .

Hint: Recall the Taylor series for  $\sin(x)$  and  $\cos(x)$ .

- 2** Suppose we can write  $e^{ix} = u(x) + iv(x)$ , where  $u(x)$  and  $v(x)$  are real functions of a real variable  $x$ . If we assume that

$$\frac{d}{dx} e^{ix} = u'(x) + iv'(x) = ie^{ix},$$

use differential equations to prove that  $u(x) = \cos(x)$  and  $v(x) = \sin(x)$ .

Hint: Since  $e^0 = 1$ , we know that  $u(0) = 1$  and  $v(0) = 0$ .

- 3** Assume that the limit from calculus

$$e^x = \lim_{n \rightarrow \infty} \left(1 + \frac{x}{n}\right)^n$$

is valid for complex values of  $x$  as well as real values. Prove that  $e^i = (\cos 1 + i \sin 1)$ .

Hint: Convert  $(1 + i/n)$  into polar form using an arctangent.

- 4** Find all possible values of  $\log(-1)$ .
- 5** Find all possible values of  $\log(\sqrt{3} - i)$ .
- 6** Find all possible values of  $1^{1/6}$ .
- 7** Find all complex solutions to the equation  $z^4 + 1 = 0$ .
- 8** Find all complex solutions to the equation  $z^3 + 8 = 0$
- 9** Find all possible values of  $(8i)^{1/3}$ .
- 10** Find five values of the expression  $i^i$ .
- 11** Find five values of the expression  $(-i)^{(i/2)}$ .
- 12** Show that when  $x$  and  $y$  are both complex, the set of all values of the expression  $x^y$  forms a geometric sequence:
- $$\{\dots, a \cdot r^{-3}, a \cdot r^{-2}, a \cdot r^{-1}, a, a \cdot r, a \cdot r^2, a \cdot r^3, \dots\}.$$
- 13** Find complex numbers  $x$  and  $y$  such that the set of values for  $x^y$  are the powers of 2:
- $$\{\dots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \dots\}.$$
- (See Problem 12. There will be more than one solution to this problem.)
- 14** Show that for a fixed  $n$ , the set of all  $n^{\text{th}}$  roots of 1 forms a group with respect to multiplication.
- 15** Prove that the group in exercise 14 is cyclic, with

$$\omega_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

as a generator. Show that any generator of this group is a primitive  $n^{\text{th}}$  root of unity.

- 16** Prove or disprove: For all complex numbers  $x$ ,  $y$ , and  $z$ ,

$$(x^z) \cdot (y^z) = (x \cdot y)^z.$$

Note:  $x^z$  and  $y^z$  may both represent *sets* of complex numbers, so the left-hand side of this equation is the set of all possible products formed.

- 17** Prove or disprove: For all complex numbers  $x$ ,  $y$ , and  $z$ ,

$$(z^x)^y = z^{(x \cdot y)}.$$

(See the note on Problem 16.)

- 18** Prove or disprove: For all complex numbers  $x$ ,  $y$ , and  $z$ ,

$$(z^x) \cdot (z^y) = z^{(x+y)}.$$

(See the note on Problem 16.)

#### Interactive Problems

- 19** Find the twelfth roots of unity, and arrange them in such a way that the circle graph puts the elements in the correct place in the complex plane, as was done in Example 11.3.
- 20** Use *SageMath* to plot the real part of  $\log(x + iy)$ , the companion of [Figure 11.3](#). Would this surface be multi-valued, as was [Figure 11.3](#)?

---

# **Answers to Odd-Numbered Problems**

## **Section 1.1**

- 1)  $q = 7, r = 4$
- 3)  $q = -19, r = 20$
- 5)  $q = 194, r = 2$
- 7)  $q = 0, r = 37$
- 9)  $q = 0, r = 0$
- 11) Since  $b = ad$  and  $c = be$  for some integers  $d$  and  $e$ ,  $c = a(de)$  is a multiple of  $a$ .
- 13) Since  $b = ad$  and  $c = ae$  for some integers  $d$  and  $e$ ,  $b - c = a(d - e)$  is a multiple of  $a$ .
- 15) Since  $b = ac$  and  $a = bd$  for some integers  $c$  and  $d$ ,  $a = acd$ , so  $cd = 1$ . This can only happen if  $c$  and  $d$  are  $\pm 1$ .
- 17) Since  $bc = ad$  for some integer  $d$ , and by Bézout's lemma,  $\gcd(a, b) = 1 = ua + vb$  for some integers  $u$  and  $v$ , we find  $c = c(ua + vb) = a(cu + vd)$  is a multiple of  $a$ .
- 19)  $(-1) \cdot 84 + 2 \cdot 48 = 12$ .
- 21)  $4 \cdot 84 + (-5) \cdot 66 = 6$ .
- 23)  $(-34) \cdot 827 + 273 \cdot 103 = 1$ .
- 25)  $(-2) \cdot (-602) + (-5) \cdot 238 = 14$ .
- 27)  $0 \cdot 0 + 1 \cdot 9 = 9$ .
- 29) Since  $xy$  is a common multiple, by the well-ordering axiom there is a least common multiple, say  $z = ax = by$ . Note that  $\gcd(a, b) = 1$ , else we can divide by  $\gcd(a, b)$  to produce an even smaller common multiple. Then there is a  $u$  and  $v$  such that  $ua + vb = 1$ , so  $uaxy + vbxy = xy$ , hence  $z(uy + vx) = xy$ .
- 31) Let  $t = \gcd(x, y)$ . First find  $r$  and  $s$  so that  $xr + ys = t = \gcd(x, y)$ . Then find  $a$  and  $w$  such that  $at + wz = \gcd(t, z) = 1$ . Then  $a(xr + ys) + wz = 1$ , so let  $u = ar$  and  $v = as$ .
- 33)  $2 \cdot 3 \cdot 23 \cdot 29$ .
- 35)  $11 \cdot 29 \cdot 31$ .
- 37)  $3 \cdot 17^2 \cdot 101$ .
- 39)  $u = -222222223, v = 1777777788$ .
- 41)  $3^4 \cdot 37^2 \cdot 333667^2$ .

## **Section 1.2**

- 1)  $\{e, n, o, r, t, x, y\}$ .
- 3) a) Not one-to-one,  $f(-1) = f(1) = 1$ . b) Not onto,  $f(x) \neq -1$ .
- 5) a) One-to-one,  $x^3 = y^3 \Rightarrow x = y$ . b) Onto,  $f(\sqrt[3]{y}) = y$ .

- 7) a) Not one-to-one,  $f(0) = f(2) = 0$ . b) Not onto,  $f(x) \neq -2$ , since  $x^2 - 2x + 2$  has complex roots.
- 9) a) One-to-one, if  $x$  even,  $y$  odd, then  $y = x + 1/2$ . b) Not onto,  $f(x) \neq 3$ .
- 11) a) One-to-one, if  $x$  even,  $y$  odd, then  $x = 2y - 1$  is odd. b) Not onto,  $f(x) \neq 4$ .
- 13) a) Not one-to-one  $f(0) = f(3) = 1$ . b) Onto, either  $f(2y - 2) = y$  or  $f(2y + 1) = y$ .
- 15) If  $2x^2 + x = 2y^2 + y = c$ , then  $x$  and  $y = (-1 \pm \sqrt{1+8c})/4$ . If  $x \neq y$ , then  $|x - y| = \sqrt{1+8c}/2$ , which is never an integer when  $c$  is an integer.
- 17)  $2^n = 2 \cdot 2^{n-1} < 2(n-1)! < n(n-1)! = n!$
- 19) If  $(n-1)^3 + 2(n-1) = 3k$ , then  $n^2 + 2n = 3(k+n^2+n+1)$
- 21) If  $6^{n-1} + 4 = 20k$ , then  $6^n + 4 = 20(6k-1)$
- 23)  $(n-1)((n-1)+1)/2 + n = n(n+1)/2$ .
- 25)  $(n-1)((n-1)+1)(2(n-1)+1)/6 + n^2 = n(n+1)(2n+1)/6$ .
- 27)  $(n-1)((n-1)+1)((n-1)+2)/3 + n(n+1) = n(n+1)(n+2)/3$ .
- 29) Suppose  $f$  were one-to-one, and let  $\tilde{B} = f(A)$ , so that  $\tilde{f} : A \rightarrow \tilde{B}$  would be a bijection. By lemma 1.6,  $|A| = |\tilde{B}|$ , but  $|\tilde{B}| \leq |B| < |A|$ .
- 31) Suppose  $f$  were not one-to-one. Then there is a case where  $f(a_1) = f(a_2)$ , and we can consider the set  $\tilde{A} = A - \{a_1\}$ , and the function  $\tilde{f} : \tilde{A} \rightarrow B$  would still be onto. But  $|\tilde{A}| < |B|$  so by Problem 30  $\tilde{f}$  cannot be onto. Hence,  $f$  is one-to-one.
- 33)  $x^4 + 2x^2$ .
- 35)  $x^3 - x^2 - x + 1$ .
- 37)  $f(x) = \begin{cases} 3x + 14 & \text{if } x \text{ is even,} \\ 6x + 2 & \text{if } x \text{ is odd.} \end{cases}$
- 39) If  $f(g(x)) = f(g(y))$ , then since  $f$  is one-to-one,  $g(x) = g(y)$ . Since  $g$  is onto,  $x = y$ .
- 41) There is some  $c \in C$  such that  $f(y) \neq c$  for all  $y \in B$ . Then  $f(g(x)) \neq c$  since  $g(x) \in B$ .
- 43) If  $x$  even and  $y$  odd,  $f(x) = f(y)$  means  $y = x + 8$  is even. Onto is proven by finding the inverse:  $f(x) = \begin{cases} x + 3 & \text{if } x \text{ is even,} \\ x - 5 & \text{if } x \text{ is odd.} \end{cases}$
- 45)  $f(x)$  is both one-to-one and onto.

### Section 1.3

- 1) a) Commutative. b) Associative,  $(a * b) * c = a * (b * c) = a + b + c - 2$ .
- 3) a) Not commutative,  $b \neq a$ . b) Associative,  $(a * b) * c = a * (b * c) = c$ .
- 5) a) Not commutative,  $a - b \neq b - a$ . b) Not associative,  $(a * b) * c = a - b - c$ ,  $a * (b * c) = a - b + c$ .
- 7) a) Commutative. b) Associative,  $(a * b) * c = a * (b * c) = abc + 2ab + 2ac + 2bc + 4a + 4b + 4c + 6$ .
- 9)  $(a * b) * c = a * (b * c) = \gcd(a, b, c)$ , since any number that divides  $a$ ,  $b$ , and  $c$  must also divide  $\gcd(\gcd(a, b), c)$  and  $\gcd(a, \gcd(b, c))$ .
- 11) Not associative, for example  $(2 * (-2)) * 3 = 0 * 3 = 0$ , but  $2 * ((-2) * 3) = 2 * 1 = 3$ .

13)

|   | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 1 | 2 | 3 | 4 |
| 3 | 0 | 1 | 2 | 3 | 4 |
| 4 | 0 | 1 | 2 | 3 | 4 |

15)

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 2 | 3 | 4 | 5 |
| 3 | 3 | 3 | 3 | 4 | 5 |
| 4 | 4 | 4 | 4 | 4 | 5 |
| 5 | 5 | 5 | 5 | 5 | 5 |

17)

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 1 | 2 | 1 | 2 |
| 3 | 1 | 1 | 3 | 1 | 1 | 3 |
| 4 | 1 | 2 | 1 | 4 | 1 | 2 |
| 5 | 1 | 1 | 1 | 1 | 5 | 1 |
| 6 | 1 | 2 | 3 | 2 | 1 | 6 |

19)

|   | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 2 | 2 | 1 | 0 | 0 | 0 | 0 |
| 3 | 3 | 2 | 1 | 0 | 0 | 0 |
| 4 | 4 | 3 | 2 | 1 | 0 | 0 |
| 5 | 5 | 4 | 3 | 2 | 1 | 0 |

- 21)  $(f * g) * h = f * (g * h)$  = the function sending  $x$  to  $f(g(h(x)))$ .
- 23) If  $l$  were a left identity and  $r$  were a right identity, then  $l = l * r = r$ .
- 25) If  $e$  were an identity, then  $\min(x, e) = x$  for all  $x$ , meaning  $e \geq x$  for all  $x$ . But there is no greatest integer.
- 27) No.  $1 - 1 = 0 \notin S$ .
- 29) Yes.
- 31) No.  $1/2 = .5 \notin S$ .
- 33) Not commutative,  $(2 * 4 = 2$ , but  $4 * 2 = 4$ ). It is associative,  $(x * y) * z$  and  $x * (y * z)$  both give the first number in the list  $\{x, y, z\}$  which is even, giving the last number if they are all odd.
- 35) No,  $A * B \neq B * A$ .

### Section 1.4

1) 20

3) 92

5) 10

7) 9

9) 5

11) 13

13) Since  $10^n \bmod 9 = 1^n \bmod 9 = 1$ , we find that

$$a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \cdots + 10^m a_m \bmod 9 = a_0 + a_1 + a_2 + \cdots + a_m \bmod 9.$$

15) 107

17) 187

19) 631

21) 4073

23) 7906

25) 11008

27) 8

29) 7

31) 16

33) 30

35) 35

37) 67

39) 376459425

41) 620871478602893110807886503707

43) 705249263948099118

### Section 1.5

1)  $\{0, 1, \frac{1}{2}, 2, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, 3, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, 4\}.$ 3) If  $a_n = b_n/b_{n+1}$ , then  $[a_n] = (b_n - (b_n \bmod b_{n+1}))/b_{n+1}$ . Then  $1/a_{n+1} = (b_{n+1} + 2(b_n - (b_n \bmod b_{n+1})) - b_n)/b_{n+1}$ . This simplifies to give  $a_{n+1} = b_{n+1}/(b_n + b_{n+1} - 2(b_n \bmod b_{n+1}))$ . Hence,  $b_{n+2} = b_n + b_{n+1} - 2(b_n \bmod b_{n+1})$ .5)  $a_{2n} = b_{2n}/b_{2n+1} = b_n/(b_n + b_{n+1}) = (b_n/b_{n+1})/((b_n/b_{n+1}) + 1) = a_n/(a_n + 1)$ .7) Let  $x = p/q$  be a rational number, and assume the statement is true for smaller  $p+q$ . If  $x \geq 1$ , then  $a_m = x - 1$  for some  $m$ , and  $a_{2m+1} = x$ . If  $x < 1$ , then  $a_m = x/(1-x)$  for some  $m$ , and  $a_{2m} = x$ .9) Because  $a_i$  can only be one of  $q$  possible integers for  $i > 0$ , at some point we must have  $a_i = a_j$ . Because  $a_{n+1}$  is determined solely on  $a_n$ ,  $a_{2i-j} = a_i$ , and the sequence will repeat from this point on.11)  $x = n.d_1d_2\dots d_1 + 10^{-i} \cdot 0.d_{i+1}d_{i+2}\dots d_{i+j} + 10^{-i-j} \cdot 0.d_{i+1}d_{i+2}\dots d_{i+j} + 10^{-i-2j} \cdot 0.d_{i+1}d_{i+2}\dots d_{i+j} + \dots$ . The series is geometric after the first term, so the sum is  $n.d_1d_2\dots d_1 + 10^{-i} \cdot 0.d_{i+1}d_{i+2}\dots d_{i+j}/(1 - 10^{-j})$ , which is rational.13) If  $p^3/q^3 = 2$  with  $p$  and  $q$  coprime, then  $2|p$ , but replacing  $p = 2r$  shows  $2|q$  too.15) If  $p^2/q^2 = 6$  with  $p$  and  $q$  coprime, then  $2|p$ , but replacing  $p = 2r$  shows  $2|q$  too.

- 17) If  $p^2/q^2 = 15$  with  $p$  and  $q$  coprime, then  $3|p$ , but replacing  $p = 3r$  shows  $3|q$  too.
- 19) If  $p^3/q^3 = 4$  with  $p$  and  $q$  coprime, then  $2|p$ , but replacing  $p = 2r$  shows  $2|q$  too.
- 21) If  $a + b$  were rational, and  $a$  was rational, then  $b = (a + b) - a$  would be rational.
- 23) If  $a \cdot b$  were rational, and  $a$  was rational and nonzero, then  $b = (a \cdot b)/a$  would be rational.
- 25) If  $\log_2(3) = p/q$  were rational, then  $2^{p/q} = 3$ , making  $2^p = 3^q$ . But  $2^p$  is even, and  $3^q$  is odd.
- 27)  $2 - \sqrt{2}$  and  $\sqrt{2}$  are both irrational, but the sum is 2.
- 29)  $a_2 = \sqrt{3} + 3$ ,  $a_{18} = \sqrt{3} + 6$ ,  $a_{146} = \sqrt{3} + 9$ .

## Section 2.1

- 1) 8 steps: Stay, RotLft, RotRt, Rot180, Flip (along horizontal axis), Spin (along vertical axis), FlipLft (exchanges NE and SW corners), and FlipRt.

|         | Stay    | RotLft  | Rot180  | RotRt   | Flip    | Spin    | FlipLft | FlipRt  |
|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| Stay    | Stay    | RotLft  | Rot180  | RotRt   | Flip    | Spin    | FlipLft | FlipRt  |
| RotLft  | RotLft  | Rot180  | RotRt   | Stay    | FlipLft | FlipRt  | Spin    | Flip    |
| Rot180  | Rot180  | RotRt   | Stay    | RotLft  | Spin    | Flip    | FlipRt  | FlipLft |
| RotRt   | RotRt   | Stay    | RotLft  | Rot180  | FlipRt  | FlipLft | Flip    | Spin    |
| Flip    | Flip    | FlipRt  | Spin    | FlipLft | Stay    | Rot180  | RotRt   | RotLft  |
| Spin    | Spin    | FlipLft | Flip    | FlipRt  | Rot180  | Stay    | RotLft  | RotRt   |
| FlipLft | FlipLft | Flip    | FlipRt  | Spin    | RotLft  | RotRt   | Stay    | Rot180  |
| FlipRt  | FlipRt  | Spin    | FlipLft | Flip    | RotRt   | RotLft  | Rot180  | Stay    |

- 3)  $e = e * e' = e'$ , so  $e = e'$ .
- 5) If  $a * b = a * c$ , then  $a^{-1} * (a * b) = a^{-1} * (a * c)$ , so  $b = c$ .
- 7) 50% (18 of 36).
- 9) After a flip and a rotation, Terry will be facing the opposite direction, so it would be a flip.
- 11)  $(\text{FlipRt} * \text{Spin})^{-1} \neq \text{FlipRt} * \text{Spin}$ .
- 13) Stay = FlipRt\*FlipRt, RotRt = FlipRt\*FlipLft, RotLft = FlipLft\*FlipRt, Spin = FlipRt\*FlipLft\*FlipRt.
- 15) Such a routine is impossible, since it involves three flips. See Problem 8.

## Section 2.2

- 1) 4.  
3) 19.  
5) 27.  
7) 40.

9)

|   | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

11)

|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

13)

|    | 0  | 2  | 4  | 6  | 8  | 10 |
|----|----|----|----|----|----|----|
| 0  | 0  | 2  | 4  | 6  | 8  | 10 |
| 2  | 2  | 4  | 6  | 8  | 10 | 0  |
| 4  | 4  | 6  | 8  | 10 | 0  | 2  |
| 6  | 6  | 8  | 10 | 0  | 2  | 4  |
| 8  | 8  | 10 | 0  | 2  | 4  | 6  |
| 10 | 10 | 0  | 2  | 4  | 6  | 8  |

15)

|   | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

17)

|    | 1  | 5  | 7  | 11 |
|----|----|----|----|----|
| 1  | 1  | 5  | 7  | 11 |
| 5  | 5  | 1  | 11 | 7  |
| 7  | 7  | 11 | 1  | 5  |
| 11 | 11 | 7  | 5  | 1  |

19)

|    | 1  | 5  | 7  | 11 | 13 | 17 |
|----|----|----|----|----|----|----|
| 1  | 1  | 5  | 7  | 11 | 13 | 17 |
| 5  | 5  | 7  | 17 | 1  | 11 | 13 |
| 7  | 7  | 17 | 13 | 5  | 1  | 11 |
| 11 | 11 | 1  | 5  | 13 | 17 | 7  |
| 13 | 13 | 11 | 1  | 17 | 7  | 5  |
| 17 | 17 | 13 | 11 | 7  | 5  | 1  |

21) Define  $x \sim y$  if  $x$  and  $y$  belong to the same subset.

- 23) 7.  
 25) 19.  
 27) 3.  
 29) 667.  
 31) 1543.  
 33) 11077.  
 35)  $n = 5, 8$ , or 12.

### Section 2.3

- 1)  $(a \cdot a) \cdot b \neq a \cdot (a \cdot b)$ .  
 3) Yes, this is a group.  
 5) 0 has no inverse.  
 7) Not closed.  
 9) Yes, this is a group.  
 11) 3 has no inverse.  
 13) Yes, this is a group.  
 15) Note that  $y$  has an inverse,  $z$ , so that  $y \cdot z = e$ . But then  $x = x \cdot (y \cdot z) = (x \cdot y) \cdot z = z$ , so  $y \cdot x = e$ .  
 17) If both  $x \cdot y_1$  and  $x \cdot y_2 = e$ , then by Problem 15,  $y_2 \cdot x = e$ , so  $y_2 = y_2 \cdot (x \cdot y_1) = (y_2 \cdot x) \cdot y_1 = y_1$ .  
 19)  $a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y)$ , so  $x = y$ .  
 21) If  $(a \cdot b)^2 = a^2 \cdot b^2$ , then  $a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$ , so  $(a^{-1} \cdot a) \cdot b \cdot a \cdot (b \cdot b^{-1}) = (a^{-1} \cdot a) \cdot a \cdot b \cdot (b \cdot b^{-1})$  giving  $b \cdot a = a \cdot b$ .  
 23) When  $n = 1$ , we have  $a \cdot b = a \cdot e \cdot b$ , which is true. Assuming true for previous  $n$ ,  $(a \cdot b)^n = (a \cdot b)^{n-1} \cdot (a \cdot b) = a \cdot (b \cdot a)^{n-2} \cdot b \cdot a \cdot b = a \cdot (b \cdot a)^{n-1} \cdot b$ .  
 25) When  $n = 1$ , we have  $a \cdot b \cdot a^{-1} = a \cdot b \cdot a^{-1}$ , which is true. Assuming true for previous  $n$ ,  $(a \cdot b \cdot a^{-1})^n = (a \cdot b \cdot a^{-1})^{n-1} \cdot (a \cdot b \cdot a^{-1}) = a \cdot b^{n-1} \cdot a^{-1} \cdot a \cdot b \cdot a^{-1} = a \cdot b^{n-1} \cdot b \cdot a^{-1} = a \cdot b^n \cdot a^{-1}$ .  
 27) If  $a^3 = e$ , then  $(a^{-1})^3 = e$ . Furthermore, if  $a \neq e$ , then  $a^{-1} \neq a$ . So the non-identity solutions pair off, and with the identity we have an odd number of solutions.

- 29)
- | .   | $a$ | $b$ | $c$ | $d$ |
|-----|-----|-----|-----|-----|
| $a$ | $b$ | $a$ | $d$ | $c$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $d$ | $c$ | $a$ | $b$ |
| $d$ | $c$ | $d$ | $b$ | $a$ |

31)

| .   | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $a$ | $b$ | $g$ | $d$ | $f$ | $a$ | $h$ | $e$ | $c$ |
| $b$ | $g$ | $e$ | $f$ | $h$ | $b$ | $c$ | $a$ | $d$ |
| $c$ | $h$ | $f$ | $b$ | $a$ | $c$ | $e$ | $d$ | $g$ |
| $d$ | $c$ | $h$ | $g$ | $b$ | $d$ | $a$ | $f$ | $e$ |
| $e$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| $f$ | $d$ | $c$ | $e$ | $g$ | $f$ | $b$ | $h$ | $a$ |
| $g$ | $e$ | $a$ | $h$ | $c$ | $g$ | $d$ | $b$ | $f$ |
| $h$ | $f$ | $d$ | $a$ | $e$ | $h$ | $g$ | $c$ | $b$ |

- 33)  $18 \rightarrow 6$ ,  $54 \rightarrow 18$ ,  $162 \rightarrow 54$ ,  $486 \rightarrow 162$ ,  $50 \rightarrow 20$ ,  $250 \rightarrow 100$ ,  $98 \rightarrow 42$ ,  $686 \rightarrow 294$ . Conjecture  $(p - 1)n/(2p)$ .

### Section 3.1

- 1) 1, 5, 7, and 11.
- 3) 1, 3, 5, 7, 9, 11, 13, and 15.
- 5) 2 and 5.
- 7) No generators
- 9) No generators
- 11) 5 and 11.
- 13) 32.
- 15) 240.
- 17) 480.
- 19) 1680.
- 21) If  $n$  has an odd prime factor  $p$ , then  $p - 1$  will be even. If  $n$  is  $2^q$  for some  $q > 1$ , then  $2^{q-1}$  is even. In all cases, there is an even factor in the formula for  $\phi(n)$ .
- 23) If  $g$  is a generator of  $G$ , and  $x, y \in G$ , then  $x = g^a$  and  $y = g^b$  for some  $a$  and  $b$ . Then  $x \cdot y = g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a = y \cdot x$ .
- 25) If  $(a \cdot b)^n = e$ , then  $a \cdot (b \cdot a)^n \cdot a^{-1} = e$ , so  $a \cdot (b \cdot a)^n = a$ , hence  $(b \cdot a)^n = e$ . Likewise, if  $(b \cdot a)^n = e$ , then  $(a \cdot b)^n = e$ . Thus, the smallest positive integer  $n$  for which  $(a \cdot b)^n = e$  is also the smallest positive integer for which  $(b \cdot a)^n = e$ .
- 27)  $(y \cdot x \cdot y^{-1})^2 = e$ , but  $y \cdot x \cdot y^{-1} \neq e$ , so  $y \cdot x \cdot y^{-1} = x$ .
- 29) Yes, 8 elements are generators: 2, 3, 8, 12, 13, 17, 22, and 23.
- 31)  $Z_n^*$  is cyclic if  $n$  is twice the power of an odd prime.

### Section 3.2

- 1) If  $b \cdot a = a \cdot b$ , then  $e = b^2 \cdot a^2 = b \cdot (b \cdot a) \cdot a = b \cdot a \cdot b \cdot a$ . If  $b \cdot a \cdot b \cdot a = e$ , then  $b \cdot a = b \cdot (b \cdot a \cdot b \cdot a) \cdot a = b^2 \cdot (a \cdot b) \cdot a^2 = a \cdot b$ .
- 3)  $b^3 \cdot a = b^2 \cdot (a^2 \cdot b) = b \cdot (a^2 \cdot b) \cdot a \cdot b = (a^2 \cdot b) \cdot a \cdot (a^2 \cdot b) \cdot b = a^2 \cdot (a^2 \cdot b) \cdot a^2 \cdot b^2 = a^4 \cdot (a^2 \cdot b) \cdot a \cdot b^2 = a^6 \cdot (a^2 \cdot b) \cdot b^2 = a^5 \cdot a^3 \cdot b^3 = a^3 \cdot b^3$ .
- 5)  $a \cdot b \cdot c^3$ .

- 7)  $a \cdot b$ .  
 9)  $b^2 \cdot c^3$ .  
 11)  $a \cdot c^3$ .  
 13)  $a \cdot c$ .  
 15)  $a \cdot b \cdot c$ .  
 17) There are 24 ways of rearranging four books.  
 19)

```
InitGroup("e")
AddGroupVar("a", "b", "c")
Define(a^2, e)
Define(b^2, e)
Define(c^3, e)
Define(b*a, a*b)
Define(c*a, b*c)
Define(c*b, a*b*c)
Group()
{e, a, b, a*b, c, a*c, b*c, a*b*c, c^2, a*c^2, b*c^2, a*b*c^2}
```

### Section 3.3

- 1)  $\{0\}$ ,  $\{0, 2, 4, 6, 8, 10\}$ ,  $\{0, 3, 6, 9\}$ ,  $\{0, 4, 8\}$ ,  $\{0, 6\}$ , and the whole group.  
 3)  $\{0\}$ ,  $\{0, 3, 6, 9, 12, 15, 18\}$ ,  $\{0, 7, 14\}$ , and the whole group.  
 5)  $\{1\}$ ,  $\{1, 3\}$ ,  $\{1, 5\}$ , and  $\{1, 7\}$ .  
 7)  $R_2(G) = 10$ ,  $R_3(G) = 9$ ,  $R_4(G) = 16$ , and  $R_6(G) = 18$ . For these examples,  $R_k(G)$  is a multiple of  $k$ .  
 9)  $R_9(G) = 9$ , and  $R_3(G) = 3$ , so six elements of order 9.  
 11) When  $n = k$ , an element is of order  $k$  if, and only if, it is a generator. If  $k$  is a divisor of  $n$ , and  $m$  is a divisor of  $k$ , then  $R_m(Z_k) = R_m(Z_n)$ . Thus, computing the elements of order  $k$  in both  $Z_k$  and  $Z_n$  will give the same results.  
 13) If  $g$  is a generator, than only  $g$  and  $g^{-1}$  have finite order.  
 15) If  $a$  and  $b$  are of finite order, then  $a^m = b^n = e$  for some  $m > 0$  and  $n > 0$ . Then  $(a \cdot b^{-1})^{mn} = e$ , so  $a \cdot b^{-1}$  is of finite order.  
 17) If  $x, y \in H$ , then  $x = a^n$  and  $y = b^n$  for some  $a, b \in G$ . Then  $x \cdot y^{-1} = a^n \cdot b^{-n} = (a \cdot b^{-1})^n$ , so  $x \cdot y^{-1}$  is in  $H$ .  
 19) Problem 18 shows  $H$  is a subgroup. If  $x = a^2 = b^2$ , then  $(a \cdot b^{-1})^2 = 1$  so  $b = a$  or  $b = a(p - 1)$ . Since  $x \mapsto x^2$  is two to one,  $H$  contains half the elements of  $Z_p^*$ .  
 21)  $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ .  
 23) The subgroup has 10 elements:  $\{e, a, a^2, a^3, a^4, b^2, a \cdot b^2, a^2 \cdot b^2, a^3 \cdot b^2, a^4 \cdot b^2\}$ .  
 25)  $f \cdot r \cdot b$  flips the top edge efficiently, and in the process cycles the remaining 5 edges, so this has order 30.

### Section 4.1

- 1)  $\{\{0, 5\}, \{1, 6\}, \{2, 7\}, \{3, 8\}, \{4, 9\}\}.$
- 3)  $\{\{0, 5, 10\}, \{1, 6, 11\}, \{2, 7, 12\}, \{3, 8, 13\}, \{4, 9, 14\}\}.$
- 5)  $\{\{1, 14\}, \{2, 13\}, \{4, 11\}, \{7, 8\}\}.$
- 7)  $\{\{1, 9\}, \{3, 11\}, \{5, 13\}, \{7, 15\}\}.$
- 9) Left cosets:  $\{\text{Stay, FlipRt}\}, \{\text{RotRt, Spin}\}, \{\text{RotLft, FlipLft}\}.$  Right cosets:  
 $\{\text{Stay, FlipRt}\}, \{\text{RotRt, FlipLft}\}, \{\text{RotLft, Spin}\}.$
- 11) 6.
- 13) 13.
- 15) 13.
- 17) 8.
- 19) 20.
- 21) 36.
- 23) Since  $(n - 1)^2 = 1$  in  $Z_n^*$ ,  $\{1, n - 1\}$  is a subgroup of order 2, so  $|Z_n^*|$  is even for  $n > 2$ .
- 25) Since  $y \in Hx$ ,  $y = hx$  for some  $h \in H$ , so  $Hy = H \cdot (hx) = (H \cdot h)x = Hx$ .
- 27) Possible orders are 1,  $p$ ,  $q$ , and  $pq$ , so a non-trivial subgroup either has order  $p$  or  $q$ . But any group of prime order is cyclic.
- 29)  $\{1\}, \{1, 2, 4, 8\}, \{1, 4, 7, 13\}, \{1, 4\}, \{1, 11\}, \{1, 14\}, \{1, 4, 11, 14\}$ , and the whole group.
- 31)  $\{1\}, \{1, 3, 7, 9\}, \{1, 9, 13, 17\}, \{1, 9\}, \{1, 11\}, \{1, 19\}, \{1, 9, 11, 19\}$ , and the whole group.
- 33) Left cosets:  $\{\{e, c^2, c, c^3\}, \{a, a \cdot c^2, a \cdot c, a \cdot c^3\}, \{b, b \cdot c^2, b \cdot c, b \cdot c^3\}, \{a \cdot b \cdot c, a \cdot b \cdot c^3, a \cdot b \cdot c^2\}, \{b^2, b^2 \cdot c, b^2 \cdot c^2, b^2 \cdot c^3\}\}, \{a \cdot b^2, a \cdot b^2 \cdot c, a \cdot b^2 \cdot c^2, a \cdot b^2 \cdot c^3\}\}.$   
Right cosets:  $\{\{e, c^2, c, c^3\}, \{a, a \cdot b \cdot c, b \cdot c^2, b^2 \cdot c^3\}, \{b, b^2 \cdot c, a \cdot c^2, a \cdot b \cdot c^3\}, \{a \cdot b^2 \cdot c^2, b \cdot c, a \cdot c \cdot b^2, a \cdot b \cdot c^3\}\}.$

### Section 4.2

- 1) 24, 28, 1, 0, 23, 9, 24, 11, 28
- 3) 5, 9, 0, 4, 24, 9, 8, 12, 26, 19
- 5) THIS IS EASY
- 7) MAKE IT SO
- 9) If  $n = pqr$ ,  $\phi(n) = (p - 1)(q - 1)(r - 1)$ . If  $x$  is coprime to  $n$ , use proposition 4.1, otherwise suppose  $x$  is a multiple of  $p$ , but not a multiple of  $qr$ . Then  $x^{rs} \equiv x \pmod{p}$ , and since  $rs \equiv 1 \pmod{(q - 1)(r - 1)}$ , proposition 4.2 shows that  $x^{rs} \equiv x \pmod{qr}$  as well. Finish with the Chinese remainder theorem (1.5).
- 11)  $f^{-1}(x) = x^{11} \pmod{51}.$
- 13)  $f^{-1}(x) = x^{29} \pmod{91}.$
- 15)  $f^{-1}(x) = x^{131} \pmod{217}.$
- 17)  $f^{-1}(x) = x^{103} \pmod{1001}.$
- 19) 1835, 1628, 1084. Inverse =  $x^{157} \pmod{2773}.$

- 21) **PowerMod(c, 10007, n)** should give 2.  
 23) Answers will vary.  
 25) “The repeating 037’s and 740’s in your n made it easy to factor.”

### Section 4.3

- 1) Since  $e \in H$ ,  $H = e \cdot H \subseteq H \cdot H$ . But  $H$  is closed with respect to multiplication, so  $H \cdot H \subseteq H$ .
- 3) Since  $e \in H$ ,  $a \in a \cdot H$ , so  $a \in H \cdot b$ . But  $a \in H \cdot a$  as well, so  $H \cdot b = H \cdot a$ , hence  $a \cdot H = H \cdot a$ .
- 5) Any element of  $h \in H$  is also in  $G$ , so  $h \cdot n \cdot h^{-1} \in N$ .
- 7) Three possible answers:  $\{e, c^2\}$ ,  $\{e, a \cdot b^2 \cdot c\}$ , or  $\{e, a \cdot b^2 \cdot c^3\}$ .
- 9) If  $g \in G$  and  $h \in Z$ , then  $g \cdot h \cdot g^{-1} = h \cdot g \cdot g^{-1} = h \in Z$ .
- 11) Let  $a$  be a generator of  $H$ , and let  $m$  be the smallest positive integer for which  $a^m \in K$ . For a given  $g \in G$ ,  $g \cdot a \cdot g^{-1} \in H$ , so  $g \cdot a \cdot g^{-1} = a^n$  for some  $n$ . Then for  $a^{sm} \in K$ ,  $g \cdot a^{sm} \cdot g^{-1} = (a \cdot a \cdot g^{-1})^{sm} = (a^n)^{sm} = (a^m)^{sn} \in K$ .
- 13) Let  $f(x) = mx + b \in G$ , and  $t(x) = qx \in T$ , so  $f^{-1}(x) = (x - b)/m$ . Then  $(f \cdot t \cdot f^{-1})(x) = f^{-1}(t(f(x))) = qx + (qb - b)/m \notin T$ . If  $f(x) = 2x + 3$ , then  $fT$  is the set of functions  $k(2x + 3)$ , whereas  $Tf$  is the set of functions  $kx + 3$ .
- 15) If  $g_1 = h_1 \cdot k_1$  and  $g_2 = h_2 \cdot k_2$ , then  $g_1 \cdot g_2^{-1} = h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1} = (h_1 \cdot h_2^{-1}) \cdot (h_2 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1}) \in H \cdot K$ , since  $K$  is normal.
- 17)  $g \cdot H \cdot K \cdot g^{-1} = (g \cdot H \cdot g^{-1}) \cdot (g \cdot K \cdot g^{-1}) = H \cdot K$ .
- 19) Subgroups are  $\{e\}$ , with cosets  $\{e\}$ ,  $\{a\}$ ,  $\{a^2\}$ ,  $\{a^3\}$ ,  $\{b\}$ ,  $\{a \cdot b\}$ ,  $\{a^2 \cdot b\}$ , and  $\{a^3 \cdot b\}$ ;  $\{e, a^2\}$ , with cosets  $\{e, a^2\}$ ,  $\{a, a^3\}$ ,  $\{b, a^2 \cdot b\}$ , and  $\{a \cdot b, a^3 \cdot b\}$ ;  $\{e, a, a^2, a^3\}$ , with cosets  $\{e, a, a^2, a^3\}$  and  $\{b, a \cdot b, a^2 \cdot b, a^3 \cdot b\}$ ;  $\{e, b, a^2, a^2 \cdot b\}$ , with cosets  $\{e, b, a^2, a^2 \cdot b\}$  and  $\{a, a \cdot b, a^3, a^3 \cdot b\}$ ;  $\{e, a \cdot b, a^2, a^3 \cdot b\}$ , with cosets  $\{e, a \cdot b, a^2, a^3 \cdot b\}$  and  $\{a, b, a^2 \cdot b, a^3\}$ ; and the whole group, with one coset containing the whole group.

### Section 4.4

1)

|            | $\{0, 5\}$ | $\{1, 6\}$ | $\{2, 7\}$ | $\{3, 8\}$ | $\{4, 9\}$ |
|------------|------------|------------|------------|------------|------------|
| $\{0, 5\}$ | $\{0, 5\}$ | $\{1, 6\}$ | $\{2, 7\}$ | $\{3, 8\}$ | $\{4, 9\}$ |
| $\{1, 6\}$ | $\{1, 6\}$ | $\{2, 7\}$ | $\{3, 8\}$ | $\{4, 9\}$ | $\{0, 5\}$ |
| $\{2, 7\}$ | $\{2, 7\}$ | $\{3, 8\}$ | $\{4, 9\}$ | $\{0, 5\}$ | $\{1, 6\}$ |
| $\{3, 8\}$ | $\{3, 8\}$ | $\{4, 9\}$ | $\{0, 5\}$ | $\{1, 6\}$ | $\{2, 7\}$ |
| $\{4, 9\}$ | $\{4, 9\}$ | $\{0, 5\}$ | $\{1, 6\}$ | $\{2, 7\}$ | $\{3, 8\}$ |

|     |                                 |                                 |                                 |                |                |                |
|-----|---------------------------------|---------------------------------|---------------------------------|----------------|----------------|----------------|
| 3)  |                                 | $\{0, 5, 10\}$                  | $\{1, 6, 11\}$                  | $\{2, 7, 12\}$ | $\{3, 8, 13\}$ | $\{4, 9, 14\}$ |
|     | $\{0, 5, 10\}$                  | $\{0, 5, 10\}$                  | $\{1, 6, 11\}$                  | $\{2, 7, 12\}$ | $\{3, 8, 13\}$ | $\{4, 9, 14\}$ |
|     | $\{1, 6, 11\}$                  | $\{1, 6, 11\}$                  | $\{2, 7, 12\}$                  | $\{3, 8, 13\}$ | $\{4, 9, 14\}$ | $\{0, 5, 10\}$ |
|     | $\{2, 7, 12\}$                  | $\{2, 7, 12\}$                  | $\{3, 8, 13\}$                  | $\{4, 9, 14\}$ | $\{0, 5, 10\}$ | $\{1, 6, 11\}$ |
|     | $\{3, 8, 13\}$                  | $\{3, 8, 13\}$                  | $\{4, 9, 14\}$                  | $\{0, 5, 10\}$ | $\{1, 6, 11\}$ | $\{2, 7, 12\}$ |
|     | $\{4, 9, 14\}$                  | $\{4, 9, 14\}$                  | $\{0, 5, 10\}$                  | $\{1, 6, 11\}$ | $\{2, 7, 12\}$ | $\{3, 8, 13\}$ |
| 5)  |                                 | $\{1, 4\}$                      | $\{2, 8\}$                      | $\{7, 13\}$    | $\{11, 14\}$   |                |
|     | $\{1, 4\}$                      | $\{1, 4\}$                      | $\{2, 8\}$                      | $\{7, 13\}$    | $\{11, 14\}$   |                |
|     | $\{2, 8\}$                      | $\{2, 8\}$                      | $\{1, 4\}$                      | $\{11, 14\}$   | $\{7, 13\}$    |                |
|     | $\{7, 13\}$                     | $\{7, 13\}$                     | $\{11, 14\}$                    | $\{1, 4\}$     | $\{2, 8\}$     |                |
|     | $\{11, 14\}$                    | $\{11, 14\}$                    | $\{7, 13\}$                     | $\{2, 8\}$     | $\{1, 4\}$     |                |
| 7)  |                                 | $\{1, 7\}$                      | $\{3, 5\}$                      | $\{9, 15\}$    | $\{11, 13\}$   |                |
|     | $\{1, 7\}$                      | $\{1, 7\}$                      | $\{3, 5\}$                      | $\{9, 15\}$    | $\{11, 13\}$   |                |
|     | $\{3, 5\}$                      | $\{3, 5\}$                      | $\{9, 15\}$                     | $\{11, 13\}$   | $\{1, 7\}$     |                |
|     | $\{9, 15\}$                     | $\{9, 15\}$                     | $\{11, 13\}$                    | $\{1, 7\}$     | $\{3, 5\}$     |                |
|     | $\{11, 13\}$                    | $\{11, 13\}$                    | $\{1, 7\}$                      | $\{3, 5\}$     | $\{9, 15\}$    |                |
| 9)  |                                 | $\{1, 5\}$                      | $\{7, 11\}$                     | $\{13, 17\}$   | $\{19, 23\}$   |                |
|     | $\{1, 5\}$                      | $\{1, 5\}$                      | $\{7, 11\}$                     | $\{13, 17\}$   | $\{19, 23\}$   |                |
|     | $\{7, 11\}$                     | $\{7, 11\}$                     | $\{1, 5\}$                      | $\{19, 23\}$   | $\{13, 17\}$   |                |
|     | $\{13, 17\}$                    | $\{13, 17\}$                    | $\{19, 23\}$                    | $\{1, 5\}$     | $\{7, 11\}$    |                |
|     | $\{19, 23\}$                    | $\{19, 23\}$                    | $\{13, 17\}$                    | $\{7, 11\}$    | $\{1, 5\}$     |                |
| 11) |                                 | $\{e, b, b^2\}$                 | $\{a, a \cdot b, a \cdot b^2\}$ |                |                |                |
|     | $\{e, b, b^2\}$                 | $\{e, b, b^2\}$                 | $\{a, a \cdot b, a \cdot b^2\}$ |                |                |                |
|     | $\{a, a \cdot b, a \cdot b^2\}$ | $\{a, a \cdot b, a \cdot b^2\}$ | $\{e, b, b^2\}$                 |                |                |                |

- 13) Each element of  $G/N$  is a set of functions  $f(x) = px + k$  for which the  $p$  is the same for all functions in the coset.
- 15) Let  $g$  be a generator of  $G$ , then  $gN$  will be a generator of  $G/N$ .
- 17) If  $h_1N$  and  $h_2N$  are two elements of  $H/N$ , then  $h_1$  and  $h_2$  are in  $H$ , and  $(h_1N \cdot (h_2N))^{-1} = (h_1 \cdot h_2^{-1}) \cdot N \in H/N$ . So  $H/N$  is a subgroup of  $G/N$ .
- 19)  $|Z_{105}^*| = 48$ ,  $H = \{1, 11, 16, 46, 71, 86\}$ , coset  $\{2, 22, 36, 37, 67, 92\}$  has order 4.

### Section 5.1

- 1) If  $f(x) = a$  and  $f(y) = b$ , then  $f^{-1}(a \cdot b) = x \cdot y = f^{-1}(a) \cdot f^{-1}(b)$ .
- 3) **Stay**  $\rightarrow e$ , **RotRt**  $\rightarrow b$ , **RotLft**  $\rightarrow b^2$ , **Spin**  $\rightarrow a$ , **FlipRt**  $\rightarrow a \cdot b$ , **FlipLft**  $\rightarrow a \cdot b^2$ .
- 5)  $Z_6 = \{0, 1, 2, 3, 4, 5\} \approx Z_7^*$  with order  $\{1, 3, 2, 6, 4, 5\}$ .
- 7)  $Z_6 = \{0, 1, 2, 3, 4, 5\} \approx Z_{14}^*$  with order  $\{1, 3, 9, 13, 11, 5\}$ .
- 9)  $Z_{10} = \{0, 1, 2, 3, \dots, 9\} \approx Z_{11}^*$  with order  $\{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$ .
- 11)  $Z_{12} = \{0, 1, 2, \dots, 11\} \approx Z_{13}^*$  with order  $\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$ .

- 13)  $Z_{12}^* = \{1, 5, 7, 11\} \approx Z_8^*$  with order  $\{1, 3, 5, 7\}$ .  
 15) Let  $g$  be a generator, and consider the function  $f(x) : \mathbb{Z} \rightarrow G$  defined by  $f(x) = g^x$ .  
 17)  $a^m = e_1$  if and only if  $\phi(a^m) = \phi(e_1) = e_2$  if and only if  $\phi(a)^m = e_2$ .  
 19) The tables for  $Z_{14}$  and  $D_7$  are too large to display here.  
 21)  $Z_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\} \approx Z_{15}^*$  with order  $\{1, 2, 8, 4, 11, 7, 13, 14\}$ .

### Section 5.2

- 1) If  $a, b \in \text{Im}(\phi)$ , then  $a = \phi(x)$ ,  $b = \phi(y)$  for some  $x, y \in G$ . Then  $a \cdot b = \phi(x \cdot y) = \phi(y \cdot x) = b \cdot a$ .  
 3)  $\phi(x \cdot y) = \phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y) = \phi(x) \cdot \phi(y)$ , since  $\cdot$  is addition in this group.  
 5)  $\phi(x \cdot y) = \phi(x + y) = x + y + 3$ , but  $\phi(x) \cdot \phi(y) = \phi(x) + \phi(y) = (x + 3) + (y + 3) = x + y + 6$ .  
 7)  $\phi(x \cdot y) = 2(x \cdot y) = 2xy$ , but  $\phi(x) \cdot \phi(y) = (2x) \cdot (2y) = 4xy$ .  
 9)  $\phi(x \cdot y) = \phi(x + y) = e^{x+y} = e^x \times e^y = \phi(x) \cdot \phi(y)$ . Image is the positive real numbers.  
 11)  $\phi(f \cdot g) = \phi(f(t) + g(t)) = f(3) + g(3) = \phi(f) + \phi(g) = \phi(f) \cdot \phi(g)$ . The kernel is the set of polynomials with 3 as a root, hence  $t - 3$  is a factor.  
 13)  $\phi(1) = 1$ ,  $\phi(7) = 13$ ,  $\phi(11) = 1$ ,  $\phi(13) = 7$ ,  $\phi(17) = 13$ ,  $\phi(19) = 19$ ,  $\phi(23) = 7$ ,  $\phi(29) = 19$ .  
 15)  $\phi(\pm 1) = 1$ ,  $\phi(\pm i) = 3$ ,  $\phi(\pm j) = 5$ ,  $\phi(\pm k) = 7$ . The 3, 5, and 7 can be permuted.  
 17) For each element  $h \in H$ ,  $f^{-1}(h)$  is a coset of  $K$ , where  $K = \text{Ker } f$ . Hence  $|f^{-1}(h)| = |K|$ . Since each element in  $H$  produces a different coset of  $K$ , the size of  $f^{-1}(H)$  is  $|H| \cdot |K|$ .  
 19) Many solutions, since  $b$  can map to either **RotLft** or **RotRt**, and  $a$  can map to **FlipLft**, **FlipRt**, or **Spin**. Any of these combinations will work.

### Section 5.3

- 1)  $Z_{10}$ ,  $Z_5$ ,  $Z_2$ , and the trivial group.  
 3)  $Z_{15}^*$ ,  $Z_4$ ,  $Z_8^*$ ,  $Z_2$ , and the trivial group.  
 5)  $Q$ ,  $Z_8^*$ ,  $Z_2$ , and the trivial group.  
 7)  $Z_{24}^*$ ,  $Z_8^*$ ,  $Z_2$ , and the trivial group.  
 9) If  $K$  is the kernel, it is sufficient to show that  $G/K$  is cyclic. If  $g$  is a generator of  $G$ , then  $gK$  is a generator of  $G/K$ , since every element can be expressed as  $g^m \cdot K = (gK)^m$ .  
 11) Ten homomorphisms, one sending all elements to  $e$ , three sending  $\{1, 3\}$  to  $e$ ,  $\{5, 7\}$  to  $a$ ,  $a \cdot b$ , or  $a \cdot b^2$  respectively, three sending  $\{1, 5\}$  to  $e$ ,  $\{3, 7\}$  to  $a$ ,  $a \cdot b$ , or  $a \cdot b^2$  respectively, and three sending  $\{1, 7\}$  to  $e$ ,  $\{3, 5\}$  to  $a$ ,  $a \cdot b$ , or  $a \cdot b^2$  respectively.  
 13) Since  $\{0, 2, 4\}$  and  $\{0, 3\}$  are normal subgroups of  $Z_6$ ,  $\phi^{-1}(\{0, 2, 4\})$  and  $\phi^{-1}(\{0, 3\})$  are normal subgroups of  $G$ .  
 15)  $H$  and  $K$  must be normal, since they have index 2. Then  $H \cdot K$  is a subgroup with more than half the elements, so  $H \cdot K = G$ . By the second

isomorphism theorem,  $G/K \approx K/(H \cap K) \approx Z_2$ . So  $H \cap K$  contains half the elements of  $K$ , hence a fourth of the elements of  $G$ , so  $G/(H \cap K)$  contains 4 elements. For every element  $a \in G$ ,  $a^2$  is in both  $H$  and  $K$ , so every element in the quotient group is of order 1 or 2. Thus,  $G/(H \cap K) \approx Z_8^*$ .

- 17)  $\{\{e, a^2\}, \{a, a^3\}\}, \{\{b, a^2 \cdot b\}, \{a \cdot b, a^3 \cdot b\}\} \approx \{\{e, a, a^2, a^3\}, \{b, a \cdot b, a^2 \cdot b, a^3 \cdot b\}\}$ .
- 19) The statement is false. A typical element of  $G/N$  is  $gN$ , whereas a typical element of  $G/H$  is  $gH$ . So  $G/H$  is not a subgroup of  $G/N$ , hence  $(G/N)/(G/H)$  is meaningless.
- 21) Kernel must be  $\{e, a \cdot b^2 \cdot c, c^2, a \cdot b^2 \cdot c^3\}$ . Several solutions, one is to let  $\phi(a) = a$ ,  $\phi(b) = b$ , and  $\phi(c) = a \cdot b^2$ .

### Section 6.1

- 1)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{smallmatrix})$ .
- 3)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 6 & 3 \end{smallmatrix})$ .
- 5)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 5 & 6 & 3 & 7 & 1 \end{smallmatrix})$ .
- 7)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 8 & 1 & 6 & 2 & 7 \end{smallmatrix})$ .

| 9)      | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
|---------|---------|---------|---------|---------|---------|---------|
|         | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(123)$ | $(123)$ | $(132)$ | $(213)$ | $(231)$ | $(312)$ | $(321)$ |
| $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(132)$ | $(132)$ | $(123)$ | $(312)$ | $(321)$ | $(213)$ | $(231)$ |
| $(213)$ | $(213)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(213)$ | $(213)$ | $(231)$ | $(123)$ | $(132)$ | $(321)$ | $(312)$ |
| $(231)$ | $(231)$ | $(123)$ | $(321)$ | $(312)$ | $(123)$ | $(132)$ |
| $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(312)$ | $(312)$ | $(321)$ | $(123)$ | $(123)$ | $(231)$ | $(213)$ |
| $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ | $(123)$ |
| $(321)$ | $(321)$ | $(312)$ | $(231)$ | $(213)$ | $(132)$ | $(123)$ |

- 11)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{smallmatrix})$ .
- 13)  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{smallmatrix})$ .
- 15)  $x = (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{smallmatrix}), (\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{smallmatrix})$ , or  $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{smallmatrix})$ .

- 17) **Right-Last-Left.**
- 19) **Right-First-Right.**

### Section 6.2

- 1)  $(2 \ 5 \ 6 \ 3 \ 4)$ .
- 3)  $(1 \ 5 \ 6 \ 4 \ 7 \ 8)(2 \ 3)$ .
- 5) Product is  $(1 \ 2)(n+1 \ n+2)$ . When  $n=2$ , we easily get  $(1 \ 2)(3 \ 4)$ , so assume that product is correct for  $n-1$ . Then by induction, the product is  $(1 \ 2)(n \ n+1)(n \ n+1 \ n+2) = (1 \ 2)(n+1 \ n+2)$ .

- 7) If  $f = \phi_1 \cdot \phi_2$ , where  $\phi_1$  and  $\phi_2$  are disjoint, then  $f^n = e$  if and only if  $\phi_1^n = e$  and  $\phi_2^n = e$ .
- 9)  $(1\ 2)(3\ 4\ 5)(6\ 7) \in A_7$ , since this is an even permutation.
- 11) Let  $N = A_n$ , which is normal subgroup of  $S_n$ . If  $H$  has an odd permutation, then  $H \cdot A_n = S_n$ , and the second isomorphism theorem shows  $H/(H \cap A_n) \approx S_n/A_n \approx Z_2$ .
- 13)  $g$  must be a 5-cycle, so  $g^5 = e$ , and so  $(g^2)^3 = g^6 = g$ . So we can reconstruct  $g$  by cubing  $g^2$ , giving  $(1\ 2\ 3\ 5\ 4)$ .
- 15) Let  $H$  be the subgroup generated by the  $n$ -cycle  $\phi = (1\ 2\ 3 \dots n)$ . Then  $\phi^{j-i}$  will map  $i$  to  $j$ .
- 17) If  $\phi = (i_1\ i_2\ i_3 \dots i_r)$  and  $f = (j_1\ j_2\ j_3 \dots j_s)$ , then  $x \cdot \phi \cdot x^{-1} = (x(i_1)\ x(i_2)\ x(i_3) \dots x(i_r))$ , and  $x \cdot f \cdot x^{-1} = (x(j_1)\ x(j_2)\ x(j_3) \dots x(j_s))$ .
- 19)  $a^2$  is a 3-cycle,  $a^3 = ()$ ,  $b^2$  is a product of two 3-cycles,  $b^3$  is a product of three 2-cycles,  $b^6 = ()$ .
- 21)  $a \cdot b \cdot a^{-1} = (2\ 4\ 3\ 5\ 6\ 7)$ . In general,  $a \cdot b \cdot a^{-1}$  will have the same cycle structure as  $b$ .

### Section 6.3

- 1)  $\left\{ \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix} \right) \right\}$ .
- 3)  $(()), (1\ 2\ 3\ 4)(5\ 6\ 7\ 8), (1\ 3)(2\ 4)(5\ 7)(6\ 8), (1\ 4\ 3\ 2)(5\ 8\ 7\ 6), (1\ 5)(2\ 8)(3\ 7)(4\ 6), (1\ 6)(2\ 5)(3\ 8)(4\ 7), (1\ 7)(2\ 6)(3\ 5)(4\ 8), (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ .
- 5)  $(()), (1\ 2)(3\ 4)(5\ 6)(7\ 8), (1\ 3)(2\ 4)(5\ 7)(6\ 8), (1\ 4)(2\ 3)(5\ 8)(6\ 7), (1\ 5)(2\ 6)(3\ 7)(4\ 8), (1\ 6)(2\ 5)(3\ 8)(4\ 7), (1\ 7)(2\ 8)(3\ 5)(4\ 6), (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ .
- 7)  $S_6$  contains a subgroup generated by  $(12)$ ,  $(34)$ , and  $(56)$ .
- 9) Applying Corollary 6.2: 35 divides  $5! \cdot |N|$ , so 7 divides  $|N|$ , hence  $H = N$ , and  $H$  is normal.
- 11) Applying Corollary 6.2: 200 divides  $8! \cdot |N|$ , so 5 divides  $|N|$ , hence either  $H = N$ , or  $|N| = 5$ .
- 13) Applying Corollary 6.2: 189 divides  $7! \cdot |N|$ , so 3 divides  $|N|$ , hence either  $H = N$ ,  $|N| = 3$ , or  $|N| = 9$ .
- 15) Applying Corollary 6.2:  $3|H|$  divides  $3! \cdot |N|$ , so  $H = N$  or  $|N| = |H|/2$ .
- 17) Any non-trivial subgroup would have order  $p$ . Applying Corollary 6.2 gives  $p^2$  dividing  $p! \cdot |N|$ , so  $N$  must be a multiple of  $p$ , giving  $H = N$ .
- 19) Since the set is finite, for a given element  $a$ , the set  $\{a, a^2, a^3, \dots\}$  must repeat, so  $a^m = a^n$  for some  $m < n$ . Then by the cancellation laws,  $a^{n-m} = 1$ , so  $a^{n-m-1} \cdot a = 1$ . Thus,  $a$  has an inverse,  $a^{n-m-1}$ .
- 21)  $\{(), (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)(10\ 11\ 12), (1\ 3\ 2)(4\ 6\ 5)(7\ 9\ 8)(10\ 12\ 11), (1\ 4\ 7\ 10)(2\ 6\ 8\ 12)(3\ 5\ 9\ 11), (1\ 5\ 7\ 11)(2\ 4\ 8\ 10)(3\ 6\ 9\ 12), (1\ 6\ 7\ 12)(2\ 5\ 8\ 11)(3\ 4\ 9\ 10), (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12), (1\ 8\ 3\ 7\ 2\ 9)(4\ 11\ 6\ 10\ 5\ 12), (1\ 9\ 2\ 7\ 3\ 8)(4\ 12\ 5\ 10\ 6\ 11), (1\ 10\ 7\ 4)(2\ 12\ 8\ 6)(3\ 11\ 9\ 5), (1\ 11\ 7\ 5)(2\ 10\ 8\ 4)(3\ 12\ 9\ 6), (1\ 12\ 7\ 6)(2\ 11\ 8\ 5)(3\ 10\ 9\ 4)\}$

### Section 6.4

- 1) 532.
- 3) 2195.
- 5) 3928.
- 7) 37387.
- 9) 29035.
- 11)  $P(3, 4, 2, 6, 5, 1)$ .
- 13)  $P(1, 5, 6, 7, 2, 3, 4)$ .
- 15)  $P(3, 4, 6, 5, 7, 1, 2)$ .
- 17)  $P(6, 4, 8, 5, 1, 2, 3, 7)$ .
- 19) Since the sequence  $a_n =$  the  $n$ th permutation contains every element of  $S_\infty^0$ , so by definition  $S_\infty^0$  is countable.
- 21) If  $\phi \in S_\infty$  and  $f \in S_\infty^0$ , then  $\phi(x)$  is moved by  $\phi(f(\phi^{-1}(x)))$  if and only if  $x$  is moved by  $f$ . This shows the count of integers moved by  $f$  and  $\phi \cdot f \cdot \phi^{-1}$  are equal. In particular,  $\phi \cdot f \cdot \phi^{-1}$  moves only finitely many integers, and hence is in  $S_\infty^0$ .
- 23)  $A_4 = \{1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24\}$ , the numbers congruent to 0 or 1 (mod 4). But **NthPerm(25)** is not in  $A_5$ .
- 25)  $P[4, 5, 1, 6, 2, 3] = (1463)(25)$  is the only solution.

### Section 7.1

- 1)  $\{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}$  corresponds to the order  $\{1, 11, 2, 7, 4, 14, 8, 13\}$ .

3)

|        | (0, 1) | (0, 3) | (0, 5) | (0, 7) | (1, 1) | (1, 3) | (1, 5) | (1, 7) |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| (0, 1) | (0, 1) | (0, 3) | (0, 5) | (0, 7) | (1, 1) | (1, 3) | (1, 5) | (1, 7) |
| (0, 3) | (0, 3) | (0, 1) | (0, 7) | (0, 5) | (1, 3) | (1, 1) | (1, 7) | (1, 5) |
| (0, 5) | (0, 5) | (0, 7) | (0, 1) | (0, 3) | (1, 5) | (1, 7) | (1, 1) | (1, 3) |
| (0, 7) | (0, 7) | (0, 5) | (0, 3) | (0, 1) | (1, 7) | (1, 5) | (1, 3) | (1, 1) |
| (1, 1) | (1, 1) | (1, 3) | (1, 5) | (1, 7) | (0, 1) | (0, 3) | (0, 5) | (0, 7) |
| (1, 3) | (1, 3) | (1, 1) | (1, 7) | (1, 5) | (0, 3) | (0, 1) | (0, 7) | (0, 5) |
| (1, 5) | (1, 5) | (1, 7) | (1, 1) | (1, 3) | (0, 5) | (0, 7) | (0, 1) | (0, 3) |
| (1, 7) | (1, 7) | (1, 5) | (1, 3) | (1, 1) | (0, 7) | (0, 5) | (0, 3) | (0, 1) |

- 5) Consider the natural homomorphism  $\phi : G \rightarrow K$  defined by  $\phi(h, k) = k$ . The kernel is  $\overline{H}$ , so by the 1st isomorphism theorem,  $G/\overline{H} \approx K$ . Similarly,  $G/\overline{K} \approx H$ .
- 7) 1 element of order 2, 2 elements of order 3, 2 elements of order 4.
- 9) 3 elements of order 2, 8 elements of order 3, no elements of order 4.
- 11) 7 elements of order 2, 8 elements of order 3, no elements of order 4.
- 13) 7 elements of order 2, 8 elements of order 3, 8 elements of order 4.
- 15)  $R_2(Z_2 \times Z_6) = 2 \cdot 2 = 4$ , whereas  $R_2(Z_{12}) = 2$ .

- 17) Suppose  $R_2(A \times B) = R_2(A) \cdot R_2(B) = 10$ , with  $R_2(A) \geq R_2(B)$ . If  $R_2(A) = 5$ ,  $A$  would have an even number of elements, but by Problem 22  $R_2(A)$  would be even. Thus,  $R_2(A) = 10$ , meaning that  $A$  has at least 10 elements, so  $B$  would have at most 2. Then  $B \approx Z_2$ , and  $R_2(B) \neq 1$ .
- 19) Put elements of  $Z_{21}^*$  in the order  $\{1, 2, 4, 8, 16, 11, 13, 5, 10, 20, 19, 17\}$ .

## Section 7.2

- 1) Since  $x^n = e$  for all  $x \in Z_n \times Z_n$ , we see that  $Z_n \times Z_n$  is not cyclic.
- 3)  $Z_{32}, Z_{16} \times Z_2, Z_8 \times Z_4, Z_8 \times Z_2 \times Z_2, Z_4 \times Z_4 \times Z_2, Z_4 \times Z_2 \times Z_2 \times Z_2$ , and  $Z_2 \times Z_2 \times Z_2 \times Z_2$ .
- 5) Only  $Z_{210}$ .
- 7)  $Z_{450} \approx Z_2 \times Z_9 \times Z_{25}, Z_2 \times Z_9 \times Z_5 \times Z_5, Z_2 \times Z_3 \times Z_3 \times Z_{25}, Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5$ .
- 9)  $Z_{600} \approx Z_8 \times Z_3 \times Z_{25}, Z_2 \times Z_4 \times Z_3 \times Z_{25}, Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_{25}, Z_8 \times Z_3 \times Z_5 \times Z_5, Z_2 \times Z_4 \times Z_3 \times Z_5 \times Z_5, Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_5 \times Z_5$ .
- 11)  $Z_{900} \approx Z_4 \times Z_9 \times Z_{25}, Z_2 \times Z_2 \times Z_9 \times Z_{25}, Z_4 \times Z_3 \times Z_3 \times Z_{25}, Z_2 \times Z_2 \times Z_3 \times Z_{25}, Z_3 \times Z_{25}, Z_4 \times Z_9 \times Z_5 \times Z_5, Z_2 \times Z_2 \times Z_9 \times Z_5 \times Z_5, Z_4 \times Z_3 \times Z_3 \times Z_5 \times Z_5, Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5$ .
- 13) Two for  $Z_{16}$ , four for  $Z_8 \times Z_2$ , 12 for  $Z_4 \times Z_4$ , and eight for  $Z_4 \times Z_2 \times Z_2$ .
- 15)  $Z_{16} \times Z_8 \times Z_2$ .
- 17)  $Z_4 \times Z_2 \times Z_5$ .
- 19) For each permutation written in terms of disjoint cycles, we can add “1-cycles” so that every number from 1 to  $n$  is mentioned. Then the sum of the sizes of the cycles will add to  $n$ . Thus, there is a one-to-one correspondence between cycle structures and partitions of  $n$ .
- 21) The exact value is  $c = \pi\sqrt{2/3} \approx 2.5651$ .

## Section 7.3

- 1) 6:  $\phi(b) = b$  or  $b^2$  (order 3),  $\phi(a) = a, a \cdot b$ , or  $a \cdot b^2$  (order 2).
- 3) 8:  $\phi(2) = 2, 7, 8$  or 13 (order 4), forcing  $\phi(4) = 4$ .  $\phi(11) = 11$  or 14 (order 2).
- 5) 24:  $\phi(a) =$  one of the 8 elements of order 3, which determines  $\phi(a^2)$ .  $\phi(b) =$  one of the six remaining elements of order 3.
- 7) Note that any automorphism must fix the identity element, leaving  $n - 1$  elements.
- 9)  $\phi(x) = x^{-1}$  is clearly one-to-one and onto, and  $\phi(x \cdot y) = y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1} = \phi(x) \cdot \phi(y)$  since the group is abelian. If  $a$  has order greater than 2,  $\phi(a) \neq a$ , so this is non-trivial.
- 11) If  $\text{Aut}(G)$  is cyclic, then so is  $\text{Inn}(G)$  with a generator  $x \mapsto g^{-1}xg$ . For each  $y \in G$ ,  $y^{-1}xy = g^{-n}xg^n$  for some  $n$ , plugging in  $x = g$  yields  $y^{-1}gy = g$ , or  $gy = yg$ . Since  $gy = yg$  for all  $y$ ,  $\text{Inn}(G) \approx \{e\}$ , and  $G$  is abelian.
- 13)  $((), (b, a^2 \cdot b)(a \cdot b, a^3 \cdot b), (a, a^3)(a \cdot b, a^3 \cdot b), (a, a^3)(b, a^2 \cdot b))$ .
- 15) All automorphisms are inner:  $((), (b, b^2)(a \cdot b, a \cdot b^2), (a, a \cdot b, a \cdot b^2), (a, a \cdot b^2)(b, b^2), (a, a \cdot b^2, a \cdot b), (a, a \cdot b)(b, b^2))$ .

- 17)  $\text{Aut}(\mathbb{Z}) \approx Z_2$ , with  $\phi_0(x) = x$ ,  $\phi_1(x) = -x$ .
- 19) Eight automorphisms:  $(\text{id})$ ,  $(2, 7)(8, 13)$ ,  $(2, 8)(7, 13)$ ,  $(2, 13)(7, 8)$ ,  
 $(2, 8)(11, 14)$ ,  $(2, 13, 8, 7)(11, 14)$ ,  $(7, 13)(11, 14)$ ,  $(2, 7, 8, 13)(11, 14)$ .
- 21) There are 20 automorphisms, generated by  $f(a) = a$ ,  $f(b) = b^2$ , and  
 $g(a) = a \cdot b$ ,  $g(b) = b$ .

### Section 7.4

1)  $(7, 7)$ .

3)  $(7, 5)$ .

5)  $(1, 1)$ .

- 7) A nontrivial homomorphism from  $Z_2$  to  $\text{Aut}(Z_8^*) \approx S_3$  must send 1 to a 2-cycle. But proposition 7.7 shows such homomorphisms are equivalent, so we may assume  $\phi_1 = (3 5)$ .  $Z_8^* \rtimes Z_2 \approx D_4$ .

|         | $(1,0)$ | $(1,1)$ | $(3,0)$ | $(3,1)$ | $(5,0)$ | $(5,1)$ | $(7,0)$ | $(7,1)$ |
|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| $(1,0)$ | $(1,0)$ | $(1,1)$ | $(3,0)$ | $(3,1)$ | $(5,0)$ | $(5,1)$ | $(7,0)$ | $(7,1)$ |
| $(1,1)$ | $(1,1)$ | $(1,0)$ | $(5,1)$ | $(5,0)$ | $(3,1)$ | $(3,0)$ | $(7,1)$ | $(7,0)$ |
| $(3,0)$ | $(3,0)$ | $(3,1)$ | $(1,0)$ | $(1,1)$ | $(7,0)$ | $(7,1)$ | $(5,0)$ | $(5,1)$ |
| $(3,1)$ | $(3,1)$ | $(3,0)$ | $(7,1)$ | $(7,0)$ | $(1,1)$ | $(1,0)$ | $(5,1)$ | $(5,0)$ |
| $(5,0)$ | $(5,0)$ | $(5,1)$ | $(7,0)$ | $(7,1)$ | $(1,0)$ | $(1,1)$ | $(3,0)$ | $(3,1)$ |
| $(5,1)$ | $(5,1)$ | $(5,0)$ | $(1,1)$ | $(1,0)$ | $(7,1)$ | $(7,0)$ | $(3,1)$ | $(3,0)$ |
| $(7,0)$ | $(7,0)$ | $(7,1)$ | $(5,0)$ | $(5,1)$ | $(3,0)$ | $(3,1)$ | $(1,0)$ | $(1,1)$ |
| $(7,1)$ | $(7,1)$ | $(7,0)$ | $(3,1)$ | $(3,0)$ | $(5,1)$ | $(5,0)$ | $(1,1)$ | $(1,0)$ |

- 9) A nontrivial homomorphism from  $Z_4$  to  $\text{Aut}(Z_3) \approx Z_2$  must send 1 and 3 to the 2-cycle  $(1 2)$ . There will only be one element of order 2.
- 11) Since  $\text{Aut}(\mathbb{Z}) \approx Z_2$ , we see that  $\phi_1(x) = -x$ . So  $(x, a) \cdot (y, b) = (x+y, a+b)$  when  $a$  is even, but  $(x, a) \cdot (y, b) = (x-y, a+b)$  when  $a$  is odd.
- 13)  $\psi_\sigma((g_1, g_2, \dots, g_n)) \cdot (h_1, h_2, \dots, h_n) = \psi_\sigma(g_1 \cdot h_1, g_2 \cdot h_2, \dots, g_n \cdot h_n) = (g_{\sigma^{-1}(1)} \cdot h_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)} \cdot h_{\sigma^{-1}(2)}, \dots, g_{\sigma^{-1}(n)} \cdot h_{\sigma^{-1}(n)}) = \psi_\sigma(g_1, g_2, \dots, g_n) \cdot \psi_\sigma(h_1, h_2, \dots, h_n)$ . Since  $\psi_{\sigma^{-1}}$  is the inverse function, we see it is an automorphism.
- 15) By Problems 13 and 14,  $\psi$  is a homomorphism from  $H$  to  $\text{Aut}(G^n)$ . Thus, the semi-direct product would have size  $|G^n| \cdot |H| = |G|^n \cdot |H|$ .
- 17) A nontrivial homomorphism from  $Z_8^*$  to  $\text{Aut}(Z_8^*) \approx S_3$  must be two-to-one, and send two of the elements to a 2-cycle. Proposition 7.7 shows that it does not matter which 2-cycle, and since the non-identity elements of  $Z_8^*$  are essentially equivalent, there is isomorphically only one  $Z_8^* \rtimes Z_8^* \approx Z_2 \times D_4$ .
- 19)  $Z_3 \text{ Wr } S_2 \approx Z_3 \times S_3$ .
- 21)  $Z_2 \text{ Wr } S_3 \approx Z_2 \times S_4$ .

### Section 8.1

- 1)  $\{1, -1\}$ .
- 3) Yes, if  $x$  and  $y$  are in the center, then  $x \cdot y = y \cdot x$ .
- 5) Clearly, if  $a \in Z(a)$  and  $b \in Z(b)$ , then  $(a, b)$  will commute with all elements in  $A \times B$ . But if either  $a$  or  $b$  are not in the center, then there is an element of  $A \times B$  which would not commute with  $(a, b)$ . Thus,

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

- 7) Let  $H = \{e, a\}$ . Since  $H$  is normal,  $g \cdot a \cdot g^{-1}$  is in  $H$  for all  $g$ . But  $g \cdot a \cdot g^{-1} \neq e$  since  $a \neq e$ . So  $g \cdot a \cdot g^{-1} = a$ , so  $g \cdot a = a \cdot g$ .
- 9) Since  $\phi(h) \in H$  for all automorphisms, in particular  $\phi(h) \in H$  for all inner automorphisms. Thus,  $g \cdot h \cdot g^{-1} \in H$  for all  $g \in G$ , so  $H$  is normal.
- 11) If  $h \in H$ , and  $\phi$  is any automorphism, then  $\phi(h)^n = \phi(h^n) = \phi(e) = e$ , so  $\phi(h) \in H$ .
- 13) Let  $\phi$  be an automorphism of  $G$ . Since  $N$  is characteristic,  $\phi(n) \in N$  for all  $n \in N$ , so  $\phi$  can be restricted to form an automorphism on  $N$ . Then  $\phi(h) \in H$  for all  $h \in H$ , since  $H$  is a characteristic subgroup of  $N$ . Hence,  $H$  is a characteristic subgroup of  $G$ .
- 15) Center =  $\{e, a^3\}$ , Quotient group  $D_6/Z(D_6) \approx S_3$ .
- 17)  $Z(D_n) = \{e\}$  if  $n$  is odd,  $Z(D_n) = \{e, a^{n/2}\}$  for  $n$  even. Note that the non-identity element corresponds to a 180 degree rotation.

### Section 8.2

- 1)  $N_{D_4}(\{e\}) = N_{D_4}(\{a^2\}) = D_4$ ,  $N_{D_4}(\{a\}) = N_{D_4}(\{a^3\}) = \{e, a, a^2, a^3\}$ ,  $N_{D_4}(\{b\}) = N_{D_4}(\{a^2 \cdot b\}) = \{e, a^2, b, a^2 \cdot b\}$ ,  $N_{D_4}(\{a \cdot b\}) = N_{D_4}(\{a^3 \cdot b\}) = \{e, a^2, a \cdot b, a^3 \cdot b\}$ .
- 3)  $N_{D_4}(\{e, a^2\}) = D_4$ ,  $N_{D_4}(\{e, b\}) = N_{D_4}(\{e, a^2 \cdot b\}) = \{e, a^2, b, a^2 \cdot b\}$ ,  $N_{D_4}(\{e, a \cdot b\}) = N_{D_4}(\{e, a^3 \cdot b\}) = \{e, a^2, a \cdot b, a^3 \cdot b\}$ .
- 5) No, since  $N_G(\{e\}) = G$  for all groups.
- 7)  $x \in N_G(\{g\}) \Leftrightarrow x \cdot g = g \cdot x \Leftrightarrow x \cdot g^{-1} = g^{-1} \cdot x \Leftrightarrow x \in N_G(\{g^{-1}\})$ .
- 9) If  $z \in Z(G)$  and  $g \in S$ , then  $z \cdot g \cdot z^{-1} = g \cdot z \cdot z^{-1} = g \in S$ .
- 11)  $\{e, a, a^2, a^3\}$ .
- 13)  $\{e, a^2, b, a^2 \cdot b\}$ .
- 15)  $\{e, a^2, b, a^2 \cdot b\}$ .
- 17)  $\{e, a, a^2, a^3, a^4\}$ .
- 19)  $D_5$ .
- 21)  $N_{D_6}(\{e\}) = N_{D_6}(\{a^3\}) = D_6$ ,  $N_{D_6}(\{a\}) = N_{D_6}(\{a^2\}) = N_{D_6}(\{a^4\}) = N_{D_6}(\{a^5\}) = \{e, a, a^2, a^3, a^4, a^5\}$ ,  $N_{D_6}(\{b\}) = N_{D_6}(\{a^3 \cdot b\}) = \{e, a^3, b, a^3 \cdot b\}$ ,  $N_{D_6}(\{a \cdot b\}) = N_{D_6}(\{a^4 \cdot b\}) = \{e, a \cdot b, a^3, a^4 \cdot b\}$ ,  $N_{D_6}(\{a^2 \cdot b\}) = N_{D_6}(\{a^5 \cdot b\}) = \{e, a^2 \cdot b, a^3, a^5 \cdot b\}$ .

### Section 8.3

- 1)  $\{e\}$ ,  $\{a^2\}$ ,  $\{a, a^3\}$ ,  $\{b, a^2 \cdot b\}$ , and  $\{a \cdot b, a^3 \cdot b\}$ .
- 3)  $\{e\}$ ,  $\{a, a \cdot b, a \cdot b^2, a \cdot b^3, a \cdot b^4\}$ ,  $\{b, b^4\}$ , and  $\{b^2, b^3\}$ .
- 5) If  $g \cdot x \cdot g^{-1} = x^{-1}$  for some  $g$ , then  $g^2 \cdot x = x \cdot g^2$ , and since  $g$  has odd order,  $(g^2)^k = g$  for some  $k$ . Thus,  $g \cdot x = x \cdot g$ , and so  $g \cdot x \cdot g^{-1} = x$ .
- 7) If  $N$  is a nontrivial normal subgroup,  $|N| \geq 13$ , so  $|N| = 30, 20$ , or  $15$  (divisors of 60).  $|N| \neq 15$ , so  $|N|$  is even, hence classes of size 1 and 15 are in  $N$ . Since  $|N| \geq 28$ ,  $|N| = 30$ , but there is no class of size 14.
- 9)  $|N| \geq 57$ , so  $|N| = 252, 168, 126, 84, 72$ , or  $63$  (divisors of 504).  $|N| \neq 63$ , so  $|N|$  is even, hence classes of size 1 and 63 are in  $N$ , making  $|N| \geq 120$ . Seven divides  $|N|$ , so all classes of order 72 are in  $N$ , making  $|N| \geq 280$ .
- 11)  $|N| \geq 85$ , so  $|N| = 546, 364, 273, 182, 156$ , or  $91$  (divisors of 1092). 13 divides  $|N|$ , hence both classes of size 84 are in  $N$ , making  $|N| \geq 260$ . Seven divides  $|N|$ , so all three classes of order 156 are in  $N$ , making  $|N| \geq 728$ .
- 13) The next largest group would be  $A_7$ , with 2520 elements. (Only 72 more elements than  $L_2(17)$ .) The next largest group  $L_2(19)$  has 3420 elements.
- 15)  $|N| \geq 316$ , so  $|N| = 10080, 6720, 5040, 4032, 3360, 2880, 2520, 2240, 2016, 1680, 1440, 1344, 1260, 1120, 1008, 960, 840, 720, 672, 630, 576, 560, 504, 480, 448, 420, 360, 336$ , or  $320$  (divisors of 20160).  $|N|$  is even, so classes of size 1 and 315 are in  $N$ , making  $|N| \geq 1576$ .  $|N| \neq 2240$ , so  $|N|$  is a multiple of 3, so the class of size 2240 is in  $N$ , making  $|N| \geq 3816$ . Seven divides  $|N|$ , so both classes of size 2880 are in  $N$ , making  $|N| \geq 9576$ . Five divides  $|N|$ , so both classes of size 4032 are in  $N$ , making  $|N| \geq 16380$ .  $A_8$  has a conjugacy class of size 112 (all 3-cycles).
- 17) 20160 elements, same as  $A_8$  and  $L_3(4)$  from Problem 15. This group is in fact isomorphic to  $A_8$ .
- 19) Nontrivial normal subgroups are  $\{1, 13016\}$  and  $\{1, 6212, 13016, 19853, 24132, 25315, 33108, 38807\}$ .

### Section 8.4

- 1)  $A_{1,1} = A_{1,2} = B_{1,1} = Z_{12}$ ,  $A_{2,1} = \{0, 6\}$ ,  $B_{1,2} = \{0, 2, 4, 6, 8, 10\}$ . The arrows show the isomorphisms  $Z_{12}/Z_{12} \approx Z_{12}/Z_{12}$ ,  $Z_{12}/Z_{12} \approx \{0, 2, 4, 6, 8, 10\}/\{0, 2, 4, 6, 8, 10\}$ ,  $Z_{12}/\{0, 3, 6, 9\} \approx \{0, 4, 8\}/\{0\}$ ,  $\{0, 3, 6, 9\}/\{0, 6\} \approx Z_{12}/\{0, 2, 4, 6, 8, 10\}$ ,  $\{0, 6\}/\{0\} \approx \{0, 2, 4, 6, 8\}/\{0, 4, 8\}$ ,  $\{0\}/\{0\} \approx \{0\}/\{0\}$ .
- 3)  $Z_{24}^* \supseteq \{1, 5, 7, 11\} \supseteq \{1, 5\} \supseteq \{1\}$ .
- 5)  $Z_{12} \times Z_{18} \supseteq \{0, 3, 6, 9\} \times Z_{18} \supseteq \{0, 6\} \times Z_{18} \subseteq \{0\} \times Z_{18} \supseteq \{0\} \times \{0, 3, 6, 9, 12, 15\} \supseteq \{0\} \times \{0, 9\} \supseteq \{0\} \times \{0\}$ .
- 7)  $D_4 \subseteq \{e, b, b^2, b^3\} \subseteq \{e, b^2\} \subseteq \{e\}$ .
- 9)  $D_6 \subseteq \{e, b, b^2, b^3, b^4, b^5\} \subseteq \{e, b^3\} \subseteq \{e\}$ .

- 11)  $A_4$  and  $\{(), (12)(34), (13)(24), (14)(23)\}$  must be in the series, and then we have three choices,  $\{(), (12)(34)\}$ ,  $\{(), (13)(24)\}$ , or  $\{(), (14)(23)\}$  for the next term in the series.
- 13)  $S_5$  and  $Z_{120}$ .
- 15) Pick a cyclic group of prime order.
- 17) Since all of the  $A_i$  and  $B_j$  are normal subgroups of  $G$ , then  $A_{i,j} = (A_{i-1} \cap B_j) \cdot A_i$  and  $B_{j,i} = (B_{j-1} \cap A_i) \cdot B_j$  are normal subgroups of  $G$  using Problem 17 from §5.3.
- 19)  $M \supseteq \{e, a, a^2, a^3, a^4, b^2, a \cdot b^2, a^2 \cdot b^2, a^3 \cdot b^2, a^4 \cdot b^2\} \supseteq \{e, a, a^2, a^3, a^4\} \supseteq \{e\}$ .

### Section 8.5

- 1) 1 element of order 1, 391 of order 2, 64880 of order 3, 2520 of order 4, 2304 of order 5, 173840 of order 6, 1440 of order 8, 2304 of order 10, 201600 of order 12, 184320 of order 15, 115200 of order 24, and 184320 elements of order 30.
- 3) The size of group is  $8! \cdot (12!/2) \cdot 3^7 \cdot 2^{11} = 432520023274489856000$ . The only nontrivial element in the center flips all 12 edges. (Rotating all 8 corners clockwise can't be done, since 8 is not a multiple of 3.)
- 5)  $a^2 \cdot b^{-1} \cdot a^{-1}$ .
- 7) The two possible moves  $(1\ 2\ 3\ 4\ 5\ 6\ 7)$  and  $(1\ 3)(2\ 6)$  are both even permutations, so the group generated by these two elements would be a subgroup of  $A_7$ .
- 9)  $a \cdot (a^2 \cdot b^{-1})^2 \cdot a^{-1}$ .
- 11)  $(a^{-1} \cdot b^{-1})^3 \cdot (a \cdot b)^3 \cdot a \cdot b^{-1} \cdot a^{-1} \cdot b^{-2}$
- 13)  $L \cdot R^{-1} \cdot L \cdot R^{-1} \cdot L \cdot R^{-2}$ .

### Section 9.1

- 1)  $(-x) \cdot y = (-x) \cdot y + [x \cdot y + -(x \cdot y)] = [(-x) \cdot y + x \cdot y] + -(x \cdot y) = [(-x) + x] \cdot y + -(x \cdot y) = 0 \cdot y + -(x \cdot y) = -(x \cdot y)$ .
- 3)  $(-x) \cdot (-y) = -((-x) \cdot y) = -(-(x \cdot y)) = x \cdot y$ .
- 5)  $(x - y) \cdot z = (x + (-y)) \cdot z = x \cdot z + (-y) \cdot z = x \cdot z + -(y \cdot z) = x \cdot z - y \cdot z$ .
- 7) Either  $(a \cdot b) \cdot x = 0$  or  $x \cdot (a \cdot b) = 0$  for some non-zero  $x$ . In the first case,  $a \cdot (b \cdot x) = 0$ , so either  $a$  is a zero divisor, or  $b \cdot x = 0$ , making  $b$  a zero divisor. The second case is similar.
- 9)  $\overline{i \cdot j} = \overline{(-i) \cdot (-j)} = k$ , yet  $\overline{i \cdot j} = \overline{k} = -k$ . What is true is that  $\overline{x_1 \cdot x_2} = \overline{x_2 \cdot x_1}$ .
- 11)  $|x_1 \cdot x_2| = \sqrt{x_1 \cdot x_2 \cdot \overline{x_1 \cdot x_2}} = \sqrt{x_1 \cdot x_2 \cdot \overline{x_2} \cdot \overline{x_1}} = \sqrt{x_1 \cdot \overline{x_1} \cdot x_2 \cdot \overline{x_2}} = \sqrt{x_1 \cdot \overline{x_1} \sqrt{x_2 \cdot \overline{x_2}}} = |x_1||x_2|$ .
- 13)  $(x + i) \cdot (x - i) = x^2 + i \cdot x - x \cdot i + 1 \neq x^2 + 1$ . (For example, if  $x = j$ .)
- 15) This set is not closed under multiplication. For example,  $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ .
- 17) Since  $G$  is an abelian group, we only need to check the associative law and the two distributive laws. But these are both trivial, since both sides would evaluate to 0.

- 19) Since  $x = (x \cdot y) \cdot x = x \cdot (y \cdot x)$ , we have  $x \cdot (e - y \cdot x) = 0$ . Since  $x$  cannot be 0 (else  $x \cdot y = 0$ ), and  $x$  is not a zero-divisor, then  $e - y \cdot x = 0$ .
- 21) When  $n = 5, 7$ , or  $11$ ,  $Z_n$  is a field. Otherwise, there are zero divisors in  $Z_n$ .

### Section 9.2

- 1)  $a^2 = a, b^2 = b$ .
- 3)  $b \cdot a = a, b^2 = b$ .
- 5)  $b \cdot a = a, a^2 = 0$ .
- 7)  $b \cdot a = a, a^2 = a$ .
- 9)  $a^2 = a, b^2 = 3b$ .
- 11)  $b^2 = c^2 = a + b + c, b \cdot a = c, c \cdot b = a$ .
- 13) By induction in  $m$ :  $m(x + y) = (m - 1)(x + y) + (x + y) = (m - 1)x + (m - 1)y + x + y = mx + my$ .
- 15) By induction in  $m$ :  $(mn)x = ((m - 1)n + n)x = ((m - 1)n)x + nx = (m - 1)(nx) + nx = m(nx)$ .
- 17) 2.
- 19) Let the identity  $e$  have order  $n$  in the additive group. Then the characteristic cannot be less than  $n$ , but  $nx = n(x \cdot e) = (ne) \cdot x = 0$  for all  $x \in R$ .
- 21) Since the additive group is abelian, it can be written as  $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ . Then the  $r$  elements  $(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)$  form a basis.
- 23) Define  $2a = 0$ , and  $a^2 = 0$ .
- 25) Define  $2a = 2b = 2c = 0, a^2 = a + c, a \cdot b = b + c, a \cdot c = c, b \cdot a = b, b^2 = b, b \cdot c = 0, c \cdot a = c, c \cdot b = c$ , and  $c^2 = 0$ .

### Section 9.3

- 1) Both  $x \cdot a = x$  and  $x \cdot b = x$  for all  $x$  in the ring, but there is no  $r$  for which  $r \cdot c = c$ , since  $r \cdot c = 0$ .
- 3)  $(x + y) \cdot (x^{-1} - x^{-2} \cdot y + x^{-3} \cdot y^2) = e + x^{-1} \cdot y - x^{-1} \cdot y - x^{-2} \cdot y^2 + x^{-2} \cdot y^2 + x^{-3} \cdot y^3 = e$ .
- 5) This is actually a field, with 6 as the unity.
- 7) Since  $(x + y)^2 = x^2 + x \cdot y + y \cdot x + y^2 = x + y$ , we have that  $x \cdot y + y \cdot x = 0$ . By Problem 6,  $x \cdot y = -x \cdot y$ , and so  $x \cdot y = y \cdot x$ .
- 9)  $(x + y)^2 = x^2 + 2x \cdot y + y^2 = x^2 + y^2$ .
- 11) For the ring defined by Tables 9.3 and 9.4,  $x = a, y = -a$ .
- 13) Obviously 0 and  $e$  satisfy  $a^2 = a$ . If  $a \neq 0$ , then  $a^{-1}$  exists, and  $a = a^2 \cdot a^{-1} = a \cdot a^{-1} = e$ .
- 15)  $(x + y)^2 = x^2 + x \cdot y + y \cdot x + y^2 = x^2 + 2xy + y^2. (x + y)^3 = (x + y)(x^2 + 2xy + y^2) = x^3 + y \cdot x^2 + 2x^2 \cdot y + 2y \cdot x \cdot y + x \cdot y^2 + y^3 = x^3 + 3x^2y + 3xy^2 + y^3$ .
- 17)  $e$  and  $g$ .
- 19)  $2a + b$  is the only irreducible element.

- 21)  $a, b, d$ , and  $f$  are prime.  
 23) Define  $2a = 2c = 0$ ,  $a^2 = a$ ,  $a \cdot c = c$ ,  $c \cdot a = 0$ , and  $c^2 = 0$ .

### Section 10.1

- 1) Subring.  $(x_1 - x_2) + (y_1 - y_2)\sqrt{5}$  and  $(x_1x_2 + 5y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{5}$  are in the set.
- 3) Not a subring, since not closed under subtraction.
- 5) Subring.  $(x_12^{y_1} - x_22^{y_2})/(2^{(y_1+y_2)})$  and  $(x_1x_2)/2^{(y_1+y_2)}$  are in the set.
- 7) Subring.  $(x_1 - x_2) + (y_1 - y_2)\sqrt[3]{2} + (z_1 - z_2)\sqrt[3]{4}$  and  $(x_1x_2 + 2y_1z_2 + 2y_2z_1) + (x_1y_2 + x_2y_1 + 2z_1z_2)\sqrt[3]{2} + (x_1z_2 + y_1y_2 + z_1x_2)\sqrt[3]{4}$  are in the set.
- 9) Not a subring, since not closed under multiplication.  $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ .
- 11) If  $a, b \in A$ , then  $a \cdot y = b \cdot y = 0$ , so  $(a - b) \cdot y = 0$  and  $(a \cdot b) \cdot y = 0$ , so  $a - b$  and  $a \cdot b$  are in  $A$ .
- 13) If  $a, b \in Z$ , and  $x \in R$ , then  $(a - b) \cdot x = a \cdot x - b \cdot x = x \cdot a - x \cdot b = x \cdot (a - b)$  and  $(a \cdot b) \cdot x = a \cdot (x \cdot b) = x \cdot (a \cdot b)$ , so  $a - b$  and  $a \cdot b$  are in  $Z$ .
- 15) 2 and 3 are in  $2\mathbb{Z} \cup 3\mathbb{Z}$ , but  $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ .
- 17)  $\{0\}$ ,  $\{0, a\}$ ,  $\{0, b\}$ ,  $\{0, c\}$ , and the whole ring.
- 19)  $\{0\}$ ,  $\{0, a, 2a, 3a\}$ ,  $\{0, b\}$ ,  $\{0, 2a\}$ ,  $\{0, b, 2a, 2a + b\}$ ,  $\{0, 2a + b\}$ ,  $\{0, a + b, 2a, 3a + b\}$ , and the whole ring.

### Section 10.2

- 1) If  $a \in X + Y$  and  $z \in R$ , then  $a = x + y$  for some  $x \in X$  and  $y \in Y$ . Then  $a \cdot z = (x \cdot z) + (y \cdot z) \in X + Y$ . Likewise,  $z \cdot a \in X + Y$ .
- 3) If  $a \in X \cdot Y$ , and  $z \in R$ , then  $a = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n$ , so  $a \cdot z = x_1 \cdot (y_1 \cdot z) + x_2 \cdot (y_2 \cdot z) + \cdots + x_n \cdot (y_n \cdot z) \in X \cdot Y$ . Likewise,  $z \cdot a \in X \cdot Y$ .
- 5) If  $a \in X \cdot Y$ , then  $a = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n \in X$ . Likewise,  $a \in Y$ , so  $a \in X \cap Y$ .
- 7)  $\{0\}$ ,  $\{0, a, 2a, 3a\}$ ,  $\{0, 2a\}$ ,  $\{0, b\}$ ,  $\{0, 2a + b, b, 2a\}$ , and the whole ring.
- 9)  $\{0\}$ ,  $\{0, c\}$ ,  $\{0, a, b, c\}$ ,  $\{0, c, d, f\}$ , and the whole ring.

11)

| +                   | $\{0, 2a\}$         | $\{a, 3a\}$         | $\{b, 2a + b\}$     | $\{a + b, 3a + b\}$ |
|---------------------|---------------------|---------------------|---------------------|---------------------|
| $\{0, 2a\}$         | $\{0, 2a\}$         | $\{a, 3a\}$         | $\{b, 2a + b\}$     | $\{a + b, 3a + b\}$ |
| $\{a, 3a\}$         | $\{a, 3a\}$         | $\{0, 2a\}$         | $\{a + b, 3a + b\}$ | $\{b, 2a + b\}$     |
| $\{b, 2a + b\}$     | $\{b, 2a + b\}$     | $\{a + b, 3a + b\}$ | $\{0, 2a\}$         | $\{a, 3a\}$         |
| $\{a + b, 3a + b\}$ | $\{a + b, 3a + b\}$ | $\{b, 2a + b\}$     | $\{a, 3a\}$         | $\{0, 2a\}$         |
| .                   | $\{0, 2a\}$         | $\{a, 3a\}$         | $\{b, 2a + b\}$     | $\{a + b, 3a + b\}$ |
| $\{0, 2a\}$         |
| $\{a, 3a\}$         | $\{0, 2a\}$         | $\{a, 3a\}$         | $\{0, 2a\}$         | $\{a, 3a\}$         |
| $\{b, 2a + b\}$     | $\{0, 2a\}$         | $\{0, 2a\}$         | $\{b, 2a + b\}$     | $\{b, 2a + b\}$     |
| $\{a + b, 3a + b\}$ | $\{0, 2a\}$         | $\{a, 3a\}$         | $\{b, 2a + b\}$     | $\{a + b, 3a + b\}$ |

13)

| +          | $\{0, c\}$ | $\{e, g\}$ | $\{a, b\}$ | $\{d, f\}$ |
|------------|------------|------------|------------|------------|
| $\{0, c\}$ | $\{0, c\}$ | $\{e, g\}$ | $\{a, b\}$ | $\{d, f\}$ |
| $\cdot$    | $\{0, c\}$ | $\{e, g\}$ | $\{a, b\}$ | $\{d, f\}$ |
| $\{e, g\}$ | $\{e, g\}$ | $\{0, c\}$ | $\{d, f\}$ | $\{a, b\}$ |
| $\{a, b\}$ | $\{a, b\}$ | $\{d, f\}$ | $\{0, c\}$ | $\{e, g\}$ |
| $\{d, f\}$ | $\{d, f\}$ | $\{a, b\}$ | $\{e, g\}$ | $\{0, c\}$ |

| +                       | $\langle 6 \rangle$     | $2 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ |
|-------------------------|-------------------------|-------------------------|-------------------------|
| $\langle 6 \rangle$     | $\langle 6 \rangle$     | $2 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ |
| $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     |
| $2 + \langle 6 \rangle$ | $2 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ | $\langle 6 \rangle$     |
| $4 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ | $\langle 6 \rangle$     | $2 + \langle 6 \rangle$ |

15)

| +                       | $\langle 6 \rangle$     | $2 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ |
|-------------------------|-------------------------|-------------------------|-------------------------|
| $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     |
| $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     | $\langle 6 \rangle$     |
| $2 + \langle 6 \rangle$ | $2 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ | $2 + \langle 6 \rangle$ |
| $4 + \langle 6 \rangle$ | $4 + \langle 6 \rangle$ | $\langle 6 \rangle$     | $2 + \langle 6 \rangle$ |

- 17) If  $a, b \in A$ , then  $a \cdot y = b \cdot y = 0$ , so  $(a - b) \cdot y = 0$ , hence  $a - b \in A$ . If  $z \in R$ , then  $(a \cdot z) \cdot y = z \cdot (a \cdot y) = 0$ , so  $A$  is an ideal.
- 19) Problem 14 of §10.1 shows it is a subring, so suppose  $a$  is nilpotent, so that  $a^m = 0$ . If  $x \in R$ ,  $(a \cdot x)^m = a^m \cdot x^m = 0$ , so  $a \cdot x$  is nilpotent.
- 21) Nontrivial ideals:  $\{0, b\}$ ,  $\{0, 2a\}$ , and  $\{0, b, 2a, 2a + b\}$ .

### Section 10.3

- 1)  $\phi(x \cdot y) = \phi(x) \cdot \phi(y) = \phi(y) \cdot \phi(x) = \phi(y \cdot x)$ . Since  $\phi$  is one-to-one,  $x \cdot y = y \cdot x$ .
- 3) If  $x \cdot y = 0$  with non-zero  $x$  and  $y$ , then  $0 = \phi(0) = \phi(x \cdot y) = \phi(x) \cdot \phi(y)$ . Since  $\phi$  is one-to-one,  $\phi(x)$  and  $\phi(y)$  are non-zero.
- 5)  $\{0, a, b, c\}$  gives a copy of  $T_4$  inside of  $T_8$ .
- 7)  $T_4^{\text{op}}$  has an element  $c$  for which  $c \cdot x = 0$  for all  $x$ ,  $T_4$  has no such element.
- 9)  $\{0, e, a, b, c, d, f, g\} \mapsto \{0, e, d, f, c, a, b, g\}$  or  $\{0, e, f, d, c, b, a, g\}$ .
- 11) No,  $2\mathbb{Z}$  has a non-zero element  $x$  for which  $x + x = x^2$ ,  $3\mathbb{Z}$  has no such element.
- 13) No,  $\mathbb{R}$  has no element for which  $x^2 + e = 0$ .
- 15)  $Z_{21}$ ,  $3Z_{63}$ ,  $7Z_{147}$ , and  $21Z_{441}$ .
- 17)  $Z_{210}$ ,  $2Z_{420}$ ,  $3Z_{630}$ ,  $5Z_{1050}$ ,  $6Z_{1260}$ ,  $7Z_{1470}$ ,  $10Z_{2100}$ ,  $14Z_{2940}$ ,  $15Z_{3150}$ ,  $21Z_{4410}$ ,  $30Z_{6300}$ ,  $35Z_{7350}$ ,  $42Z_{8820}$ ,  $70Z_{14700}$ ,  $105Z_{22050}$  and  $210Z_{44100}$ .
- 19)
- {0, 6a}, {a, 7a}, {2a, 8a}, {3a, 9a}, {4a, 10a}, {5a, 11a}  $\leftrightarrow$  {0, b, 2b, 3b, 4b, 5b}.
- 21) 4 rings:  $Z_6$ ,  $2Z_{12}$ ,  $3Z_{18}$  and  $6Z_{36}$ .

### Section 10.4

- 1)  $\{0, 1, 2, 3, 4, 5\} \mapsto \{0, 0, 0, 0, 0, 0\}$ ,  $\{0, 1, 2, 3, 4, 5\}$ ,  $\{0, 3, 0, 3, 0, 3\}$ , or  $\{0, 4, 2, 0, 4, 2\}$ .
- 3)  $2 = \phi(1 \cdot 1) \neq \phi(1) \cdot \phi(1) = 4$ .
- 5) No.  $4 = \phi(1 \cdot 1) \neq \phi(1) \cdot \phi(1) = 16$ .

- 7) Yes, since clearly  $\phi(x+y) = (x+y) \bmod 5 = \phi(x) + \phi(y)$ , and  $\phi(x \cdot y) = (x \cdot y) \bmod 5 = \phi(x) \cdot \phi(y)$ .
- 9) No.  $0 = \phi(0) = \phi(1+1) \neq \phi(1) + \phi(1) = 2$ .
- 11)  $\phi(x) + \phi(y) = a+c - (b+d)i = \phi(x+y)$ ,  $\phi(x) \cdot \phi(y) = (a-bi)(c-di) = ac - bd - (bc+ad)i = \phi(x \cdot y)$ .
- 13) If  $x^n = 0$ , then  $\phi(x)^n = \phi(x^n) = \phi(0) = 0$ , so  $\phi(x)$  is nilpotent.
- 15) From Example 10.5, all ideals of  $\mathbb{Z}$  are of the form  $\langle n \rangle$ . If  $n$  is prime, then  $x \cdot y \in \langle n \rangle$  means  $x \cdot y$  is a multiple of  $n$ , which by Euclid's lemma (1.4) says either  $x$  or  $y$  is in  $\langle n \rangle$ , so  $\langle n \rangle$  is a prime ideal. If  $n$  is not prime, then  $n$  factors as  $x \cdot y$ , and  $x \cdot y \in \langle n \rangle$ , but neither  $x$  or  $y$  are in  $\langle n \rangle$ .
- 17) Let  $I$  be a prime ideal, and suppose non-zero elements of  $R/I$  multiply to give the zero element, that is,  $(a+I) \cdot (b+I) = a \cdot b + I = I$ . Then  $a \cdot b \in I$ , so either  $a$  or  $b$  is in  $I$ , giving a contradiction. If  $I$  is not a prime ideal, there is an  $a$  and  $b$  not in  $I$  for which  $a \cdot b \in I$ . But then  $(a+I) \cdot (b+I) = I$ , so  $R/I$  has zero divisors.
- 19) If  $k \in K$  and  $a \in I$ ,  $a \cdot k \in K$  since  $K$  is an ideal of  $R$ , so  $K$  is an ideal of  $I$  as well. The mapping  $\phi : R/K \mapsto R/I$  given by  $\phi(x+K) = x+I$  is a homomorphism, whose image is all of  $x+I$ , and whose kernel is  $I/K$ . So  $I/K$  is an ideal of  $R/K$ , and by the first isomorphism theorem for rings (10.2),  $(R/K)/(I/K) \approx I/K$ .
- 21)

```

I2 = Ideal (R, 2*a + b)
Q = Coset (R, I2)
i = RingHomo (R, Q)
HomoDef (i, a, a + I2)
HomoDef (i, b, b + I2)
FinishHomo (i)
'Homomorphism defined'

```

- 23) Only two possibilities:  $a$  maps to  $a$  or  $b-a$ , and  $b$  maps to  $2 \cdot a$ .

## Section 11.1

- 1)  $b$ .
- 3)  $2ax^2 + ax + b$ .
- 5)  $2ax^3 + 2ax^2 + bx$ .
- 7)  $x^2 + (2+2i)x + 2i$ .
- 9)  $(1+i)x^2 + (2+i)x + 1+i$ .
- 11)  $2x^3 + 2x^2 + ix + 2i$ .
- 13)  $D$  would have no zero divisors, so we can use Proposition 11.2, and the characteristic is a prime number  $p$ . Then the additive order of all non-zero elements is  $p$ .

15)

| + | 0 | e | a | b |
|---|---|---|---|---|
| 0 | 0 | e | a | b |
| e | e | 0 | b | a |
| a | a | b | 0 | e |
| b | b | a | e | 0 |

| · | 0 | e | a | b |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| e | 0 | e | a | b |
| a | 0 | a | b | e |
| b | 0 | b | e | a |

17)  $0^3 = 0$ ,  $1^3 = 1$ ,  $2^3 = 2$ ,  $i^3 = 2i$ ,  $(2i)^3 = i$ ,  $(1+i)^3 = 1+2i$ ,  $(2+i)^3 = 2+2i$ ,  $(1+2i)^3 = 1+i$ ,  $(2+2i)^3 = 2+i$ .

19) The kernel of the homomorphism from Problem 18 is found by setting  $x^3 = 0$ . But since there are no zero-divisors, this can only happen if  $x = 0$ . Since the kernel is the trivial subring, the homomorphism is one-to-one.

21)  $x^2 + 1$ ,  $x^2 + x + 2$ ,  $x^2 + 2x + 2$ ,  $2x^2 + 2$ ,  $2x^2 + x + 1$ ,  $2x^2 + 2x + 1$ .

23)  $x^3$ ,  $x^3 + 1$ ,  $x^3 + x$ ,  $x^3 + x + 1$ ,  $x^3 + x^2$ ,  $x^3 + x^2 + 1$ ,  $x^3 + x^2 + x$ ,  $x^3 + x^2 + x + 1$ .

25) All factorizations reveal triple roots. Reason: For real numbers,  $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$ , but since we are working mod 3,  $(x+y)^3 = x^3 + y^3$ .

## Section 11.2

1)  $\left(\frac{-a}{b}\right) + \left(\frac{a}{b}\right) = \left(\frac{-a \cdot b + a \cdot b}{b^2}\right) = \left(\frac{0}{b^2}\right) = \left(\frac{0}{z}\right).$

3)  $\left(\frac{u}{v}\right) \cdot \left(\left(\frac{x}{y}\right) \cdot \left(\frac{z}{w}\right)\right) = \left(\frac{u}{v}\right) \cdot \left(\frac{xz}{yw}\right) = \left(\frac{uxz}{vyw}\right) = \left(\frac{ux}{vy}\right) \cdot \left(\frac{z}{w}\right) = \left(\left(\frac{u}{v}\right) \cdot \left(\frac{x}{y}\right)\right) \cdot \left(\frac{z}{w}\right).$

5) Isomorphism given by  $0 \mapsto \{(0, 1), (0, 2), (0, 3), (0, 4)\}$ ,

$1 \mapsto \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ ,  $2 \mapsto \{(2, 1), (4, 2), (1, 3), (3, 4)\}$ ,

$3 \mapsto \{(3, 1), (1, 2), (4, 3), (2, 4)\}$ ,  $4 \mapsto \{(4, 1), (3, 2), (2, 3), (1, 4)\}$ .

7) Every rational number  $p/q$  can be put in the form  $(2p)/(2q)$ , so there is a natural mapping from  $\mathbb{Q}$  to the quotient field.

9)  $((1+i)x + i + 2)((1+2i)x + i) = (x + 1 + 2i)(2x + 2i) = 2x^2 + 2x + 2 + 2i$ .

11)  $(x^3 + x^2 + 1)/(x^4 + x)$ .

13)  $x^2/(x^3 + 1)$ .

15)  $(x^3 + x^2)/(x^2 + x + 1)$ .

17)  $(x^3 + x^2)/(x^4 + x^2 + 1)$ .

19) The square of every element is the same as replacing every  $x$  with  $x^2$ .

Reason: because of Problem 9 of §9.3,  $\phi(x) = x^2$  is a ring homomorphism.

21) Cross multiplying,  $(3x+3a)(2x) = ((a+1)x)((1-a)x+5+a) = 6x^2+6ax$ .

## Section 11.3

1)

$$\begin{aligned} e^i &= 1 + \frac{i}{1!} + \frac{-1}{2!} + \frac{-i}{3!} + \frac{1}{4!} + \frac{i}{5!} + \dots \\ &= \left(1 - \frac{1}{2!} + \frac{1}{4!} - \dots\right) + i \left(\frac{1}{1!} - \frac{1}{3!} + \frac{1}{5!} - \dots\right) = \cos 1 + i \sin 1. \end{aligned}$$

3)

$$1 + \frac{i}{n} = \sqrt{1 + \frac{1}{n^2}} (\cos(\tan^{-1}(1/n)) + i \sin(\tan^{-1}(1/n))),$$

so

$$\left(1 + \frac{i}{n}\right)^n = \left(1 + \frac{1}{n^2}\right)^{n/2} (\cos(n \tan^{-1}(1/n)) + i \sin(n \tan^{-1}(1/n))).$$

But

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n^2}\right)^{n/2} = 1 \quad \text{and} \quad \lim_{n \rightarrow \infty} n \tan^{-1}(1/n) = 1$$

by L'Hôpital's rule.

- 5)  $\ln 2 - \pi/6 + 2k\pi i$ , where  $k \in \mathbb{Z}$ .  
 7)  $\sqrt{2}/2 \pm i\sqrt{2}/2, -\sqrt{2}/2 \pm i\sqrt{2}/2$ .  
 9)  $-2i, \pm\sqrt{3} + i$ .  
 11)  $\dots, e^{-7\pi/4}, e^{-3\pi/4}, e^{\pi/4}, e^{5\pi/4}, e^{9\pi/4}, \dots$   
 13)  $(1)^{i \ln 2/(2\pi)}$ .  
 15) From DeMoivre's theorem, all solutions  $z^n = 1$  are of the form  $z = \cos(2k\pi/n) + i \sin(2k\pi/n) = (\cos(2\pi/n) + i \sin(2\pi/n))^k$ . Thus,  $\omega_n$  generates the group. A generator of this group would be  $\omega_n^k$ , where  $k$  is coprime to  $n$ , hence a primitive  $n$ -th root of unity.  
 17) False:  $(2^2)^{1/2} = 4^{1/2} = \pm 2$ , yet  $2^{(2 \cdot 1/2)} = 2^1 = 2$ .  
 19)

```
H = [I, 1/2 + I*sqrt(3)/2, I/2 + sqrt(3)/2,
     1, -I/2 + sqrt(3)/2, 1/2 - I*sqrt(3)/2,
     -I, -1/2 - I*sqrt(3)/2, -I/2 - sqrt(3)/2,
     -1, I/2 - sqrt(3)/2, -1/2 + I*sqrt(3)/2]
CircleGraph(H, Mult(sqrt(3) + I/2))
```



Taylor & Francis  
Taylor & Francis Group  
<http://taylorandfrancis.com>

---

# Bibliography

The following list not only gives the books and articles mentioned in the text but also additional references that may help students explore related topics.

## Undergraduate textbooks on Abstract Algebra

1. J. B. Fraleigh, *A First Course in Abstract Algebra*, 8th ed., Addison Wesley, Boston (2009).
2. J. A. Gallian, *Contemporary Abstract Algebra*, 8th ed., Houghton Mifflin, Boston (2013).
3. J. Gilbert and L. Gilbert, *Elements of Modern Algebra*, 8th ed., PWS Publishing Co., Boston (2014).
4. L. J. Goldstein, *Abstract Algebra, A First Course*, Prentice-Hall, Englewood Cliffs, New Jersey (1973).
5. I. N. Herstein, *Abstract Algebra*, Macmillan Publishing Company, New York (1986).
6. T. W. Hungerford, *Abstract Algebra, An Introduction*, Saunders College Publishing, Philadelphia (1990).
7. J. J. Rotman, *A First Course in Abstract Algebra*, Prentice-Hall, Upper Saddle River, New Jersey (1996).

## Graduate textbooks on Abstract Algebra

8. I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, New York (1975).
9. J. F. Humphrey, *A Course in Group Theory*, Oxford University Press, Oxford (1996).
10. D. S. Malik, J. N. Mordeson, and M. K. Sen, *Fundamentals of Abstract Algebra*, McGraw-Hill, New York (1997).

## Sources for historical information

11. D. M. Burton, *The History of Mathematics, An Introduction*, 6th ed., McGraw-Hill, Boston (2007).
12. J. H. Eves, *An Introduction to the History of Mathematics*, 6th ed., Saunders College Publishing, Fort Worth (1990).

**Other sources**

13. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford (1985).
14. The GAP Group, *GAP Reference Manual*, Release 4.4.12, <http://www.gap-system.org>.
15. I. S. Reed and G. Solomon, “Polynomial Codes over Certain Finite Fields,” *SIAM Journal of Applied Math.*, **8** (1960) pp. 300–304.
16. “Reed-Solomon error correction,” Wikipedia, the free encyclopedia, <http://en.wikipedia.org>.
17. W. Paulsen, “Calkin-Wilf Sequences for Irrational Numbers,” *The Fibonacci Quarterly*, **61**:1 (2023) pp. 51–57.

---

# Index

Page numbers are underlined in the index when they represent the definition or the main source of information about the subject indexed. Boldface page numbers refer to sections for which the entire section pertains to the topic. References to problems are in italics. Occasionally, both underlining and italics are appropriate, should a homework problem introduce a new concept. Note that in these cases, only the homework problems are indexed, and not the answers in the back, even though the answers often shed more light on the topic.

- $A_4$ , 171, 189, 197, 245, 255  
 $A_5$ , 189, 246, 248, 251, 252  
 $A_6$ , 247, 251, 254, 267  
 $A_n$ , 170, 235, 247  
    is simple, 248  
Abel, Niels, 253  
abelian group, 60, 94, 120, 126,  
    143, **198**, 208, 210, 235,  
    237, 278, 282, 286, 292  
absolute value, 282, **360**  
associative property, 46, 59, 83,  
    223, 289, 353, 356  
automorphism  
    for a group, 211, 213, 216,  
        219, 221, 222, 227, 230,  
        231  
    for a ring, 358, 359  
group of automorphisms, **210**,  
    212, 213, 215, 221  
    inner, 215, 217, 235  
    outer, 218  
 $\text{Aut}(Z_{24}^*)$ , 220, 249, 251, 252, 262  
basis for a finite ring, 286, **292**,  
    292  
Bézout's lemma, 5  
binary operation, 21, 52, 55, 59,  
    65  
binomial theorem, **298**
- Boolean ring, 298  
canonical homomorphism, 147, **151**,  
    154, 202  
Cantor, Georg, 37, 39  
    theorem, 37, 200  
Cauchy, Augustin, 209  
Cayley, Arthur, 181, 183  
    table, 45, 53, 58  
    theorem, **173**, 175, 180, 183  
        generalized, 179, 180, 183  
center of a group, 233, 234, 238,  
    265  
centerless, 235, 248, 249  
centralizer, *see* normalizer  
characteristic, 285, 292, 298, 341,  
    342  
    subgroup, 238  
Chevalley groups, 251, 252  
chief series, 264  
Chinese remainder theorem, 30,  
    33, 72, 108, 199, 321  
closure property, 59, 123  
commutative  
    diagram, 147, **151**, 155, 332  
    group, *see* abelian group  
    ring, 278, 280, 289, 291, 298,  
        315, 336  
composition

- factors, [257](#), [262](#), [262](#)
- of functions, [61](#), [147](#), [154](#), [159](#)
- series, [256](#), [257](#), [263](#), [262](#)
- conjugacy class, [243](#), [244](#), [252](#), [254](#)
- conjugate, [243](#), [247](#), [248](#)
  - complex, [359](#)
  - quaternion, [282](#)
- coprime, [5](#), [30](#), [33](#), [57](#), [60](#), [70](#), [101](#), [106](#), [198](#), [321](#), [364](#)
- cosets
  - of a subgroup, [96](#), [98](#), [102](#), [116](#), [117](#), [118](#), [122](#), [126](#), [145](#), [177](#), [179](#)
  - of a subring, [306](#), [308](#), [309](#), [310](#), [366](#)
- countable set, [35](#), [36](#), [37](#)
- cycle, [164](#), [171](#), [172](#), [184](#), [214](#), [215](#), [235](#)
  - decomposition, [167](#)
- cyclic
  - group, [73](#), [75](#), [86](#), [88](#), [91](#), [101](#), [126](#), [129](#), [135](#), [172](#), [190](#), [207](#), [208](#), [237](#), [251](#), [364](#), [369](#)
    - see also*  $Z_n$
  - ring, [291](#), [319](#), [320](#), [321](#), [322](#)
- $D_4$ , [48](#), [132](#), [133](#), [177](#), [179](#), [180](#), [221](#), [234](#), [263](#)
- $D_5$ , [135](#), [221](#), [237](#), [242](#), [252](#), [263](#)
- $D_6$ , [238](#), [263](#)
- $D_n$ , [133](#), [238](#)
  - decomposition of a group, [193](#), [201](#), [203](#), [205](#), [206](#), [208](#), [267](#)
- Dedekind, Richard, [334](#)
  - domain, [335](#)
- degree of polynomial, [336](#), [340](#), [345](#)
- dimension of a vector space, [276](#)
- direct product, [190](#), [198](#), [203](#), [205](#), [208](#)
- disjoint cycles, [166](#), [172](#), [182](#), [244](#)
- distributive property, [278](#), [310](#), [353](#)
- division algorithm, [2](#), [5](#), [27](#), [187](#)
- division ring, [280](#), [296](#), [298](#)
  - see also* field, skew field
- duplicate the cube, [10](#)
- equivalence
  - classes [51](#), [244](#), [348](#), [353](#)
  - relationship, [50](#), [244](#), [347](#)
- Euclid [7](#), [10](#), [11](#)
- Euclidean algorithm [5](#), [32](#)
- Euler totient function,
  - see* totient function
- even permutation,
  - see* permutation
- exponential (complex), [365](#), [367](#)
- ExpressAsWord, [269](#), [273](#)
- factorization
  - integer [1](#), [5](#), [8](#), [9](#), [72](#), [110](#), [207](#), [262](#)
  - polynomial [344](#)
- Fermat, Pierre de, [102](#), [103](#)
- field, [280](#), [296](#), [311](#), [337](#), [346](#), [355](#)
  - of quotients, [346](#), [349](#)
- freshman's dream, [298](#)
- GCD, *see* greatest common divisor
- generators
  - of a group, [68](#), [69](#), [75](#), [76](#), [132](#), [138](#), [194](#), [369](#)
  - of a ring, [283](#), [286](#), [288](#), [290](#), [319](#)
- greatest common divisor [5](#), [11](#), [90](#), [91](#), [321](#), [321](#)
- group, [59](#), [65](#), [73](#), [82](#), [101](#), [129](#), [134](#), [135](#), [136](#), [175](#), [212](#), [278](#)
- holomorph, [231](#)
- homomorphism
  - of groups, [136](#), [143](#), [144](#), [145](#), [151](#), [169](#), [179](#), [222](#), [225](#), [227](#), [230](#), [365](#)

- of rings, 317, 326, 327, 328, 329, 331, 333, 358
- ideal, 309, 311, 312, 313, 329, 331
  - left, 315
- idempotent, 298
- identity, 46, 48, 59, 61, 137, 162, 165, 190, 195, 278, 279, 282, 288, 289, 293, 302
- image, 140, 142, 144, 329
- index
  - of a subgroup, 102, 120, 156
  - of this book, 401
- induction, 4, 15, 19, 62, 63, 74, 166, 169, 171, 200, 201, 205, 284, 298, 363
- inverse, 46, 48, 57, 59, 279, 280, 293, 295, 296, 299, 353
- invertible element, 59, 147, 279, 293, 295
- irreducible element, 299
- isomorphism
  - of groups, 128, 135, 145, 146, 161, 196
  - of rings, 316, 317, 322
- theorems, 145, 150, 154, 331, 335
- Jordan-Hölder theorem, 262, 264
- kernel, 141, 142, 143, 144, 179, 329, 330, 366
- Kummer, Ernst, 314
- Lagrange's theorem, 100, 101, 105, 117, 130, 245
- Latin square, 47, 64, 66, 82, 275
- linear functions, 61, 121
- logarithm (complex), 366, 369
- modulo, 49, 55, 57, 59, 94, 108, 123, 275, 343, 346
- mutually coprime, 33
- nilpotent, 305, 315
- Noether, Emmy, 281
- normal
  - closure, 241, 246, 251
  - series, 255, 256, 263
    - see also* subnormal series
- subgroup, 116, 118, 121, 121, 122, 124, 141, 143, 146, 149, 150, 152, 154, 170, 180, 182, 196, 217, 223, 225, 234, 236, 239, 241, 244, 246, 247, 249, 254, 255, 260, 310
- normalizer, 239, 240, 242, 243
- octahedral group, 81, 82, 116, 122, 124, 124, 138, 152, 147, 160, 217
  - see also*  $S_4$
- order
  - of a group, 61, 100, 102, 106, 128, 134, 175, 180, 207, 208
  - of an element, 70, 81, 82, 88, 94, 95, 101, 163, 172, 196, 283
  - of a ring, 292, 322, 325
- permutation, 78, 79, 157, 163, 165, 167, 173, 175, 211, 212, 219
  - see also*  $S_n$
- alternating, *see* even
- even, 170, 172, 189, 266
  - see also*  $A_n$
- odd, 170, 189
- ordering, 184, 185, 189, 219
- PID, *see* principal ideal domain
- pigeonhole principle, 16, 65, 107, 161, 322
- polynomials, 144, 336, 337, 340, 345
- prime
  - element of a ring, 299, 335
  - factorization, 3, 110, 207
  - ideal, 335

- integer, [1](#), [3](#), [4](#), [72](#), [94](#), [108](#), [109](#), [110](#), [182](#), [201](#), [313](#), [341](#)
- order, [101](#), [129](#), [200](#), [247](#), [251](#), [262](#), [294](#), [296](#)
- primitive  $n$ -th root of unity, [364](#), [369](#)
- principal ideal, [312](#)
  - domain, [313](#)
  - ring, [312](#)
- Pyraminx<sup>TM</sup>, [92](#), [93](#), [95](#), [264](#), [271](#)
- quadratic residues, [94](#)
- quasidihedral group, [229](#)
- quaternion group, [132](#), [138](#), [144](#), [173](#), [182](#), [184](#), [215](#), [218](#), [237](#), [240](#), [252](#), [263](#), [275](#), [276](#)
- quaternions, [276](#), [280](#), [282](#), [333](#)
- quotient
  - group, [122](#), [125](#), [145](#), [153](#), [154](#), [218](#), [235](#), [238](#), [257](#), [309](#)
  - ring, [306](#), [309](#), [310](#), [315](#), [325](#), [330](#)
- reducible, *see* irreducible
- reductio ad absurdum, [4](#)
- refinement, [256](#), [258](#), [260](#), [262](#), [263](#)
- reflexive property, *see* equivalence relation
- ring, [274](#), [278](#), [279](#), [282](#), [285](#), [286](#), [288](#), [292](#), [294](#), [298](#), [300](#), [304](#), [306](#), [309](#), [316](#), [319](#), [326](#), [329](#), [331](#), [335](#), [336](#), [358](#)
  - see also* commutative ring, division ring
- with identity,
  - see* unity ring
- without zero divisors, [279](#), [294](#), [296](#), [341](#), [343](#), [351](#)
- Rivest-Shamir-Adleman, [110](#), [113](#)
- RSA encryption, *see* Rivest-Shamir-Adleman
- Rubik's Cube<sup>®</sup>, [270](#), [271](#)
- $S_3$ , [79](#), [82](#), [84](#), [85](#), [120](#), [124](#), [127](#), [128](#), [131](#), [134](#), [144](#), [156](#), [163](#), [194](#), [196](#), [197](#), [218](#), [221](#), [235](#), [241](#)
- $S_4$ , [160](#), [163](#), [179](#), [180](#), [217](#), [236](#), [244](#), [246](#), [255](#)
- $S_5$ , [163](#), [180](#), [262](#)
- $S_n$ , [159](#), [160](#), [170](#), [172](#), [235](#), [249](#)
  - subgroups of, [175](#), [179](#), [180](#)
- semi-direct product, [222](#), [231](#)
- simple group, [247](#), [248](#), [249](#), [252](#), [262](#)
- skew field, [280](#), [311](#)
  - see also* quaternions
- solvable
  - group, [262](#)
- sporadic groups, [251](#), [252](#)
- Stern's diatomic sequence, [40](#)
- subfield, [355](#)
- subgroup, [83](#), [93](#), [94](#), [95](#), [98](#), [100](#), [102](#), [118](#), [120](#), [121](#), [126](#), [129](#), [140](#), [143](#), [148](#), [149](#), [150](#), [152](#), [156](#), [172](#), [175](#), [179](#), [180](#), [193](#), [198](#), [201](#), [212](#), [220](#), [223](#), [225](#), [239](#), [259](#), [271](#)
  - see also* normal subgroup
- subnormal series, [255](#), [256](#), [258](#), [260](#), [263](#)
- subring, [300](#), [305](#), [306](#), [309](#), [311](#), [313](#), [324](#), [328](#), [333](#)
- symmetric
  - group, *see*  $S_3$ ,  $S_4$ ,  $S_5$ ,  $S_n$
  - property, *see* equivalence relation
- $T_4$ , [296](#), [299](#), [306](#), [324](#)
- $T_8$ , [291](#), [292](#), [296](#), [299](#), [306](#), [324](#)
- Terry's group, [44](#), [49](#), [60](#), [73](#), [79](#), [97](#), [102](#), [144](#)
  - see also*  $S_3$

- torsion subgroup, [94](#)  
 totient function, [71](#), [72](#), [74](#), [101](#)  
 transitive  
     property, *see* equivalence relation  
     subgroup, [172](#), [183](#)  
 transpose, [324](#)  
 transposition, [168](#), [169](#), [214](#), [244](#)  
 trisect an angle, [10](#)
- UFD, *see* unique factorization domain  
 unique factorization, [3](#), [353](#)  
     domain (UFD), [314](#)  
 unity ring, [278](#), [282](#), [288](#), [289](#),  
     [293](#), [295](#), [297](#), [299](#), [292](#)
- vector, [276](#)
- well defined function [13](#), [18](#), [63](#),  
     [152](#), [169](#), [179](#), [316](#), [321](#),  
     [332](#), [348](#)
- well ordering axiom [3](#), [15](#), [5](#)
- wreath product, [231](#), [232](#),
- $Z_5$ , [76](#), [180](#)  
 $Z_6$ , [275](#), [280](#), [325](#), [326](#), [333](#)  
 $Z_8$ , [210](#), [213](#)  
 $Z_{10}$ , [68](#), [96](#), [317](#)  
 $Z_{12}$ , [90](#), [93](#), [125](#), [258](#), [263](#), [325](#)  
 $Z_{15}$ , [293](#)  
 $Z_n$ , [60](#), [70](#), [75](#), [88](#), [91](#), [94](#), [123](#),  
     [129](#), [190](#), [198](#), [208](#), [213](#),  
     [292](#), [293](#), [294](#), [296](#), [311](#),  
     [316](#), [317](#), [319](#), [321](#), [364](#)  
 $Z_p$  ( $p$  prime), [129](#), [200](#), [247](#), [249](#),  
     [262](#), [294](#), [296](#), [369](#)  
 $Z_8^*$ , [73](#), [76](#), [129](#), [144](#), [156](#), [180](#),  
     [194](#), [196](#), [213](#), [213](#), [218](#),  
     [246](#), [325](#)  
 $Z_{15}^*$ , [56](#), [93](#), [125](#), [144](#), [180](#), [191](#),  
     [193](#), [196](#), [221](#), [263](#), [284](#),  
     [288](#), [306](#), [323](#)  
 $Z_{24}^*$ , [131](#), [182](#), [203](#), [218](#), [263](#), [290](#),  
     [292](#), [306](#), [323](#)
- $Z_{33}^*$ , [105](#)  
 $Z_n^*$ , [60](#), [94](#), [102](#), [109](#), [144](#), [213](#)  
 zero divisors, [279](#), [280](#), [289](#), [294](#),  
     [295](#), [342](#), [343](#)  
     *see also* ring without zero divisors  
 zero homomorphism, [327](#)  
 zero of polynomial, *see* root