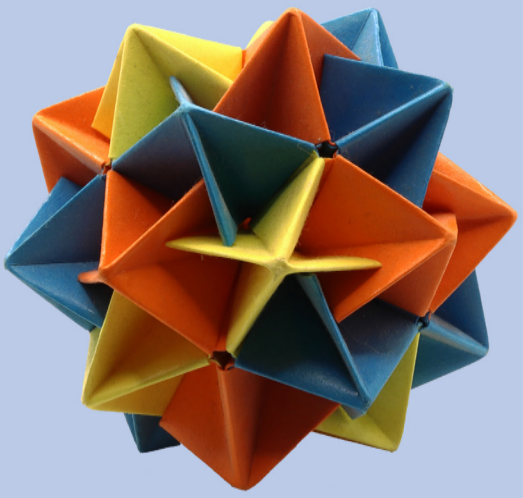
TEXTBOOKS IN MATHEMATICS

ABSTRACT ALGEBRA

A First Course

SECOND EDITION

Stephen Lovett



$$\frac{1}{|A_5|}\sum_{\sigma\in A_5}|X^\sigma|$$

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Abstract Algebra

Textbooks in Mathematics

Series editors:
Al Boggess, Kenneth H. Rosen

Elementary Number Theory
Gove Effinger, Gary L. Mullen

Philosophy of Mathematics
Classic and Contemporary Studies
Ahmet Cevik

An Introduction to Complex Analysis and the Laplace Transform
Vladimir Eiderman

An Invitation to Abstract Algebra
Steven J. Rosenberg

Numerical Analysis and Scientific Computation
Jeffery J. Leader

Introduction to Linear Algebra
Computation, Application and Theory
Mark J. DeBonis

The Elements of Advanced Mathematics, Fifth Edition
Steven G. Krantz

Differential Equations
Theory, Technique, and Practice, Third Edition
Steven G. Krantz

Real Analysis and Foundations, Fifth Edition
Steven G. Krantz

Geometry and Its Applications, Third Edition
Walter J. Meyer

Transition to Advanced Mathematics
Danilo R. Diedrichs and Stephen Lovett

Modeling Change and Uncertainty
Machine Learning and Other Techniques
William P. Fox and Robert E. Burks

Abstract Algebra
A First Course, Second Edition
Stephen Lovett

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

Abstract Algebra

A First Course

Second Edition

Stephen Lovett

Wheaton College, USA

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

Second edition published 2022
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

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

© 2022 Taylor & Francis, LLC

First edition published by CRC Press 2016

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

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 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

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

Library of Congress Cataloging-in-Publication Data

Names: Lovett, Stephen (Stephen T.), author.
Title: Abstract algebra : a first course / authored by Stephen Lovett, Wheaton College, USA.
Description: Second edition. | Boca Raton : Chapman & Hall, CRC Press, 2022. | Series: Textbooks in mathematics | Includes bibliographical references and index.
Identifiers: LCCN 2021062210 (print) | LCCN 2021062211 (ebook) | ISBN 9781032289397 (hardback) | ISBN 9781032289410 (paperback) | ISBN 9781003299233 (ebook)
Subjects: LCSH: Algebra, Abstract--Textbooks.
Classification: LCC QA162 .L68 2022 (print) | LCC QA162 (ebook) | DDC 512/.02--dc23/eng20220415
LC record available at https://lccn.loc.gov/2021062210
LC ebook record available at https://lccn.loc.gov/2021062211

ISBN: 978-1-032-28939-7 (hbk)
ISBN: 978-1-032-28941-0 (pbk)
ISBN: 978-1-003-29923-3 (ebk)

DOI: 10.1201/9781003299233

Typeset in CMR10
by KnowledgeWorks Global Ltd.

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

Access the Support Material at: www.routledge.com/9781032289397.

Contents

Preface to Instructors

This textbook intends to serve as a first course in abstract algebra. Students are expected to possess a background in linear algebra and some basic exposure to logic, set theory, and proofs, usually in the form of a course in discrete mathematics or a transition course. The selection of topics serves both of the common trends in such a course: a balanced introduction to groups, rings, and fields; or a course that primarily emphasizes group theory. However, the book offers enough flexibility to craft many other pathways. By design, the writing style remains student-centered, conscientiously motivating definitions and offering many illustrative examples. Various sections, or sometimes just examples or exercises, introduce applications to geometry, number theory, cryptography, and many other areas.

Order and Selection of Topics

With 48 sections, each written to correspond to a one-hour contact period, this book offers various possible paths through a one-semester introduction to abstract algebra. Though Chapter 1 begins right away with the theory of groups, an instructor may wish to use some of the sections from the Appendix (complex numbers, set theory, elementary number theory) as preliminary content or review. To create a course that offers an approximately balanced introduction to groups, rings, and fields, the instructor could select to use Chapters 1 through 5 and perhaps opt to skip Sections 1.11, 1.12, and 1.13 in the chapter on group theory, which discusses groups in geometry, the Diffie-Hellman public key algorithm, and monoids, respectively. To design a course that emphasizes group theory, the author could complete all of Chapters 1 and 2, select an appropriate number of sections from the next three chapters on rings and fields, and then complete Chapter 6, which offers topics in group theory, including group actions and semi-direct products.

Besides the application sections, the instructor may wish to add color to the course by spending a little more time on some subsections marked as optional or by devoting a few days to student projects or various computer algebra systems designed for abstract algebra.

Software and Computer Algebra Systems

There exist a number of commercial computer algebra systems (CAS) (e.g., *Maple*, *Mathematica*, *MATLAB*) that provide packages that implement certain calculations that are useful in algebra. There also exist several free CAS that are specifically designed for computations in algebra (e.g., *SageMath*, *Magma*, and *Macaulay2*). It is impossible in this textbook to offer a tutorial on each one. Though the reader should visit the various CAS help pages, we occasionally end a section by discussing a few commands or libraries of commands that are relevant to that section.

This textbook will draw examples from *Maple*[1] and SageMath or more briefly Sage[2]. *Maple* comes with its own user interface that involves either a Worksheet Mode or Document Mode. The company MapleSoft offers excellent online help files and programming guides for every aspect of this CAS. (Though we do not explicitly describe the commands for *Mathematica*, they are similar in structure to *Maple*.)

To interact with SageMath, the user will employ either the SageMath shell or a Jupyter notebook. Sage is built on Python[3] so it natively incorporates syntax from Python and itself can easily be called from a Python script. For example, Python's `Combinatorics` module offers commands for calculating the order of a permutation group, i.e., a group defined as a subgroup of the symmetric group S_n, but Sage subsumes this.

Unless indicated by CAS, it is generally expected that the computations in the exercises be done by hand and not require the use of a CAS.

Projects

Another feature of this book is the project ideas, listed at the end of each chapter. The project ideas come in two flavors: investigative or expository.

The investigative projects briefly present a topic and pose open-ended questions that invite the student to explore the topic, asking them to try to answer their own questions. Investigative projects may involve computations, utilize some programming, or lead the student to try to prove something original (or original to them). For investigative projects, students should not consult outside sources, or only do so minimally for background. Indeed, it

[1] *Maple* is made by MapleSoft, whose website is https://www.maplesoft.com/

[2] Previously known as SAGE for "System for Algebra and Geometry Experimentation," the official website for SageMath is https://www.sagemath.org/

[3] The website https://docs.sympy.org/latest/modules/index.html lists all the modules available through SymPy, the Python library for symbolic mathematics.

is possible to find sources on many of the investigative projects, but finding such sources is not the point of an investigative project.

Expository projects invite the student to explore a topic with algebraic content or pertain to a particular mathematician's work through responsible research. The exploration should involve multiple sources and the paper should offer a report in the students' own words, and offering their own insights as they can. In contrast to investigative projects, expository projects rely on the use of outside (library) sources and cite them appropriately.

A possible rubric for grading projects involves the "4Cs of projects". The projects should be (1) Clear: Use proper prose, follow the structure of a paper, and provide proper references; (2) Correct: Proofs and calculations must be accurate; (3) Complete: Address all the questions or questions one should naturally address associated with the investigation; and (4) Creative: Evidence creative problem-solving or question-asking skills.

When they require letters of recommendation, graduate schools and sometimes other employers want to know a student's potential for research or other type of work (independent or team-oriented). If a student has not landed one of the few coveted REU spots during their undergraduate years, speaking to the student's participation in class does not answer that rubric well. A faculty person who assigns projects will have some speaking points for rubric on a letter of recommendation for a student.

Habits of Notation and Expression

This book regularly uses $\Longrightarrow$ for logical implication and $\Longleftrightarrow$ for logical equivalence. More precisely, if $P(x, y, \ldots)$ is a predicate with some variables and $Q(x, y, \ldots)$ is another predicate using the same variables, then

$$P(x, y, \ldots) \Longrightarrow Q(x, y, \ldots) \quad \text{means} \quad \forall x \forall y \ldots \big(P(x, y, \ldots) \longrightarrow Q(x, y, \ldots)\big)$$

and

$$P(x, y, \ldots) \Longleftrightarrow Q(x, y, \ldots) \quad \text{means} \quad \forall x \forall y \ldots \big(P(x, y, \ldots) \longleftrightarrow Q(x, y, \ldots)\big).$$

As another habit of expression particular to this author, the textbook is careful to always and only use the expression "Assume [hypothesis]" as the beginning of a proof by contradiction. Like so, the reader can know ahead of time that whenever he or she sees this expression, the assumption will eventually lead to a contradiction.

Solutions Manual

A solutions manual for all exercises is available by request. Faculty may obtain one by contacting me directly at

stephen.lovett@wheaton.edu

or at

www.routledge.com/9781032289397

Furthermore, the author invites faculty using this textbook to email their suggestions for improvement and other project ideas for inclusion in future editions.

Acknowledgments

First, I must thank the reviewers and my publisher for many helpful suggestions for improvements. The book would not be what it is without their advice. Next, I must thank the mathematics majors at Wheaton College (IL) who served for many years as the test environment for many topics, exercises, and projects. I am indebted to Wheaton College (IL) for the funding provided through the Aldeen Grant that contributed to portions of this textbook. I especially thank the students who offered specific feedback on the draft versions of this book, in particular Kelly McBride, Roland Hesse, and David Garringer. Joel Stapleton, Caleb DeMoss, Daniel Bradley, and Jeffrey Burge deserve special gratitude for working on the solutions manual to the textbook. I also must thank Justin Brown for test running the book and offering valuable feedback. I also thank Africa Nazarene University for hosting my sabbatical, during which I wrote a major portion of this textbook.

Preface to Students

What is Abstract Algebra?

When a student of mathematics studies abstract algebra, he or she inevitably faces questions in the vein of, "What makes the algebra abstract?" or "What is it good for?" or, more teasingly, "I finished algebra in high school; why are you still studying it as a math major?" On the other hand, since undergraduate mathematics curriculum designers nearly always include an algebra requirement, then these questions illustrate an awareness gap by the general public about advanced mathematics. Consequently, we try to answer this question up front: "What is abstract algebra?"

Algebra, in its broadest sense, describes a way of thinking about classes of sets equipped with binary operations. In high school algebra, a student explores properties of operations ($+$, $-$, $\times$, and $\div$) on real numbers. In contrast, abstract algebra studies properties of operations without specifying what types of numbers or objects we work with. Hence, any theorem established in the abstract context holds not only for real numbers but for every possible algebraic structure that has operations with the stated properties.

Linear algebra follows a similar process of abstraction. After an introduction to systems of linear equations, it explores algebraic properties of vectors in $\mathbb{R}^n$ along with properties and operations of $m \times n$ matrices. Then, a linear algebra course generalizes these concepts to abstract (or general) vector spaces. Theorems in abstract linear algebra not only apply to n-tuples of real numbers but imply profound consequences for analysis, differential equations, statistics, and so on.

A typical first course in abstract algebra introduces the structures of groups, rings, and fields. There are many other interesting and fruitful algebraic structures but these three have many applications within other branches of mathematics – in number theory, topology, geometry, analysis, and statistics. Outside of pure mathematics, scientists have noted applications of abstract algebra to advanced physics, inorganic chemistry, methods of computation, information security, and various forms of art, including music theory. (See [18], [10], [9], or [12].)

Strategies for Studying

From a student's perspective, one of the biggest challenges to modern algebra is its abstraction. Calculus, linear algebra, and differential equations can be taught from many perspectives, but often most of the exercises simply require the student to carefully follow a certain prescribed algorithm. In contrast, in abstract algebra (and other advanced topics) students do not learn as many specific algorithms and the exercises challenge the student to prove new results using the theorems presented in the text. The student then becomes an active participant in the development of the field.

In this textbook, however, for many exercises (though not all) the student will find useful ideas either in a similar example or informative strategies in the proofs of the theorems in the section. Therefore, though the theorems are critical, it is very useful to spend time studying the examples and the proofs of theorems. Furthermore, to get a full experience of the material, we encourage the reader to peruse the exercises in order to see some of the interesting consequences of the theory.

Projects

This book offers a unique feature in the lists of projects at the end of each section. Graduate schools always, and potential employers sometimes, want to know about a mathematics student's potential for research. Even if an undergraduate student does not get one of the coveted spots in an official REU (Research Experience for Undergraduates) or write a senior thesis, the expository writing or the exploratory work required by a project offers a vehicle for a faculty person to assess the student's potential for research. So the author of this textbook does not view projects as just something extra or cute, but rather an opportunity for a student to work on and demonstrate his or her potential for open-ended investigation.

1

Groups

As a field in mathematics, group theory did not develop in the order that this book follows. Historians of mathematics generally credit Evariste Galois with first writing down the current definition of a group. Galois introduced groups in his study of symmetries among the roots of polynomials. Galois' methods turned out to be exceedingly fruitful and led to a whole area called Galois theory, a topic sometimes covered in a second course in abstract algebra.

As mathematicians separated the concept of a group from Galois' application, they realized two things. First, groups occur naturally in many areas of mathematics. Second, group theory presents many challenging problems and profound results in its own right. Like modern calculus texts that slowly lead to the derivative concept after a rigorous definition of the limit, we begin with the definition of a group and methodically prove results with a view toward as many applications as possible, rather than a single application.

Groups form another algebraic structure, like vector spaces. Unlike vector spaces, which require between 8 and 10 axioms (depending on how we organize the definition), the definition for a group only requires three axioms. Given the relative brevity of the definition for a group, the richness of the theory of groups and the vast number of applications may come as a surprise to readers.

In Section 1.1 we precede a general introduction to groups with an interesting example from geometry. Sections 1.2 through 1.4 introduce the axioms for groups, present many elementary examples, establish some elementary properties of group elements, and then discuss the concept of classification. Section 1.5 introduces the symmetric group, a family of groups that plays a central role in group theory.

Sections 1.6 and 1.7 study subgroups, how to describe them, or how to prove that a given subset is a subgroup, while Section 1.8 borrows from the Hasse diagrams of a partial order to provide a visual representation of subgroups within a group. Section 1.9 introduces the concept of a homomorphism between groups, functions that preserve the group structure. Section 1.10 introduces a particular method to describe the content and structure of a group and introduces the fundamental notion of a free group.

The last three sections are optional to a concise introduction to group theory. Sections 1.11 and 1.12 provide two applications of group theory, one to patterns in geometry and the other to information security. Finally, Section 1.13 introduces the concept of a monoid, offering an example of another common algebraic structure, similar to groups but with looser axioms.

DOI: 10.1201/9781003299233-1

1.1 Symmetries of a Regular Polygon

1.1.1 Dihedral Symmetries

Let $n \geq 3$ and consider a regular n-sided polygon, P_n. Call $V = \{v_1, v_2, \ldots, v_n\}$ the set of vertices of P_n as a subset of the Euclidean plane $\mathbb{R}^2$. For simplicity, we often imagine the center of P_n at the origin and that the vertex v_1 on the positive x-axis.

A *symmetry* of a regular n-gon is a bijection $\sigma : V \to V$ that is the restriction of a bijection $F : \mathbb{R}^2 \to \mathbb{R}^2$, that leaves the overall vertex-edge structure of P_n in place; i.e., if the unordered pair $\{v_i, v_j\}$ are the end points of an edge of the regular n-gon, then $\{\sigma(v_i), \sigma(v_j)\}$ is also an edge.

Consider, for example, a regular hexagon P_6 and the bijection $\sigma : V \to V$ such that $\sigma(v_1) = v_2$, $\sigma(v_2) = v_1$, and σ stays fixed on all the other vertices. Then σ is not a symmetry of P_6 because it fails to preserve the vertex-edge structure of the hexagon. As we see in Figure 1.1, though $\{v_2, v_3\}$ is an edge of the hexagon, while $\{\sigma(v_2), \sigma(v_3)\}$ are not the endpoints of an edge of the hexagon.

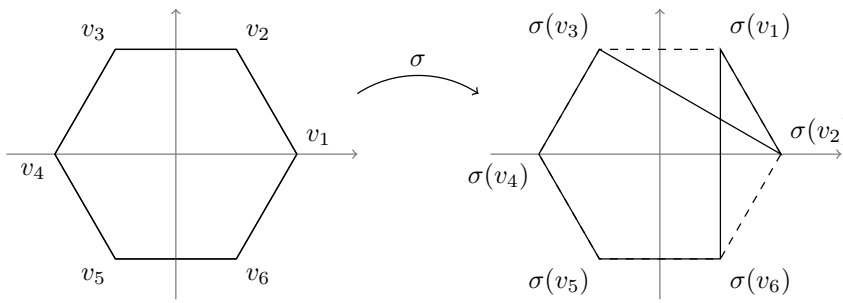


FIGURE 1.1: Not a hexagon symmetry.

In contrast, consider the bijection $\tau : V \to V$ defined by

$$\tau(v_1) = v_2,\ \tau(v_2) = v_1,\ \tau(v_3) = v_6,\ \tau(v_4) = v_5,\ \tau(v_5) = v_4,\ \tau(v_6) = v_3.$$

This bijection on the vertices is a symmetry of the hexagon because it preserves the edge structure of the hexagon. Figure 1.2 shows that τ can be realized as the reflection through the line L as drawn.

Definition 1.1.1

We denote by D_n the set of symmetries of the regular n-gon and call it the set of *dihedral* symmetries.

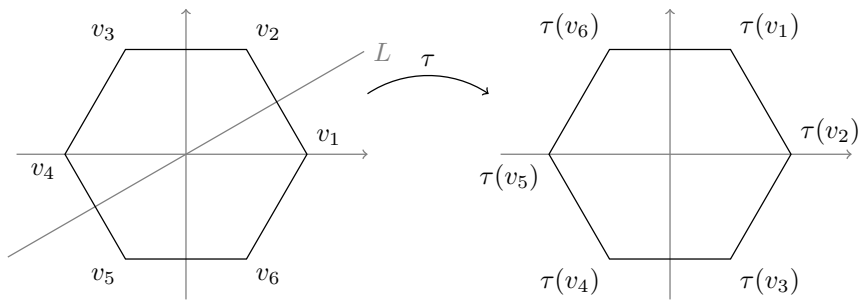


FIGURE 1.2: A reflection symmetry of the hexagon.

To count the number of bijections on the set $V = \{v_1, v_2, \ldots, v_n\}$, we note that a bijection $f : V \to V$ can map $f(v_1)$ to any element in V; then it can map $f(v_2)$ to any element in $V \setminus \{f(v_1)\}$; then it can map $f(v_3)$ to any element in $V \setminus \{f(v_1), f(v_2)\}$; and so on. Hence, there are

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!$$

distinct bijections on V.

However, a symmetry $\sigma \in D_n$ can map $\sigma(v_1)$ to any element in V (n options), but then σ must map v_2 to a vertex adjacent to $\sigma(v_1)$ (2 options). Once $\sigma(v_1)$ and $\sigma(v_2)$ are known, all remaining $\sigma(v_i)$ for $3 \leq i \leq n$ are determined. In particular, $\sigma(v_3)$ must be the vertex adjacent to $\sigma(v_2)$ that is not $\sigma(v_1)$; $\sigma(v_4)$ must be the vertex adjacent to $\sigma(v_3)$ that is not $\sigma(v_2)$; and so on. This reasoning leads to the following proposition.

Proposition 1.1.2

The cardinality of D_n is $|D_n| = 2n$.

It is not difficult to identify these symmetries by their geometric meaning. Half of the symmetries in D_n are rotations that shift vertices k spots counterclockwise, for k ranging from 0 to $n-1$. For the rest of this section, we denote by R_α the rotation around center of the polygon of angle α. The rotation $R_{2\pi k/n}$ of angle $2\pi k/n$ on the set of vertices, performs

$$R_{2\pi k/n}(v_i) = v_{((i-1+k) \bmod n)+1} \qquad \text{for all } 1 \leq i \leq n.$$

Note that R_0 is the identity function on V.

As remarked above, regular n-gons possess symmetries that correspond to reflections through lines that pass through the center of the polygon. Supposing the regular n-gon is centered at the origin and with a vertex on the x-axis, then there are n distinct reflection symmetries, each corresponding to a line through the origin and making an angle of $\pi k/n$ with the x-axis, for

$0 \leq k \leq n-1$. The reflection symmetry in Figure 1.2 is through a line that makes an angle of $\pi/6$ with respect to the x-axis. In this section, we denote by F_β the reflection symmetry through the line that makes an angle of β with the x-axis.

Since $|D_n| = 2n$, the rotations and reflections account for all dihedral symmetries.

If two bijections on V preserve the polygon structure, then their composition does as well. Consequently, the function composition of two dihedral symmetries is again another dihedral symmetry and thus $\circ$ is a binary operation on D_n. However, having listed the dihedral symmetries as rotations or reflections, it is interesting to determine the result of the composition of two symmetries as another symmetry.

First, it is easy to see that rotations compose as follows:

$$R_\alpha \circ R_\beta = R_{\alpha+\beta},$$

where we subtract 2π from $\alpha+\beta$ if $\alpha+\beta \geq 2\pi$. However, the composition of a given rotation and a given reflection or the composition of two reflections is not as obvious. There are various ways to calculate the compositions. The first is to determine how the function composition acts on the vertices. For example, let $n = 6$ and consider the compositions of $R_{2\pi/3}$ and $F_{\pi/6}$.

v_i	v_1	v_2	v_3	v_4	v_5	v_6
$R_{2\pi/3}(v_i)$	v_3	v_4	v_5	v_6	v_1	v_2
$F_{\pi/6}(v_i)$	v_2	v_1	v_6	v_5	v_4	v_3
$(F_{\pi/6} \circ R_{2\pi/3})(v_i)$	v_6	v_5	v_4	v_3	v_2	v_1
$(R_{2\pi/3} \circ F_{\pi/6})(v_i)$	v_4	v_3	v_2	v_1	v_6	v_5

From this table and by inspection on how the compositions act on the vertices, we determine that

$$F_{\pi/6} \circ R_{2\pi/3} = F_{5\pi/6} \qquad \text{and} \qquad R_{2\pi/3} \circ F_{\pi/6} = F_{\pi/2}.$$

We notice with this example that the composition operation is not commutative.

Another approach to determining the composition of elements comes from linear algebra. Rotations about the origin by an angle α and reflections through a line through the origin making an angle β with the x-axis are linear transformations. With respect to the standard basis, these two types of linear transformations respectively correspond to the following 2×2 matrices

$$R_\alpha : \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \qquad \text{and} \qquad F_\beta : \begin{pmatrix} \cos 2\beta & \sin 2\beta \\ \sin 2\beta & -\cos 2\beta \end{pmatrix}. \tag{1.1}$$

For example, let $n = 6$ and consider the composition of $F_{\pi/6}$ and $F_{\pi/3}$.

The composition symmetry corresponds to the matrix product

$$\begin{aligned} F_{\pi/6} \circ F_{\pi/3} : \ & \begin{pmatrix} \cos\frac{\pi}{3} & \sin\frac{\pi}{3} \\ \sin\frac{\pi}{3} & -\cos\frac{\pi}{3} \end{pmatrix} \begin{pmatrix} \cos\frac{2\pi}{3} & \sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & -\cos\frac{2\pi}{3} \end{pmatrix} \\ &= \begin{pmatrix} \cos\frac{\pi}{3}\cos\frac{2\pi}{3} + \sin\frac{\pi}{3}\sin\frac{2\pi}{3} & \cos\frac{\pi}{3}\sin\frac{2\pi}{3} - \sin\frac{\pi}{3}\cos\frac{2\pi}{3} \\ \sin\frac{\pi}{3}\cos\frac{2\pi}{3} - \cos\frac{\pi}{3}\sin\frac{2\pi}{3} & \sin\frac{\pi}{3}\sin\frac{2\pi}{3} + \cos\frac{\pi}{3}\cos\frac{2\pi}{3} \end{pmatrix} \\ &= \begin{pmatrix} \cos\frac{\pi}{3} & \sin\frac{\pi}{3} \\ -\sin\frac{\pi}{3} & \cos\frac{\pi}{3} \end{pmatrix}. \end{aligned}$$

This matrix corresponds to a rotation and shows that

$$F_{\pi/6} \circ F_{\pi/3} = R_{-\pi/3} = R_{5\pi/3}.$$

Moving to symmetries of the square, whether we use one method or the other, the following table gives all their compositions.

$a \setminus b$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	F_0	$F_{\pi/4}$	$F_{\pi/2}$	$F_{3\pi/4}$
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	F_0	$F_{\pi/4}$	$F_{\pi/2}$	$F_{3\pi/4}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0	$F_{\pi/4}$	$F_{\pi/2}$	$F_{3\pi/4}$	F_0
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	$F_{\pi/2}$	$F_{3\pi/4}$	F_0	$F_{\pi/4}$
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π	$F_{3\pi/4}$	F_0	$F_{\pi/4}$	$F_{\pi/2}$
F_0	F_0	$F_{3\pi/4}$	$F_{\pi/2}$	$F_{\pi/4}$	R_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$
$F_{\pi/4}$	$F_{\pi/4}$	F_0	$F_{3\pi/4}$	$F_{\pi/2}$	$R_{\pi/2}$	R_0	$R_{3\pi/2}$	R_π
$F_{\pi/2}$	$F_{\pi/2}$	$F_{\pi/4}$	F_0	$F_{3\pi/4}$	R_π	$R_{\pi/2}$	R_0	$R_{3\pi/2}$
$F_{3\pi/4}$	$F_{3\pi/4}$	$F_{\pi/2}$	$F_{\pi/4}$	F_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$	R_0

(1.2)

From this table, we can answer many questions about the composition operator on D_4. For example, if asked what $f \in D_4$ satisfies $R_{3\pi/2} \circ f = F_0$, we simply look in the row corresponding to $a = R_{3\pi/2}$ (the fourth row) for the b that gives the composition of F_0. A priori, without any further theory, there does not have to exist such an f, but in this case there does and $f = F_{\pi/4}$.

Some other properties of the composition operation on D_n are not as easy to identify directly from the table in (1.2). For example, by Proposition A.2.12, $\circ$ is associative on D_n. Verifying associativity from the table in (1.2) would require checking $8^3 = 512$ equalities. Also, $\circ$ has an identity on D_n, namely R_0. Indeed R_0 is the identity function on V. Finally, every element in D_n has an inverse: the inverse to $R_{2\pi k/n}$ is $R_{2\pi(n-k)/n}$ and the inverse to $F_{\pi k/n}$ is itself. We leave the proof of the following proposition as an exercise.

Proposition 1.1.3

Let n be a fixed integer with $n \geq 3$. Then the dihedral symmetries R_α and F_β satisfy the following relations:

$$R_\alpha \circ F_\beta = F_{\alpha/2+\beta}, \quad F_\alpha \circ R_\beta = F_{\alpha-\beta/2}, \quad \text{and} \quad F_\alpha \circ F_\beta = R_{2(\alpha-\beta)}.$$

Proof. (See Exercise 1.1.7.) □

1.1.2 Abstract Notation

We introduce a notation that is briefer and aligns with the abstract notation that we will regularly use in group theory.

Having fixed an integer $n \geq 3$, denote by r the rotation of angle $2\pi/n$, by s the reflection through the x-axis, and by ι the identity function. In other words,

$$r = R_{2\pi/n}, \quad s = F_0, \quad \text{and} \quad \iota = R_0.$$

In abstract notation, similar to our habit of notation for multiplication of real variables, we write ab to mean $a \circ b$ for two elements $a, b \in D_n$. Borrowing from a theorem in the next section (Proposition 1.2.13), since $\circ$ is associative, an expression such as $rrsr$ is well-defined, regardless of the order in which we pair terms to perform the composition. In this example, with $n = 4$,

$$rrsr = R_{\pi/2} \circ R_{\pi/2} \circ F_0 \circ R_{\pi/2} = R_\pi \circ F_0 \circ R_{\pi/2} = F_{\pi/2} \circ R_{\pi/2} = F_{\pi/4}.$$

To simplify notations, if $a \in D_n$ and $k \in \mathbb{N}^*$, then we write a^k to represent

$$a^k = \overbrace{aaa \cdots a}^{k \text{ times}}.$$

Hence, we write r^2sr for $rrsr$. Since composition $\circ$ is not commutative, r^3s is not necessarily equal to r^2sr.

From Proposition 1.1.3, it is not hard to see that

$$r^k = R_{2\pi k/n} \quad \text{and} \quad r^k s = F_{\pi k/n},$$

where k satisfies $0 \leq k \leq n-1$. Consequently, as a set

$$D_n = \{\iota, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

The symbols r and s have a few interesting properties. First, $r^n = \iota$ and $s^2 = \iota$. These are obvious as long as we do not forget the geometric meaning of the functions r and s. Less obvious is the equality in the following proposition.

Proposition 1.1.4

Let n be an integer $n \geq 3$. Then in D_n equipped with the composition operation,

$$sr = r^{n-1}s.$$

Proof. We first prove that $rsr = s$. By Exercise 1.1.7, the composition of a rotation with a reflection is a reflection. Hence, $(rs)r$ is a reflection. For any n, r maps v_1 to v_2, then s maps v_2 to v_n, and then r maps v_n to $v-1$. Hence, rsr is a reflection that keeps v_1 fixed. There is only one reflection in D_n that keeps v_1 fixed, namely s.

We now compose r^{n-1} on the left of the identity $rsr = s$. We get $r^nsr = r^{n-1}s$. Since $r^n = \iota$, we obtain $sr = r^{n-1}s$. □

Corollary 1.1.5

Consider the dihedral symmetries D_n with $n \geq 3$. Then

$$sr^k = r^{n-k}s.$$

Proof. This follows by a repeated application of Proposition 1.1.4. □

1.1.3 Geometric Objects with Dihedral Symmetry

Regular polygons are not the only objects that possess dihedral symmetry. Any subset of the plane is said to have dihedral D_n symmetry if the set remains unchanged when the plane is transformed by all the rotations and reflections in D_n in reference to a given center C and an axis L.

For example, both shapes in Figure 1.3 possess D_6 dihedral symmetry.

FIGURE 1.3: Shapes with D_6 symmetry.

In Figure 1.4, the shape on the left displays D_7 symmetry while the shape on the right displays D_5 symmetry.

FIGURE 1.4: Shapes with D_7 and D_5 symmetry, respectively.

On the other hand, consider the curve in Figure 1.5. There does not exist an axis through which the shape is preserved under a reflection. Consequently, the shape does not possess D_3 symmetry. It does however, have rotational symmetry with the smallest rotation angle of $2\pi/3$.

If we know that a geometric pattern has a certain dihedral symmetry, we only need to draw a certain portion of the shape before it is possible to determine the rest of the object. Let $\mathcal{F}$ be a set of bijections of the plane and

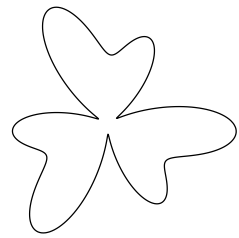


FIGURE 1.5: Only rotational symmetry.

let S be a subset of the plane that is preserved by all the functions in $\mathcal{F}$, i.e., $f(S) = S$ for all $f \in \mathcal{F}$. We say that a subset S' *generates* S by $\mathcal{F}$ if

$$S = \bigcup_{f \in \mathcal{F}} f(S').$$

For example, consider the shapes shown in Figure 1.6. In both instances, S_0 is a different generating subset for the subset S that has dihedral symmetry.

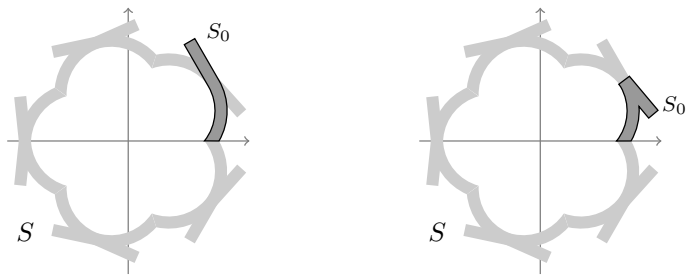


FIGURE 1.6: D_5 symmetry with generating subsets.

Exercises for Section 1.1

1. Use diagrams to describe all the dihedral symmetries of the equilateral triangle.
2. Write down the composition table for D_4.
3. Determine what r^3sr^4sr corresponds to in dihedral symmetry of D_8.
4. Determine what sr^6sr^5srs corresponds to as a dihedral symmetry of D_9.
5. Let n be an even integer with $n \geq 4$. Prove that in D_n, the element $r^{n/2}$ satisfies $r^{n/2}w = wr^{n/2}$ for all $w \in D_n$.
6. Let n be an arbitrary integer $n \geq 3$. Show that an expression of the form

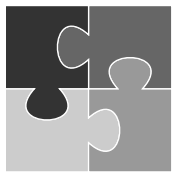
   $$r^a s^b r^c s^d \dots$$

   is a rotation if and only if the sum of the powers on s is even.

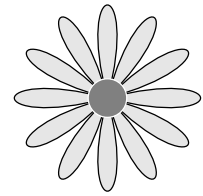
7. Using (1.1) and linear algebra prove that

$$R_\alpha \circ F_\beta = F_{\alpha/2+\beta}, \quad F_\alpha \circ R_\beta = F_{\alpha-\beta/2}, \quad \text{and} \quad F_\alpha \circ F_\beta = R_{2(\alpha-\beta)}.$$

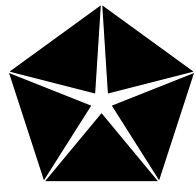
8. Describe the symmetries of an ellipse with unequal half-axes.
9. Determine the set of symmetries for each of the following shapes.

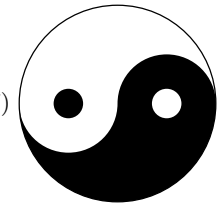
(a) 

(b) 

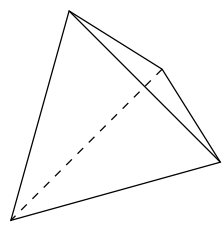
(c) 

(d) 

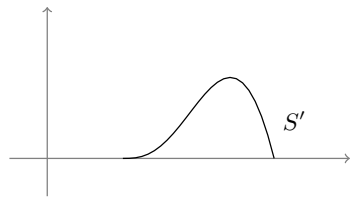
(e) 

(f) 

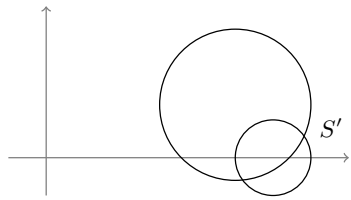
10. Sketch a pattern/shape (possibly a commonly known logo) that has D_8 symmetry but does not have D_n symmetry for $n > 8$.
11. Sketch a pattern/shape (possibly a commonly known logo) that has rotational symmetry of angle $\frac{\pi}{2}$ but does not have full D_4 symmetry.
12. Consider a regular tetrahedron. We call a *rigid motion* of the tetrahedron any rotation or composition of rotations in $\mathbb{R}^3$ that map a regular tetrahedron back into itself, though possibly changing specific vertices, edges, and faces. Rigid motions of solids do not include reflections through a plane.
    (a) Call $\mathcal{R}$ the set of rigid motions of a regular tetrahedron. Prove $|\mathcal{R}| = 12$.
    (b) Using a labeling of the tetrahedron, explicitly list all rigid motions of the tetrahedron.
    (c) Explain why function composition $\circ$ is a binary operation on $\mathcal{R}$.



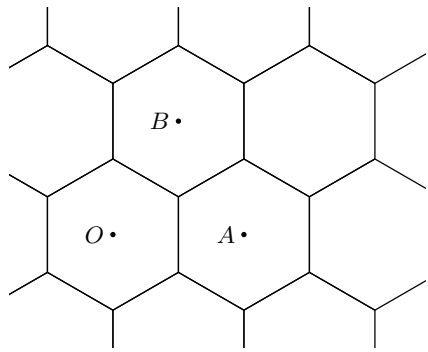
13. Consider the diagram S' below. Sketch the diagram S that has S' as a generating subset under (a) D_4 symmetry; (b) only rotational square symmetry. [Assume reflection through the x-axis is one of the reflections.]



14. Consider the diagram S' below. Sketch the diagram S that has S' as generating subset under (a) D_3 symmetry; (b) only the rotations in D_3. [Assume reflection through the x-axis is one of the reflections.]



15. Consider the hexagonal tiling pattern on the plane drawn below.



Define r as the rotation by 60° about O and t as the translation by the vector $\overrightarrow{OA}$, i.e., that maps the whole plane one hexagon to the right. We denote by $\circ$ the operation of composition on functions $\mathbb{R}^2 \to \mathbb{R}^2$ and we denote by r^{-1} and t^{-1} the inverse functions to r and t. [Recall that rotations and translations are examples of isometries (transformations that preserve distances) in the plane. A theorem in geometry states that an isometry is completely determined by its behavior on a nondegenerate triangle.]

(a) Determine the images O', A', and B' of O, A, and B respectively under the composition $r \circ t$. Deduce that $r \circ t$ is the symmetry of translation by the vector $\overrightarrow{OB}$. [Hint: Note that $t(O) = A$ and that $(r \circ t)(O) = r(A) = B$, so $O' = B$, but plot A' and B'.]

(b) Determine the images O'', A'', and B'' of O, A, and B respectively under the composition $t \circ r$ and deduce that $r \circ t$ and $t \circ r$ are not equal as symmetries of the plane.

(c) Show that $t \circ r \circ t^{-1}$ is the rotation of 60° about the point A. Find (and justify) a similar expression for the rotation of 60° about the point B.

(d) Describe in geometric terms the composition $r \circ t \circ r^2 \circ t^{-1} \circ r^{-1}$.

1.2 Introduction to Groups

1.2.1 Group Axioms

As we now jump into group theory with both feet, the reader might not immediately see the value in the definition of a group. The plethora of examples we provide subsequent to the definition will begin to showcase the breadth of applications.

Definition 1.2.1

A *group* is a pair $(G, *)$ where G is a set and $*$ is a binary operation on G that satisfies the following properties:

(1) associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;

(2) identity: there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$;

(3) inverses: for all $a \in G$, there exists $b \in G$ such that $a*b = b*a = e$.

By Proposition A.2.16, if any binary operation has an identity, then that identity is unique. Similarly, any element in a group has exactly one inverse element.

Proposition 1.2.2

Let $(G, *)$ be a group. Then for all $a \in G$, there exists a unique inverse element to a.

Proof. Let $a \in G$ be arbitrary and suppose that b_1 and b_2 satisfy the properties of the inverse axiom for the element a. Then

$$\begin{aligned} b_1 &= b_1 * e && \text{by identity axiom} \\ &= b_1 * (a * b_2) && \text{by inverse axiom} \\ &= (b_1 * a) * b_2 && \text{by associativity} \\ &= e * b_2 && \text{by definition of } b_1 \\ &= b_2 && \text{by identity axiom.} \end{aligned}$$

Therefore, for all $a \in G$ there exists a unique inverse. □

Since every group element has a unique inverse, our notation for inverses can reflect this. We denote the inverse element of a by a^{-1}.

The defining properties of a group are often called the *group axioms*. In common language, one often uses the term "axiom" to mean a truth that is self-evident. That is not the sense in which we use the term "axiom." In algebra, when we say that such and such are the axioms of a given algebraic structure, we mean the defining properties listed as (1)–(3) in Definition 1.2.1.

In the group axioms, there is no assumption that the binary operation $*$ is commutative. We say that two particular elements $a, b \in G$ commute (or commute with each other) if $a * b = b * a$.

Definition 1.2.3

A group $(G, *)$ is called *abelian* if for all $a, b \in G$, $a * b = b * a$.

The term *abelian* is named after Niels Abel (1802–1829), one of the founders of group theory.

Usually, the groups we encounter possess a binary operation with a natural description. Sometimes, however, it is useful or even necessary to list out all operation pairings. If $(G, *)$ is a finite group and if we label all the elements as $G = \{g_1, g_2, \ldots, g_n\}$, then the group's *Cayley table*[1] is the $n \times n$ array in which the (i, j)th entry is the result of the operation $g_i * g_j$. When listing the elements in a group it is customary that g_1 be the identity element of the group.

1.2.2 A Few Examples

It is important to develop a robust list of examples of groups that show the breadth and restriction of the group axioms.

Example 1.2.4. The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are groups. In each case, addition is associative and has 0 as the identity element. For a given element a, the additive inverse is $-a$. △

Example 1.2.5. The pairs $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, and $(\mathbb{C}^*, \times)$ are groups. Recall that A^* mean $A - \{0\}$ when A is a set that includes 0. In each group, 1 is the multiplicative identity, and, for a given element a, the (multiplicative) inverse is $\frac{1}{a}$. Note that $(\mathbb{Z}^*, \times)$ is not a group because it fails the inverse axiom. For example, there is no nonzero integer b such that $2b = 1$.

On the other hand $(\mathbb{Q}^{>0}, \times)$ and $(\mathbb{R}^{>0}, \times)$ are groups. Multiplication is a binary operation on $\mathbb{Q}^{>0}$ and on $\mathbb{R}^{>0}$, and it satisfies all the axioms. △

Example 1.2.6. A vector space V is a group under vector addition with $\vec{0}$ as the identity. The (additive) inverse of a vector $\vec{v}$ is $-\vec{v}$. Note that the scalar multiplication of a vector spaces has no bearing on the group properties of vector addition. △

[1] The Cayley table is named after the British mathematician, Arthur Cayley (1821–1895).

Example 1.2.7. In Section A.6, we introduced modular arithmetic. Recall that $\mathbb{Z}/n\mathbb{Z}$ represents the set of congruence classes modulo n and that $U(n)$ is the subset of $\mathbb{Z}/n\mathbb{Z}$ of elements with multiplicative inverses. Given any integer $n \geq 2$, both $(\mathbb{Z}/n\mathbb{Z}, +)$ and $(U(n), \times)$ are groups. The element $\overline{0}$ is the identity in $\mathbb{Z}/n\mathbb{Z}$ and the element $\overline{1}$ is the identity $U(n)$.

The tables for addition in (A.13) and (A.14) are the Cayley tables for $(\mathbb{Z}/5\mathbb{Z}, +)$ and $(\mathbb{Z}/6\mathbb{Z}, +)$. By ignoring the column and row for $\overline{0}$ in the multiplication table in Equation (A.13), we obtain the Cayley table for $(U(5), \times)$.

$\times$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

△

All the examples so far are of abelian groups. We began this chapter by introducing dihedral symmetries precisely because it offers an example of a nonabelian group.

Example 1.2.8 (Dihedral Groups). Let $n \geq 3$ be an integer. The pair $(D_n, \circ)$, where D_n is the set of dihedral symmetries of a regular n-gon and $\circ$ is function composition, is a group. We call $(D_n, \circ)$ the nth dihedral group. Since $rs = sr^{-1}$ and $r^{-1} \neq r$ for any $n \geq 3$, the group $(D_n, \circ)$ is not abelian. The table given in Equation (1.2) is the Cayley table for D_6. △

Example 1.2.9. The pair $(\mathbb{R}^3, \times)$, where $\times$ is the vector cross product, is not a group. In fact, $\times$ fails all of the axioms for a group. First of all $\times$ is not associative. Indeed, if $\vec{\imath}$, $\vec{\jmath}$, and $\vec{k}$ are respectively the unit vectors in the x-, y-, and z- directions, then

$$\vec{\imath} \times (\vec{\imath} \times \vec{\jmath}) = \vec{\imath} \times \vec{k} = -\vec{\jmath} \neq (\vec{\imath} \times \vec{\imath}) \times \vec{\jmath} = \vec{0} \times \vec{\jmath} = \vec{0}.$$

Furthermore, $\times$ has no identity element. For any nonzero vector $\vec{a}$ and any other vector $\vec{v}$, the product $\vec{a} \times \vec{v}$ is perpendicular to $\vec{a}$ or is $\vec{0}$. Hence, for no vector $\vec{v}$ do we have $\vec{a} \times \vec{v} = \vec{a}$. Since $\times$ has no identity, the question about having inverses becomes moot. △

Example 1.2.10. Let S be a set with at least 1 element. The pair $(\mathcal{P}(S), \cup)$ is not a group. The union operation $\cup$ on $\mathcal{P}(S)$ is both associative and has an identity $\emptyset$. However, if $A \neq \emptyset$, there does not exist a set $B \subseteq S$ such that $A \cup B = \emptyset$. Hence, $(\mathcal{P}(S), \cup)$ does not have inverses. △

Example 1.2.11 (Matrix Groups). Let n be a positive integer. The set of $n \times n$ invertible matrices with real coefficients is a group with the multiplication operation. In this group, the identity is the identity matrix and the inverse of a matrix A is the matrix inverse A^{-1}. This group is called the *general linear group* of degree n over $\mathbb{R}$, and is denoted by $\mathrm{GL}_n(\mathbb{R})$.

In Section 3.3, we discuss properties of matrices in more generality. However, without yet providing the full algebraic theory, we point out that in order to perform matrix addition, matrix multiplication, matrix inverses, and even the Gauss-Jordan elimination, we need the entries of the matrix to come from a field. (See Definition 3.1.22.) Though we did not name them as such, the fields we have encountered so far are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number.

Suppose that F represents $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{F}_p$. Of key importance is the fact that an $n \times n$ matrix A with coefficients in F is invertible if and only if the columns are linearly independent, which is also equivalent to $\det(A) \neq 0$. We denote by $\mathrm{GL}_n(F)$ the general linear group of degree n over F and we always denote the identity matrix by I.

As an explicit example, consider $\mathrm{GL}_2(\mathbb{F}_5)$. The number of 2×2 matrices over $\mathbb{F}_5$ is $5^4 = 625$. However, not all are invertible. To determine the cardinality $\mathrm{GL}_2(\mathbb{F}_5)$, we consider the columns of a matrix A, which must be linearly independent. The only condition on the first column is that it is not all 0. Hence, there are $5^2 - 1 = 24$ options for the first column. Given the first column, the only necessary condition on the second column is that it is not a $\mathbb{F}_5$-multiple of the first column. This accounts for $5^2 - 5 = 20$ (all columns minus the 5 multiples of the first column) options. Hence, $\mathrm{GL}_2(\mathbb{F}_5)$ has $24 \times 20 = 480$ elements.

An example of multiplication in $\mathrm{GL}_2(\mathbb{F}_5)$ is

$$\begin{pmatrix} \bar{1} & \bar{3} \\ \bar{2} & \bar{4} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{3} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1}+\bar{9} & \bar{1}+\bar{6} \\ \bar{2}+\overline{12} & \bar{2}+\bar{8} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{4} & \bar{0} \end{pmatrix}$$

while the following illustrates calculating the inverse of a matrix

$$\begin{pmatrix} \bar{3} & \bar{3} \\ \bar{2} & \bar{1} \end{pmatrix}^{-1} = (\bar{3} - \bar{2} \cdot \bar{3})^{-1} \begin{pmatrix} \bar{1} & -\bar{3} \\ -\bar{2} & \bar{3} \end{pmatrix} = \bar{3} \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{3} & \bar{3} \end{pmatrix} = \begin{pmatrix} \bar{3} & \bar{1} \\ \bar{4} & \bar{4} \end{pmatrix},$$

where the second equality holds because $\bar{2}^{-1} = \bar{3}$ in $\mathbb{F}_p$. The reader should verify that all the matrices involved in the above calculations have a nonzero determinant in $\mathbb{F}_5$. △

1.2.3 Notation for Arbitrary Groups

In group theory, we will regularly discuss the properties of an arbitrary group. In this case, instead of writing the operation as $a * b$, where $*$ represents some unspecified binary operation, it is common to write the generic group operation as ab. With this convention of notation, it is also common to indicate the identity in an arbitrary group as 1 instead of e. In this chapter, however, we will continue to write e for the arbitrary group identity in order to avoid confusion. Finally, with arbitrary groups, we denote the inverse of an element a as a^{-1}.

This shorthand of notation should not surprise us too much. We already developed a similar habit with vector spaces. When discussing an arbitrary vector space, we regularly say, "Let V be a vector space." So though, in a strict sense, V is only the set of the vector space, we implicitly understand that part of the information of a vector space is the addition of vectors (some operation usually denoted $+$) and the scalar multiplication of vectors.

By a similar abuse of language, we often refer, for example, to "the dihedral group D_n," as opposed to "the dihedral group $(D_n, \circ)$." Similarly, when we talk about "the group $\mathbb{Z}/n\mathbb{Z}$," we mean $(\mathbb{Z}/n\mathbb{Z}, +)$ because $(\mathbb{Z}/n\mathbb{Z}, \times)$ is not a group. And when we refer to "the group $U(n)$," we mean the group $(U(n), \times)$. We will explicitly list the pair of set and binary operation if there could be confusion as to which binary operation the group refers. Furthermore, as we already saw with D_n, even if a group is equipped with a natural operation, we often just write ab to indicate that operation. Following the analogy with multiplication, in a group G, if $a \in G$ and k is a positive integer, by a^k we mean

$$a^k \stackrel{\text{def}}{=} \overbrace{aa\cdots a}^{k \text{ times}}.$$

We extend the power notation so that $a^0 = e$ and $a^{-k} = \left(a^{-1}\right)^k$, for any positive integer k.

Groups that involve addition give an exception to the above habit of notation. In that case, we always write $a + b$ for the operation, $-a$ for the inverse, and, if k is a positive integer,

$$k \cdot a \stackrel{\text{def}}{=} \overbrace{a + a + \cdots + a}^{k \text{ times}}. \tag{1.3}$$

We refer to $k \cdot a$ as a multiple of a instead of as a power. Again, we extend the notation to nonpositive "multiples" just as above with powers.

Proposition 1.2.12

Let G be a group and let $x \in G$. For all $n, m \in \mathbb{Z}$, the following identities hold

$$\text{(a) } x^m x^n = x^{m+n} \quad \text{(b) } (x^m)^n = x^{mn}$$

Proof. (Left as an exercise for the reader. See Exercise 1.3.11.) □

1.2.4 First Properties

The following proposition holds for any associative binary operation and does not require the other two axioms of group theory.

Proposition 1.2.13

Let S be a set and let $\star$ be a binary operation on S that is associative. In an operation expression with a finite number of terms,

$$a_1 \star a_2 \star \cdots \star a_n \qquad \text{with } n \geq 3, \tag{1.4}$$

all possible orders in which we pair operations (i.e., parentheses orders) are equal.

Proof. Before starting the proof, we define a temporary but useful notation. Given a sequence $a_1, a_2, \ldots, a_k$ of elements in S, by analogy with the $\sum$ notation, we define

$$\bigstar_{i=1}^{k} a_i \stackrel{\text{def}}{=} (\cdots((a_1 \star a_2) \star a_3) \cdots a_{k-1}) \star a_k.$$

In this notation, we perform the operations in (1.4) from left to right. Note that if $k = 1$, the expression is equal to the element a_1.

We prove by (strong) induction on n, that every operation expression in (1.4) is equal to $\bigstar_{i=1}^{n} a_i$.

The basis step with $n \geq 3$ is precisely the assumption that $\star$ is associative.

We now assume that the proposition is true for all integers k with $3 \leq k \leq n$. Consider an operation expression (1.4) involving $n+1$ terms. Suppose without loss of generality that the last operation performed occurs between the jth and $(j+1)$th term, i.e.,

$$q = (\overbrace{\text{operation expression}_1}^{j \text{ terms}}) \star (\overbrace{\text{operation expression}_2}^{n-j \text{ terms}}).$$

Since both operation expressions involve n terms or less, by the induction hypothesis

$$q = \left(\bigstar_{i=1}^{j} a_i\right) \star \left(\bigstar_{i=j+1}^{n} a_i\right).$$

Furthermore,

$$\begin{aligned} q &= \left(\bigstar_{i=1}^{j} a_i\right) \star \left(a_{j+1} \star \left(\bigstar_{i=j+2}^{n} a_i\right)\right) && \text{by the induction hypothesis} \\ &= \left(\left(\bigstar_{i=1}^{j} a_i\right) \star a_{j+1}\right) \star \left(\bigstar_{i=j+2}^{n} a_i\right) && \text{by associativity} \\ &= \left(\bigstar_{i=1}^{j+1} a_i\right) \star \left(\bigstar_{i=j+2}^{n} a_i\right). \end{aligned}$$

Repeating this $n - j - 2$ more times, we conclude that

$$q = \bigstar_{i=1}^{n+1} a_i.$$

The proposition follows. □

The following proposition lists properties of binary operations particular to the context of group theory.

Proposition 1.2.14

Let $(G, *)$ be a group.

(1) The identity in G is unique.

(2) For each $a \in G$, the inverse of a is unique.

(3) For all $a \in G$, $(a^{-1})^{-1} = a$.

(4) For all $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof. We have already seen (1) and (2) in Proposition A.2.16 and Proposition 1.2.2, respectively.

For (3), by definition of the inverse of a we have $a * (a^{-1}) = (a^{-1}) * a = e$. However, this shows that a satisfies the inverse axiom for the element a^{-1}.

For (4), we have

$$\begin{aligned}
&(a*b)^{-1} * (a*b) = e \\
&\quad\iff ((a*b)^{-1} * a) * b = e && \text{associativity} \\
&\quad\iff (((a*b)^{-1} * a) * b) * b^{-1} = e * b^{-1} && \text{operate } *b^{-1} \\
&\quad\iff ((a*b)^{-1} * a) * (b * b^{-1}) = b^{-1} && \text{assoc and id} \\
&\quad\iff ((a*b)^{-1} * a) * e = b^{-1} && \text{inverse axiom} \\
&\quad\iff (a*b)^{-1} * a = b^{-1} && \text{identity axiom} \\
&\quad\iff (a*b)^{-1} = b^{-1} * a^{-1}.
\end{aligned}$$

□

Proposition 1.2.15 (Cancellation Law)

A group G satisfies the left and right cancellation laws, namely

$$au = av \implies u = v \qquad \text{(Left cancellation)}$$
$$ub = vb \implies u = v. \qquad \text{(Right cancellation)}$$

Proof. If $au = av$, then operating on the left by a^{-1}, we obtain

$$a^{-1}au = a^{-1}av \implies eu = ev \implies u = v.$$

Similarly, if $ub = vb$, then by operating the equality on the right by b^{-1}, we obtain

$$ubb^{-1} = vbb^{-1} \implies ue = ve \implies u = v.$$

□

It is important to note that Proposition 1.2.15 does not claim that $au = va$ implies $u = v$. In fact, $au = va$ implies $u = v$ if and only if a commutes with u or v.

The Cancellation Law leads to an interesting property about the Cayley table for a finite group. In combinatorics, a *Latin square* is an $n \times n$ array, filled with n different symbols in such a way that each symbol appears exactly once in each column and exactly once in each row. Since $au = av$ implies $u = v$, in the row corresponding to a, each distinct column has a different group element entry. Hence, each row of the Cayley table contains n different group elements. Similarly, right cancellation implies that in a given column, different rows have different group elements. Thus, the Cayley graph for every group is a Latin square.

1.2.5 Useful CAS Commands

In linear algebra, the theorem that every vector space has a basis gives us a standard method to describe elements in vector spaces, especially finite dimensional ones: (1) find a basis $\mathcal{B}$ of the vector space; (2) express a given vector by its coordinates with respect to $\mathcal{B}$. No corresponding theorem exists in group theory. Hence, one of the initial challenging questions of group theory is how to describe a group and its elements in a standard way. This is particularly important for implementing computational packages that study groups. There exist a few common methods and we will introduce them in parallel with the development of needed theory.

In *Maple* version 16 or below, the command `with(group);` accesses the appropriate package. In *Maple* version 17 or higher, the `group` package was deprecated in favor of `with(GroupTheory);`. The help files, whether provided by the program or those available online[2] provide a list of commands and capabilities. Doing a search on "GroupTheory" locates the help file for the `GroupTheory` package. The student might find useful the `LinearAlgebra` package or, to support Example 1.2.11, the linear algebra package for modular arithmetic.

Consider the following lines of *Maple* code, in which the left justified text is the code and the centered text is the printed result of the code.

Maple

$with(LinearAlgebra[Modular]):$

$A := Mod(11, Matrix([[1, 2], [7, 9]]), integer[]);$

$$A := \begin{bmatrix} 1 & 2 \\ 7 & 9 \end{bmatrix}$$

$B := Mod(11, Matrix([[2, 3], [1, 10]]), integer[]);$

$$B := \begin{bmatrix} 2 & 3 \\ 1 & 10 \end{bmatrix}$$

[2] See https://www.maplesoft.com/support/help/category.aspx?cid=162

$Determinant(11, A)$;

$$6$$

$Multiply(11, A, B)$;

$$\begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix}$$

$MatrixPower(11, A, 5)$;

$$\begin{bmatrix} 8 & 5 \\ 1 & 6 \end{bmatrix}$$

The first line makes active the linear algebra package for modular arithmetic. The next two code lines define matrices A and B respectively, both defined in $\mathbb{Z}/11\mathbb{Z}$. The next three lines calculate respective the determinant of A, the produce of AB, and the power A^5, always assuming we work in $\mathbb{Z}/11\mathbb{Z}$.

For SAGE, a browser search for "SageMath groups" will bring up references manuals and tutorials for group theory. Perhaps the gentlest introductory tutorial is entitled "Group theory and Sage."[3] We show here below the commands and approximate look for the same calculations in the console for SageMath for those we did above in *Maple*.

Sage

```
sage: M=MatrixSpace(GF(11),2,2)
sage: A=M([1,2, 7,9])
sage: B=M([2,3, 1,10])
sage: A.determinant()
6
sage: A*B
[4 1]
[1 1]
sage: A^5
[8 5]
[1 6]
```

In each of the lines, `sage:` is the command line prompt for Sage, where the user inputs their commands. The lines without that prompt indicate the results of calculations. The first line defines the set of 2×2 matrices defined over the field $\mathbb{F}_{11}$. (Note that `GF(11)` reads as general field mod 11.) The `M` in the lines of code defining A and B identify them as elements of the matrix space M.

Because of the abstract nature of group theory, the available commands in various CAS implement computations ranging from elementary to specialized for group theorists. In subsequent sections, we will occasionally discuss useful commands in one or another CAS that assist with group theory investigations.

[3] https://doc.sagemath.org/html/en/thematic_tutorials/group_theory.html

Exercises for Section 1.2

In Exercises 1.2.1 through 1.2.14, decide whether the given set and the operation pair forms a group. If it is, prove it. If it is not, decide which axioms fail. You should always check that the symbol is in fact a binary operation on the given set.

1. The pair $(\mathbb{N}, +)$.
2. The pair $(\mathbb{Q} - \{-1\}, *)$, where $*$ is defined by $a*b = a + b + ab$.
3. The pair $(\mathbb{Q} - \{0\}, \div)$, with $a \div b = \frac{a}{b}$.
4. The pair $(A, +)$, where $A = \{x \in \mathbb{Q} \,|\, |x| < 1\}$.
5. The pair $(\mathbb{Z} \times \mathbb{Z}, *)$, where $(a, b) * (c, d) = (ad + bc, bd)$.
6. The pair $([0, 1), \boxplus)$, where $x \boxplus y = x + y - \lfloor x + y \rfloor$.
7. The pair $(A, +)$, where A is the set of rational numbers that when reduced have a denominator of 1 or 3.
8. The pair $(A, +)$, where $A = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Q}\}$.
9. The pair $(A, \times)$, where $A = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Q}\}$.
10. The pair $(A, \times)$, where $A = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Q} \text{ and } (a, b) \neq (0, 0)\}$. [Hint: First show that $\sqrt{5}$ is irrational.]
11. The pair $(U(20), +)$.
12. The pair $(\mathcal{P}(S), \triangle)$, where S is any set and $\triangle$ is the symmetric difference of two sets.
13. The pair $(G, \times)$, where $G = \{z \in \mathbb{C} \,\big|\, |z| = 1\}$.
14. The pair $(\mathcal{D}, *)$, where $\mathcal{D}$ is the set of open disks in $\mathbb{R}^2$, including the empty set $\emptyset$, and where $D_1 * D_2$ is the unique open disk of least radius that encloses both D_1 and D_2.
15. Construct the Cayley table for $U(15)$.
16. Prove that a group is abelian if and only if its Cayley table is symmetric across the main diagonal.
17. Prove that $S = \{2^a 5^b \,|\, a, b \in \mathbb{Z}\}$, as a subset of rational numbers, is a group under multiplication.
18. Prove that the set $\{\overline{1}, \overline{13}, \overline{29}, \overline{41}\}$ is a group under multiplication modulo 42.
19. Prove that if a group G satisfies $x^2 = e$ for all $x \in G$, then G is abelian.
20. Prove that if a group G satisfies $(xy)^{-1} = x^{-1}y^{-1}$ for all $x, y \in G$, then G is abelian.
21. Let $g_1, g_2, g_3 \in G$. What is $(g_1 g_2 g_3)^{-1}$? Generalize your result.
22. Prove that every cyclic group is abelian.
23. Prove that $\mathrm{GL}_n(\mathbb{F}_p)$ contains

$$(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

elements. [Hint: Use the fact the $\mathrm{GL}_n(\mathbb{F}_p)$ consists of $n \times n$ matrices with coefficients in $\mathbb{F}_p$ that have columns that are linearly independent.]

24. Write out the Cayley table for $\mathrm{GL}_2(\mathbb{F}_2)$.

25. In the given general linear group, for the given matrices A and B, calculate the products A^2, AB, and B^{-1}.

    (a) $GL_2(\mathbb{F}_3)$ with $A = \begin{pmatrix} \overline{0} & \overline{2} \\ \overline{2} & \overline{1} \end{pmatrix}$ and $B = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{2} \end{pmatrix}$.

    (b) $GL_2(\mathbb{F}_5)$ with $A = \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{4} & \overline{1} \end{pmatrix}$ and $B = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{2} & \overline{3} \end{pmatrix}$.

    (c) $GL_2(\mathbb{F}_7)$ with $A = \begin{pmatrix} \overline{4} & \overline{6} \\ \overline{3} & \overline{2} \end{pmatrix}$ and $B = \begin{pmatrix} \overline{5} & \overline{4} \\ \overline{3} & \overline{2} \end{pmatrix}$.

26. Let F be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{F}_p$. The *Heisenberg group* with coefficients in F is

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(F) \,\middle|\, a, b, c \in F \right\}.$$

    (a) Show that $H(F)$ is a group under matrix multiplication.

    (b) Explicitly show the inverse of an element in $H(F)$.

1.3 Properties of Group Elements

As we progress through group theory, we will encounter more and more internal structure to groups that is not readily apparent from the three axioms for groups. This section introduces a few elementary properties of group operations.

1.3.1 Order of Elements

Definition 1.3.1

Let G be a group.

(1) If G is finite, we call the cardinality of $|G|$ the *order* of the group.

(2) Let $x \in G$. If $x^k = e$ for some positive integer k, then we call the *order* of x, denoted $|x|$, the smallest positive value of n such that $x^n = e$. If there exists no positive n such that $x^n = e$, then we say that the order of x is infinite.

Recall that if G is finite, $|G|$ is simply the number of elements in G. If G is infinite, the set theoretic notion of cardinality is more general.

Note that the order of a group element g is $|g| = 1$ if and only if g is the group's identity element.

As a reminder, we list the orders of a few groups encountered so far:

$$\begin{aligned} |D_n| &= 2n, && \text{(Proposition 1.1.2)} \\ |\mathbb{Z}/n\mathbb{Z}| &= n, \\ |U(n)| &= \phi(n), && \text{(Corollary A.6.9)} \\ |\operatorname{GL}_n(\mathbb{F}_p)| &= (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}). && \text{(Exercise 1.2.23)} \end{aligned}$$

Example 1.3.2. Consider the group $G = (\mathbb{Z}/20\mathbb{Z}, +)$. We calculate the orders of $\bar{5}$ and $\bar{3}$. Since the group has $+$ as its operation, "powers" means multiples. Instead of writing $\bar{a}^k$ with $\bar{a} \in \mathbb{Z}/20\mathbb{Z}$ and $k \in \mathbb{N}$ (which evokes multiplicative powers), we write $k \cdot \bar{a}$.

For $\bar{5}$, we calculate directly that

$$2 \cdot \bar{5} = \overline{10}, \quad 3 \cdot \bar{5} = \overline{15}, \quad 4 \cdot \bar{5} = \overline{20} = \bar{0}.$$

Hence, $|\bar{5}| = 4$. However, for $\bar{3}$ we notice the pattern

$$\begin{aligned} k \cdot \bar{3} &= \overline{3k} && \text{for } 0 \le k \le 6, \\ k \cdot \bar{3} &= \overline{3(k-7)+1} && \text{for } 7 \le k \le 13, \\ k \cdot \bar{3} &= \overline{3(k-14)+2} && \text{for } 14 \le k \le 20. \end{aligned}$$

This shows that the first positive integer k such that $k \cdot \bar{3} = \bar{0}$ is 20. Hence, $|\bar{3}| = 20$. △

Example 1.3.3. Consider the group $\operatorname{GL}_2(\mathbb{F}_3)$ and we calculate the order of

$$g = \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$$

by evaluating various powers of g:

$$\begin{aligned} g &= \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, & g^2 &= g \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}, \\ g^3 &= g^2 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix}, & g^4 &= g^3 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}, \\ g^5 &= g^4 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{0} \end{pmatrix}, & g^6 &= g^5 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix}, \\ g^7 &= g^6 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}, & g^8 &= g^7 \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}. \end{aligned}$$

From these calculations, we determine that the order of g is $|g| = 8$. △

When studying a specific group, determining the orders of elements in groups is particularly useful. We present a number of propositions concerning the powers and orders of elements.

Proposition 1.3.4

If G is a finite group and $g \in G$, then $|g|$ is finite.

Proof. Let $g \in G$ be any element. Consider the sequence of powers $\{g^i \mid i \in \mathbb{N}\}$. This is a subset of G. By the pigeon-hole principle, two elements in the set of powers must be equal. Hence, there exist nonnegative integers $i < j$ with $g^j = g^i$. Operating on both sides by $(g^{-1})^i$, we get $g^{j-i} = e$. Hence, g has finite order. □

Proposition 1.3.5

Let G be any group and let $x \in G$. Then $\left|x^{-1}\right| = |x|$.

Proof. (Left as an exercise for the reader. See Exercise 1.3.19.) □

We point out that if $x^n = e$, then $x^{-1} = x^{n-1}$.

Proposition 1.3.6

Let $x \in G$ with $x^n = e$ and $x^m = e$, then $x^d = e$ where $d = \gcd(m, n)$.

Proof. From Proposition A.5.10, the greatest common divisor $d = \gcd(m, n)$ can be written as a linear combination $sm + tn = d$, for some $s, t \in \mathbb{Z}$. Then

$$x^d = x^{sm+tn} = (x^m)^s (x^n)^t = e^s\, e^t = e.$$ □

Corollary 1.3.7

Suppose that x is an element of a group G with $x^m = e$. Then the order $|x|$ divides m.

Proof. If $|x| = n$, then $x^n = x^m = e$. By Proposition 1.3.6, $x^{\gcd(m,n)} = e$. However, n is the least positive integer k such that $x^k = e$. Furthermore, since $1 \leq \gcd(m, n) \leq n$, this minimality condition $\gcd(m, n) = n$. This implies that n divides m. □

Proposition 1.3.8

Let G be a group and let $a \in \mathbb{N}^*$. Then we have the following results about orders:

(1) If $|x| = \infty$, then $|x^a| = \infty$.

(2) If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{\gcd(n, a)}$.

Proof. For (1), assume that x^a has finite order k. Then $(x^a)^k = x^{ak} = e$. This contradicts $|x| = \infty$. Hence, x^a has infinite order.

For (2), let $y = x^a$ and $d = \gcd(n, a)$. Writing $n = db$ and $a = dc$, by Exercise A.5.11, we know that $\gcd(b, c) = 1$. Then

$$y^b = x^{ab} = x^{bcd} = x^{nc} = e^c = e.$$

By Corollary 1.3.7, the order $|y|$ divides b. Conversely, suppose that $|y| = k$. Then k divides b. Since $y^k = x^{ak} = e$, then $n|ak$. Thus $db|dck$, which implies that $b|ck$. However, $\gcd(b, c) = 1$, so we conclude that $b|k$. However, since $b|k$ and $k|b$ and $b, k \in \mathbb{N}^*$, we can conclude that $b = k$.

Hence, $|y| = |x^a| = b = n/d = n/\gcd(a, n)$. □

Proposition 1.3.8 presents two noteworthy cases. If $\gcd(a, n) = 1$, then $|x^a| = n$. Second, if a divides n, then $|x^a| = n/a$.

It is important to point out that in a general group, there is very little that can be said about the relationship between $|xy|$, $|x|$, and $|y|$ for two elements $x, y \in G$. For example, consider the dihedral group D_n. Both s and rs refer to reflections through lines and hence have order 2. However, $s(sr) = r$, and r has order n. Thus, given any integer n, there exists a group where $|g_1| = 2$ and $|g_2| = 2$ and $|g_1 g_2| = n$.

Example 1.3.9. In D_{10}, we know that $|r| = 10$. Proposition 1.3.8 allows us to immediately determine the orders of all the elements r^k. For $k = 1, 3, 7, 9$, which are relatively prime to 10, we have $|r^k| = 10$. For $k = 2, 4, 6, 8$, we have $\gcd(10, k) = 2$ so $|r^k| = 10/2 = 5$. And finally, $|r^5| = 10/\gcd(10, 5) = 2$. △

Example 1.3.10. In $\mathbb{Z}/20\mathbb{Z}$, we know that $|\overline{1}| = 20$. Then $\overline{12} = 12 \cdot \overline{1}$, so $a = 12$ in Proposition 1.3.8(2). Hence the order of $\overline{12}$ in $\mathbb{Z}/20\mathbb{Z}$ is $|\overline{12}| = 20/\gcd(20, 12) = 20/4 = 5$. △

1.3.2 Cyclic Groups

The process of simply considering the successive powers of an element gives rise to an important class of groups.

Definition 1.3.11

A group G is called *cyclic* if there exists an element $x \in G$ such that every element of $g \in G$ we have $g = x^k$ for some $k \in \mathbb{Z}$. The element x is called a *generator* of G.

For example, we notice that for all integers $n \geq 2$, the group $\mathbb{Z}/n\mathbb{Z}$ (with addition as the operation) is a cyclic group because all elements of $\mathbb{Z}/n\mathbb{Z}$ are multiples of $\overline{1}$. As we saw in Section A.6, one of the main differences with usual arithmetic is that $n \cdot \overline{1} = \overline{0}$. The intuitive sense that the powers (or multiples) of an element "cycle back" motivate the terminology of cyclic group.

Remark 1.3.12. We point out that a finite group G is cyclic if and only if there exists an element $g \in G$ such that $|g| = |G|$. △

Cyclic groups do not have to be finite though. The group $(\mathbb{Z}, +)$ is also cyclic because every element in $\mathbb{Z}$ is obtained by $n \cdot 1$ with $n \in \mathbb{Z}$.

Example 1.3.13. Consider the group $U(14)$. The elements are

$$U(14) = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}.$$

This group is cyclic because, for example, the powers of $\overline{3}$ gives all the elements of $U(14)$:

i	1	2	3	4	5	6
$\overline{3}^i$	$\overline{3}$	$\overline{9}$	$\overline{13}$	$\overline{11}$	$\overline{5}$	$\overline{1}$

We note that the powers of $\overline{3}$ will then cycle around, because $\overline{3}^7 = \overline{3}^6 \cdot \overline{3} = \overline{3}$, then $\overline{3}^8 = \overline{9}$, and so on. △

Example 1.3.14. At first glance, someone might think that to prove that a group is not cyclic we would need to calculate the order of every element. If no element has the same order as the cardinality of the group, only then we could say that the group is not cyclic. However, by an application of the theorems in this section, we may be able to conclude the group is not cyclic with much less work.

As an example, suppose we wish to determine if $U(200)$ is cyclic. Note that $|U(200)| = \phi(200) = 80$. The most obvious thing to try is to start calculating the powers of $\overline{3}$. Without showing all the powers here, we can check that $|\overline{3}| = 20$. So we conclude immediately that $\overline{3}$ is not a generator of $U(200)$. In this list, we would find that $\overline{3}^{10} = \overline{49}$. This implies (and also using Proposition 1.3.8) that $|\overline{49}| = 2$. It is easy to see that $\overline{199}^2 = (\overline{-1})^2 = \overline{1}$, so $|\overline{199}| = 2$. Now if $U(200)$ were cyclic with generator $\overline{a}$, then $|\overline{a}| = 80$. Also by Proposition 1.3.8, an element $\overline{a}^k$ has order 2 if and only if $\gcd(k, 80) = 40$. However, the only integer k with $1 \leq k \leq 80$ such that $\gcd(k, 80) = 40$ is 40 itself. Hence, a cyclic of order 80 has at most one element of order 2. Since $U(200)$ has more than one element of order 2, it is not a cyclic group. △

Definition 1.3.15 (Finite Cyclic Groups)

Let n be a positive integer. We denote by Z_n the group with elements $\{e, x, x^2, \ldots, x^{n-1}\}$, where x has the property that $x^n = e$. This group is sometimes generically called *the cyclic group* of order n.

It is important to emphasize in this notation that we do not define the group as existing in any previously known arithmetic context. The element x does not represent some complex number or matrix or any other object. We have simply defined how it operates symbolically.

1.3.3 Useful CAS Commands

The `GroupTheory` package in *Maple* has the commands `GroupOrder` and `ElementOrder`, which implement a calculation of the order of a group and the order of an element in a group. We will wait a few sections to illustrate `ElementOrder` because we need a little more group theory background to describe how CASs implement groups and elements of groups. However, we can already give the following example of `GroupOrder`.

Maple

$with(GroupTheory)$:

$G := GL(3, 5)$;

$$G := GL(3, 5)$$

$GroupOrder(G)$;

$$1488000$$

$IsAbelian(G)$;

$$false$$

This defines G as the general linear group of invertible 3×3 matrices with coefficients in $\mathbb{Z}/5\mathbb{Z}$. Here the object class of G is the whole group. The next command finds the order (cardinality) of the group. Finally, the last line illustrates a command that asks whether the group is abelian or not.

The following code in Sage implements the same thing.

Sage

```
sage: G=GL(3,GF(5))
sage: G.order()
1488000
sage: G.is_abelian()
False
```

Many CASs offer similar commands that test true/false properties about groups as a whole (e.g., finite, simple, perfect, solvable, nilpotent). These commands always look like *IsAbelian* in *Maple* or `is_abelian()` in Sage.

Without a `GroupElement()` command, we can find the orders of elements in a group simply by running a for loop to calculate all the powers of an element up to a certain point and verifying when we reach the identity. Suppose we revisit the example of *Maple* code in Section 1.2.5 the command

$seq(A^{\wedge}i, i = 1..20)$;

prints out a list of all the powers of the matrix A, from A to A^{20} in the group $\mathrm{GL}_2(\mathbb{F}_{11})$. We can accomplish the same thing in Sage with the following code

```
sage: G=GL(2,GF(11))
sage: A=G([1,2,7,9])
sage: [A^n for n in range(1,20)]
        (not listed)
sage: A.order()
40
```

(For the sake of space, we did not list output of the third line.) In particular, SAGE offers a command to calculate the order of any group element.

EXERCISES FOR SECTION 1.3

1. Find the orders of $\bar{5}$ and $\bar{6}$ in $(\mathbb{Z}/21\mathbb{Z}, +)$.
2. Calculate the order $\overline{20}$ in $\mathbb{Z}/52\mathbb{Z}$.
3. Calculate the order of $\overline{285}$ in the group $\mathbb{Z}/360\mathbb{Z}$.
4. Calculate the order of r^{16} in D_{24}.
5. Find the orders of all the elements in $(\mathbb{Z}/18\mathbb{Z}, +)$.
6. Find the orders of all the elements in $U(21)$. Deduce that $U(21)$ is not cyclic.
7. Find the orders of all the elements in Z_{20}.
8. Show that for all integers $n \geq 1$, the element
$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$
in $\mathrm{GL}_2(\mathbb{R})$ has order n.
9. In $\mathrm{GL}_2(\mathbb{F}_3)$, find the orders of the following elements:
$$\text{(a) } A = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix}, \quad \text{(b) } B = \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \quad \text{(c) } C = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{0} & \bar{2} \end{pmatrix}.$$
10. Prove that if $A \in \mathrm{GL}_n(\mathbb{R})$ has order $|A| = k$, then all eigenvalues λ of A satisfy $\lambda^k = 1$.
11. Prove Proposition 1.2.12. [Hint: Pay careful attention to when powers are negative, zero, or positive.]
12. Determine if $U(11)$ a cyclic group.
13. Determine if $U(10)$ a cyclic group.
14. Determine if $U(36)$ a cyclic group.
15. Find all the generators of the cyclic group Z_{40}.
16. Find all the generators of the cyclic group $\mathbb{Z}/36\mathbb{Z}$.
17. Let p be an odd prime.
    (a) Use the Binomial Theorem to prove that $(1+p)^{p^n} \equiv 1 \pmod{p^{n+1}}$ for all positive integers n.
    (b) Prove also that $(1+p)^{p^{n-1}} \not\equiv 1 \pmod{p^{n+1}}$ for all positive integers n.
    (c) Conclude that $\overline{1+p}$ has order p^n in $U(p^{n+1})$.

18. Prove that $(\mathbb{Q}, +)$ is not a cyclic group.
19. Prove Proposition 1.3.5.
20. Let G be a group such that for all $a, b, c, d, x \in G$, the identity $axb = cxd$ implies $ab = cd$. Prove that G is abelian.
21. Let a and b be elements in a group G. Prove that if a and b commute, then the order of ab divides $\text{lcm}(|a|, |b|)$.
22. Find a nonabelian group G and two elements $a, b \in G$ such that $|ab|$ does not divide $\text{lcm}(|a|, |b|)$.
23. Let $x \in G$ be an element of finite order n. Prove that $e, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.
24. Prove that for elements x and y in any group G we have $|x| = |yxy^{-1}|$.
25. Use the preceding exercise to show that for any elements g_1 and g_2 in a group $|g_1 g_2| = |g_2 g_1|$, even if g_1 and g_2 do not commute.
26. Prove that the group of rigid motions of the cube has order 24.
27. Prove that the group of rigid motions of the octahedron has order 24.
28. Prove that the group of rigid motions of a classic soccer ball has order 60.

29. (CAS) Using a computer algebra system find all the orders of all the elements in $\text{GL}_2(\mathbb{F}_3)$.
30. (CAS) Using a CAS and some programming, find the number of elements in $\text{GL}_2(\mathbb{F}_5)$ of any given order. [Hint: Use a dictionary in SAGE or a hash table in *Maple*.]

1.4 Concept of a Classification Theorem

One of the recurring themes in group theory is whether we can find all groups with certain stated properties. A theorem that answers a question like this is called a classification theorem. In fact, such classification questions play key roles throughout abstract algebra and regularly drive directions of investigation. Often, these theorems are quite profound. Though we are just at the beginning of group theory and such problems require many more concepts than we have developed yet, it is valuable to keep classification questions in the back of our minds for motivation.

1.4.1 Direct Sum of Groups

A useful perspective behind considering classification question involves thinking about how to create new (larger) groups, from smaller ones. The direct sum of two groups is one such method.

Definition 1.4.1 (Direct Sum)

Let $(G, *)$ and $(H, \star)$ be two groups. The *direct sum* of the groups is a new group $(G \times H, \cdot)$ where the set operation is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \star h_2).$$

The direct sum is denoted by $G \oplus H$.

We observe that the identity of $G \oplus H$ is (e_G, e_H), the identity of G paired with the identity of H.

The direct sum generalizes to any finite number of groups. For example, the group $(\mathbb{R}^3, +)$ is the triple direct sum of group $(\mathbb{R}, +)$ with itself. The reader should feel free to imagine all sorts of possibilities now, e.g., $\mathbb{Z}/9\mathbb{Z} \oplus D_{10}$, $\mathbb{Z} \oplus Z_2 \oplus Z_2$, $\mathrm{GL}_2(\mathbb{F}_7) \oplus U(21)$, and so on.

Example 1.4.2. Consider the group $Z_4 \oplus Z_2$. We can list the elements of this group as

$$Z_4 \oplus Z_2 = \{(x^m, y^n) \,|\, x^4 = e \text{ and } y^2 = e\}.$$

(To avoid confusion, we should not use the same letter for the generator of Z_4 and of Z_2. After all, they are different elements and from different groups.) We point out that $Z_4 \oplus Z_2$ is not another cyclic group. The size is $|Z_4 \oplus Z_2| = 8$. However, in a cyclic group of order 8 generated by some element z, only the element z^4 has order 2. However, in $Z_4 \oplus Z_2$, both (x^2, e) and (e, y) have order 2. Thus $Z_4 \oplus Z_2$ is not cyclic.

It is easy to prove that $Z_4 \oplus Z_2$ is abelian. Let $(x^i, y^j), (x^a, y^b) \in Z_4 \oplus Z_2$. Then

$$(x^i, y^j)(x^a, y^b) = (x^i x^a, y^j y^b) = (x^{i+a}, y^{j+b}) = (x^a x^i, y^b y^j) = (x^a, y^b)(x^i, y^j).$$

Since $Z_4 \oplus Z_2$ is abelian, it does not behave like D_4, which is not abelian. Hence, we have found three groups of order 8 with different properties: Z_8, $Z_4 \oplus Z_2$ and D_4. △

In the previous section, we pointed out that knowing the orders of two elements g_1, g_2 in a group G, we do not readily know the order of $g_1 g_2$. However, with direct sums, a theorem gives us a relationship among orders.

Theorem 1.4.3

Let $G_1, \ldots, G_n$ be groups and let $(g_1, \ldots, g_n) \in G_1 \oplus \cdots \oplus G_n$ be an element in the direct sum. Then the order of $(g_1, \ldots, g_n)$ is

$$\big|(g_1, \ldots, g_n)\big| = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$

Proof. Call $M = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$ and let e_i be the identity in G_i for each $i = 1, 2, \ldots, n$. By definition, $(g_1, g_2, \ldots, g_n)^m = (e_1, e_2, \ldots, e_n)$ if and only if $g_i^m = e_i$ for all i. By Corollary 1.3.7, $|g_i|$ divides m for all i and thus $M \mid m$.

Suppose now that k is the order of $(g_1, g_2, \ldots, g_n)$, namely the least positive integer m such that $(g_1, g_2, \ldots, g_n)^m = (e_1, e_2, \ldots, e_n)$. Then by the preceding paragraph, $M \mid k$. However, M is a multiple of $|g_i|$ for each i, and hence,

$$(g_1, g_2, \ldots, g_n)^M = (g_1^M, g_2^M, \ldots, g_n^M) = (e_1, e_2, \ldots, e_n).$$

Hence, by Corollary 1.3.7, k divides M. Since M and k are positive numbers that divide each other, $M = k$. The theorem follows. □

1.4.2 Classification Theorems

Classification theorems usually require theorems not yet at our disposal, e.g., Lagrange's Theorem, Cauchy's Theorem, Sylow's Theorem, and so on. Nonetheless, this section explores what we can discover for possibilities of small groups using the Cayley table or orders of elements.

Example 1.4.4 (Groups of Order 4). We propose to find all groups of order 4 by filling out all possible Cayley tables. Suppose that $G = \{e, a, b, c\}$ with a, b, and c distinct nonidentity group elements. A priori, all we know about the Cayley graph is the first column and first row.

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Note that if a group G contains an element g of order n, then $\{e, g, g^2, \ldots, g^{n-1}\}$ is a subset of n distinct elements. (See Exercise 1.3.23.) Hence, a group of order 4 cannot contain an element of order 5 or higher.

Suppose that G contains an element of order 4, say, the element a. Then $G = \{e, a, a^2, a^3\}$. Without loss of generality, we can call $b = a^2$ and $c = a^3$

and the Cayley table becomes the following.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

We recognize this table as corresponding to the cyclic group Z_4.

Assume that G does not contain an element of order 4 but contains one of order 3. Without loss of generality, suppose that $|a| = 3$. Then $G = \{e, a, a^2, c\}$, with all elements distinct. The element ac cannot be equal to a^k for any k for then $c = a^{k-1}$, a contradiction. Furthermore, we cannot have $ac = c$ for then $a = e$, again a contradiction. Hence, a group of order 4 cannot contain an element of order 3.

Suppose now that all nonidentity elements in G have order 2. Filling out the Cayley table, this means that we have e in the entries on the main diagonal. We claim that $ab = c$. This is because ab cannot be e because a is its own inverse and $a \neq b$; ab cannot be a because this would imply that $b = e$; and ab cannot be b because this would imply that $a = e$. Once, we place c in the table corresponding to ab, by virtue of the Cayley table being a Latin square, we can fill out every other entry. We get:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(1.5)

This group is often denoted by V_4 and called the Klein-4 group. Our approach covered all possible cases for orders of elements in a group of order 4 so we conclude that Z_4 and V_4 are the only two groups of order 4. △

The conclusion of the previous example might seem striking at first. In particular, we already know two groups of order 4 that have different properties: Z_4 and $Z_2 \oplus Z_2$. Consequently, V_4 and $Z_2 \oplus Z_2$ must in some sense be the same group. However, we do not yet have the background to fully develop an intuitive concept of sameness for groups. We return to that issue in Section 1.9. Nevertheless, if we write $Z_2 = \{e, x\}$ with $x^2 = e$, then it is an easy check to see (1.5) is the Cayley table for $Z_2 \oplus Z_2$ with $a = (x, e)$ and $b = (e, x)$.

Example 1.4.5. Though a more complete problem would be to find all groups of order 8, we propose to tackle a slightly simpler problem: to find all groups G of order 8 that contain an element x of order 4. Let y be another element in G that is distinct from any power of x. With these criteria, we know so far that G contains the distinct elements e, x, x^2, x^3, y. The element xy cannot be

e because that would imply $y = x^3$;
x because that would imply $y = e$;
x^2 because that would imply $y = x$;
x^3 because that would imply $y = x^2$;
y because that would imply $x = e$.

So xy is a new element of G. By similar reasonings that we leave to the reader, the elements x^2y and x^3y are distinct from all the others. Hence, G must contain the 8 distinct elements

$$\{e, x, x^2, x^3, y, xy, x^2y, x^3y\}. \tag{1.6}$$

We now consider various possibilities for the order of y.

Suppose first that $|y| = 2$. Consider the element yx. With a reason by cases similar to that above, yx cannot be e, x, x^2, x^3, or y. Thus, there are three cases: (1) $yx = x^3y$; (2) $yx = xy$; and (3) $yx = x^2y$.

Case 1. If $yx = x^3y$, then the group is in fact D_4, the dihedral group of the square, where x serves the role of r and y serves the role of s.

Case 2. If $yx = xy$, then x and y commute, so $x^sy^t = y^tx^s$ for all s, t and so G is abelian. We leave it up to the reader to show that this group is $Z_4 \oplus Z_2$.

Case 3. If $yx = x^2y$, then $yxy = x^2$. Hence,

$$x = y^2xy^2 = y(yxy)y = yx^2y = yxy^2xy = (yxy)(yxy) = x^4 = e.$$

We conclude that $x = e$, which contradicts the assumption that x has order 4. Hence, there exists no group of order 8 with an element x of order 4 and an element y of order 2 with $yx = x^2y$.

Suppose that $|y| = 3$. Consider the element y^2 in G. A quick proof by cases shows that y^2 cannot be any of the eight distinct elements listed in (1.6). Hence, there exists no group of order 8 containing an element of order 4 and one of order 3.

Suppose that $|y| = 4$. Again, we consider the element y^2. If there exists a group with all the conditions we have so far, then y^2 must be equal to an element in (1.6). Now $|y^2| = 4/2 = 2$ so y^2 cannot be e, x, x^3, or y, which have orders $1, 4, 4, 4$, respectively. Furthermore, y^2 cannot be equal to xy, (respectively x^2y or x^3y) because that would imply $x = y$ (respectively $x^2 = y$ or $x^3 = y$), which is against the assumptions on x and y. The only remaining possibility is $y^2 = x^2$.

We focus on this latter possibility, namely a group G containing x and y with $|x| = 4$, $|y| = 4$, $y \notin \{e, x, x^2, x^3\}$ and $x^2 = y^2$. If we now consider the element yx, we can quickly eliminate all possibilities except xy and x^3y. If $G = Z_4 \oplus Z_2 = \{(z, w) \,|\, z^4 = e \text{ and } w^2 = e\}$, then setting $x = (z, e)$ and $y = (z, w)$, it is easy to check that $Z_4 \oplus Z_2$ satisfies $x^2 = y^2$ and $yx = xy$.

So that is not new. On the other hand, if $yx = xy^3$, then G is a nonabelian group in which $x, x^3, y, y^3 = x^2y$ are elements of order 4. However, D_4 is the only nonabelian group of order 8 that we have encountered so far and in D_4 only r and r^3 have order 4. Hence, G must be a new group. △

We now introduce the new group identified in this example but using the symbols traditionally associated with it.

Example 1.4.6 (The Quaternion Group). The quaternion group, denoted by Q_8, contains the following eight elements:

$$1, -1, i, -i, j, -j, k, -k.$$

The operations on the elements are in part inspired by how the imaginary number operates on itself. In particular, 1 is the identity element and multiplication by (-1) changes the sign of any element. We also have

$$\begin{array}{lll} i^2 = -1, & i^3 = -i, & i^4 = 1, \\ j^2 = -1, & j^3 = -j, & j^4 = 1, \\ k^2 = -1, & k^3 = -k, & k^4 = 1, \\ ij = k, & jk = i, & ki = j, \\ ji = -k, & kj = -i, & ik = -j. \end{array}$$

Furthermore, if a and b are i, j, or k, then

$$(-a)b = (-1)(ab) \quad \text{and} \quad (-a)(-b) = ab.$$

Matching symbols to Example 1.4.5, note that $i^4 = j^4 = 1$, $i^2 = -1 = j^2$, and $ji = -k = (-i)j = i^3j$. This shows that Q_8 is indeed the new group of order 8 discovered at the end of the previous example. △

A bigger classification question would involve finding all the groups of order 8. We could solve this problem at this point, but we will soon encounter theorems that establish more internal structure on groups that would make such questions easier. Consequently, we delay most classification questions until later.

Exercises for Section 1.4

1. Find the orders of all the elements in $Z_4 \oplus Z_2$.
2. What is the largest order of an element in $Z_{75} \oplus Z_{100}$? Illustrate with a specific element.
3. Show that $Z_5 \oplus Z_2$ is cyclic.
4. Show that $Z_4 \oplus Z_2$ is not cyclic.
5. Construct the Cayley table for $Z_3 \oplus Z_3$.
6. Let A and B be groups. Prove that the direct sum $A \oplus B$ is abelian if and only if A and B are both abelian.

7. Let G and H be two finite groups. Prove that $G \oplus H$ is cyclic if and only if G and H are both cyclic with $\gcd(|G|, |H|) = 1$.

8. Let $G_1, G_2, \ldots, G_n$ be n finite groups. Prove that $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is cyclic if and only if G_i is cyclic for all $i = 1, 2, \ldots, n$ and $\gcd(|G_i|, |G_j|) = 1$ for all $i \neq j$. [Hint: Use Exercise 1.4.7 and induction.]

9. Find all groups of order 5.

10. We consider groups of order 6. We know that Z_6 is a group of order 6. We now look for all the others. Let G be any group of order 6 that is not Z_6, i.e., does not contain an element of order 6.
    (a) Show that G cannot have an element of order 7 or greater.
    (b) Show that G cannot have an element of order 5.
    (c) Show that G cannot have an element of order 4.
    (d) Show that the nonidentity elements of G have order 2 or 3.
    (e) Conclude that there exist only two subgroups of order 6. In particular, there exists one abelian group of order 6 (the cyclic group Z_6) and one nonabelian group of order 6 (D_3 is such a group).

    [Comment: We will encounter a number of nonabelian groups of order 6 but the result of this exercise establishes that they are all in some sense the same. We will make precise this notion of sameness in Section 1.9.3.]

11. Let $G = \{e, v, w, x, y, z\}$ be a group of order 6. For the following partial table, decide if it can be completed to the Cayley table of some G and if so fill it in. [Hint: You may need to use associativity.]

	e	v	w	x	y	z
e	–	–	–	–	–	–
v	–	–	–	–	w	–
w	–	–	–	–	–	e
x	–	–	–	–	–	–
y	–	z	–	–	–	–
z	–	–	–	v	–	–

12. Let $G = \{e, t, u, v, w, x, y, z\}$ be a group of order 8. For the following partial table, decide if it can be completed to the Cayley table of some G and if so fill it in. [Hint: You may need to use associativity.]

	e	t	u	v	w	x	y	z
e	–	–	–	–	–	–	–	–
t	–	–	–	–	–	–	–	e
u	–	–	e	–	–	y	x	t
v	–	–	–	u	–	t	–	–
w	–	x	v	–	–	–	–	y
x	–	–	–	z	–	–	–	–
y	–	–	–	t	z	–	–	–
z	–	–	–	–	x	–	–	u

1.5 Symmetric Groups

Symmetric groups play a key role in group theory and in countless applications. This section introduces the terminology and elementary properties of symmetric groups.

1.5.1 Permutations

Definition 1.5.1

Let A be a nonempty set. Define S_A as the set of all bijections from A to itself.

Proposition 1.5.2

The pair $(S_A, \circ)$ is a group, where the operation $\circ$ is function composition.

Proof. The composition of two bijections is a bijection so composition is a binary operation on S_A.

Proposition A.2.12 establishes that $\circ$ is associative in S_A.

The function $id_A : A \to A$ such that $id_A(x) = x$ for all $x \in A$ is the group identity.

Since $f \in S_A$ is a bijection, there exists an inverse function, denoted $f^{-1} : A \to A$. By definition of the inverse function,

$$f \circ f^{-1} = f^{-1} \circ f = id_A.$$

Hence, $(S_A, \circ)$ has inverses. S_A satisfies all the axioms of a group. □

We call S_A the *symmetric group* on A. In the case that $A = \{1, 2, \ldots, n\}$, then we write S_n instead of the cumbersome $S_{\{1,2,\ldots,n\}}$. We call the elements of S_A *permutations* of A.

Proposition 1.5.3

$|S_n| = n!$.

Proof. The order of S_n is the number of distinct bijections on $\{1, 2, \ldots, n\}$. To enumerate the bijections, we first count the injections f from $\{1, 2, \ldots, n\}$ to itself. Note that there are n options for $f(1)$. Since $f(2) \neq f(1)$, for each choice of $f(1)$, there are $n-1$ choices for $f(2)$. Given values for $f(1)$ and $f(2)$, there are $n-2$ possible choices for $f(3)$ and so on. Since an enumeration of injections requires an n-part decision, we use the product rule, giving us

$$n(n-1)(n-2)\cdots 3 \times 2 \times 1 = n!\,.$$

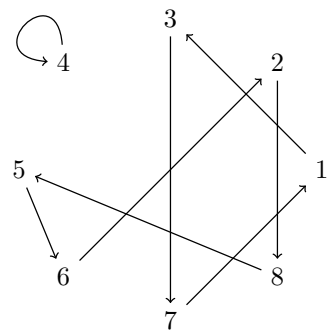


FIGURE 1.7: A permutation as a directed graph.

However, for any such injection f has n distinct images, so is also a bijection. Thus, $|S_n| = n!$. □

Symmetric groups arise in a variety of natural contexts. In a 100-meter Olympic race, eight runners are given lane numbers. The function from the runner's lane number to the rank they place in the race is a permutation of S_8. A cryptogram is a word game in which someone writes a message but replacing each letter of the alphabet with another letter and a second person attempts to recover the original message. The first person's choice of how to scramble the letters of the alphabet is a permutation in S_a, where a is the number of letters in the alphabet used. When someone shuffles a deck of 52 cards, the resulting reordering of the cards represents a permutation in S_{52}.

We need a few convenient ways to visualize and represent a permutation on $\{1, 2, \ldots, n\}$.

Directed Graph. A visual method of representing a permutation $\sigma \in S_n$ involves using a directed graph. Each element of $\{1, 2, \ldots, n\}$ is written as a point on the plane and we draw an arrow from a to b if $f(a) = b$. In this way, a permutation will create a directed graph in which one arrow leaves each point and arrives at each point. See Figure 1.7 for an example.

Chart Notation. Another way of writing a permutation is to record in a chart or matrix the outputs like

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Using the chart notation, the permutation in Figure 1.7 is written as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 4 & 6 & 2 & 1 & 5 \end{pmatrix}.$$

n-tuple. If the value n is clear from context, then the top row of the chart notation is redundant. Hence, we can represent the permutation σ by the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Using the n-tuple notation, the permutation in Figure 1.7 is written as $\sigma = (3, 8, 7, 4, 6, 2, 1, 5)$.

Cycle Notation. A different notation turns out to be more useful for the purposes of group theory. In cycle notation, the expression

$$\sigma = (a_1\, a_2\, \cdots a_{m_1})(a_{m_1+1}\, a_{m_1+2} \cdots a_{m_2}) \cdots (a_{m_{k-1}+1}\, a_{m_{k-1}+2} \cdots a_{m_k}),$$

where a_ℓ are distinct elements in $\{1, 2, \ldots, n\}$, means that for any index i,

$$\sigma(a_i) = \begin{cases} a_{i+1} & \text{if } i \neq m_j \text{ for all } j \\ a_{m_{j-1}+1} & \text{if } i = m_j \text{ for some } j, \end{cases}$$

where $m_0 = 0$. Any of the expressions $(a_{m_{j-1}+1}\, a_{m_{j-1}+2} \cdots a_{m_j})$ is called a *cycle* because σ "cycles" through these elements in order as σ iterates. Using the cycle notation for the permutation in Figure 1.7 is

$$\sigma = (1\,3\,7)(2\,8\,5\,6)(4).$$

There are many different ways of expressing a permutation using the cycle notation. For example, as cycles, $(1\,3\,7) = (3\,7\,1) = (7\,1\,3)$. Standard cycle notation imposes four additional habits. (1) If σ is the identity function, we just write $\sigma = \mathrm{id}$. (Advanced texts commonly refer to the identity permutation as 1 but, for the moment, we will use id in order to avoid confusion.) (2) We write each cycle of σ starting with the lowest integer in the cycle. (3) The order in which we list the cycles of σ is such that initial elements of each cycle are in increasing order. (4) Finally, we omit any cycle of length 1. We say that a permutation in S_n is written in *standard* cycle notation if it satisfies these requirements. The standard cycle notation for the permutation in Figure 1.7 is $\sigma = (1\,3\,7)(2\,8\,5\,6)$.

Definition 1.5.4

- An *m-cycle* is a permutation that in standard cycle notation consists of only one cycle of length m.
- Two cycles are called *disjoint* if they involve no common integers.
- A 2-cycle is also called a *transposition*.

We use the special term transposition for a 2-cycle because it simply interchanges (transposes) two elements and leaves the rest fixed. By the construction, the cycles that appear in the standard cycle notation for a permutation are all disjoint.

Example 1.5.5. To illustrate the cycle notation, we list all the permutations in S_4 in standard cycle notation:

$(1\,2\,3\,4)$, $(1\,2\,4\,3)$, $(1\,3\,2\,4)$, $(1\,3\,4\,2)$, $(1\,4\,2\,3)$, $(1\,4\,3\,2)$,
$(1\,2\,3)$, $(1\,3\,2)$, $(1\,2\,4)$, $(1\,4\,2)$, $(1\,3\,4)$, $(1\,4\,3)$, $(2\,3\,4)$, $(2\,4\,3)$,
$(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$,
$(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$,
id.

As a simple counting exercise, we verify that we have all the 3-cycles by calculating how many there should be. Each cycle consists of 3 integers. The number of ways of choosing 3 from 4 integers is $\binom{4}{3}$. For each selection of 3 integers, after writing the least integer first, there are $2! = 2$ options for how to order the remaining two integers in the 3-cycle. Hence, there are $2 \cdot \binom{4}{3} = 8$ three-cycles in S_4. △

The *cycle type* of a permutation describes how many disjoint cycles of a given length make up the standard cycle notation of that permutation. Hence, we say that $(1\,3)(2\,4)$ is of cycle type $(a\,b)(c\,d)$, or of type $2, 2$.

Example 1.5.6. As another example, consider the symmetric group S_6. There are $6! = 720$ elements in S_6. We count how many permutations there are in S_6 of a given cycle type. In order to count the 6-cycles, note that every integer from 1 to 6 appears in the cycle notation of a 6-cycle. In standard cycle notation, we write 1 first and then all $5! = 120$ orderings of $\{2, 3, 4, 5, 6\}$ give distinct 6-cycles. Hence, there are 120 6-cycles in S_6.

We now count the permutations in S_6 of the form $\sigma = (a_1\,a_2\,a_3)(a_4\,a_5\,a_6)$. The standard cycle notation of a permutation has $a_1 = 1$. To choose the values in a_2 and a_3, there are 5 choices for a_2 and then 4 remaining choices for a_3. With a_1, a_2, and a_3 chosen, we know that $\{a_4, a_5, a_6\} = \{1, 2, 3, 4, 5, 6\} - \{a_1, a_2, a_3\}$. The value of a_4 must be the minimum value of $\{a_4, a_5, a_6\}$. Then there are two ways to order the two remaining elements in the second 3-cycle. Hence, there are $5 \cdot 4 \cdot 2 = 40$ permutations that consist of the product of two disjoint 3-cycles.

Cycle type	Number of elements
id	1
$(a\,b)$	$\binom{6}{2} = 15$
$(a\,b\,c)$	$2 \cdot \binom{6}{3} = 40$
$(a\,b\,c\,d)$	$3!\binom{6}{4} = 90$
$(a\,b\,c\,d\,e)$	$4!\binom{6}{5} = 144$
$(a\,b\,c\,d\,e\,f)$	$5! = 120$
$(a\,b\,c\,d)(e\,f)$	$3!\binom{6}{4} = 90$
$(a\,b\,c)(d\,e\,f)$	40
$(a\,b\,c)(d\,e)$	$2\binom{6}{3} = 120$
$(a\,b)(c\,d)$	$\frac{1}{2}\binom{6}{2}\binom{4}{2} = 45$
$(a\,b)(c\,d)(e\,f)$	$\binom{6}{2}\binom{4}{2}/3! = 15$
Total:	720

The above table counts all the different permutations in S_6, organized by lengths of cycles in standard cycle notation. △

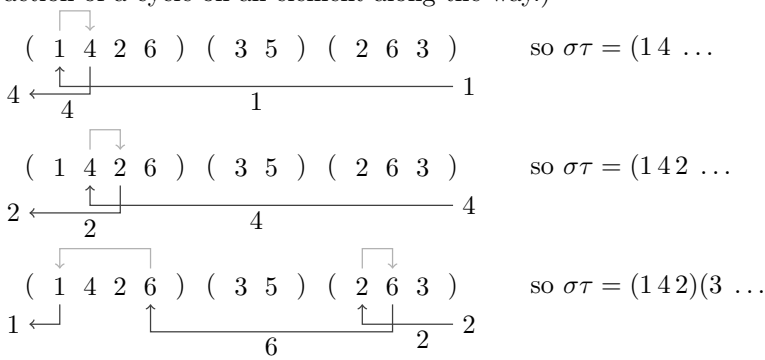
1.5.2 Operations in Cycle Notation

When calculating operations in the symmetric group, we must remember that permutations are bijective functions and that function composition is read from right to left. Because of this, if $\sigma, \tau \in S_A$, then the composition $\sigma\tau$ (short for $\sigma \circ \tau$) means the bijection where we apply τ first and then σ.

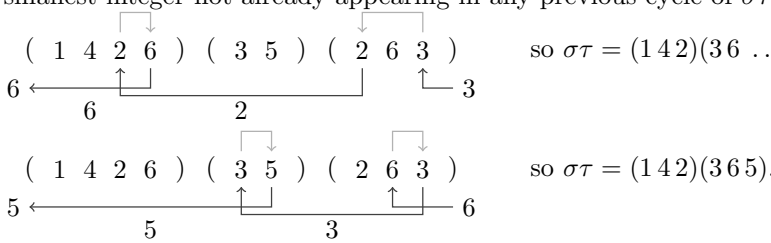
Consider the following example in which we determine the cycle notation for a product. Suppose that we are in S_6 and $\sigma = (1\,4\,2\,6)(3\,5)$ and $\tau = (2\,6\,3)$. We write

$$\sigma\tau = (1\,4\,2\,6)(3\,5)(2\,6\,3)$$

and read from right to left how $\sigma\tau$ maps the integers as a composition of cycles, not necessarily disjoint now. (In the diagrams below, the arrows beneath the permutation indicate the direction of reading and the arrows above indicate the action of a cycle on an element along the way.)



Note that since $\sigma\tau(2) = 1$, we closed the first cycle and start a new cycle with the smallest integer not already appearing in any previous cycle of $\sigma\tau$.



And we are done. We closed the cycle at the end of 5 because all integers 1 through 6 already appear in the standard cycle notation of $\sigma\tau$ so the cycle must be closed. However, it is a good practice to verify by the same method that $\sigma\tau(5) = 3$.

It should be obvious that the cycle notation expresses a permutation as the composition of disjoint cycles.

Proposition 1.5.7

Disjoint cycles in S_n commute.

Proof. Let $\sigma, \tau \in S_n$ be disjoint cycles. We have three cases, depending on i.

If i is one of the integers in the cycle of τ, then $\tau(i)$ is another integer in the cycle of τ. Since the cycles are disjoint, $\sigma(\tau(i)) = \tau(i)$. On the other hand, since i is not in the cycle σ, $\sigma(i) = i$ so $\tau(\sigma(i)) = \tau(i)$.

If i is one of the integers in the cycle of σ, then $\sigma(i)$ is another integer in the cycle of σ. Since the cycles are disjoint, $\tau(\sigma(i)) = \sigma(i)$. On the other hand, since i is not in the cycle τ, as above, $\tau(i) = i$, so $\sigma(\tau(i)) = \sigma(i)$.

If i is neither one of the integers in the cycle of σ nor one of the integers in the cycle of τ, then $\sigma(\tau(i)) = \sigma(i) = i$ and $\tau(\sigma(i)) = \tau(i) = i$.

Hence, $\sigma(\tau(i)) = \tau(\sigma(i))$ for all $i \in \{1, 2, \ldots, n\}$ so $\sigma\tau = \tau\sigma$. □

The fact that disjoint cycles commute implies that to understand powers and inverses of permutations, understanding of how powers and inverses work on cycles is sufficient. Indeed, if $\tau_1, \tau_2, \ldots, \tau_k$ are disjoint cycles and $\sigma = \tau_1\tau_2\cdots\tau_k$, then

$$\sigma^m = \tau_1^m\tau_2^m\cdots\tau_k^m, \text{ for all } m \in \mathbb{Z}, \quad \text{including} \quad \sigma^{-1} = \tau_1^{-1}\tau_2^{-1}\cdots\tau_k^{-1}.$$

Consequently, some properties about a permutation σ and its powers depend only on the cycle type of σ. We leave a number of these results for the exercises but we state one proposition here because of its importance.

Proposition 1.5.8

For all $\sigma \in S_n$, the order $|\sigma|$ is the least common multiple of the lengths of the disjoint cycles in the standard cycle notation of σ.

Proof. (Left as an exercise for the reader. See Exercise 1.5.19.) □

The cycle notation also makes it easy to find the inverse of a permutation. The inverse function to a permutation σ simply involves reading the cycle notation backwards.

Example 1.5.9. Let $\sigma = (1\,3\,7)(2\,5\,4)(6\ 10)$ in S_{10}. We propose to calculate σ^{-1} and then to determine the order of σ by calculating all the powers of σ.

To calculate σ^{-1}, we read the cycles backwards so

$$\sigma^{-1} = (7\,3\,1)(4\,5\,2)(10\ 6) = (1\,7\,3)(2\,4\,5)(6\ 10).$$

The second equals follows by rewriting the cycle with the lowest integer first. This is equivalent to starting at the lowest integer in the cycle and reading the cycle backwards.

For the powers of σ we have

$$\begin{aligned}
\sigma &= (1\,3\,7)(2\,5\,4)(6\ 10),\\
\sigma^2 &= (1\,3\,7)(2\,5\,4)(6\ 10)(1\,3\,7)(2\,5\,4)(6\ 10) = (1\,7\,3)(2\,4\,5),\\
\sigma^3 &= \sigma^2\sigma = (1\,7\,3)(2\,4\,5)(1\,3\,7)(2\,5\,4)(6\ 10) = (6\ 10),\\
\sigma^4 &= \sigma^3\sigma = (6\ 10)(1\,3\,7)(2\,5\,4)(6\ 10) = (1\,3\,7)(2\,5\,4),\\
\sigma^5 &= \sigma^4\sigma = (1\,3\,7)(2\,5\,4)(1\,3\,7)(2\,5\,4)(6\ 10) = (1\,7\,3)(2\,4\,5)(6\ 10),\\
\sigma^6 &= \sigma^5\sigma = (1\,7\,3)(2\,4\,5)(6\ 10)(1\,3\,7)(2\,5\,4)(6\ 10) = \mathrm{id}.
\end{aligned}$$

This shows that $|\sigma| = 6$ and thereby illustrates Proposition 1.5.8. △

We briefly consider the product of cycles that are not disjoint. Some of the simplest products involve two transpositions,

$$(1\,2)(1\,3) = (1\,3\,2) \quad \text{and} \quad (1\,3)(1\,2) = (1\,2\,3).$$

The fact that these products are different establishes the following proposition.

Proposition 1.5.10

The group S_n is nonabelian for all $n \geq 3$.

1.5.3 Inversions of a Permutation

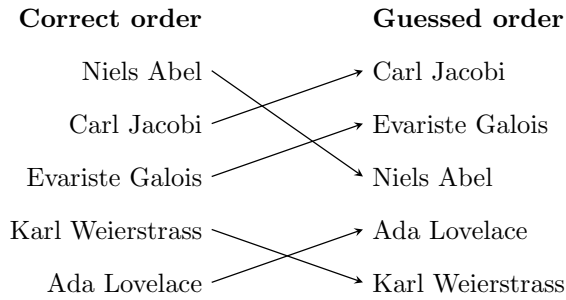
Permutations play a central role in combinatorics, a field that studies techniques for counting the possible arrangements in any kind of discrete structure. We end this section with a brief discussion on the inversions of a permutation. This concept will come in handy when we discuss even and odd permutations in the next sections.

As a motivating example, suppose that we consider 5 events in history and attempt to remember the order in which they occurred. There are $5! = 120$ possible orderings of this time line. Suppose that we number the events in historical order as E_1, E_2, E_3, E_4, E_5 and suppose that someone guesses the historical order as G_1, G_2, G_3, G_4, G_5. Any guess about their historical order corresponds to a permutation $\sigma \in S_5$ via

$$G_{\sigma(i)} = E_i \qquad \text{for all } i \in \{1, 2, 3, 4, 5\}.$$

This means that the person guessed the actual ith historical event to be the $\sigma(i)$th event in chronological order.

Suppose that someone guesses the chronological order of the births of five mathematicians and puts them in the following order.



The corresponding permutation is $\sigma = (1\,3\,2)(4\,5)$.

What is a natural way to evaluate how incorrect the guess is? If a guess was correct except for interchanging the first two, i.e., $\sigma = (1\,2)$, that should not be considered egregious. The worst guess would completely reverse the chronological order, i.e., $\sigma = (1\,5)(2\,4)$. A measure of incorrectness for the guessed ordering is to count the number of *inversions*.

Definition 1.5.11

Let n be an integer with $n \geq 2$. Define T_n as the set of ordered pairs

$$T_n = \left\{(i,j) \in \{1,2,\ldots,n\}^2 \,|\, i < j\right\}.$$

The number of *inversions* of $\sigma \in S_n$ is number

$$\mathrm{inv}(\sigma) = \left|\{(i,j) \in T_n \,|\, \sigma(i) > \sigma(j)\}\right|.$$

In other words, T_n consists of all possible pairs (i,j) of indices, where the first index is less than the second. Then $\mathrm{inv}(\sigma)$ is the number of times σ reverses the order of the pair. The set T_n has cardinality

$$|T_n| = \sum_{i=1}^{n-1}(n-i) = n(n-1) - \sum_{i=1}^{n-1} i = n(n-1) - \frac{(n-1)n}{2} = \frac{(n-1)n}{2}.$$

Hence, $0 \leq \mathrm{inv}(\sigma) \leq \frac{1}{2}n(n-1)$.

In the above example about birth order of five mathematicians, σ acts on the pairs of T_5. The table lists (i,j) on top and $(\sigma(i),\sigma(j))$ on the bottom row, showing the inversions in bold.

$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$	$(2,3)$	$(2,4)$	$(2,5)$	$(3,4)$	$(3,5)$	$(4,5)$
$\mathbf{(3,1)}$	$\mathbf{(3,2)}$	$(3,5)$	$(3,4)$	$(1,2)$	$(1,5)$	$(1,4)$	$(2,5)$	$(2,4)$	$\mathbf{(5,4)}$

Hence, we count that $\mathrm{inv}(\sigma) = 3$.

Definition 1.5.12

A permutation $\sigma \in S_n$ is called *even* (resp. *odd*) if $\mathrm{inv}(\sigma)$ is an even (resp. odd) integer. The designation even or odd is called the *parity* of the permutation σ.

1.5.4 Useful CAS Commands

Both *Maple* and SAGE offer commands to determine the order, the parity, the cycle type and many other properties of permutations. We encourage the reader to explore these.

In *Maple*, the command `Perm` to define a permutation is immediately available but some of the commands for computing with permutations are in the `GroupTheory` package. The *Maple* help files provide a tutorial entitled *Working with Permutations*. The following code illustrates a few commands that are relevant to the content of this section.

Maple

```
s := Perm([[1, 4, 3], [2, 6]]) :
t := Perm([6, 1, 3, 4, 2, 5]):
s[2];
                                  6
with(GroupTheory) :
s^(-1);
                              (1,3,4)(2,6)
s.t;
                             (1,4,3,6)(2,5)
```

The first and second lines define the permutations s and t, the first in standard cycle notation, the second using the n-tuple notation. The third line shows how to apply the permutation s as a function to the input of 2. The next line brings in the `GroupTheory` package that contains commands and methods to operate on permutations. The last two lines calculate the inverse s^{-1} and composition st.

Illustrating *Maple*'s programming language, the next block of code defines a procedure that counts the number of inversions of a permutation.

Maple

```
CountInversions :=proc(p)
  local n, i, j, sum := 0;
  n := PermDegree(p);
  for i from 1 to n − 1 do
   for j from i + 1 to n do
    if p[i] > p[j] then sum := sum + 1; fi:
   od:
  od:
  return sum;
end:

CountInversions(t);
                                  7
```

There are a number of ways to define permutations in Sage and we encourage the reader to consult the documentation files online entitled "Permutations" or "Permutation group elements." The first of the webpages describes methods associated with permutations that are more relevant for combinatorics with the latter focus more on applications to group theory. The following code illustrates the same commands as the *Maple* code, but then shows a few commands related to inversions.

Sage

```
sage: G=SymmetricGroup(6)
sage: s=G("(1,4,3)(2,6)")
sage: t=G([6,1,3,4,2,5])
sage: s(2)
6
sage: s.inverse()
(1,3,4)(2,6)
sage: s*t
(1,4,3,6)(2,5)
sage: tp=Permutation(t)
sage: tp
[6, 1, 3, 4, 2, 5]
sage: tp.number_of_inversions()
7
sage: tp.inversions()
[(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (3, 5), (4, 5)]
```

The first `sage:` line defines the group G as S_6. The next five lines implement the same commands as the first block of *Maple* code above. However, note that in Sage, the permutations are understood as elements of the group G. The command `tp=Permutation(t)` defines `tp` as the same permutation as `t` but expressed in a permutation object class. In this class, Sage always writes permutations as n-tuples, illustrated by the line `sage: tp`. The last two lines illustrate useful methods from this object class. The following code gives an example of Sage using Python code to calculate

$$\sum_{\sigma \in S_6} \mathrm{inv}(\sigma).$$

Sage

```
sage: G=SymmetricGroup(6)
sage: sum=0
sage: for p in G:
....:     pp=Permutation(p)
```